

Practical Paranoia™ macOS 10.13

Security Essentials

- ✓ The Easiest
- ✓ Step-By-Step
- ✓ Most Comprehensive
- ✓ Guide To Securing Data and Communications
- ✓ On Your Home and Office macOS Computer

Marc L. Mintz, MBA-IT, ACTC, ACSP

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Copyright © 2016, 2017, 2018 by The Practical Paranoid, LLC.

Notice of Rights: All rights reserved. No part of this document may be reproduced or transmitted in any form by any means without the prior written permission of the author. For information on obtaining permission for reprints and excerpts, contact the author at marc@thepracticalparanoid.com, +1 888.504.5591.

Notice of Liability: The information in this document is presented on an *As Is* basis, without warranty. While every precaution has been taken in the preparation of this document, the author shall have no liability to any person or entity with respect to any loss or damage caused by or alleged to be caused directly or indirectly by the instructions contained in this document, or by the software and hardware products described within it. It is provided with the understanding that no professional relationship exists, and no professional security or Information Technology services have been offered between the author or the publisher and the reader. If security or Information Technology expert assistance is required, the services of a professional person should be sought.

Trademarks: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the author was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified in this document are used in editorial fashion only and for the benefit of such companies with no intention of infringement of trademark. No such use, or the use of the trade name, is intended to convey endorsement or other affiliation within this document.

Editions: v1.0 20170918 • v1.01 20170923 • v1.1 20171001 • v1.2 20171022 • v1.3 20180325 • v2 20180420 • v2.1 20180422

Cover design by Ed Brandt

ISBN-10: 1976513650

ISBN-13: 978-1976513657

Dedication

*To Candace,
without whose support and encouragement
this work would not be possible*

Contents At A Glance

Dedication.....	3
Contents At A Glance	5
Contents In Detail	7
1 Thank You For Studying Practical Paranoia!	19
2 Introduction.....	21
3 Data Loss	35
4 Passwords	63
5 System And Application Updates	103
6 User Accounts	115
7 Storage Device	145
8 Sleep And Screen Saver	157
9 Malware	163
10 Firewall.....	193
11 Firmware Password	205
12 Lost Or Stolen Device	209
13 Local Network.....	225
14 Web Browsing.....	271
15 Email.....	363
16 Apple ID And iCloud	461
17 Documents	479
18 Voice, Video, And Instant Message Communications.....	527
19 Internet Activity	549
20 Social Media	595

Contents In Detail

21 When It Is Time To Say Goodbye	659
22 Miscellaneous	671
23 The Final Word	681
macOS 10.13 Security Checklist	683
Revision Log	689
Index.....	692

Contents In Detail

Dedication.....	3
Contents At A Glance	5
Contents In Detail	7
1 Thank You For Studying Practical Paranoia!	19
2 Introduction.....	21
2.1 Who Should Study This Course	22
2.2 What is Unique About This Course and Book.....	23
2.3 Why Worry?.....	25
2.4 Reality Check	27
2.5 About The Author.....	29
2.6 Practical Paranoia Updates	30
2.6.1 Newsletter	30
2.6.2 Blog.....	30
2.6.3 Facebook	30
2.6.4 Practical Paranoia Paperback Book Upgrades	30
2.6.5 Practical Paranoia Kindle Updates	31
2.6.6 Practical Paranoia Online Live Student Edition Updates	31
2.7 Notes for Instructors, Teachers, And Professors.....	32
2.8 Update Bounty.....	33
3 Data Loss	35
3.1 The Need for Backups	36
3.1.1 Assignment: Format The Backup Drive For Time Machine Or Carbon Copy Cloner	41
3.1.2 Assignment: Configure Time Machine.....	44
3.1.3 Assignment: Integrity Test The Time Machine Backup.....	46
3.1.4 Assignment: Install And Configure Carbon Copy Cloner.....	47
3.1.5 Assignment: Test Run The First Clone Backup.....	53
3.1.6 Assignment: Encrypt The Clone Backup.....	56
3.1.7 Assignment: Integrity Test The Clone Backup	59
4 Passwords	63
4.1 The Great Awakening.....	64

Contents In Detail

4.2	Strong Passwords	65
4.2.1	Assignment: Create A Strong User Account Password.....	68
4.3	Keychain	72
4.3.1	Assignment: View An Existing Keychain Record	75
4.4	Challenge Questions	79
4.4.1	Assignment: Store Challenge Q&A In The Keychain.....	79
4.4.2	Assignment: Access Secure Data From Keychain	82
4.5	Harden The Keychain.....	85
4.5.1	Assignment: Harden The Keychain With A Timed Lock	85
4.6	Synchronize Keychain Across macOS And iOS Devices	88
4.6.1	Assignment: Activate iCloud Keychain Synchronization	88
4.7	LastPass	92
4.7.1	Assignment: Install LastPass.....	92
4.7.2	Assignment: Use LastPass To Save Website Authentication Credentials	96
4.7.3	Assignment: Use LastPass To Auto Fill Website Authentication	98
4.8	Password Policies	99
4.8.1	Assignment: Password Policies With macOS Server.....	99
5	System And Application Updates	103
5.1	System Updates	104
5.1.1	Assignment: Configure Apple System And Application Update Schedule	105
5.2	Manage Application Updates With MacUpdate Desktop.....	108
5.2.1	Assignment: Install And Configure MacUpdate Desktop	108
5.2.2	Assignment: Application Updates With MacUpdate Desktop	112
5.3	Additional Reading.....	113
6	User Accounts	115
6.1	User Accounts	116
6.2	Never Log In As An Administrator	118
6.2.1	Assignment: Enable The Root User	118
6.2.2	Assignment: Login As The Root User.....	122
6.2.3	Assignment: Change The Root User Password.....	125
6.2.4	Assignment: Disable the Root User.....	126
6.2.5	Assignment: Create an Administrative User Account.....	126
6.2.6	Assignment: Change From Administrator To Standard User.	127

Contents In Detail

6.3	Application Whitelisting And More With Parental Controls.....	129
6.3.1	Assignment: Configure A Parental Controls Account	130
6.3.2	Assignment: View Parental Controls Logs.....	141
6.4	Policy Banner	143
6.4.1	Assignment: Create A Policy Banner	143
7	Storage Device	145
7.1	Block Access To Storage Devices.....	146
7.1.1	Assignment: Disable USB, FireWire, And Thunderbolt Storage Device Access	146
7.1.2	Assignment: Enable USB, FireWire, and Thunderbolt Storage Device Access	147
7.2	FileVault 2 Full Disk Encryption	148
7.2.1	Assignment: Boot Into Target Disk Mode.....	149
7.2.2	Assignment: Boot Into Recovery HD Mode.....	149
7.2.3	Assignment: Boot Into Single-User Mode.....	150
7.2.4	Assignment: Enable And Configure FileVault 2	150
7.3	FileVault Resistance To Brute Force Attack	154
7.4	Remotely Access And Reboot a FileVault Drive.....	155
7.4.1	Assignment: Temporarily Disable FileVault	155
8	Sleep And Screen Saver	157
8.1	Require Password After Sleep Or Screen Saver	158
8.1.1	Assignment: Require Password After Sleep Or Screen Saver	158
9	Malware	163
9.1	Anti-Malware	164
9.1.1	Assignment: Install And Configure Bitdefender (Home Users Only)	168
9.1.2	Assignment: Install And Configure Bitdefender GravityZone Endpoint Security (Business Users)	180
9.2	Additional Reading.....	192
10	Firewall.....	193
10.1	Firewall.....	194
10.1.1	Assignment: Activate The Firewall.....	195
10.1.2	Assignment: Close Unnecessary Ports	198
11	Firmware Password	205
11.1	EFI Chip.....	206

Contents In Detail

11.1.1	Assignment: Enable The Firmware Password	206
11.1.2	Assignment: Test The Firmware Password	207
11.1.3	Assignment: Remove The Firmware Password	207
12	Lost Or Stolen Device	209
12.1	Find My Mac.....	210
12.1.1	Assignment: Activate And Configure Find My Mac	210
12.1.2	Assignment: Use Find My Mac From A Computer	217
12.1.3	Assignment: Use Find My Mac From An iPhone or iPad.....	221
12.2	Prey	224
13	Local Network.....	225
13.1	Ethernet Broadcasting.....	226
13.2	Ethernet Insertion	227
13.3	Wi-Fi Encryption Protocols	228
13.4	Routers: An Overview	230
13.4.1	Assignment: Determine Your Wi-Fi Encryption Protocol	231
13.4.2	Assignment: Secure An Apple Airport Extreme Base Station.....	233
13.4.3	Assignment: Configure WPA2 On A Non-Apple Router	237
13.5	Use MAC Address To Limit Wi-Fi Access.....	241
13.5.1	Assignment: Restrict Access By MAC Address On An Apple Airport.....	241
13.5.2	Assignment: Restrict Access By MAC Address To A Non-Apple Router	249
13.6	Router Penetration	258
13.6.1	Assignment: Verify Apple Airport Port Security Configuration	259
13.6.2	Assignment: Verify Non-Apple Airport Router Security Configuration	265
14	Web Browsing.....	271
14.1	HTTPS	272
14.1.1	Assignment: Install HTTPS Everywhere.....	274
14.2	Choose a Browser.....	276
14.2.1	Assignment: Secure Browsing With Brave	277
14.3	Private Browsing	281
14.3.1	Assignment: Safari Private Browsing.....	281
14.3.2	Assignment: Firefox Private Browsing.....	283
14.3.3	Assignment: Google Chrome Incognito Mode	284

Contents In Detail

14.4	Secure Web Searches.....	286
14.4.1	Assignment: Make DuckDuckGo Your Safari Search Engine 286	
14.4.2	Assignment: Make DuckDuckGo Your Firefox Search Engine 287	
14.4.3	Assignment: Make DuckDuckGo Your Chrome Search Engine 288	
14.5	Clear History.....	290
14.5.1	Assignment: Clear The Safari History.....	290
14.5.2	Assignment: Clear The Firefox Browsing History.....	291
14.5.3	Assignment: Clear The Chrome History	292
14.6	Browser Plug-Ins.....	294
14.6.1	Assignment: Install TrafficLight Plug-In For Safari.....	294
14.6.2	Assignment: Install TrafficLight Plug-In For Google Chrome 295	
14.6.3	Assignment: Install TrafficLight For Firefox	297
14.6.4	Assignment: Find And Remove Extensions From Safari.....	299
14.6.5	Assignment: Find And Remove Extensions From Chrome....	299
14.6.6	Assignment: Find And Remove Add-Ons From Firefox.....	300
14.7	Fraudulent Websites	302
14.8	Do Not Track.....	306
14.8.1	Assignment: Secure Safari.....	307
14.8.2	Assignment: Secure Firefox.....	308
14.8.3	Assignment: Secure Chrome.....	310
14.8.4	Assignment: Install Ghostery For Safari	312
14.8.5	Assignment: Install Ghostery For Chrome	314
14.8.6	Assignment: Install Ghostery For Firefox	317
14.8.7	Assignment: View Your Device Fingerprint	324
14.9	Adobe Flash And Java.....	328
14.9.1	Assignment: Configure Oracle Java for Automatic Updates..	328
14.10	Web Scams.....	330
14.10.1	Recovering From A Web Scam.....	330
14.11	Tor 333	
14.11.1	Assignment: Install Tor For Anonymous Internet Browsing..	335
14.11.2	Assignment: Configure Tor Preferences.....	346
14.12	Onion Sites And The Deep Web	357
14.13	Have I Been Pwned	358

Contents In Detail

14.13.1 Assignment: Has Your Email Been Hacked	358
14.13.2 Assignment: What To Do Now That You Have Been Breached 361	
15 Email.....	363
15.1 The Killer App	364
15.2 Phishing	365
15.3 Email Encryption Protocols	367
15.4 TLS and SSL With Mail App.....	368
15.4.1 Assignment: Determine If Sender And Recipient Can Use TLS 368	
15.5 Require Google Mail To Be TLS Secured.....	371
15.5.1 Assignment: Configure Google G-Suite Mail For Only TLS.	371
15.6 HTTPS With Web Mail	373
15.6.1 Assignment: Configure Web Mail To Use HTTPS.....	373
15.7 End-To-End Secure Email With ProtonMail	374
15.7.1 Assignment: Create a ProtonMail Account	375
15.7.2 Assignment: Create And Send An Encrypted ProtonMail Email 379	
15.7.3 Assignment: Receive And Respond To A ProtonMail Secure Email.....	383
15.8 End-To-End Secure Email With GNU Privacy Guard	389
15.8.1 Assignment: Install GPG And Generate A Public Key	390
15.8.2 Assignment: Add Other Email Addresses To A Public Key ..	393
15.8.3 Assignment: Configure GPGMail Preferences	400
15.8.4 Assignment: Install A Friend's Public Key	402
15.8.5 Assignment: Send A GPG-Encrypted And Signed Email	403
15.8.6 Assignment: Receive A GPG-Encrypted And Signed Email .	405
15.8.7 Assignment: Encrypt And Sign Files With GPGServices	407
15.9 End-To-End Secure Email With S/MIME	413
15.9.1 Assignment: Acquire A Free Class 1 S/MIME Certificate.....	414
15.9.2 Assignment: Acquire A Class 3 S/MIME Certificate For Business Use	419
15.9.3 Assignment: Purchase A Class 3 S/MIME Certificate For Business Use	424
15.9.4 Assignment: Install A Business S/MIME Certificate.....	433
15.9.5 Assignment: Exchange Public Keys With Others.....	436
15.9.6 Assignment: Send S/MIME Encrypted Email	439

Contents In Detail

15.10	Virtru Email Encryption	442
15.10.1	Assignment: Create A Free Virtru For Gmail Account.....	443
15.10.2	Assignment: Send Encrypted Gmail With Virtru.....	448
15.10.3	Receive and Reply To A Virtru-Encrypted Email	450
15.11	Email Validation with SPF, DKIM, and DMARC.....	453
15.11.1	Assignment: Configure SPF.....	453
15.11.2	Assignment: Configure DKIM.....	457
15.11.3	Assignment: Sign Email With The Domain Key	458
15.11.4	Assignment: Configure DMARC.....	458
16	Apple ID And iCloud	461
16.1	Apple ID And iCloud	462
16.1.1	Assignment: Create An Apple ID.....	463
16.1.2	Assignment: Enable 2-Factor Authentication	467
16.1.3	Assignment: Sign In To Your iCloud Account.....	473
16.1.4	Assignment: Remove A Device From Two-Factor Authentication	476
17	Documents	479
17.1	Document Security	480
17.2	Password Protect A Document Within Its Application	481
17.2.1	Assignment: Encrypt An MS Word Document.....	481
17.3	Encrypt A PDF Document.....	484
17.3.1	Assignment: Convert A Document To PDF For Password Protection	484
17.4	Encrypt a Folder For Only macOS Use.....	487
17.4.1	Assignment: Create An Encrypted Disk image.....	487
17.5	Encrypt A Folder For Cross Platform Use With Zip.....	490
17.5.1	Assignment: Encrypt A File Or Folder Using Zip	490
17.5.2	Assignment: Open An Encrypted Zip Archive	496
17.6	Cross-Platform Disk Encryption	498
17.6.1	Assignment: Download And Install VeraCrypt	498
17.6.2	Assignment: Configure VeraCrypt.....	501
17.6.3	Assignment: Create A VeraCrypt Container.....	508
17.6.4	Assignment: Mount An Encrypted VeraCrypt Container.....	520
18	Voice, Video, And Instant Message Communications.....	527
18.1	Voice, Video, And Instant Messaging Communications.....	528
18.2	HIPAA Considerations	530

Contents In Detail

18.3	Wire	531
18.3.1	Assignment: Install Wire	531
18.3.2	Assignment: Invite PeopleTo Wire	535
18.3.3	Assignment: Import Contacts Into Wire.....	540
18.3.4	Assignment: Secure Instant Message A Wire Friend.....	541
18.3.5	Assignment: Secure Voice Call With A Wire Friend.....	544
18.3.6	Assignment: Secure Video Conference With A Wire Friend.....	547
19	Internet Activity	549
19.1	VPN–Virtual Private Network	550
19.2	Gateway VPN.....	551
19.2.1	Assignment: Search For A VPN Host	555
19.3	NordVPN	557
19.3.1	Assignment: Create A NordVPN Account	557
19.3.2	Assignment: Configure IKEv2 VPN With NordVPN.....	560
19.4	Resolving Email Conflicts With VPN.....	566
19.5	Mesh VPN.....	567
19.6	LogMeIn Hamachi.....	568
19.6.1	Assignment: Create a LogMeIn Hamachi Account.....	568
19.6.2	Assignment: Add Users To A Hamachi VPN Network	581
19.6.3	Assignment: File Sharing Within A Hamachi VPN Network	590
19.6.4	Assignment: Screen Share Within Hamachi VPN	592
19.6.5	Assignment: Exit the Hamachi VPN Network.....	593
20	Social Media	595
20.1	What, Me Worry?.....	596
20.2	Protecting Your Privacy On Social Media.....	597
20.3	Facebook.....	598
20.3.1	Assignment: Facebook Security And Login	598
20.3.2	Assignment: Facebook Privacy Settings.....	603
20.3.3	Assignment: Timeline And Tagging Settings.....	605
20.3.4	Assignment: Facebook Manage Blocking	606
20.3.5	Assignment: Facebook Public Posts.....	608
20.3.6	Assignment: Facebook Apps.....	609
20.3.7	Assignment: What Does Facebook Know About You	619
20.4	LinkedIn.....	626
20.4.1	Assignment: LinkedIn Account Security.....	626
20.4.2	Assignment: Find What LinkedIn Knows About You	632

Contents In Detail

20.5	Google	635
20.5.1	Assignment: Manage Your Google Account Access and Security Settings.....	635
20.5.2	Assignment: Enable Google 2-Step Verification.....	650
20.5.3	Find What Google Knows About You	655
21	When It Is Time To Say Goodbye	659
21.1	Preparing a Computer for Sale or Disposal	660
21.1.1	Assignment: Prepare Your Mac For Sale Or Disposal.....	660
21.1.2	Assignment: Secure Erase The Drive.....	664
21.1.3	Assignment: Install macOS 10.13	669
22	Miscellaneous	671
22.1	Date And Time Settings.....	672
22.2	Assignment: Configure Date & Time.....	673
22.3	Securing Hardware Components.....	674
22.4	National Institute Of Standards And Technology (NIST).....	676
22.4.1	NIST-Specific Security Settings	676
22.5	United States Computer Emergency Readiness Team (US-CERT).....	678
22.6	International Organization For Standardization (ISO)	679
23	The Final Word	681
23.1	Additional Reading.....	682
	macOS 10.13 Security Checklist	683
	Revision Log.....	689
	Index.....	692

PRACTICAL PARANOIA MACOS 10.13 SECURITY ESSENTIALS

MARC L. MINTZ, MBA-IT, ACTC, ACSP

13 Local Network

I am concerned for the security of our great Nation; not so much because of any threat from without, but because of the insidious forces working from within.

–General Douglas MacArthur¹

What You Will Learn In This Chapter

- Ethernet broadcasting
- Ethernet insertion
- Wi-Fi encryption protocols
- Determine your Wi-Fi encryption protocol
- Secure an Apple Airport
- Configure WPA2 on a non-Apple router
- Restrict access by MAC address on an Apple router
- Restrict access by MAC address on a non-Apple router
- Verify Apple Airport security configuration
- Verify non-Apple Airport router security configuration

¹ https://en.wikipedia.org/wiki/Douglas_MacArthur

13.1 Ethernet Broadcasting

It is common wisdom that Ethernet is more secure than Wi-Fi. But as with most things we believe, this is not accurate.

There are two security issues with Ethernet: Broadcasting and Insertion. At the most fundamental level, what is happening when data travels through Ethernet is that electrons are traveling along a metal cable. There are two unintended consequences that occur whenever electrons go for a ride—heat generation, and the creation of an electromagnetic field. For our purposes, heat isn't an issue. But the electromagnetic field is.

Sending data through copper wire effectively turns that wire into a very large antenna that is broadcasting your data through radio waves. If you have the right receiver and translation software, you can easily capture every bit of data being sent and received along that cable.

This vulnerability is not something about which the average person or business would or should be concerned. On the other hand, if you or your business requires the utmost in security, it is mandatory to add encryption to your Ethernet network.

Speaking specifically about macOS, computer-to-computer communications are not encrypted, and so are not recommended. When using computer-to-macOS/OS X Server communications, then all communications are encrypted. For business, this means that users should not do file sharing between themselves, but instead copy any file to the Server for others to copy back to their own computers.

13.2 Ethernet Insertion

You would notice if someone came into your home, plugged a computer into your network, and sat there watching data go by. But in the typical business, nobody would notice.

Ethernet and Wi-Fi networks can be protected from unwanted insertions by implementing the 802.1x protocol (often referred to as RADIUS)

https://en.wikipedia.org/wiki/IEEE_802.1X. This protocol works with both Ethernet and Wi-Fi, mandating that anyone attempting to join the network authenticate with their own personal name and password. This is unlike the typical Wi-Fi authentication that uses the same password for everyone.

To implement 802.1x you need to have either a macOS/OS X, Windows, or Linux Server running within your network, or one of the many other 802.1x appliances that are available. Details on how to configure 802.1x are beyond the scope of this book. Please consult the following for more information:

- *OS X Server Administrator Guide*²
- *Jedda*³
- *OS X Server Essentials 10.11*⁴
- *Microsoft TechNet documentation*⁵

² <https://help.apple.com/advancedserveradmin/mac/>

³ <https://jedda.me/2012/11/configuring-basic-radius-os-108-server/>

⁴ https://www.amazon.com/Support-Essentials-10-11-Supporting-Troubleshooting/dp/013442820X/ref=sr_1_1?ie=UTF8&qid=1468196548&sr=8-1&keywords=OS+X+10.11+server

⁵ <https://technet.microsoft.com/en-us/library/hh831831.aspx>

13.3 Wi-Fi Encryption Protocols

Right out of the box almost all Wi-Fi base stations are insecure. Anyone that can pick up the signal can connect. This allows them not only to use your bandwidth to access the Internet, but also to see all the other data—such as usernames and passwords—that are travelling on that network. To start securing your Wi-Fi, add strong password protection with encryption.

Although cellular networks do use encryption, the protocol in use has been broken for many years, making it easy for a novice hacker to see all the data passing on it. In addition, it is common practice for police and other government law enforcement agencies to set up their own cellular towers with the purpose of harvesting data.

To prevent your data from being seen while on a cellular network or an unencrypted Wi-Fi network, it is necessary to use VPN (Virtual Private Network) encryption (more on that later.) If the Wi-Fi network is properly encrypted, you should have little concern over the security and privacy of your data.

Below you will find the brief on each of the Wi-Fi encryption protocols.

- **WEP⁶** (Wired Equivalency Protocol) was the first encryption protocol for Wi-Fi. Introduced in 1999, it was quickly broken, and by 2003 was replaced by WPA and WPA2 (Wi-Fi Protected Access). Any Wi-Fi base station manufactured in the past 5 years will offer WPA and WPA2, in addition to WEP.

There is only one reason to ever use WEP—you simply have no other option. Kids driving by your home can likely break into your WEP network before leaving the block.

- **WPA⁷** (Wi-Fi Protected Access) superseded WEP in 2003. Although it is a great advancement, it too has been broken. As with WEP, the only reason to use WPA is that you have no other option.

⁶ http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

⁷ http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- **WPA2**⁸ is the only protocol considered secure. WPA2 superseded WPA in 2004. Although in the past year WPA2 has been broken, it is very difficult to do, and with strong passwords or with 802.1x still provides military-grade protection for your wireless networks.

There are two encryption algorithms that can be used—*TKIP* and *AES* (technically known as CCMP, but virtually all vendors refer to it as AES.) TKIP has been compromised and is no longer recommended. If your Wi-Fi device allows the option of AES, use only that. If it only allows for TKIP, trash the unit and purchase a more modern device.

⁸ http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

13.4 Routers: An Overview

The connection point between your Internet Service Provider (ISP) and your Local Area Network (LAN) is most likely a router. A router is a device designed to connect two different types of networks, and provide resources for them to interact.

Common brands of routers include: Cisco, Ubiquiti, Mesh, Linksys, Netgear, D-Link, Apple, and the many unbranded devices that Internet Service Providers lease to their customers.

Some newer routers, especially those provided by ISPs are all-in-one units containing several, if not all the components below:

- **Modem**⁹. The hardware that decodes and modulates the signal from your Internet provider to your cable or telephone jack. This is most likely to be a separate component if more than one device exists for your Internet connection.
- **Router**¹⁰. A component that runs a specialized program, which allows hundreds of different devices to interact on a network, usually sharing a single IP address to the Internet. Routers use *Network Address Translation* (NAT) to convert and direct Internet traffic from websites to your computer and from your computer to other computers and peripherals on the *Local Area Network* (LAN).
- **Firewall**¹¹. Software which inspects data traffic between the internet and internally connected devices
- **Intrusion Detection System and Intrusion Prevention System**¹². These features perform deep packet inspection to further protect the network from outside intruders.

⁹ <https://en.wikipedia.org/wiki/Modem>

¹⁰ [https://en.wikipedia.org/wiki/Router_\(computing\)](https://en.wikipedia.org/wiki/Router_(computing))

¹¹ [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))

¹² https://en.wikipedia.org/wiki/Deep_packet_inspection

- **Network Switch**¹³. A hardware component that allows multiple devices to be connected simultaneously and interact with the router
- **Access Point**¹⁴. A hardware component that allows tens or hundreds of wireless (Wi-Fi) devices to connect to it.

Every router has at least some basic security controls built in, including the ability to filter out what it thinks are attempts to hack into your network, and the ability to forward specific types of data packets to a specific computer within your LAN, or to point specific types of data packets to a specific computer on the Internet.

Malware, hackers, criminals, and even some government agencies, sometimes attempt to alter these configurations so that either the malware or the perpetrators have an easier time harvesting your data. Because of this, it is wise to routinely inspect the condition of your router. How often is *routine*? Within larger or security-conscious organizations with high-value data, it is common to have a network administrator dedicated to maintaining watch over the status of network equipment. For a small business or household, once every few months wouldn't be too often.

13.4.1 Assignment: Determine Your Wi-Fi Encryption Protocol

You find yourself at a hotel with Wi-Fi and the need to access the Internet. You have the need to ensure that your data is not intercepted. How do you determine if the Wi-Fi network is using WPA or WPA2 instead of WEP? Just attempt to access the network, and the dialog box will tell what protocol is in use.

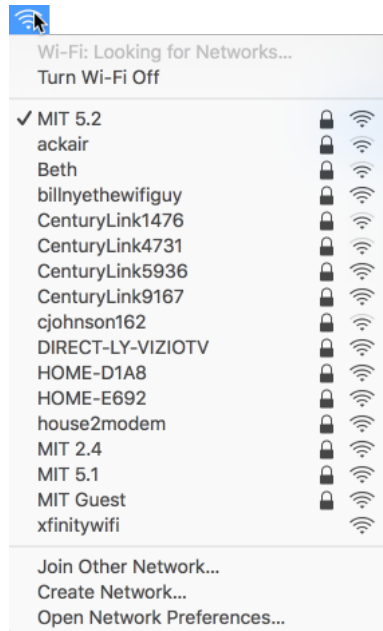
For this assignment, take yourself to a location that has an available Wi-Fi network. Your own home will do.

¹³ https://en.wikipedia.org/wiki/Network_switch

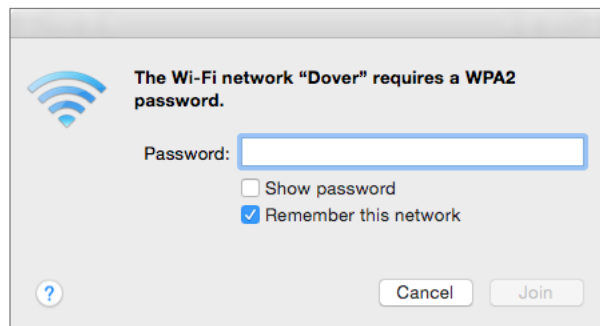
¹⁴ https://en.wikipedia.org/wiki/Wireless_access_point

13 Local Network

1. From the *Wi-Fi* icon in the menu bar, select the target network.



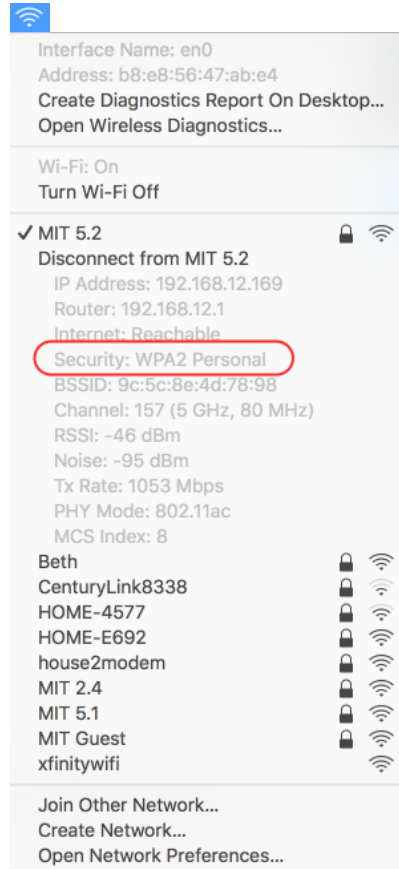
2. The authentication window will appear, requesting authentication and informing you of the security protocol.
 - If it does not appear, either the network does not use encryption, or your Keychain may be storing the password from a previous time you were connected.



If you have already connected to the Wi-Fi network and don't recall which security protocol it uses, you can find it from the Wi-Fi menu icon.

13 Local Network

3. Hold down the *Option* key while clicking on the Wi-Fi menu icon. The Wi-Fi submenu will display with expanded information, including the encryption protocol in use, if any.



If the protocol is WPA2, life is all rainbows and unicorns. If it is anything else, *everything* you do on that network is clearly visible to others and I strongly recommend not using this network unless you have installed *VPN* software to encrypt your Internet traffic (more on this later.)

13.4.2 Assignment: Secure An Apple Airport Extreme Base Station

Every Wi-Fi base station model has its own unique configuration method. We will detail how to configure your Apple Airport Extreme for WPA2 protection.

13 Local Network

In this assignment, you configure an Apple Airport Extreme base station.

- Note: If in a classroom environment, the instructor will demonstrate while the students observe.
1. Open *Airport Utility.app*, located in your */Applications/Utilities* folder. Select the target base station.
 2. The target base station information pane will appear. Select the *Edit* button.



3. If so prompted, enter the administrator name and password for the base station.

13 Local Network

4. Select the *Base Station* tab. Enter a strong administration password here.

The screenshot shows the 'AirPort Utility' window with the 'Base Station' tab selected. The 'Base Station Name' field is filled with 'MIT AEBS'. The 'Base Station Password' and 'Verify Password' fields are masked with dots. The 'Remember this password in my keychain' checkbox is checked, and the 'Allow setup over WAN' checkbox is unchecked. Below this, a text block explains the 'Back to My Mac' feature. A table lists the configured Macs, with 'marcmintz@mac.com' shown and a green status dot. At the bottom are 'Cancel' and 'Update' buttons.

AirPort Utility

Base Station Internet Wireless Network Disks

Base Station Name: MIT AEBS

Base Station Password:

Verify Password:

☒ Remember this password in my keychain

☐ Allow setup over WAN

Using Back to My Mac you can access this AirPort base station for services such as file sharing from your other computers that have Back to My Mac enabled. Click Add (+) and enter your Apple ID and password.

Back to My Mac:

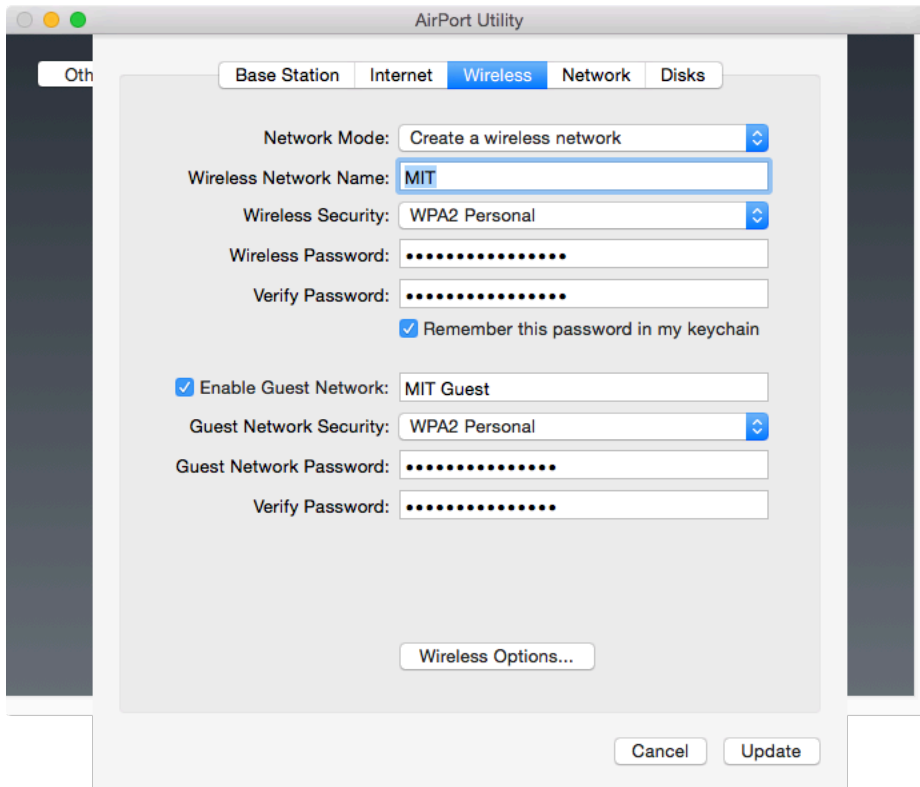
Apple ID	Status
marcmintz@mac.com	●

+ - Edit

Cancel Update

13 Local Network

5. Select the *Wireless* tab and then configure as follows.



- From the Wireless Security pop-up menu, select *WPA2 Personal*. If you have older wireless equipment, you may need to change this to *WPA/WPA2 Personal* to offer compatibility with your older equipment. Keep in mind that doing so severely compromises your network security.
- In the *Wireless Password* and *Verify Password* fields, enter a strong password.

6. Click the *Update* button.

7. *Quit* AirPort Utility.app.

Congratulations! All traffic across your Wi-Fi network is now securely encrypted.

13.4.3 Assignment: Configure WPA2 On A Non-Apple Router

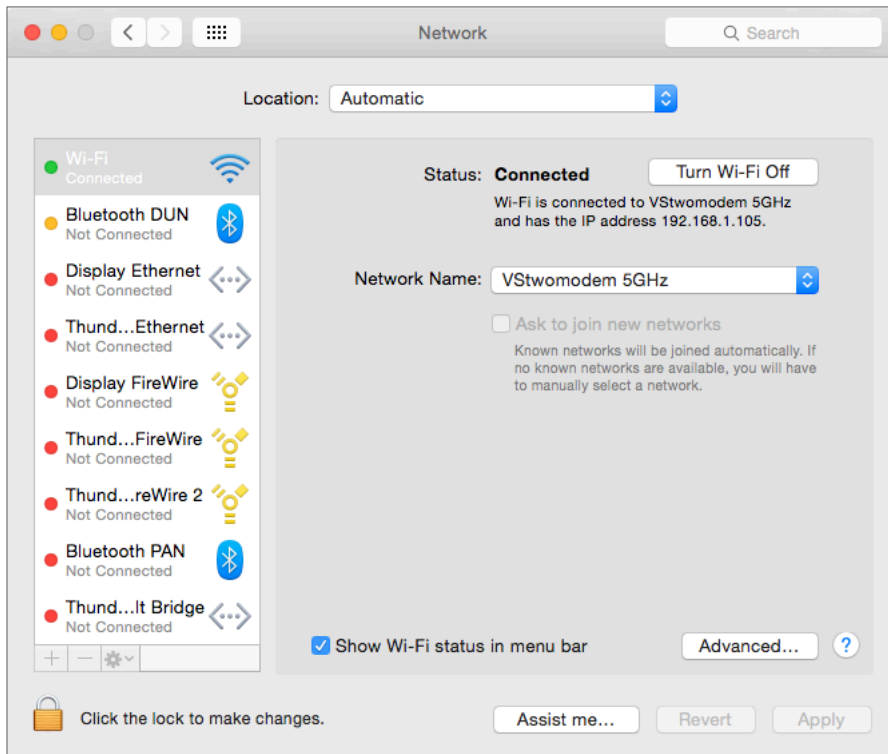
Although all Wi-Fi routers or base stations are configured differently, most follow a basic template. In this assignment, we will be using an ASUS RT-AC3200. We will assume you are on a network with a similarly managed router.

In this assignment, you configure your Wi-Fi router to use the secure WPA2 protocol.

- Note: If this assignment is performed in a class, the instructor will demonstrate while the students observe.

Find the IP address of your Wi-Fi router.

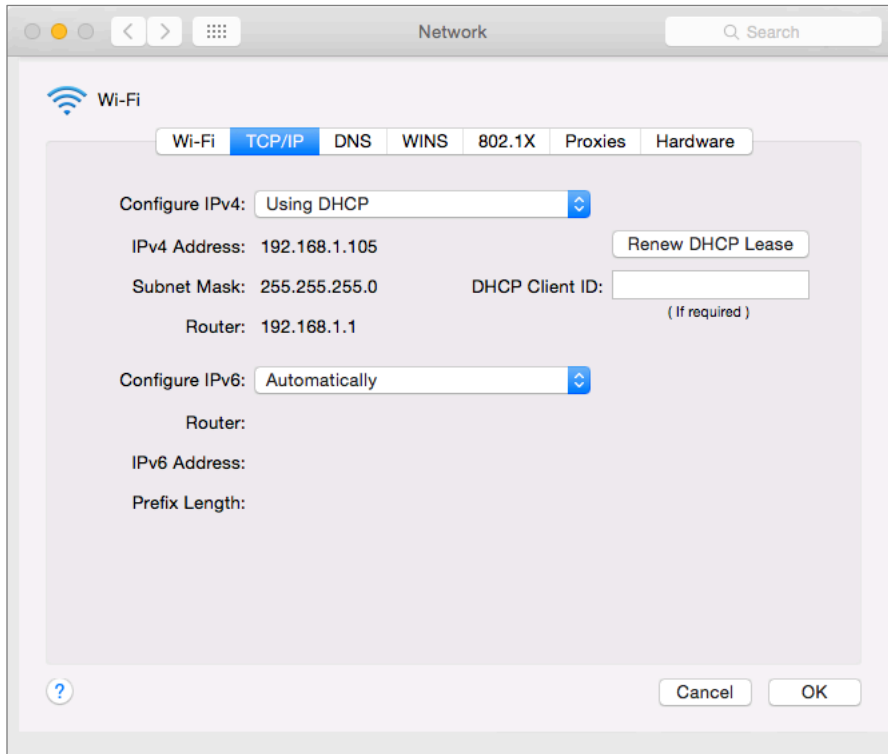
1. Open the *Apple* menu > *System Preferences* > *Network*.



2. If needed, click the lock icon and authenticate as an administrator.
3. Select the *Advanced* button.

13 Local Network

4. Select the *TCP/IP* tab.



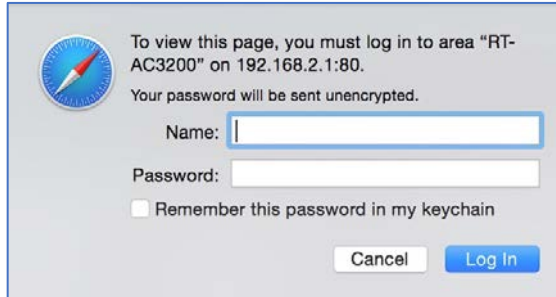
5. About half way down on the left side you will find the *Router* address. This is your Wi-Fi base station or router IP address.
6. Close System Preferences.

Configure Router For WPA2

7. Open a web browser.
8. In the URL or Address field, enter the IP address of the Wi-Fi base station or router.

13 Local Network

9. At the *Authentication* window, enter the administrator user name and password. This will be the administrator of the router, not of your computer.



To view this page, you must log in to area "RT-AC3200" on 192.168.2.1:80.
Your password will be sent unencrypted.

Name:

Password:

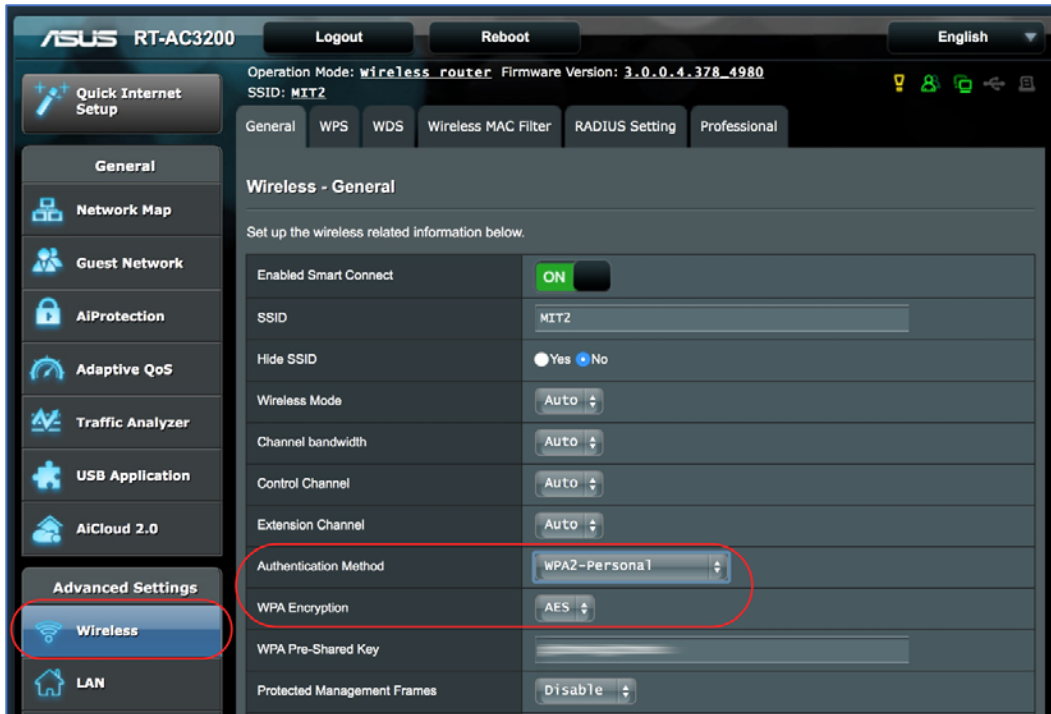
☐ Remember this password in my keychain

10. The router control panel will appear.



13 Local Network

11. From the sidebar, select the *Wireless* button. This will display the options available with your Wi-Fi. Of interest to us now is the *Authentication Method* and *WPA Encryption*. Verify that your Wi-Fi is configured to use the *WPA2* protocol. If it isn't, select it now, and then enter your desired strong password to access the network.



- Note: If your router has the option of using either *AES* or *TKIP*, select *AES*. The *TKIP* encryption scheme has been broken and is easily hacked.
 - Note: Although the *WPA2 Enterprise* is the strongest security (even higher than *WPA2*), it requires network administrator skills and hardware that are outside the scope of this book.
12. If any changes were made, click the *Apply* button to save the changes.
 13. Close the browser window to exit out of your router.
- Congratulations! All traffic on your Wi-Fi is now securely encrypted.

13.5 Use MAC Address To Limit Wi-Fi Access

Every device that can connect to a TCP network has a unique *MAC Address*¹⁵ (Media Access Control). This address specifies the manufacturer of the device, and a device-specific number. Don't go to sleep on me yet! This MAC address can be used with most Wi-Fi base stations to limit what devices can connect to your network.

Although every Wi-Fi base station has a unique interface to filter by MAC address, they all operate on the same principle—either allow anyone with the proper password to gain access to the network, or allow anyone with the proper password *and* proper MAC address access to the network. In this way, you can easily lock down your Wi-Fi to only approved devices. So even if an employee knows the password, they are unable to connect their iPhone or personal computer to the Wi-Fi unless the MAC address for those devices are on the list.

13.5.1 Assignment: Restrict Access By MAC Address On An Apple Airport

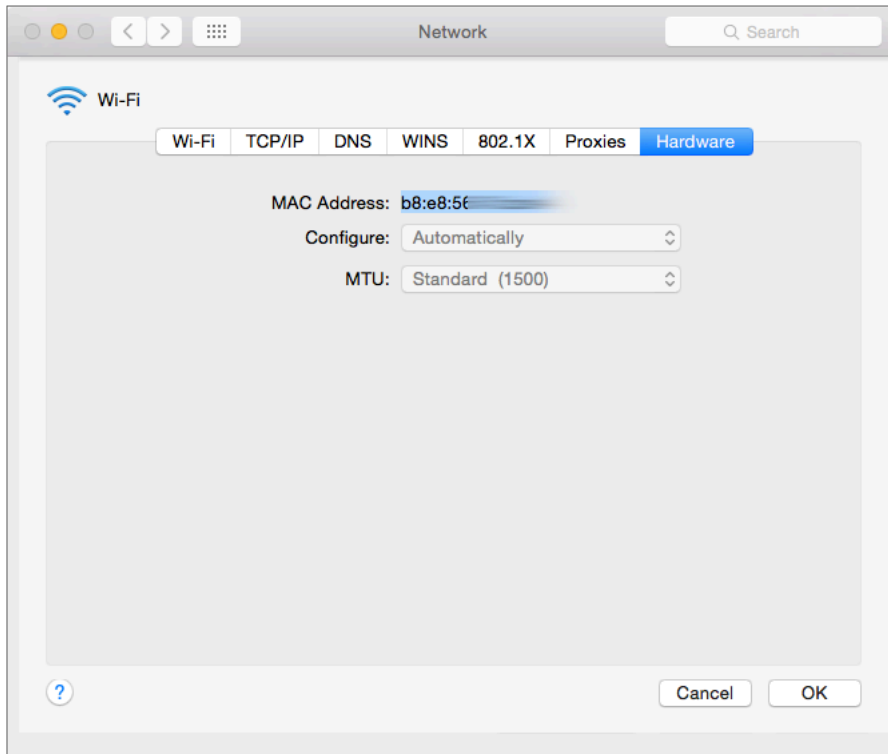
In this assignment, you configure your Apple Airport to allow only desired devices to connect.

- Note: If this assignment is performed in a class, the instructor will demonstrate while the students observe.

¹⁵ http://en.wikipedia.org/wiki/MAC_address

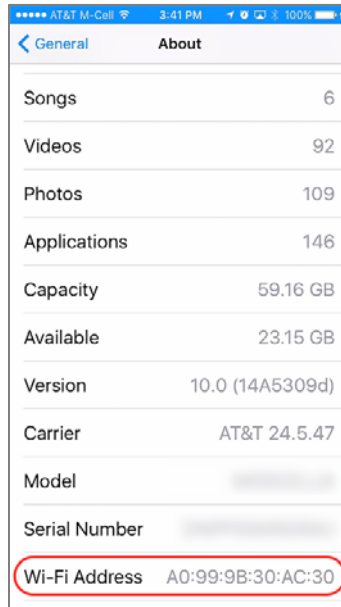
Make A List Of Devices Permitted Access To Your Wi-Fi Network

1. The MAC address of a macOS/OS X computer may be found in the *System Preferences > Network > Advanced...* button > *Hardware* tab.

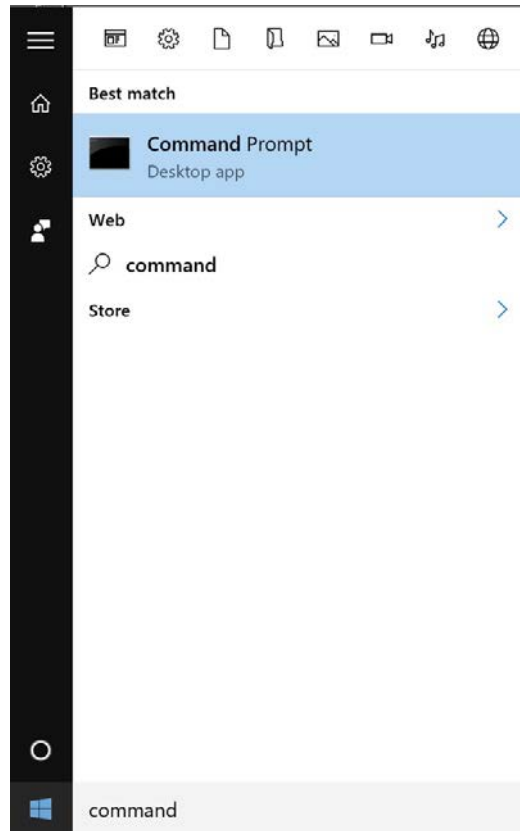


13 Local Network

2. The MAC address of an iPhone may be found in the *Settings > General > About > Wi-Fi Address* field

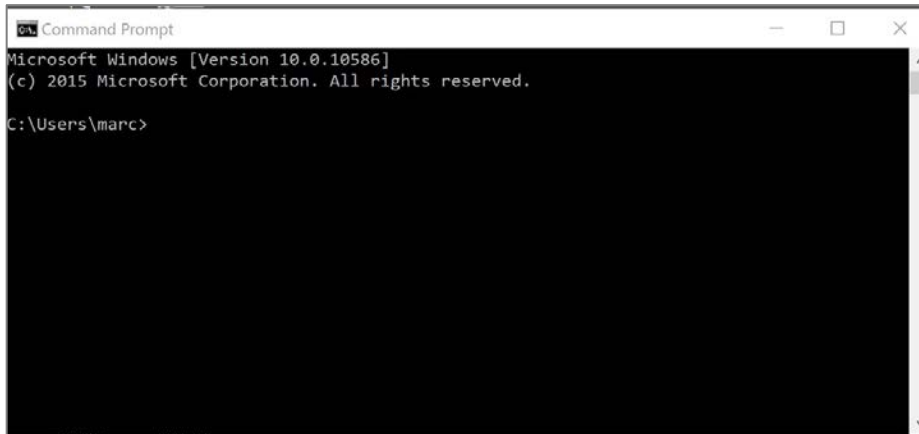


3. The MAC address of a Windows device can be found with the `ipconfig` command in the command prompt.
 - a) In Windows 10, click in the *Search the Web and Windows* field in the bottom left corner, and then enter *command prompt*. Double-click on *Command Prompt* in the *Best match* pop-up.



13 Local Network

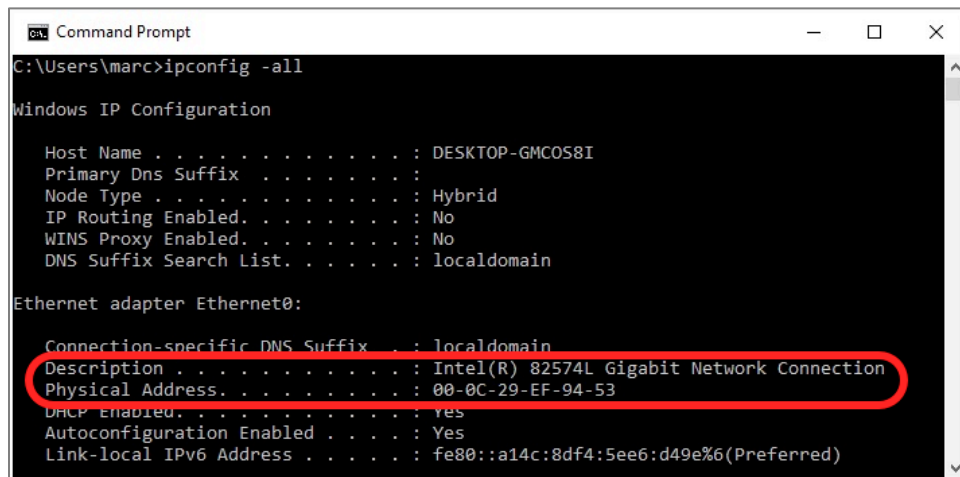
b) The Command Prompt window appears.



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\marc>
```

c) Enter `ipconfig -all`. A listing of all network addresses for the device appears. The MAC address will show as the *Physical Address*.



```
Command Prompt
C:\Users\marc>ipconfig -all

Windows IP Configuration

Host Name . . . . . : DESKTOP-GMCO58I
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

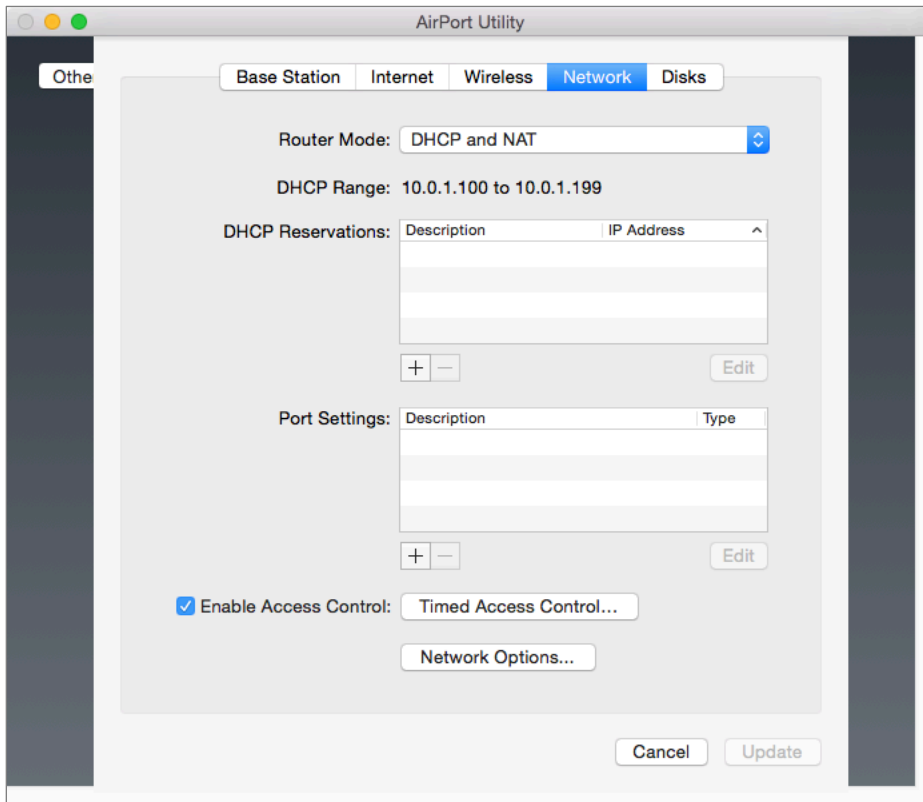
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-EF-94-53
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a14c:8df4:5ee6:d49e%6(Preferred)
```

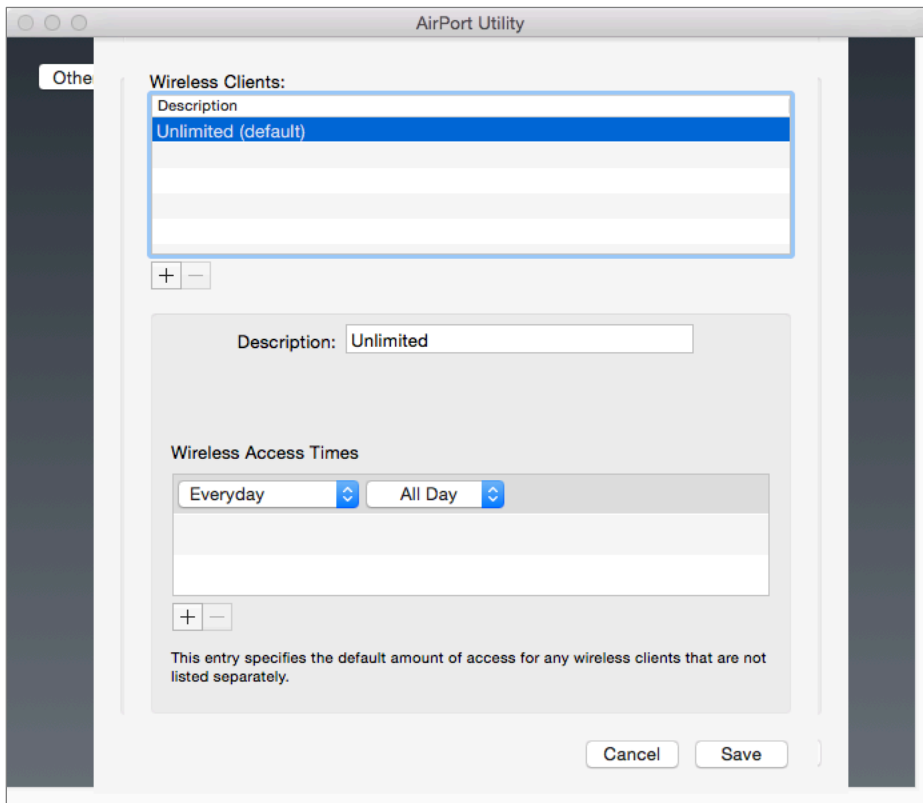
d) Close the Command Prompt.

Configure Your Airport To Allow Only These Devices

4. Launch Airport Utility. Located in the */Applications/Utilities* folder.
5. Select your *Airport base station*, select the *Edit* button, and if necessary, authenticate for access.
6. Select the Network tab, enable the Enable Access Control check box, and then select the Timed Access Control... button.

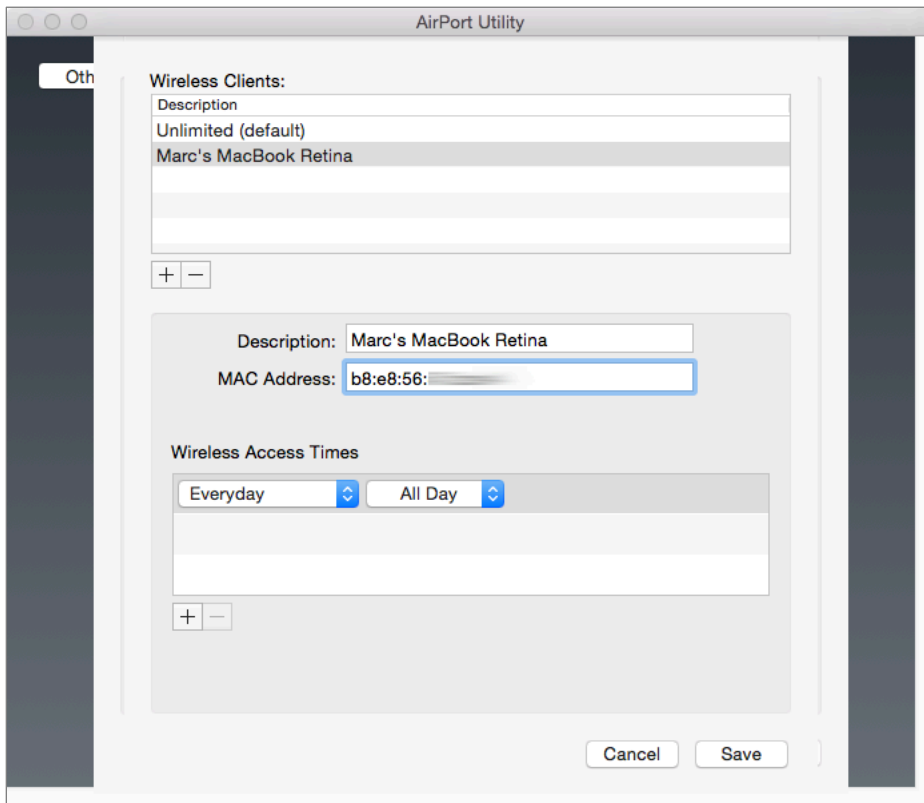


7. The *Timed Access Control* window appears.



13 Local Network

8. At the bottom left of the *Wireless Clients* field, select the + button. Configure as below:



- *Description*: Enter a human-recognizable description of the device to be allowed access.
 - *MAC Address*: Enter the MAC address of the device.
9. Repeat step 6 for every wireless device to have access to your network.
 10. Select the Save button.
 11. Any device not listed will be immediately dropped from your network.
 12. Quit AirPort Utility.

Congratulations! You have secured your wireless network so that only authorized devices are granted access.

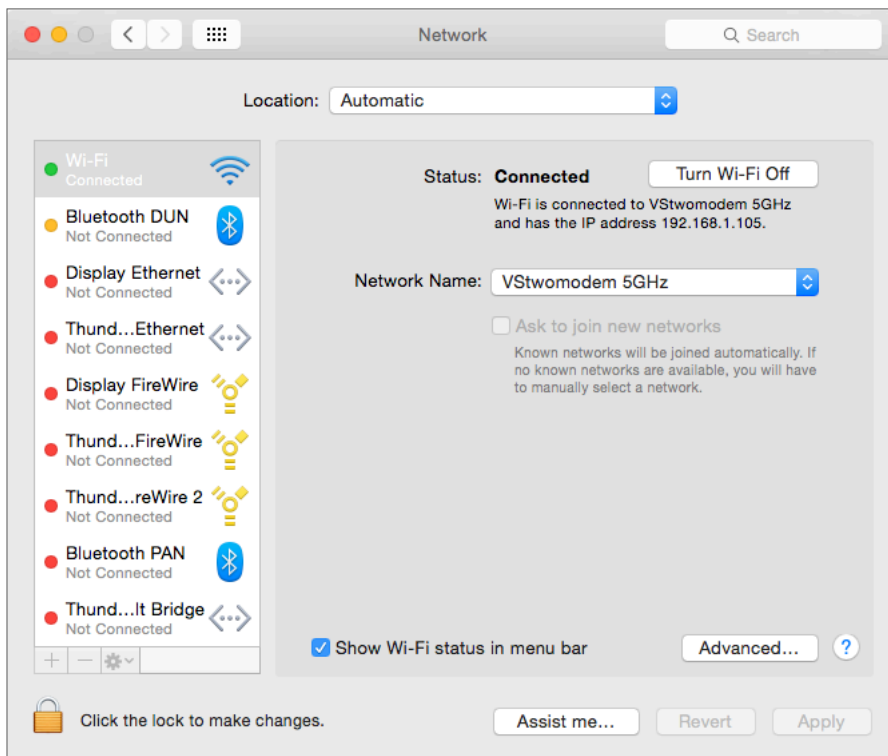
13.5.2 Assignment: Restrict Access By MAC Address To A Non-Apple Router

In this assignment, you configure a non-Apple wireless router to allow only desired devices to connect. Although every wireless router or Wi-Fi base station is configured differently, they tend to use a similar template. In this example, we will be using an Asus RT-AC3200.

- Note: If this assignment is performed in a class, the instructor will demonstrate while the students observe.

Find And Record The IP address Of Your Wireless Router

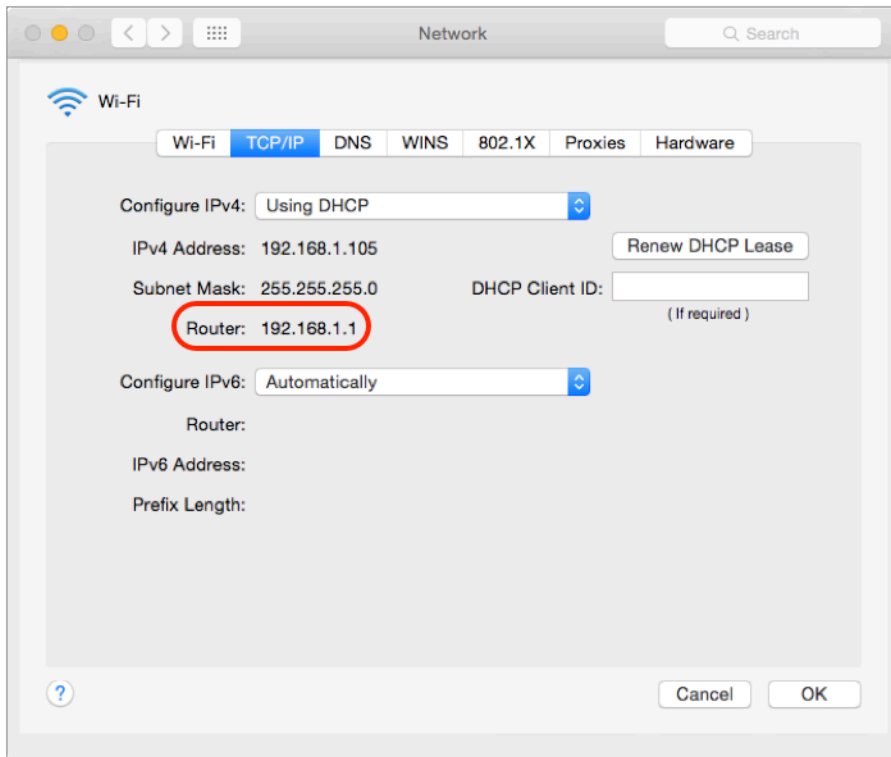
1. Open *Apple* menu > *System Preferences* > *Network*.



2. If necessary, unlock the preference.
3. Select the *Advanced* button.

13 Local Network

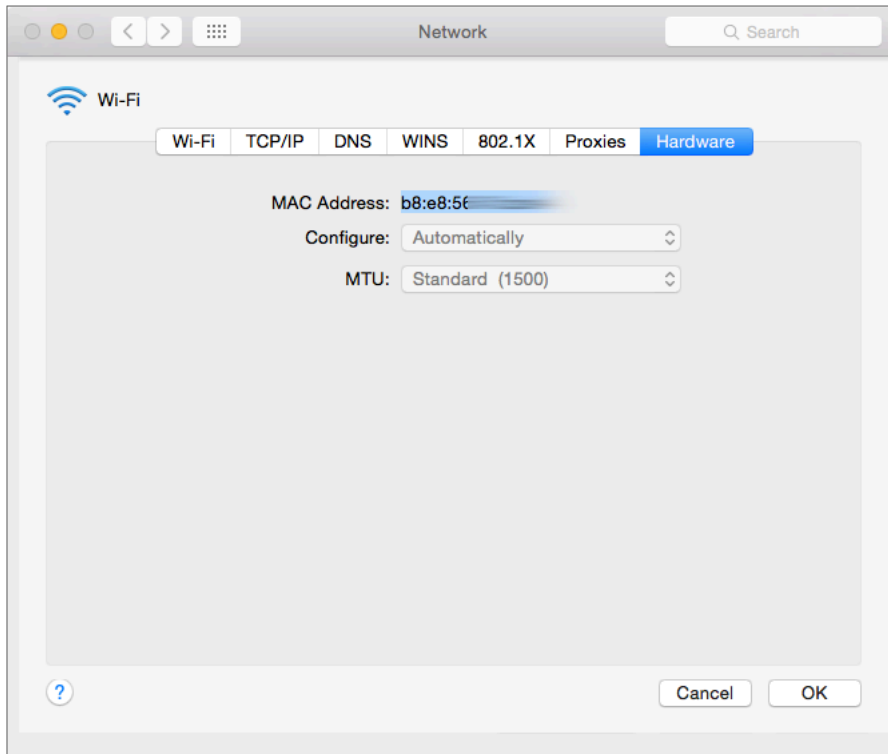
4. Select the *TCP/IP* tab. The wireless router/Wi-Fi base station IP address will be found at the *Router:* field.



5. Quit System Preferences.

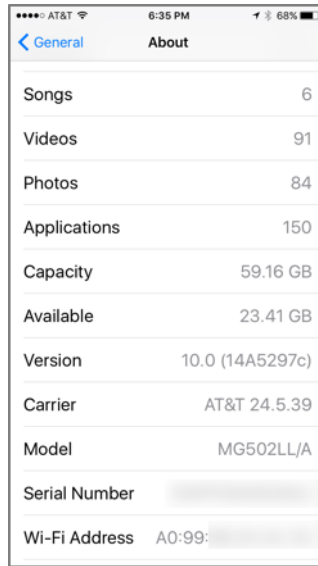
Make A List of Devices Permitted Access To Your Wi-Fi network

6. The MAC address of a Macintosh may be found in the *System Preferences* > *Network* > *Advanced...* button > *Hardware* tab.

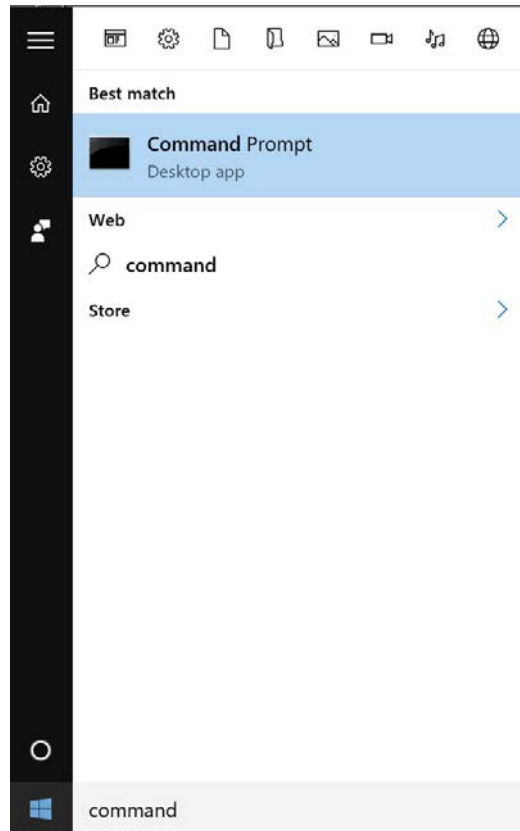


13 Local Network

7. The MAC address of an iPhone may be found in the *Settings > General > About > Wi-Fi Address* field.

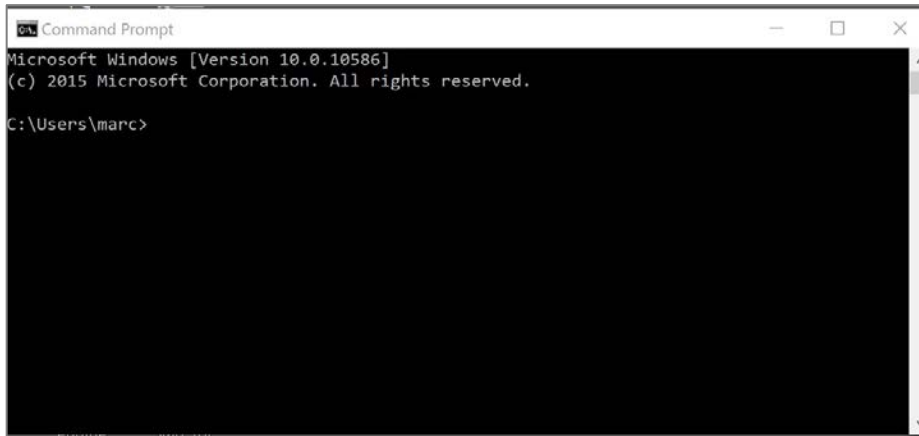


8. The MAC address of a Windows 10 device can be found with the `ipconfig` command in the command prompt.
 - a) In Windows 10, click in the *Search the Web and Windows* field in the bottom left corner, and then enter *command prompt*. Double-click on *Command Prompt* in the *Best match* pop-up.

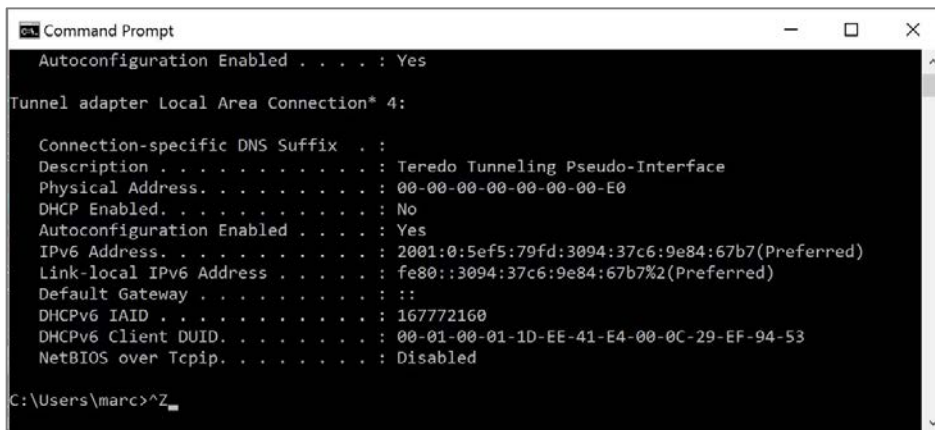


13 Local Network

b) The *Command Prompt* window appears.



c) Enter *ipconfig -all*. A listing of all network addresses for the device appears. The MAC address will show as the *Physical Address*.

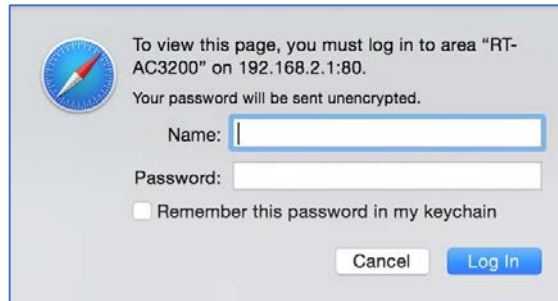


d) Close the Command Prompt.

Create A List In Your Router Of Allowed Devices

9. Launch a web browser.
10. Enter the IP address of the wireless router.
11. In the *URL* or *Address* field, enter the IP address of the wireless router.
12. At the *Authentication* window, enter the user name and password of the router administrator. This is not the administrator of your computer.

13 Local Network



To view this page, you must log in to area "RT-AC3200" on 192.168.2.1:80.
Your password will be sent unencrypted.

Name:

Password:

☐ Remember this password in my keychain

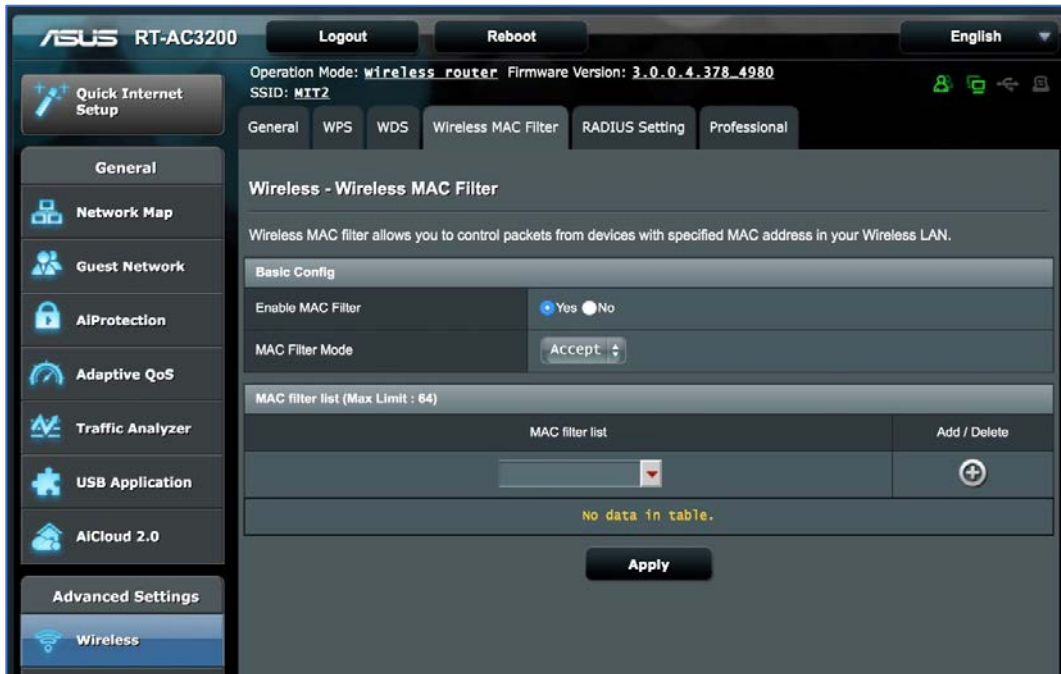
13. The wireless router control panel will appear.

- Please keep in mind that all routers—even from the same company—have slightly different interfaces.



13 Local Network

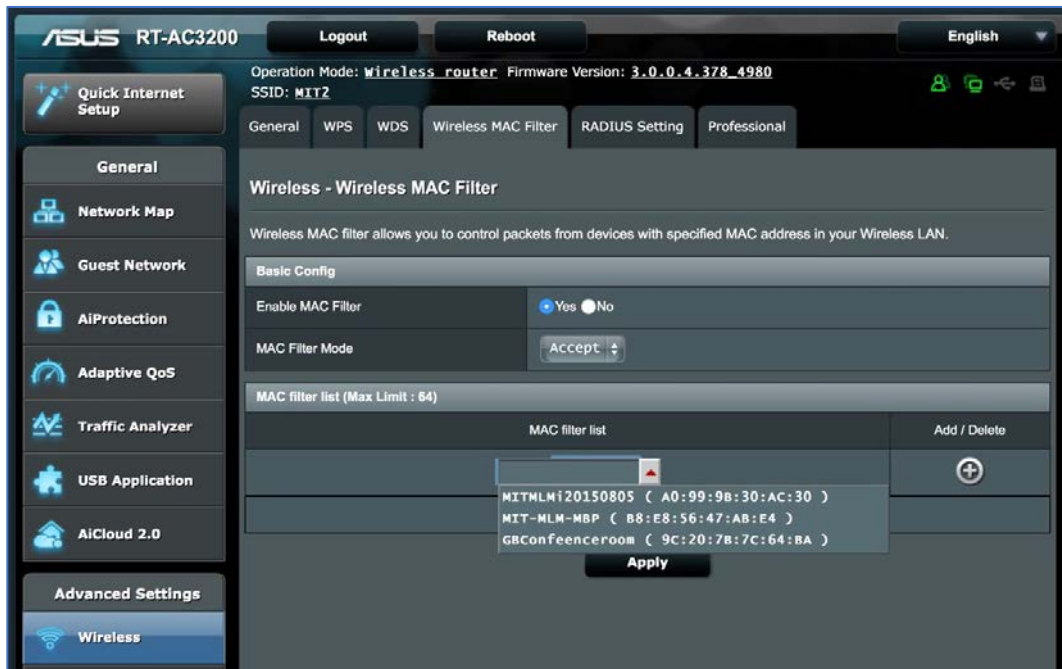
14. From the sidebar select *Wireless*, select the *Wireless MAC Filter* tab, enable the *Yes* radio button for *Enable MAC Filter*, and then set the *MAC Filter Mode* pop-up menu to *Accept*.



15. Clicking the disclosure triangle beneath the *MAC filter list* displays all the devices currently connected to the router via Wi-Fi. Selecting any of these

13 Local Network

adds its MAC address to the *MAC filter list*. You may also manually enter a MAC address to this field.



16. With a desired MAC address entered in to the *MAC filter list* field, click the *Add/Delete* button to add the device to the list.
 17. Repeat the previous 2 steps for each device to be allowed onto the Wi-Fi network.
 18. Click the *Apply* button to save changes.
 19. Close the browser window to exit out of your wireless router.
- Congratulations! You have secured your wireless network so that only authorized devices are granted access.

13.6 Router Penetration

The connection point between your Internet provider cable, DSL, fiber, radio, etc. and your Local Area Network (LAN) is a *Router*. A router is a device designed to connect two different types of networks.

Every router has at least some basic security controls built in, including the ability to filter out what it thinks are attempts to hack into your network, and the ability to forward specific types of data packets to a specific computer within your LAN, or to point specific types of data packets to a specific computer on the Internet.

Malware often attempts to alter these configurations so that either the malware or the criminals behind the malware have an easier time harvesting your data. Because of this, it is wise to routinely inspect the condition of your router. How often is “routine?” Within larger and security-conscious organizations, it is common to have a network administrator dedicated to maintaining watch over the status of network equipment. For a small business or household, once every month wouldn’t be too often.

Common areas of router penetration include:

- **Port forwarding**¹⁶: Port forwarding is useful if you have a service such as a web server running that you wish to be accessible from the internet. However, if ports are being forwarded without purpose, the firewall is being bypassed and your internal computers may be visible from the internet.
- **DMZ**¹⁷: Related to Port Forwarding is the DMZ, or De-Militarized Zone. DMZ is typically used to route *all* external traffic for a specific IP address, regardless of service request, to a specific computer. Unless there is a unique need, it should remain disabled.
- **RAM-Resident Malware**: Some router malware make their home in the RAM of the router. In this way, they can take control of your data traffic without showing in the interface.

¹⁶ https://en.wikipedia.org/wiki/Port_forwarding

¹⁷ [https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))

- **Firmware¹⁸:** It is vital to keep the router firmware up to date. Just as with any software, router firmware will always have vulnerabilities. Over time, criminals (including some government organizations) discover how to use these vulnerabilities to their benefit. Keeping the firmware updated helps to stay a step ahead of this problem.

13.6.1 Assignment: Verify Apple Airport Port Security Configuration

In this assignment, you verify the integrity of your Apple Airport (Extreme or Express) base station.

- Note: If this assignment is performed in a class, the instructor will demonstrate while the students observe.

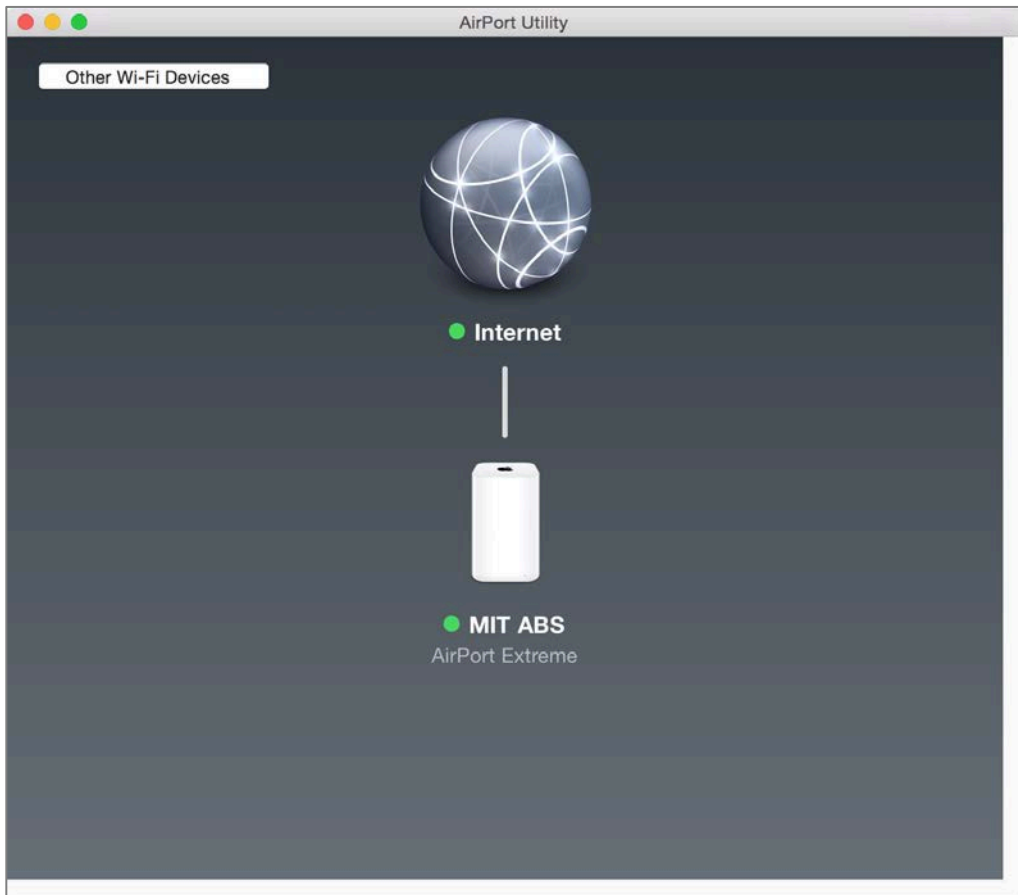
Some malware will make its home in the router RAM. Also, over time router RAM may accumulate corruption. The fix for both issues is the same—power cycling.

1. After verifying that all users have disconnected from the Internet and have closed any connections to other devices on the network, pull the power cord from the back of the Apple Airport.
2. Wait a minute.
3. Plug the power cord back into the Apple Airport. It may take up to two minutes for it to be fully operational.

¹⁸ <https://en.wikipedia.org/wiki/Firmware>

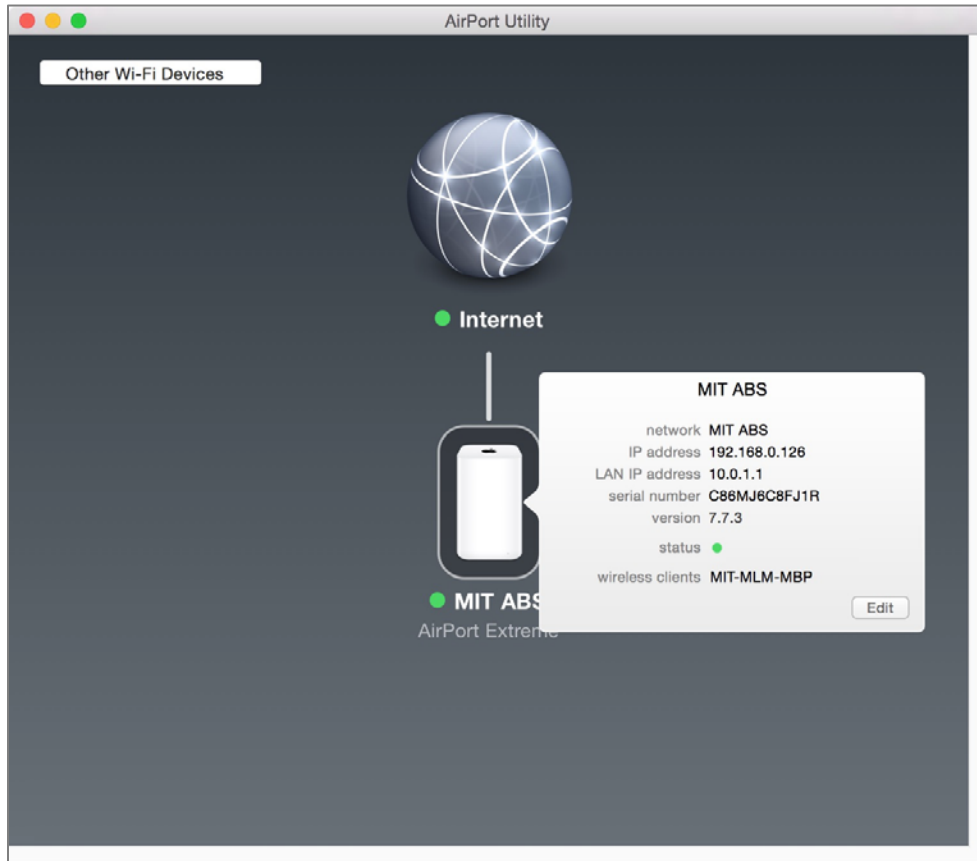
13 Local Network

4. Open *Airport Utility*, located in */Applications/Utilities*. The main window opens. Click on the target base station (in this example, the *MIT ABS*.)



Verify There Are No Reported Problems Or Firmware Updates Available

5. In the pop-up window, to the right of *Status*, verify that there are no reported problems and that no update notification is present. If either condition exists, select the associated button to either resolve the issue or update firmware.



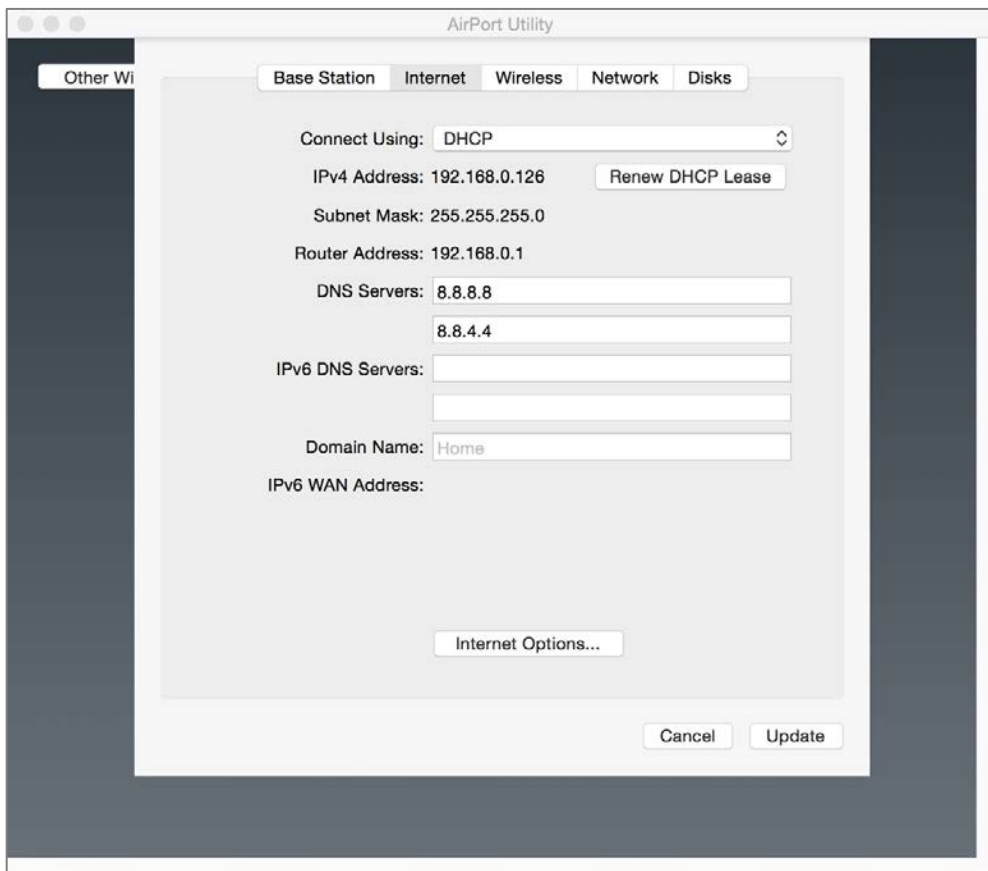
6. If there are no issues, select the *Edit* button.

Verify DNS Servers Are Configured Properly

7. Select the *Internet* tab. Look in the *DNS Servers* fields and verify these are set to the IP address of the servers you wish to use. If you are uncertain, these may be set to:

13 Local Network

- DNS Servers under the control of your Internet provider. You may contact them for the proper IP addresses.
- DNS Servers under the control of your organization. You may contact your IT department for the proper IP addresses.
- The IP address of your modem (not recommended, as you don't have certainty that the modem has not been compromised.)
- Any of the thousands of free and commercial DNS providers. In this example, we are using Google DNS.

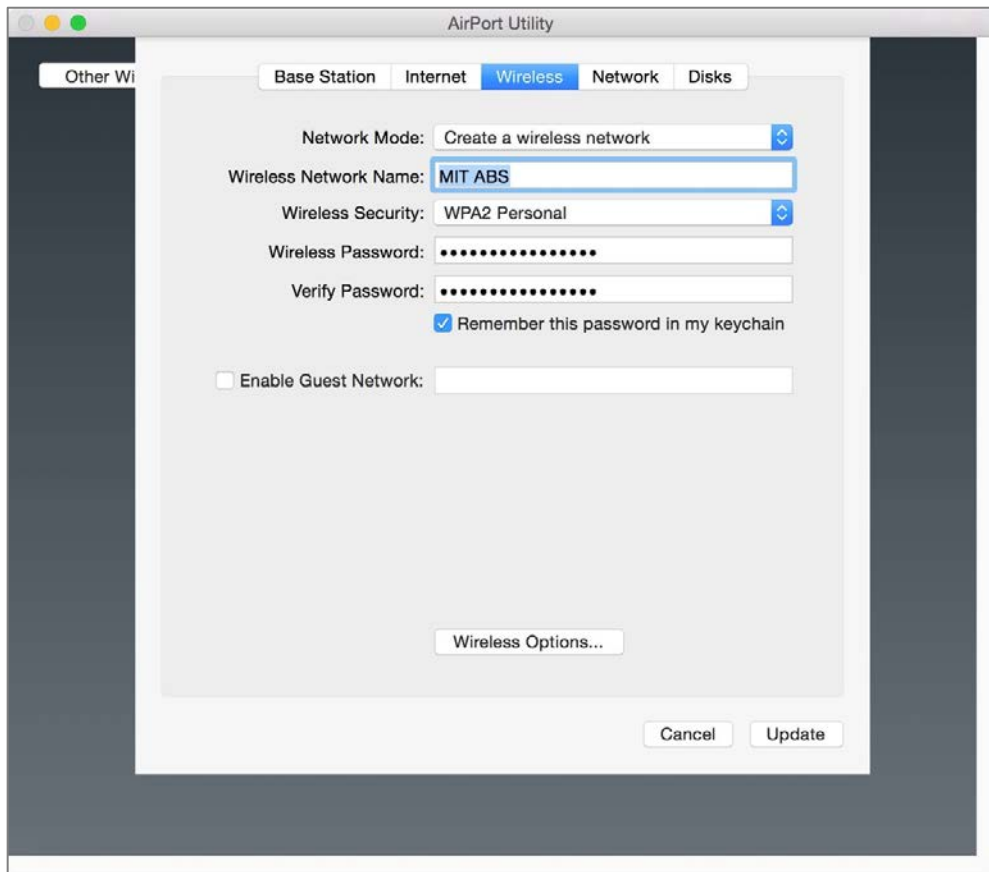


8. If changes to your *DNS Servers* has been made, select the *Apply* button.

Verify Encryption Is In Place

13 Local Network

9. Select the *Wireless* tab.
10. Verify the *Wireless Security* field is set to *WPA2 Personal*, or if you know you have a RADIUS¹⁹ server within your environment, *WPA2 Enterprise*.



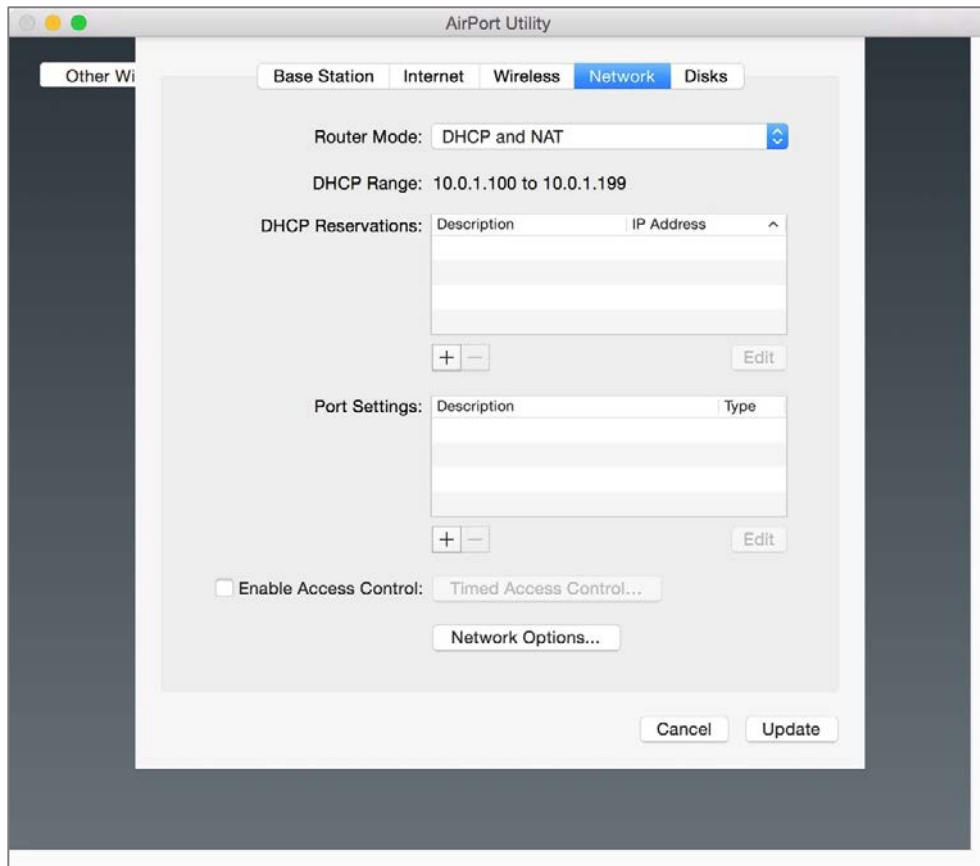
11. If changes have been made, select the *Update* button.

¹⁹ <https://en.wikipedia.org/wiki/RADIUS>

13 Local Network

Verify Port Forwarding

12. Select the *Network* tab. If there are any settings in the *Port Settings* area, verify there is a demonstrable business need for them, and that they are pointing to the proper devices. If not, remove them.
13. If any changes have been made, select the *Update* button.



14. Quit Airport Utility.

You are in great shape. Be sure to repeat this check at least monthly.

13.6.2 Assignment: Verify Non-Apple Airport Router Security Configuration

In the example below, I'm using an ASUS RT-AC3200. Although all routers have a somewhat different interface, most share the same functions.

In this assignment, you verify the security configuration of a non-Apple Router.

- Note: If this assignment is performed in a class, the instructor will demonstrate while the students observe.

Remove Any RAM-Resident Malware

Some malware will make its home in the router RAM. Also, over time router RAM may accumulate corruption. The fix for both issues is the same—power cycling.

1. After verifying that all users have disconnected from the Internet and have closed any connections to other devices on the network, power off the router. If yours does not have an on/off switch, pull the power cord from the back of the router.
2. Remove the router batteries (if any).
3. Wait a minute.
4. Insert the router batteries (if any).
5. Power on the router. It may take up to 3 minutes for it to be fully operational.
6. Open a browser and enter the IP address of your router.
7. At the prompt, enter the administrator user name and password.

Verify Router Firmware Is Up To Date

8. Select *Administration* from the sidebar, and then select the *Firmware Upgrade* tab.
9. Scroll down to the *Firmware Version* field. The currently installed version number is listed.

13 Local Network

10. To the right of this field is the *Check* button. Select it.

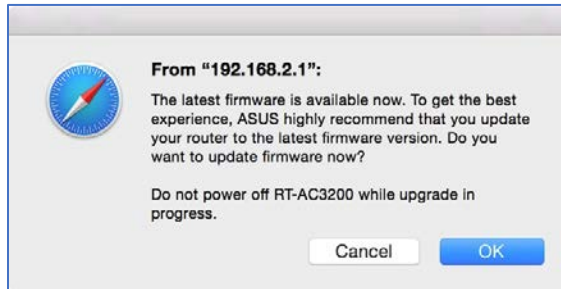
The screenshot displays the ASUS RT-AC3200 web interface. At the top, there are links for 'Logout' and 'Reboot', and a language dropdown set to 'English'. The main header shows 'Operation Mode: wireless router' and 'Firmware Version: 3.0.0.4.378_4980'. Below this, there are tabs for 'Operation Mode', 'System', 'Firmware Upgrade', and 'Restore/Save/Upload Setting'. The 'Firmware Upgrade' tab is active, showing a section titled 'Administration - Firmware Upgrade'. This section includes a 'Note' with four points regarding firmware updates and a table with the following data:

Product ID	RT-AC3200
Signature Version	1.064
Firmware Version	3.0.0.4.378_4980-g8c12667 <input type="button" value="Check"/>
New Firmware File	<input type="button" value="Choose File"/> no file selected

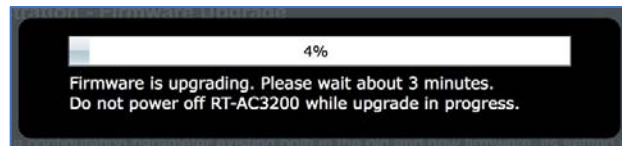
Below the table is an 'Upload' button. The left sidebar contains a 'Quick Internet Setup' button and a list of settings categories: General, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, USB Application, AiCloud 2.0, Advanced Settings, Wireless, LAN, WAN, IPv6, VPN, Firewall, and Administration (which is currently selected).

13 Local Network

11. A dialog box will display, stating either the firmware is up to date, or a new version is available.



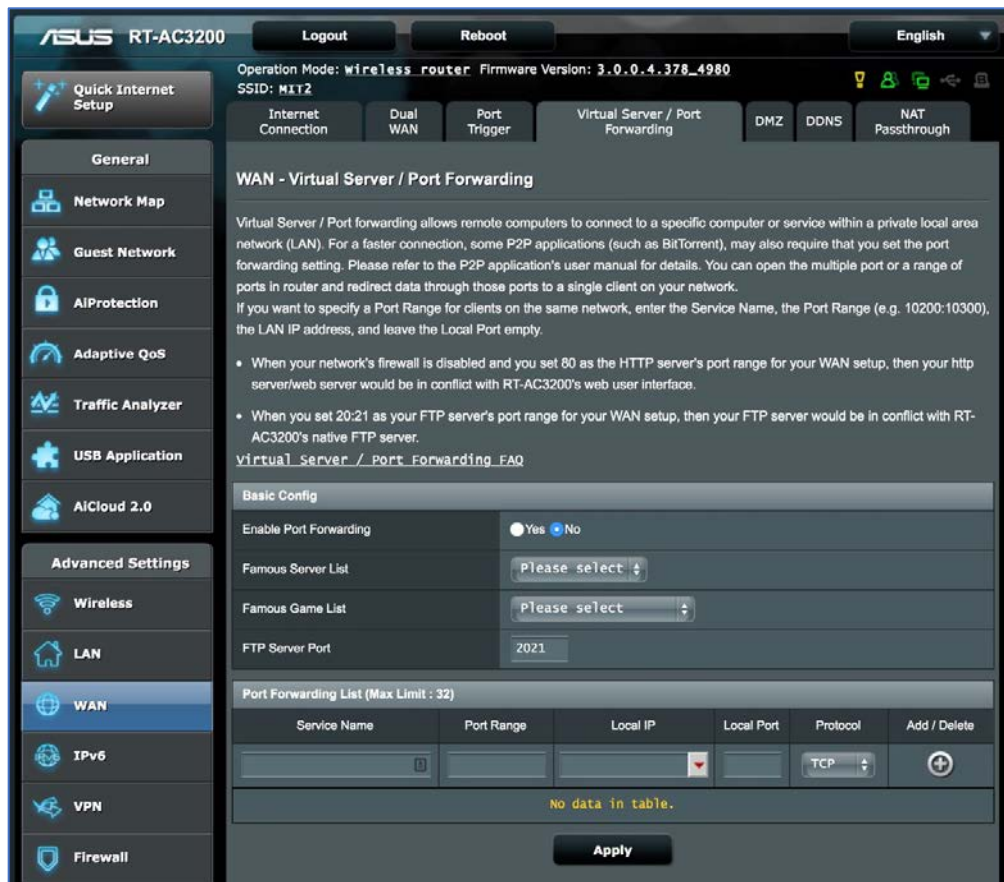
12. In this example, there is a more recent version, so we will select the *OK* button to download and install the update. If there is no new version available, exit the browser.
13. Note: During the download/install, the router will be offline, breaking Internet access for all on the network.
14. The firmware is downloaded.



15. When the download/install completes, you may exit the browser.

Verify No Unnecessary Port Forwarding

16. In the sidebar select *WAN*, select the *Virtual Server/Port Forwarding* tab, scroll down to the *Basic Config* area. View if *Enable Port Forwarding* is set to *Yes*. If it is, verify there is a demonstrable business need for this feature to be on. More information will be found in the next step.

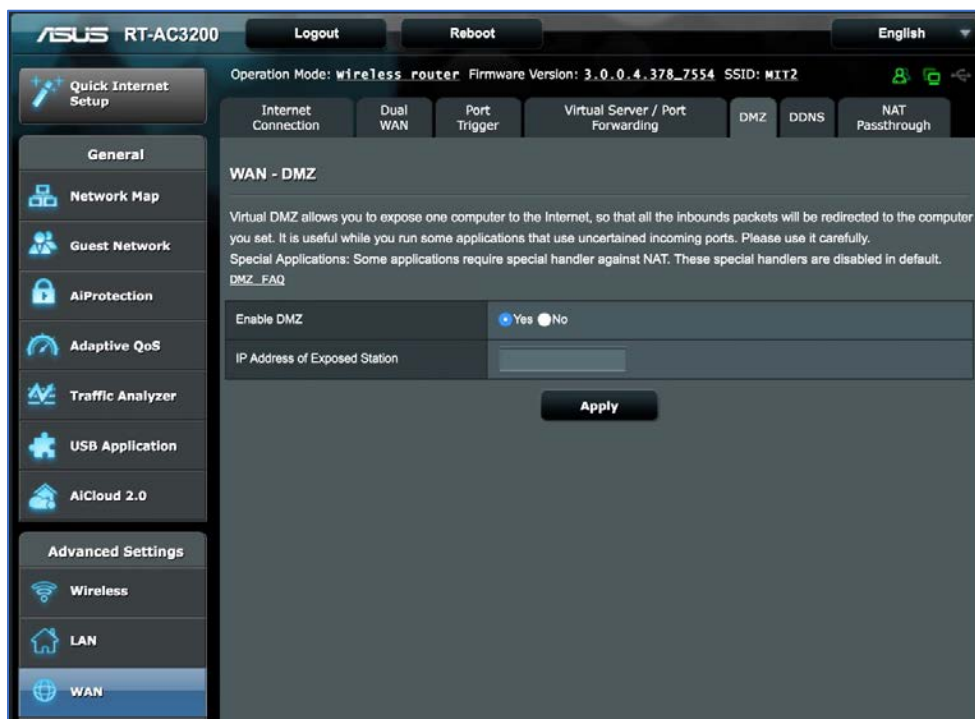


17. Scroll further down to the *Port Forwarding List* area. If Port Forwarding is turned on, this area will list which network services are being routed to which devices. Verify there is a demonstrable business need for this configuration. If not, then turn *Enable Port Forwarding* to *No*.
18. Select the *Apply* button.

Verify DMZ Configuration

Similar to Port Forwarding is *DMZ*. When *DMZ* is enabled, all inbound packets are routed to that device. This allows a single device on your network to be accessible from the Internet. This presents a very high level of vulnerability for that device. Unless there is a demonstrated business need for this function, and adequate steps have been taken to prevent unwanted penetration, turn *DMZ* off.

19. From the router control panel sidebar, select *WAN*, and then select the *DMZ* tab.



20. Scroll down to the *Enable DMZ* area. If it is set to *Yes*, verify there is a demonstrable business need for this function. The next step will provide additional information.
21. Below *Enable DMZ* is *IP Address of Exposed Station*. If *DMZ* is enabled, verify there is a true need for it based on this device. If not, set *Enable DMZ* to *No*.
22. If changes were made, select the *Apply* button.

23. Exit the browser.

Congratulations, your router is in great shape. Remember to perform this same checkup at least monthly.

14 Web Browsing

Distrust and caution are the parents of security.

–Benjamin Franklin¹

What You Will Learn In This Chapter

- Install HTTPS Everywhere
- Choose a browser
- Enable private browsing
- Enable secure web searches
- Clear browser history
- Install browser plug-ins
- Find and remove browser extensions
- Detect fraudulent websites
- Issues with Adobe Flash and Java
- Recover from a web scam
- Install Tor for anonymous browsing
- Find if you've been pwned

¹ https://en.wikipedia.org/wiki/Benjamin_Franklin

14.1 HTTPS

Due to an extraordinary marketing campaign, everyone knows the catchphrase: *What happens in Vegas, stays in Vegas*. With few exceptions, web surfers think the same thing about their visits.

Most websites use HTTP² (Hypertext Transport Protocol) to relay information and requests between user and website and back again. HTTP sends all data in clear text—anyone snooping on your network connection anywhere between your computer and the web server can easily see everything that you are doing.

Typically, the only exceptions you will come across are financial and medical sites, as they are mandated by law to use HTTPS³ (Hypertext Transport Protocol Secure). HTTPS uses the SSL⁴ (Secure Socket Layer) encryption protocol to ensure that all traffic between the user and server is military-grade encrypted.

- Note: With the recent changes in Google Search Engine Optimization⁵ (SEO) guidelines that give a higher priority to HTTPS sites, it will soon become common for sites to use encryption.

Although it is unlikely that you would ever be in the position to enter your password or bank account into an unsecure web page, you are almost guaranteed to enter your identity information, such as full name, address, phone number, and social security number. It is effortless for an identity thief to copy this information.

Anytime that you visit a web page that is secured using https, it will be reflected in the URL or address field of your web browser.

In the following example, I visit Wikipedia.org by entering *http://www.wikipedia.org* in my browser address field:

² https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

³ <https://en.wikipedia.org/wiki/HTTPS>

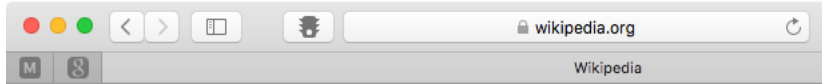
⁴ https://en.wikipedia.org/wiki/Transport_Layer_Security

⁵ https://en.wikipedia.org/wiki/Search_engine_optimization

14 Web Browsing



In the next example, I visit Wikipedia again, but this time I enter *https://www.wikipedia.org* in the address field:



Note how the address field reflects that I am now connected securely by displaying *https* and the *Lock* icon. Each browser will indicate security slightly differently—some displaying just the *https*, some just the lock.

- Note: As of this writing, Wikipedia has implemented automatic forwarding from HTTP to HTTPS, so if you enter *http://wikipedia.org*, you are automatically forwarded to *https://wikipedia.org*.

Now that I am connected securely to Wikipedia, snoops will not be able to see my actions. However, they still can see that I am connected to Wikipedia. If you would like to shield yourself completely, continue reading to our chapter on using a Virtual Private Network (VPN.)

Having to remember to connect via HTTPS for each web page is an impossible task. First, you have other, more important items to store in your synapses. Second, many websites do not have an HTTPS option, resulting in many error pages and wasted time during the day.

There are two options to resolve this:

- Automate the attempt to connect to sites via HTTPS
- Encrypt your entire online session using VPN

Using VPN is covered in a later chapter. Automating the attempt to connect via HTTPS is both easy and free. All it requires is a freeware plug-in, *HTTPS Everywhere*.

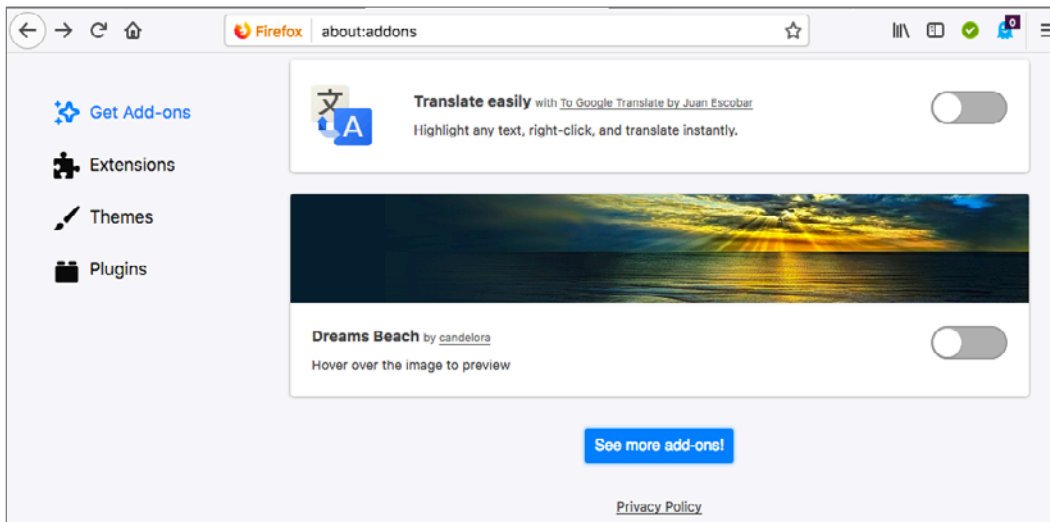
HTTPS Everywhere is available for Firefox, Opera, and Chrome. Unfortunately, this currently leaves Safari users without the option. If you are happy to use either of these two browsers instead of Safari, there is no reason not to install HTTPS Everywhere!

14.1.1 Assignment: Install HTTPS Everywhere

HTTPS Everywhere is available for Firefox, Opera, and Chrome.

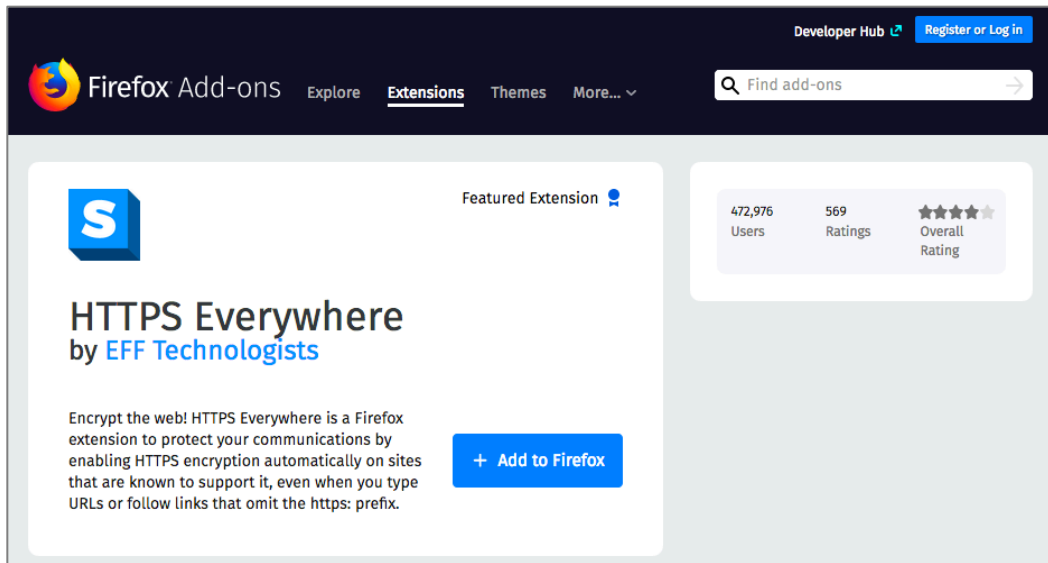
In this assignment, you install HTTPS Everywhere into Firefox.

1. If the Firefox browser is not currently installed, open Safari, and then go to <http://firefox.com> to download Firefox.
2. Open Firefox.
3. Select the *Tools* menu > *Add-ons*.
4. Select *Get Add-ons* from the sidebar, scroll to the bottom of the page, and then select the *See more add-ons!* button.



5. In the *Search* field, enter *https everywhere*, and then press the *Return* key. Matching items will appear below.

14 Web Browsing



6. Select the *Add to Firefox*. HTTPS Everywhere will download.
 7. At the *Add HTTPS Everywhere?* confirmation window, select the *Add* button, and then the *OK* button.
 8. HTTPS Everywhere is now installed in Firefox.
- You can repeat this process for Chrome and Opera.

14.2 Choose a Browser

There are many web browsers available on the market, with each placing a different emphasis on various features. The most popular browsers for macOS are Safari, Mozilla Firefox, and Google Chrome. Safari is included with macOS, while Chrome and Firefox are available as free downloads. Why might you want to replace Safari with another browser? Chrome integrates tightly with Google's own services, offering features such as direct voice translation and an ultra-minimalistic interface. Firefox touts itself as the most privacy-respecting browsers, and while that is a subjective claim, Firefox does not transmit your data to Google or any other 3rd party company every time you search using the address bar box. While Google considers this "non-identifying information", IP addresses are identifying at the Internet Service Provider level. This functionality can be changed, and with some tweaking, it is possible to make Chrome more privacy focused.

Browser	Platform	Price	Notable Features	Privacy
Brave	Android, iOS, macOS, Linux, Windows	Free	Speed Built-in HTTPS Everywhere Malware protection Ad block	High
Chrome	Android, iOS, Linux, macOS, Windows	Free	Speed Google Services Integration History and Bookmarks can be shared between your devices running Chrome	Fair
Edge	Windows 10	Free (included with Windows 10)	Active X Windows Integration	Fair
Firefox	Android, iOS, Linux, macOS, Windows	Free (Open Source)	Add-ons Privacy History and Bookmarks	Good

14 Web Browsing

			can be shared between your devices running Firefox	
Safari	macOS, iOS	Free (included with macOS/OS X and iOS)	History and Bookmarks can be shared between all your macOS and iOS devices	Good

14.2.1 Assignment: Secure Browsing With Brave

Brave was designed to be the most secure browser available. It includes anti-malware, ad-blocking, HTTPS Everywhere.

In this assignment, you install the Brave browser to help ensure a more secure browsing experience.

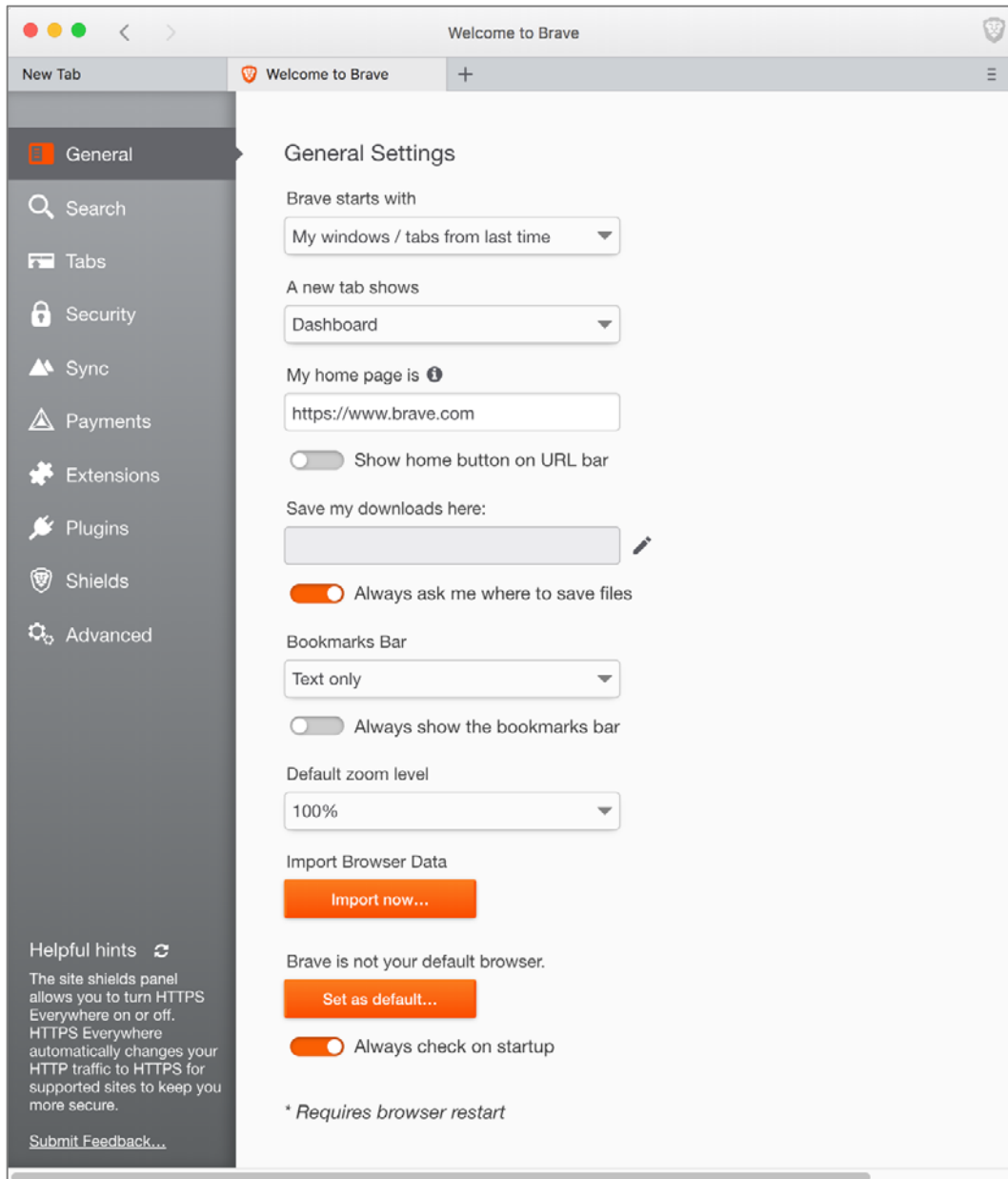
Download Brave

1. Open a web browser, and then surf to *<https://www.brave.com>*
2. Click the *Download* button.
3. At the *Download Brave* page, select *Download Brave*. Brave will download to your computer.
4. Double-click to open the *Brave.dmg* file.
5. Drag Brave into your Applications folder.

Configure Brave

6. Open the Brave browser.
7. Select the *Brave* menu > *Preferences*.

8. From the sidebar, select *General*.



9. Scroll down, and then select the *Import Now...* button.

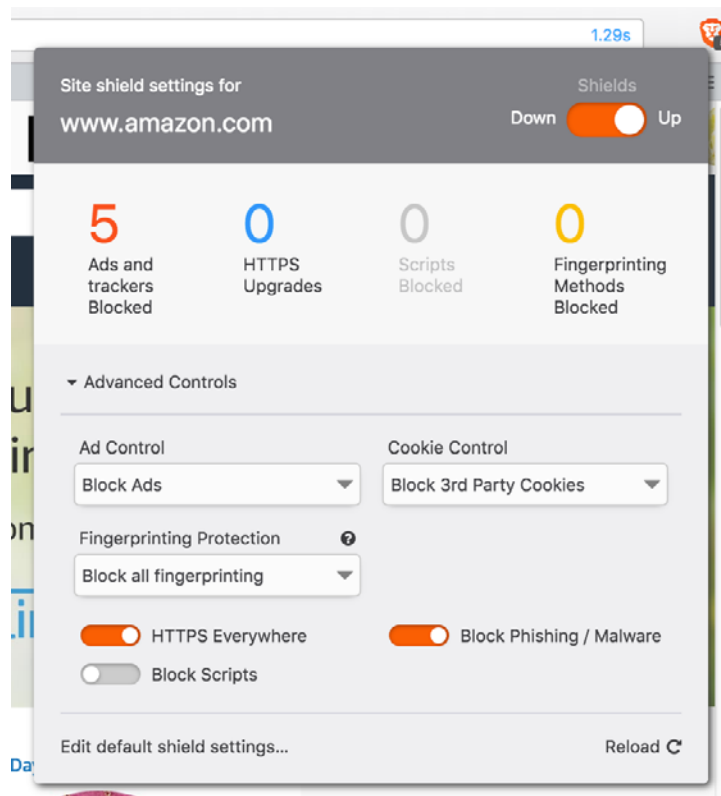
10. Select what data and settings you want to import, and then select the *Import* button.
11. Configure the rest of the *General* settings to your taste.
12. From the sidebar, select *Search*.
13. From the list of search engines, select *DuckDuckGo*.
14. Configure the rest of the *Search Engines* settings to your taste.
15. From the sidebar, select *Tabs*, and then configure to your taste.
16. From the sidebar, select *Security*.
17. Scroll to the bottom of the page, and then enable *Do Not Track*.
18. Enable *Strict Site Isolation*.
19. Configure the rest of *Security* page to your taste.
20. You may be prompted to restart Brave to enable these settings. Do so now.
21. Select and configure to your taste the *Sync*, *Payments*, *Extensions*, and *Plugins* pages.
22. From the sidebar, select *Shields*.
23. From the *Ad Control* pop-up menu, select *Block Ads*.
24. From the *Cookie Control* pop-up menu, select either *Block 3rd Party Cookies*, or *Block All Cookies*.
25. From the *Fingerprinting Protection* pop-up menu, select *Block All Fingerprinting*.
26. Enable *HTTPS Everywhere*.
27. Leave *Block Scripts* disabled. Unfortunately, most sites requires scripts to run properly.
28. Enable *Block Phishing / Malware*.
29. Enable *Display block count badge on shields button*.
30. From the sidebar, select *Advanced*.
31. Enable *Use hardware acceleration when available*.
32. Enable *Enable Smooth Scrolling*.

- 33. Configure the rest of the *Advanced* page to your taste.
- 34. You may be prompted to restart Brave to enable these settings. Do so now.
- 35. Once restarted, you are ready to surf the web.

Customizing For Each Website

Brave can be customized on a site-by-site basis.

- 36. With Brave open, visit a website (in my example, Amazon.com).
- 37. The Brave Shield in the top right corner display how many trackers have been blocked.
- 38. Click the Brave Shield. The Shield configuration window will open.



- 39. If a website is behaving poorly due to the default Brave settings, this is where you can create a custom setting for this site.

14.3 Private Browsing

Private Mode (Safari), *Private Browsing* (Firefox), and *Incognito Mode* (Chrome), are features that prevent any normally cached data from being written to storage while using a browser. This data includes browsing history, passwords, user names, list of downloads, cookies, and cached files. This is an essential tool if you work on a computer where your account is shared (what's with that?.), or if there is the possibility that someone else will examine your browsing habits. This does not prevent your company IT department or Internet Provider from seeing or recording your browsing habits.

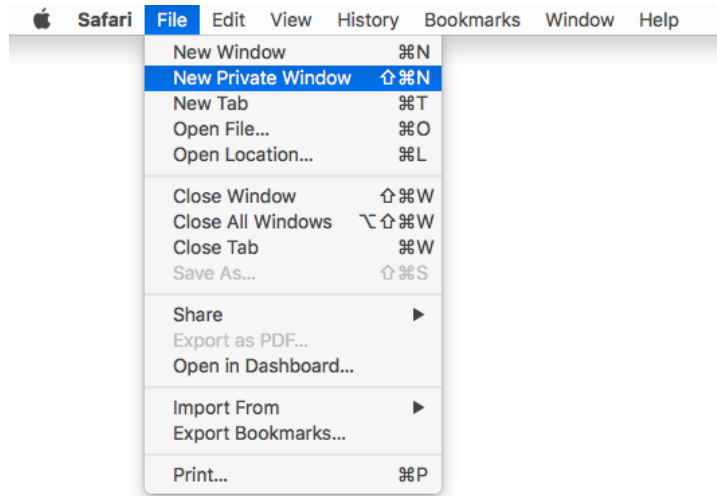
14.3.1 Assignment: Safari Private Browsing

Before we secure your website travels from roaming eyes out on the Internet, we should first be secure from the roaming eyes on the home front. If you have secured your computer to this point, including: Strong password, nobody else has access to your account, your *System Preferences > Security & Privacy* are set to *Require password after sleep or screen saver begins*, it is unlikely that you also need to implement *Safari Private Browsing*. But just in case...

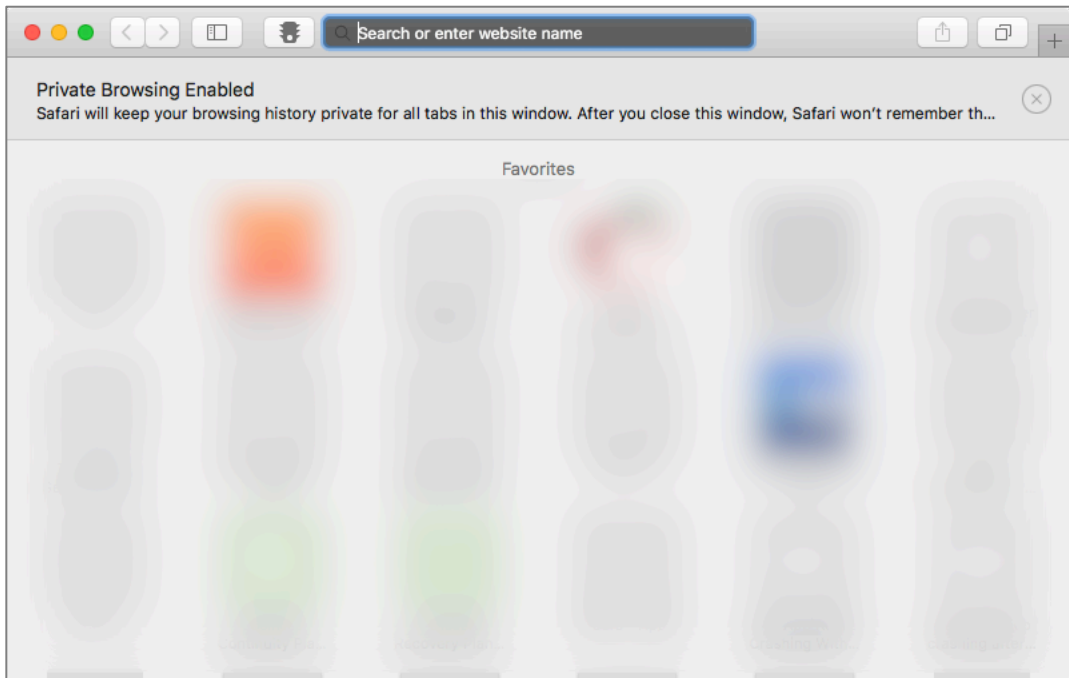
In this assignment, you enable Private Browsing within Safari

14 Web Browsing

1. From the *Safari File* menu, select *New Private Window*.



2. A new Safari window will appear. You can see that you are in *Private Browsing* by the *Search* field being dark.

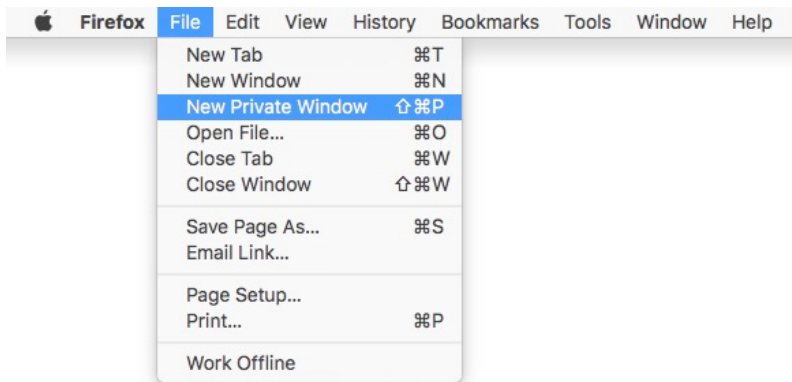


Sites that are visited from within this window will leave no trace in the *History*, and cookies are not shared with any other browsing windows.

14.3.2 Assignment: Firefox Private Browsing

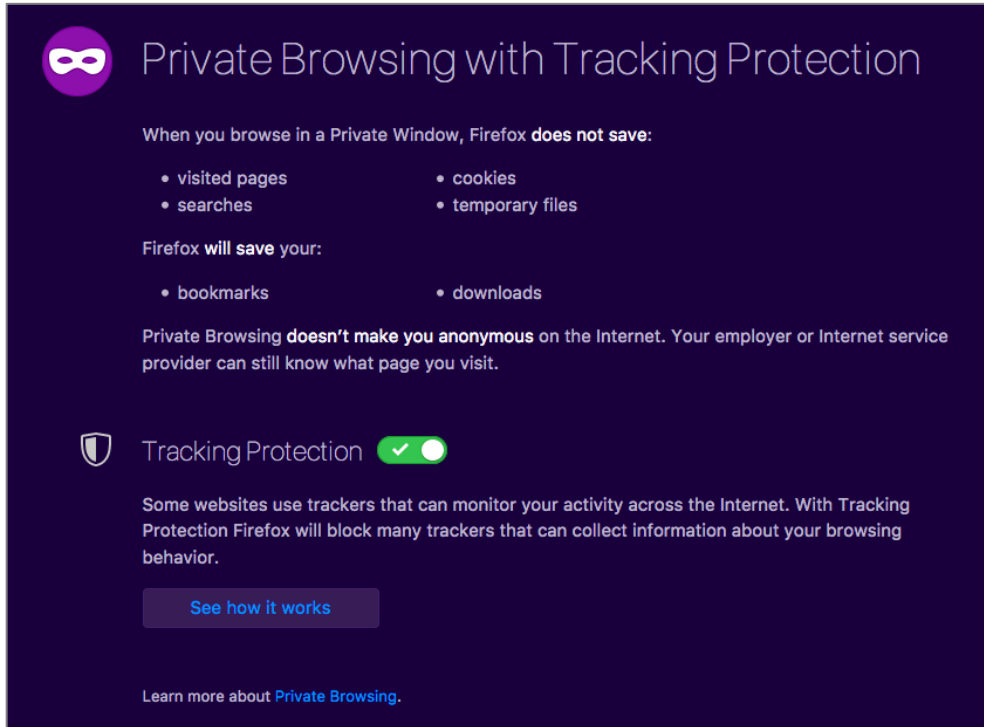
If you prefer Firefox to Safari, then let us enable its private browsing.

1. Launch Firefox.
2. Select the Firefox *File* menu > *New Private Window*.



14 Web Browsing

3. A new *Private Window* opens, informing that you are now, well, browsing privately.
 - Note: A Firefox *Private Window* will display a mask icon in the left side of a private tab, and in the top right corner of a private window.

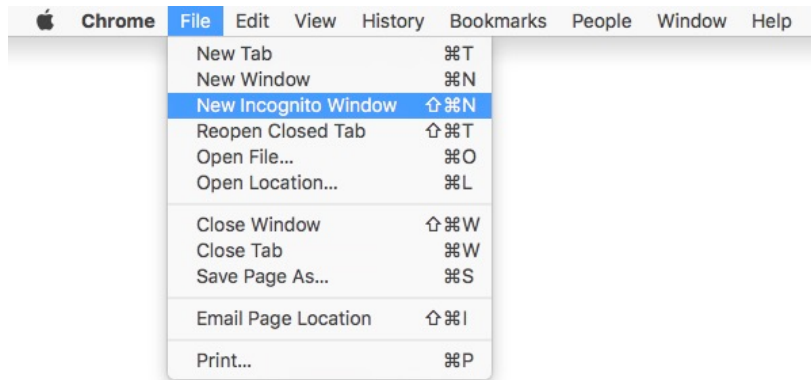


14.3.3 Assignment: Google Chrome Incognito Mode

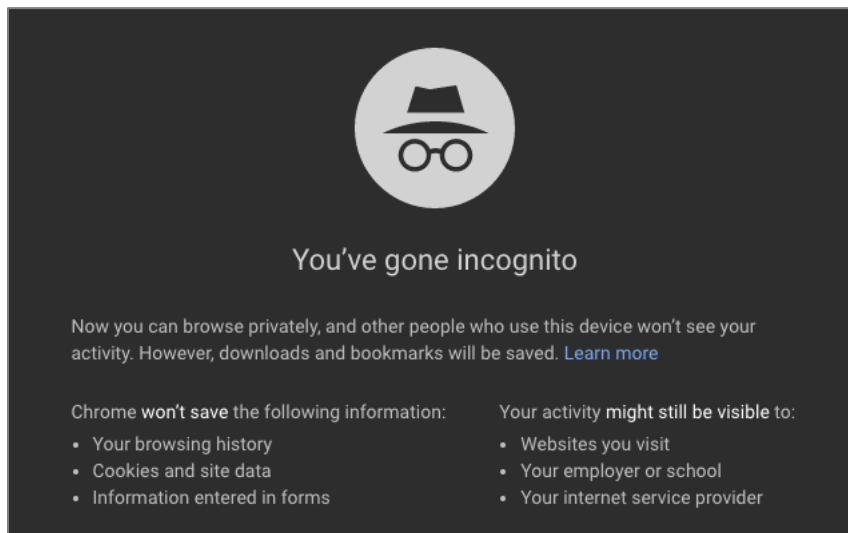
If your preference leans toward Google Chrome, you can enable its *Incognito Mode*.

1. Launch Google Chrome.
2. Select the *File* menu > *New Incognito Window*.

14 Web Browsing



3. A new *Incognito Window* opens, informing that you have now, gone incognito.
 - Note: A Chrome *Incognito Window* will display the incognito icon in the top right corner, and the title bar will turn dark.



14.4 Secure Web Searches

With most web browsers, when performing a search, the search criteria and sites visited are collected and stored by the search engine. The Cookies assigned from one website can communicate with other sites and webpages you open. Also, most search engines record your searches and build a profile of your search history so that your search results will be unique and tailored to your interests.

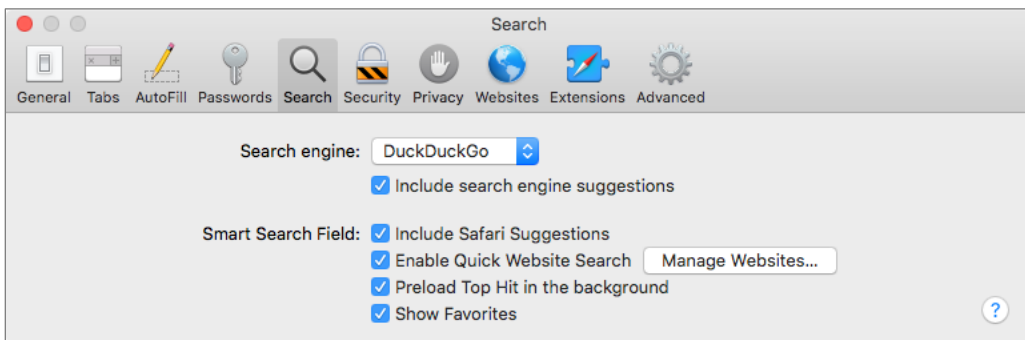
Not so with the *DuckDuckGo* search engine. DuckDuckGo's policy is that it keeps no information on user searches, nor does it track search queries via IP addresses. Subsequently, all search results are identical for everyone.

Starting with OS X 10.10, Safari offers the option to make DuckDuckGo your default search engine. This is a big step towards providing a better level of privacy on the Web.

14.4.1 Assignment: Make DuckDuckGo Your Safari Search Engine

In this assignment, you change the default Safari search engine from Google to the secure search engine DuckDuckGo.

1. Open Safari.
2. Open the *Safari* menu > *Preferences*.
3. Select the *Search* icon from the Toolbar.
4. From the *Search Engine* pop-up menu, select *DuckDuckGo*.



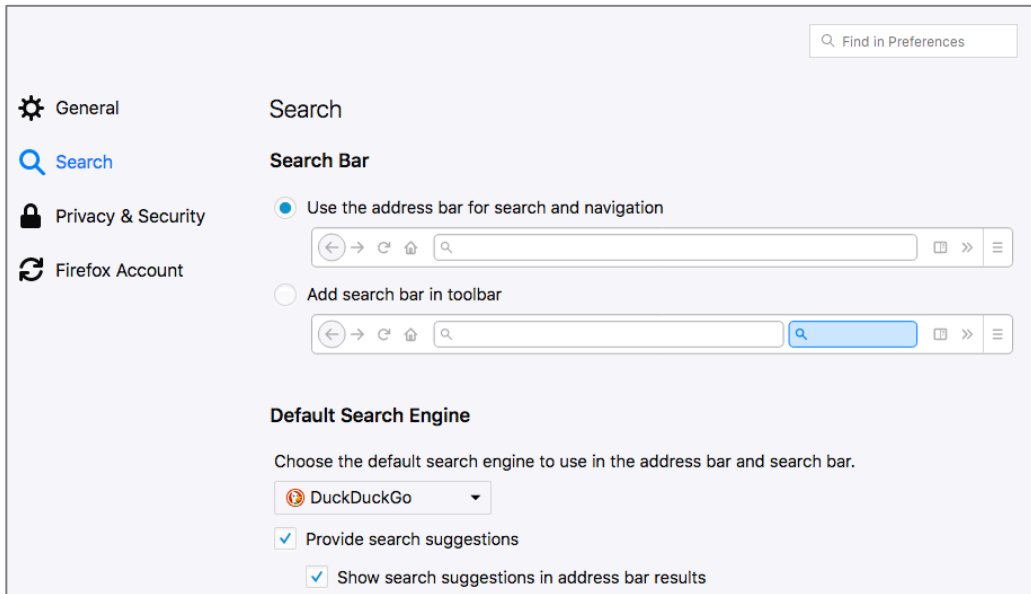
5. Close the Preferences window.

From now on, your default search engine for Safari will be *DuckDuckGo*, hiding your search activities.

14.4.2 Assignment: Make DuckDuckGo Your Firefox Search Engine

In this assignment, you change the default Firefox search engine to the secure DuckDuckGo.

1. Open Firefox.
2. Select the *Firefox* menu > *Preferences*.
3. Select *Search* from the sidebar, and then select *DuckDuckGo* from the *Default Search Engine* pop-up menu.



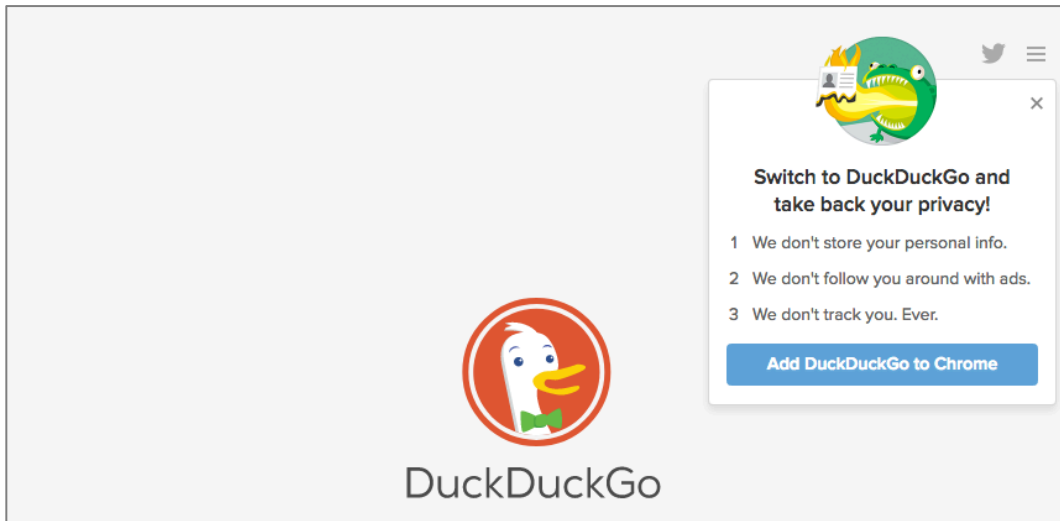
4. Close the Preferences window.

From now on, your default search engine for Firefox will be *DuckDuckGo*, hiding your search activities.

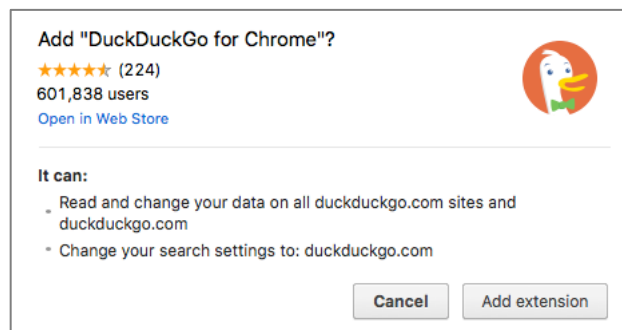
14.4.3 Assignment: Make DuckDuckGo Your Chrome Search Engine

In this assignment, you change the default Chrome search engine to DuckDuckGo.

1. Open Chrome.
2. Go to *<https://duckduckgo.com>*.
3. On the DuckDuckGo home page, select *Add DuckDuckGo to Chrome*.

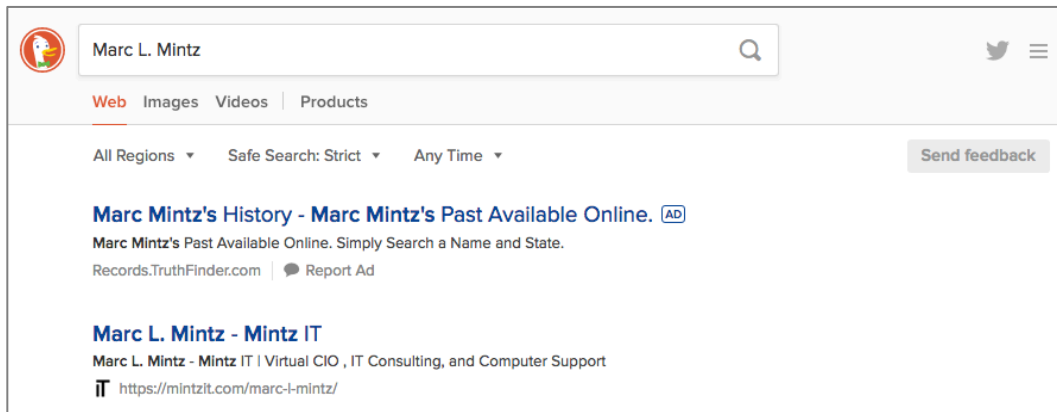


4. At the *Add DuckDuckGo for Chrome?* Window, select *Add Extension*.



14 Web Browsing

5. To verify DuckDuckGo is the new default search engine, perform a search in Chrome. Note the Duck logo.



From now on, your default search engine for Chrome will be *DuckDuckGo*, hiding your search activities.

14.5 Clear History

By default, every browser maintains a full history of every site you have visited. Should someone gain access to your device, they will be able to view your browsing history.

You just realized that: 1) Your mother is coming over, 2) you have been naughty on the web all day, 3) you did not turn on Private Browsing, and 4) your mom will feel insulted if you insist that an account for her must to be created instead of accepting her protest: *Oh, baby, I only need to check my AOL email. Just let me get on your account for a minute.*

Is it time to panic?

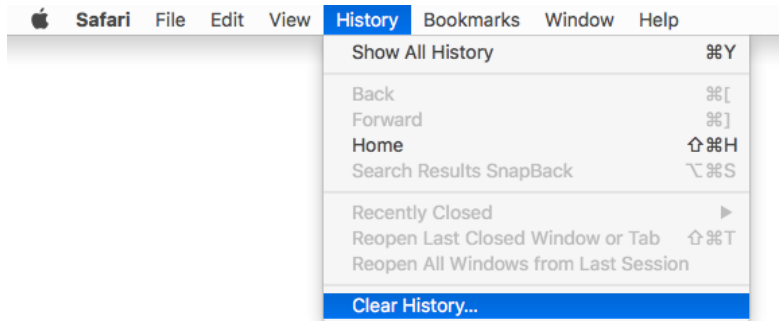
Not yet! You can erase your entire (steamy) browsing history in one click.

14.5.1 Assignment: Clear The Safari History

In this assignment, you clear your entire browsing history in Safari.

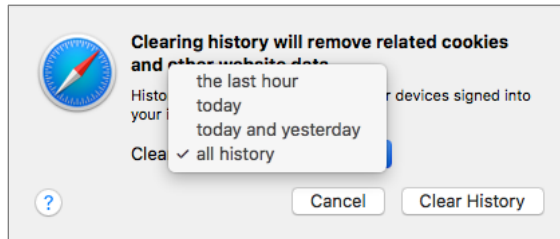
- Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Safari, and then select the *History* menu > *Clear History...*



14 Web Browsing

2. A dialog box opens asking for what time frame you wish to clear your history. Make your selection, and then select the *Clear History* button.



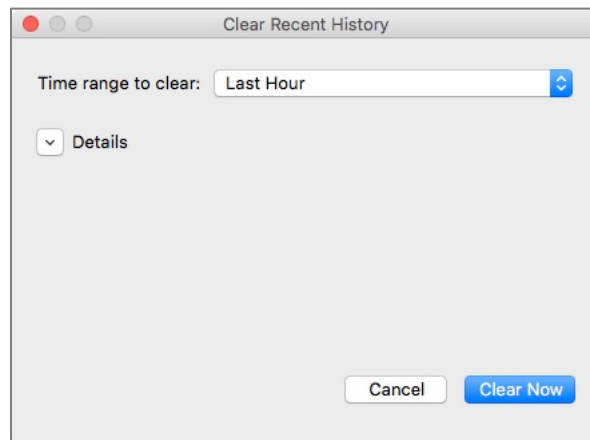
The Safari history is now cleared as you defined.

14.5.2 Assignment: Clear The Firefox Browsing History

In this assignment, you clear your Firefox browsing history.

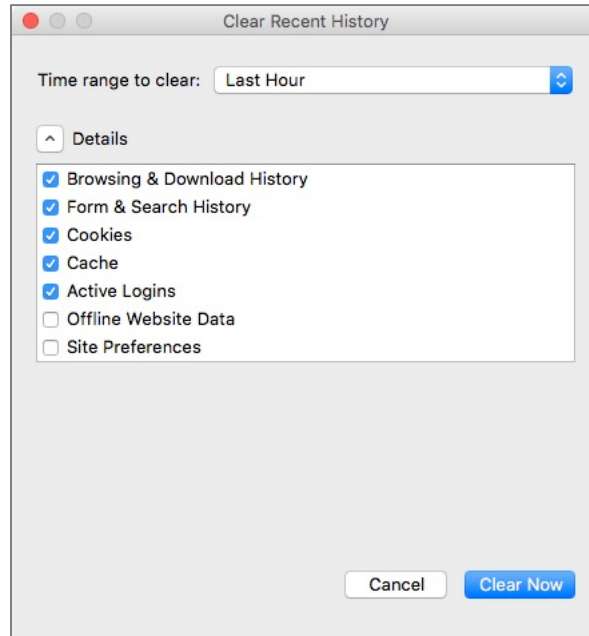
Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Firefox.
2. Select the *History* menu > *Clear Recent History...* The *Clear All History* window opens.



14 Web Browsing

3. Select the *Details* disclosure button to expand your options.



4. Select the *Time range to clear*, which history items are to be cleared, and then click the *Clear Now*.
5. Close the *Clear Recent History* window.

The Firefox history is now history.

14.5.3 Assignment: Clear The Chrome History

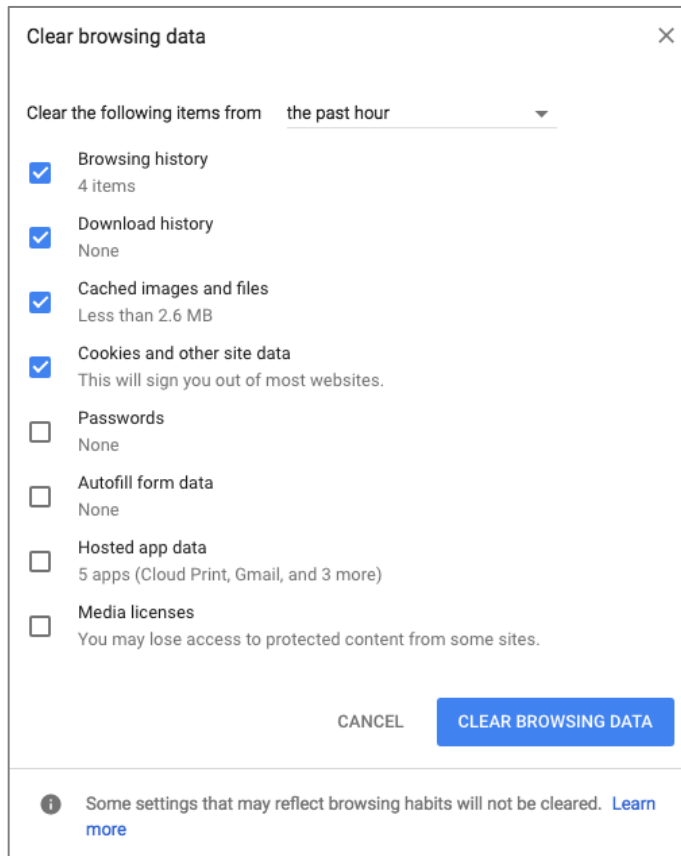
In this assignment, you clear your browsing history in Chrome.

- Note: Be forewarned, there is no recovery from this action. If you wish to keep your history, pass on this assignment.

1. Open Chrome.

14 Web Browsing

2. Select the *Chrome* menu > *Clear Browsing Data...* The *Clear Browsing Data* window opens.



3. Select which items are to be cleared, and then click the *Clear Browsing data* button.

Done!

14.6 Browser Plug-Ins

One of the great advances in personal computer software development was the concept of plug-ins or extensions⁶. These small strings of code add functionality to the host application. In the case of web browsers, this may be anything from the ability to encrypt web-based email, to viewing proprietary video formats.

The bad news about plug-ins is that they run with the full power of the host application. This means that a malicious plug-in may have the power to secretly redirect your web browser to fake websites (such as a phony copy of your bank), or harvest all your passwords, monitor your purchases, etc.

There are many malicious plug-ins. It is vital to only install those plug-ins that you need to install, to know which plug-ins are installed, and to rid yourself of unnecessary plug-ins.

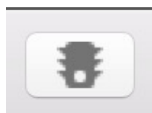
14.6.1 Assignment: Install TrafficLight Plug-In For Safari

In this assignment, you search for extensions for Safari, and then install the *TrafficLight* anti-malicious website extension.

- Note: Prior to macOS 10.13, Safari Extensions were found in a separate area of the Apple website. Starting with macOS 10.13, Safari Extensions are moving to the Mac App Store. As of this writing, Apple was in transition with how to acquire and install Safari Extensions, with almost all Safari Extensions still found on the Apple site, and none on the Mac App Store.
1. Open Safari.
 2. Select the *Safari* menu > *Safari Extensions...* The *Safari Extensions* page opens. Scroll down to see the featured Extensions located on the Apple Safari Extensions site. You may also search for Extensions in this area.
 3. Assuming Apple will quickly migrate Extensions to the Mac App Store, Select *Go to the Mac App Store*.

⁶ [https://en.wikipedia.org/wiki/Plug-in_\(computing\)](https://en.wikipedia.org/wiki/Plug-in_(computing))

4. The Mac App Store opens to *Safari Extensions*. Select the *Popular*, *Recent*, or *Categories* links to explore the available *Safari Extensions*.
5. Explore and review some of the available extensions.
6. In the *Search* field, enter *TrafficLight*, and then tap the *Return* key. The *TrafficLight* from *Bitdefender* page opens. TrafficLight is a browser extension that adds protection from malicious websites. If you happen upon a compromised or malicious site, it will alert you and provide a button to back out of the site before your system is penetrated.
7. Select the *Install now* link located under the description of TrafficLight.
8. When installation completes, you will see a traffic light icon in your Safari tool bar.



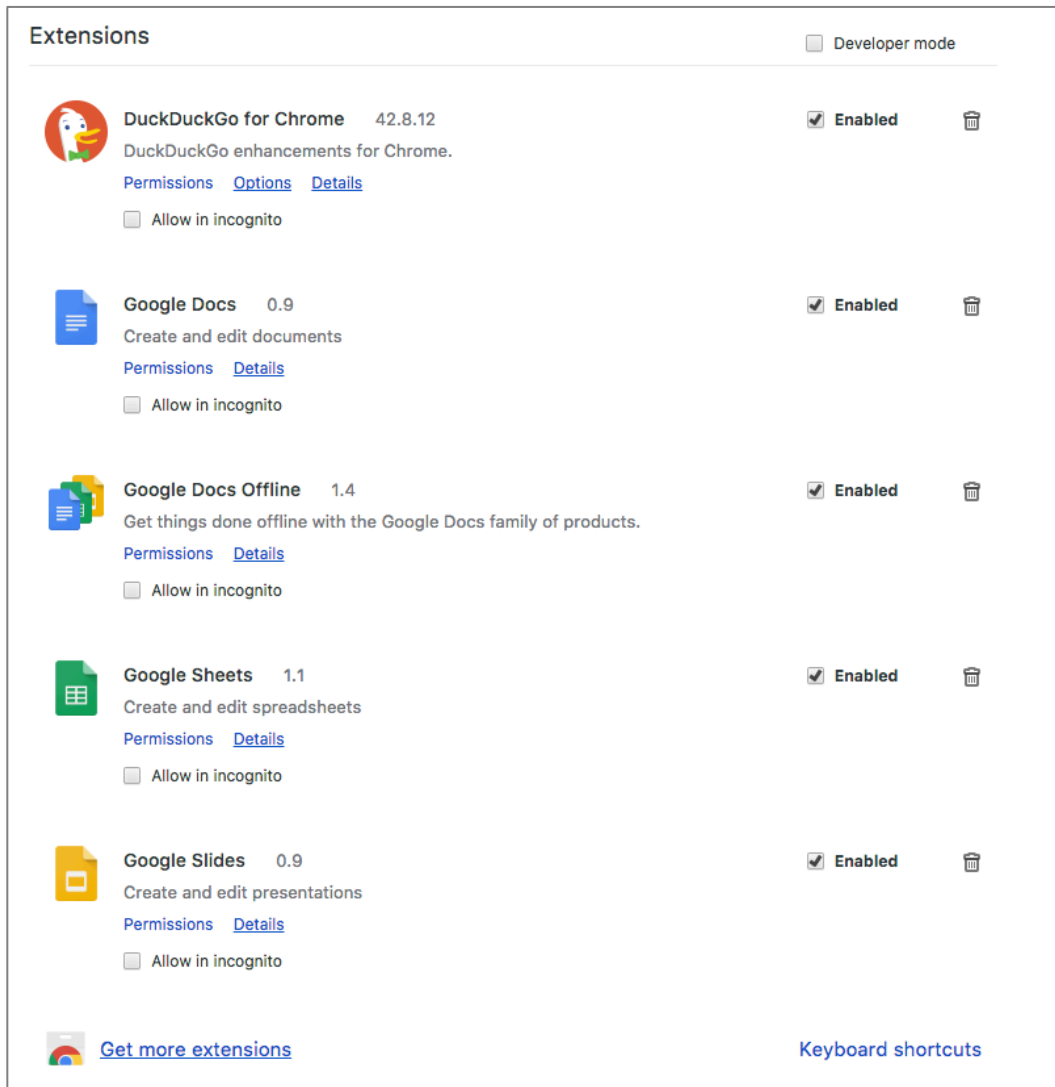
14.6.2 Assignment: Install TrafficLight Plug-In For Google Chrome

In this assignment, you search for extensions for Chrome, and install the *TrafficLight* anti-malicious website extension.

1. Open Google Chrome.

14 Web Browsing

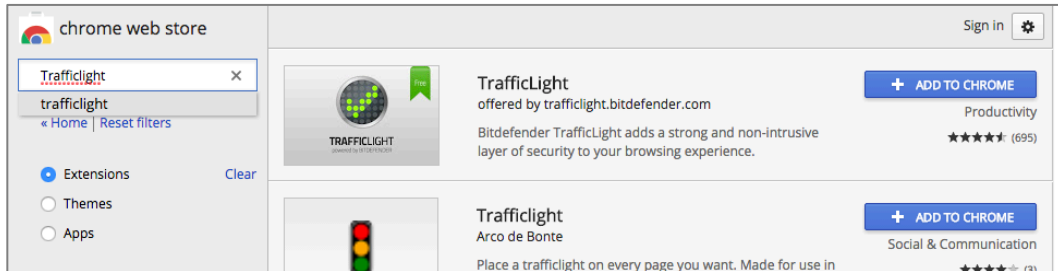
2. Select the *Menu* icon (3 lines at the right edge of the tool bar) > *More Tools* > *Extensions*. Any currently installed extensions will display.



3. Scroll to the bottom of the page, and then select *Get More Extensions*.
4. Explore the available extensions.

14 Web Browsing

5. In the sidebar, select *Extensions*, in the *Search the store* field, enter *TrafficLight*, and then tap the *Return* or *Enter* key. The results page appears.



6. In the *TrafficLight* offered by *trafficlight Bitdefender* area, select the *Add To Chrome* button. If prompted to confirm, confirm the addition.
7. At the *Add TrafficLight?* Window, select *Add extension*.
8. Once installed, you will see the TrafficLight icon in the Chrome tool bar—a green dot.



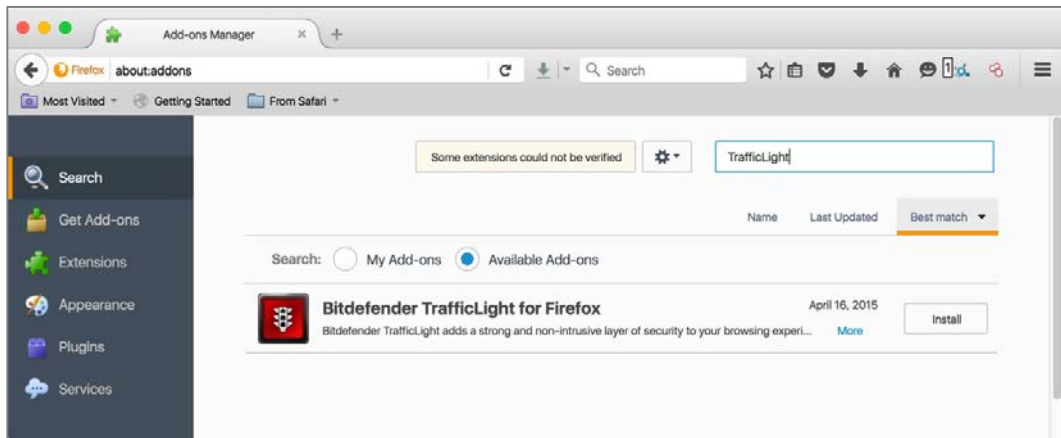
14.6.3 Assignment: Install TrafficLight For Firefox

In this assignment, you search for plug-ins for Firefox, and install the *TrafficLight* anti-malicious website extension.

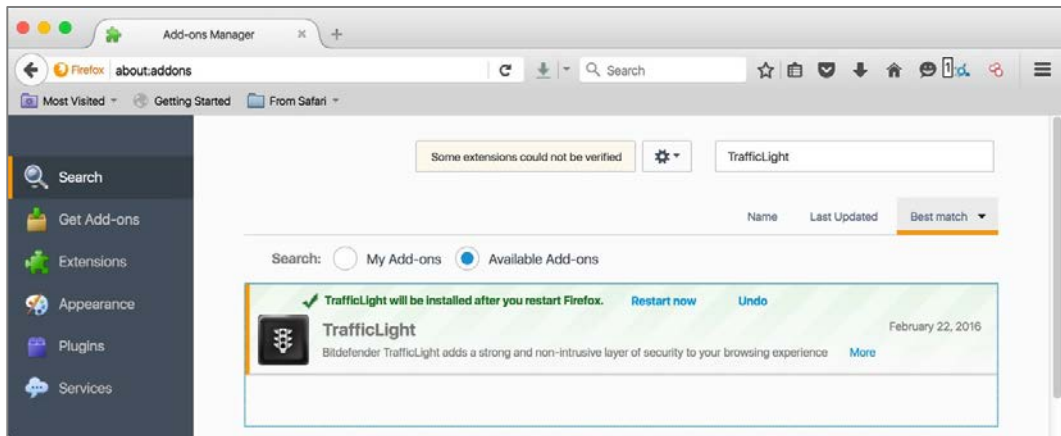
1. Open Firefox.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons*.
3. Select *Get Add-ons* from the left sidebar.
4. Explore the available add-ons.

14 Web Browsing

5. In the *Search all add-ons* field, enter *TrafficLight*, and then tap the *Return* key. The results page appears.



6. In the Bitdefender TrafficLight for Firefox area, select the Install button.
7. At the confirmation window, confirm OK.
8. Once installed, select the Restart now link.



9. Once installed, you will see the TrafficLight icon in the Chrome tool bar—a green dot.



14.6.4 Assignment: Find And Remove Extensions From Safari

In this assignment, you see the installed Safari Extensions, determine if they are what you need, and remove those that are not needed.

1. Open Safari.
2. Select the *Safari* menu > *Preferences*.
3. From the Preferences tool bar, select *Extensions*.
4. All currently installed Extensions will display in the sidebar.
5. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
6. If you determine you don't want any Extensions installed, select the target Extension in the sidebar, and then select the *Uninstall* button under the target extension.

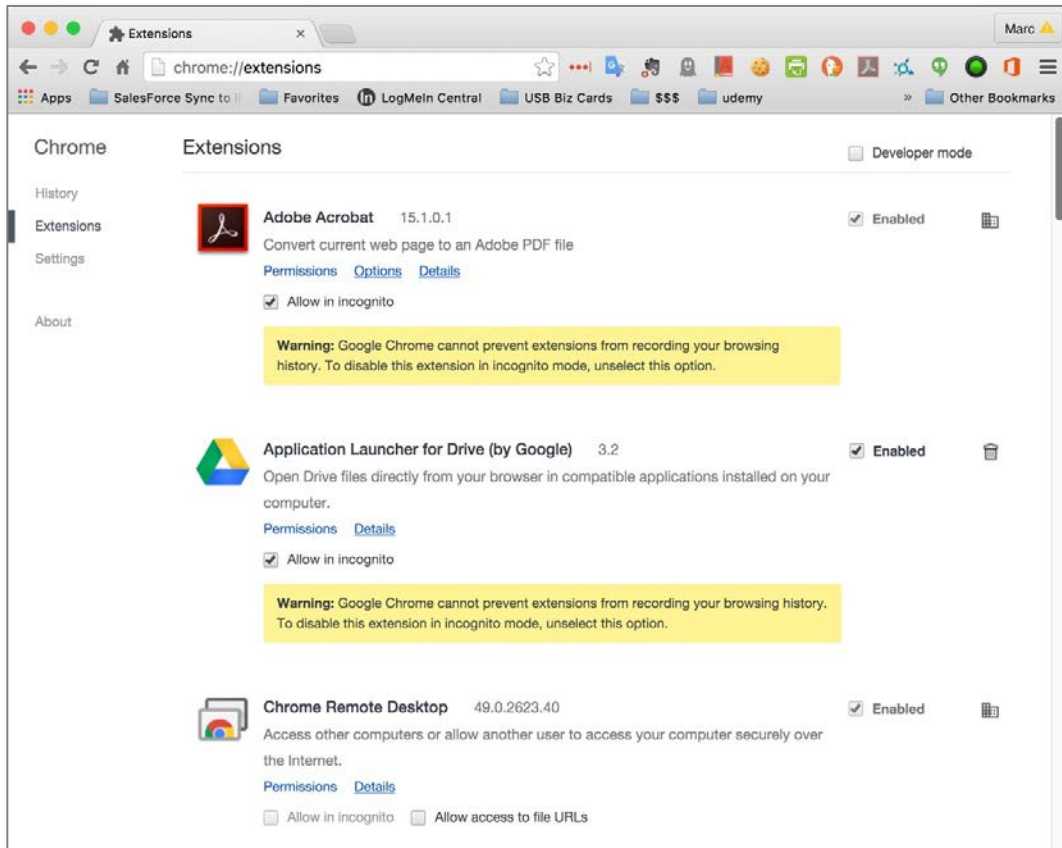
14.6.5 Assignment: Find And Remove Extensions From Chrome

In this assignment, you see the installed Chrome Extensions, determine if they are what you need, and remove those that are not needed.

1. Open Chrome.

14 Web Browsing

2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Settings*.
3. Select *Extensions* from the left sidebar. The *Chrome Extensions* page opens.



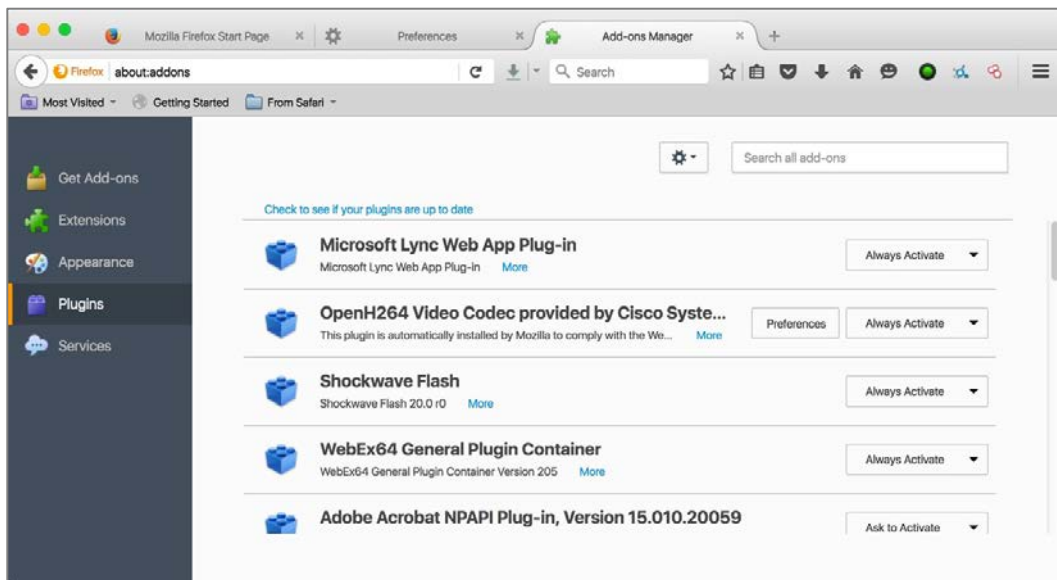
4. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
5. If you determine you don't want any Extensions installed, click the *Trash* icon to the far right.

14.6.6 Assignment: Find And Remove Add-Ons From Firefox

In this assignment, you see the installed Firefox Extensions, determine if they are what you need to be installed, and remove those that are not needed.

14 Web Browsing

1. Open Firefox.
2. Select the *Menu* menu (3 lines at the right edge of the tool bar) > *Add-ons*.
3. Select *Extensions* from the left sidebar.
6. If you see any Extensions that you do not remember installing, perform an Internet search to discover what they do, and if they present a vulnerability.
7. If you determine you don't want any Extensions installed, click the *Remove* button to the far right.
8. Select *Plugins* from the left sidebar.

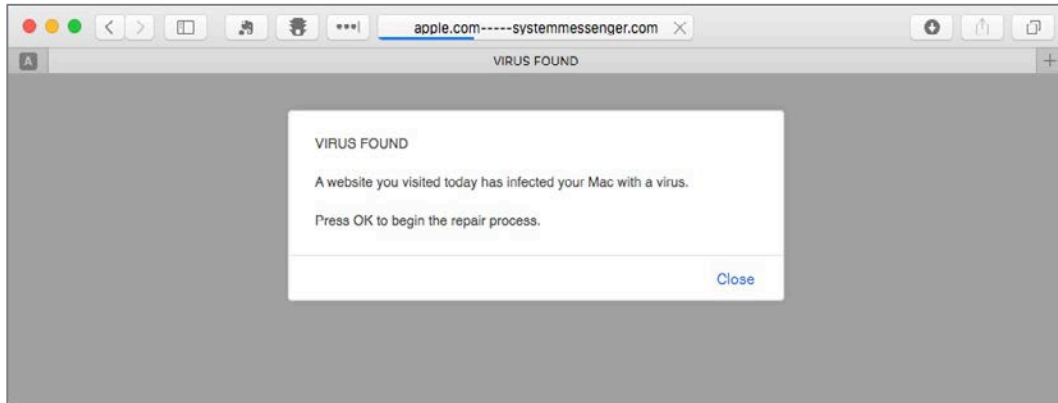


9. Perform an Internet search on any plugins that are unfamiliar to you. If you determine you don't want one active, select *Never Activate* from the pop-up menu to the far right.

14.7 Fraudulent Websites

As of this writing, there are over 1,000,000,000 active websites⁷. Within that, there may be millions of fraudulent websites. Of the diverse types of fraud found on the Internet⁸, among the most common are websites that misrepresent who they are. This may be in the form of appearing like Bank of America, but with a URL of perhaps <http://bankofamerica.cm>, instead of the true <http://bankofamerica.com>. In this case, the criminal is hoping for someone to make the typo. Once at their site, you would enter your account and password as typical. The difference is that this time, the criminal now has your credentials—and all your money within minutes.

As a side note, in this specific example as of the time of this writing, this URL actually *is* as scam site. But not for the scheme mentioned. When I went to <http://bankofamerica.cm>, I was routed to the following:



If we look at the full URL, it is: <http://apple.com-----systemmessenger.com/dgkg/?city=Albuquerque®ion=New%20Mexico&country=US&ip=71.222.135.33&isp=Qwest%20Communications%20Company%20Llc&os=OS%20X&osv=OS%20X%2010.11%20El%20Capitan&browser=Safari&browserversion=Safari%209&volumdata=BASE64dmlkLi4wMDAwMDAwNi01Yzg0LTRjNjYtODAwMC0wMDAwMDAwMDAwMDBfX3ZwaWQuLmRl...>

⁷ <http://www.internetlivestats.com/total-number-of-websites/>

⁸ https://en.wikipedia.org/wiki/Internet_fraud

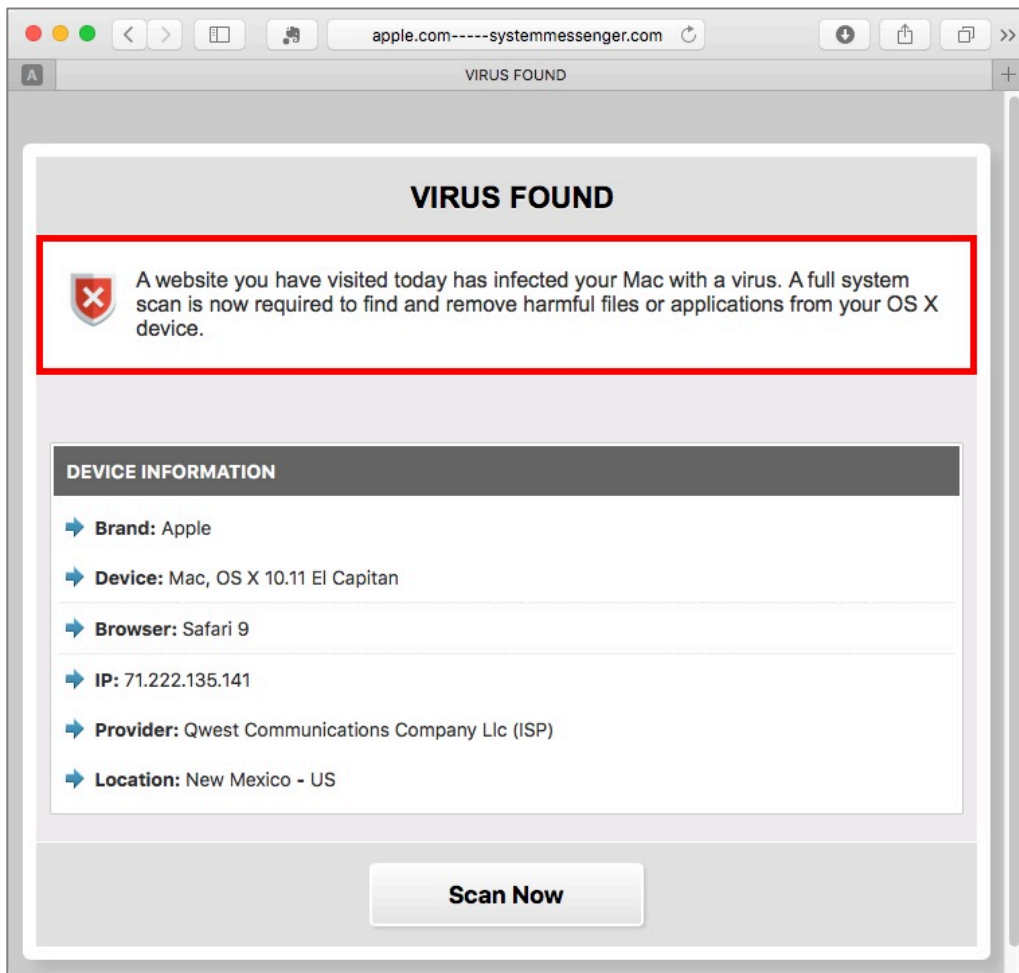
14 Web Browsing

From this URL, we can see that the criminal site attempts to appear as though it is Apple reporting that I have a virus.

They have also discerned my city, state, IP address, Internet provider (Qwest Communications), that I am using OS X 10.11 El Capitan, with Safari version 9.

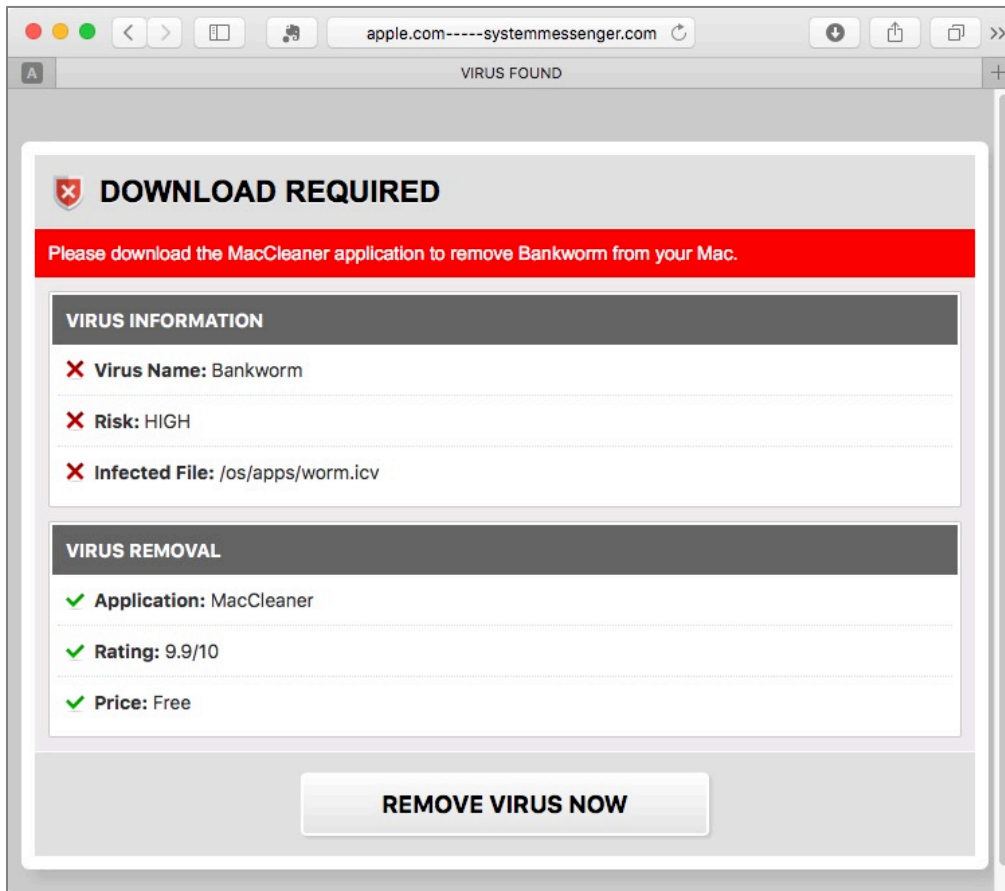
If I were the typical user, I'd probably think there was a virus present and press the *OK* button as recommended. You may have also noticed the criminal was bright enough to do all of this, but not bright enough to put an *OK* button in the script!

So, I press the *Close* button. I'm presented with a new window:



14 Web Browsing

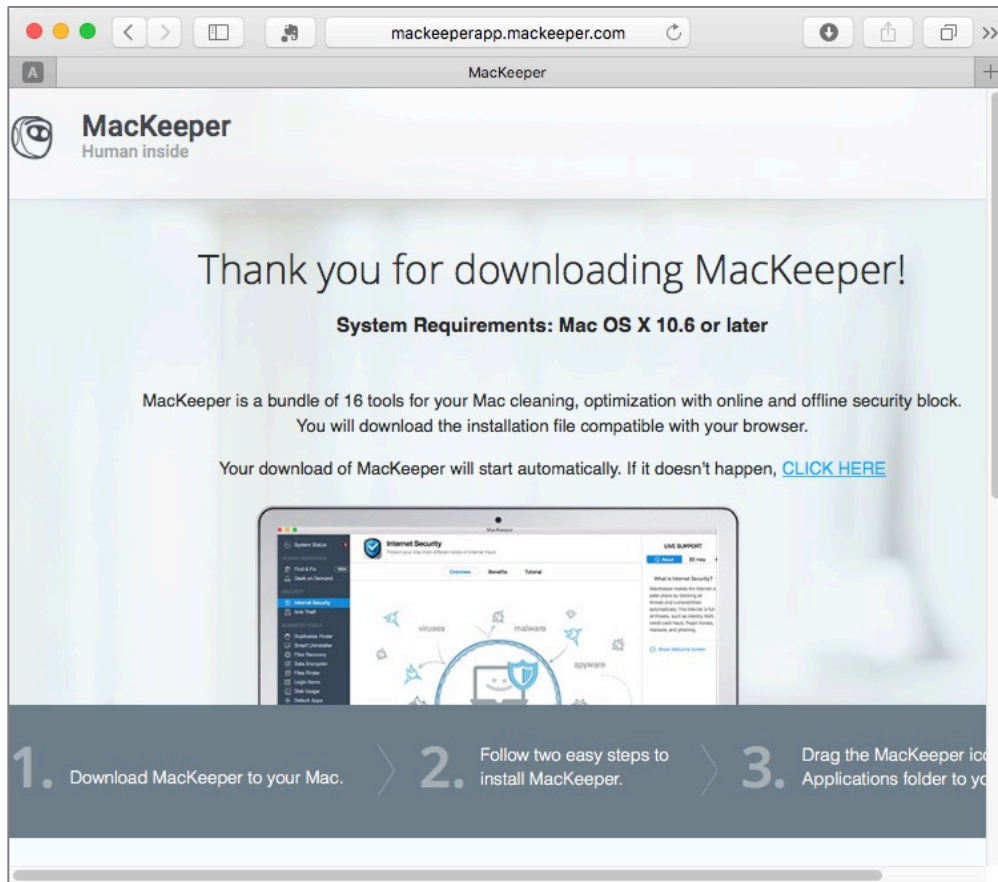
Hey, who needs an *OK* button when the *Close* button will do the intended scam! So, let's see what happens when clicking the *Scan Now* button:



Appears they think I am infected with the *Bankworm* virus (which may or may not be a real malware name), and the infected file is in `/os/apps/worm.icv`. The only real problem I see is that there is no such file, and no such directory.

14 Web Browsing

But they are offering a free solution to my non-existent problem. Let's see where that takes us by clicking the *Remove Virus Now* button:



MacKeeper?! Really! This product lost a class action lawsuit for deceptively advertising its functionality⁹.

If you have followed along so far, just trash the MacKeeper download.

So, how to protect yourself against fraudulent sites? We will go through the few steps that can be taken, but the most important tool is your awareness.

⁹ <https://topclassactions.com/lawsuit-settlements/closed-settlements/94767-mackeeper-class-action-settlement/>

14.8 Do Not Track

Most websites track which pages you visit, how long you stay on each page, and other metrics to better understand their visitors. That is a little creepy. Imagine going to the library, and having a librarian looking over your shoulder as you scan the card catalogue, and records each of the books and pages you glanced at.

Now let's take the analogy further. You leave the library and go across town to have lunch, and then shop for shoes. You look around and the same librarian is still watching and recording not only everything you have eaten, but everything you looked at on the menu.

Later you go for a date, and the librarian is sitting right behind you in the theater, noting who you are with, what scenes you reacted to, and more.

Web browsing isn't much different—except the snoop is normally invisible in the form of cookies, trackers, and browser fingerprinting.

Any website can initiate cookies on your browser. These keep a record of the pages you visit on the site. But they have evolved to report all the other places you visit and things that you do. This is why you can visit Amazon, look up my books, quit the web browser, launch it, go to okcupid, and see an ad for my books!

In addition, there are 3rd-party trackers that are integrated with many sites. When you visit one site, you are uniquely identified. In this way, when you visit another site, the tracker knows who you are. Trackers are able to piece together a solid psychological, sociological, and financial profile on you.

There is the option to disable cookies, but most of your websites will demand they be enabled to visit the site.

Trackers are invisible by default. However, we do have tools to thwart them. Some web browsers have a preference setting to ask web sites not to track you. Notice that is *ask*. Good luck with that.

We can take *Do Not Track* to another level. To do this, we need to install a browser extension which prevents sites from tracking you. There are several available.

Device fingerprinting, however, is a bit more of a problem. When opening a webpage, it is possible for the site (or a search engine) to uniquely identify your device amongst the hundreds of millions of other devices on the internet. Once you have been fingerprinted, it is easy to track your activity across the internet. As ghastly as this is, there is currently little that can be done.

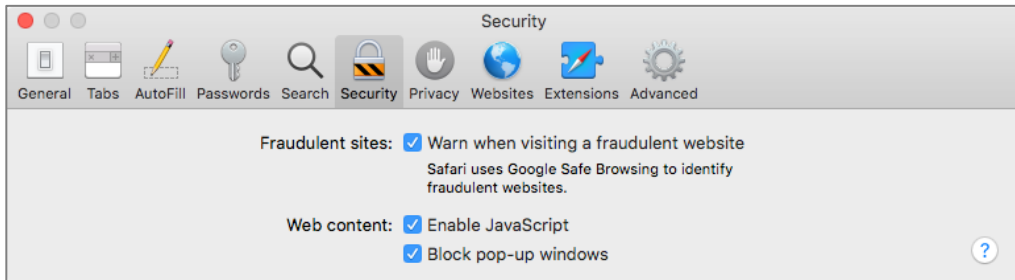
There are promises from browser developers to build in fingerprinting blocking technology. But it is currently only reasonably implemented in Tor. There are browser extensions to block fingerprinting, but these are in early stage development and not very effective.

The only 100% solution at this time is to use a bootable thumb drive with Tails installed, and then do nothing to alter the drive or OS setup. When booting from this Tails, you will look exactly like all of the other Tails users, and it will be impossible to fingerprint you.

14.8.1 Assignment: Secure Safari

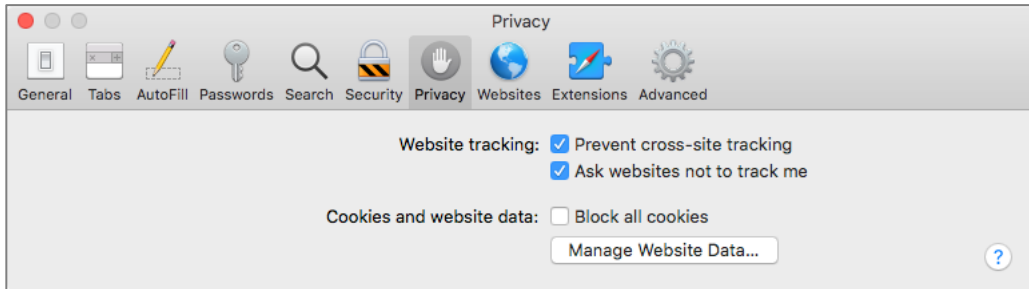
In this assignment, you secure Safari.

1. Open Safari, click the *Safari* menu > *Preferences* > *Security*.
2. Enable *Warn when visiting a fraudulent website*.



14 Web Browsing

3. Select the *Privacy* tab.

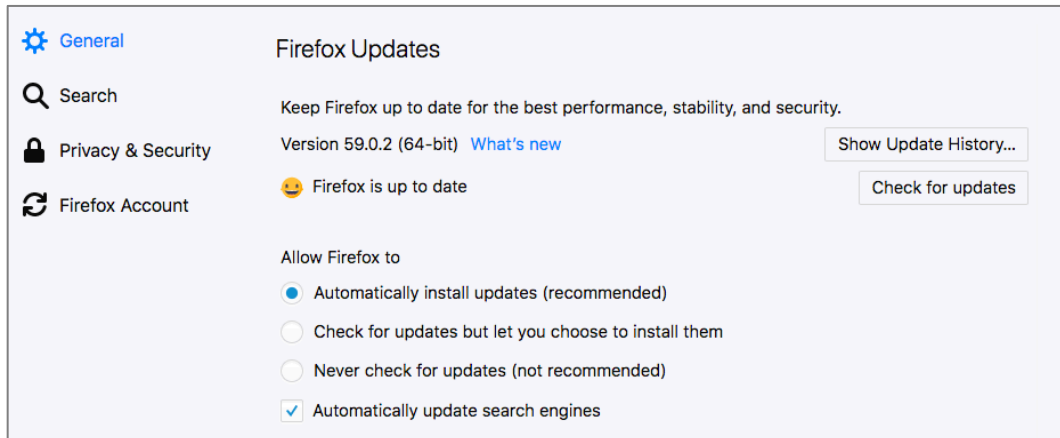


4. Enable *Website tracking: Prevent cross-site tracking*
5. Enable *Website tracking: Ask websites not to track me*.
6. Close Safari Preferences.

14.8.2 Assignment: Secure Firefox

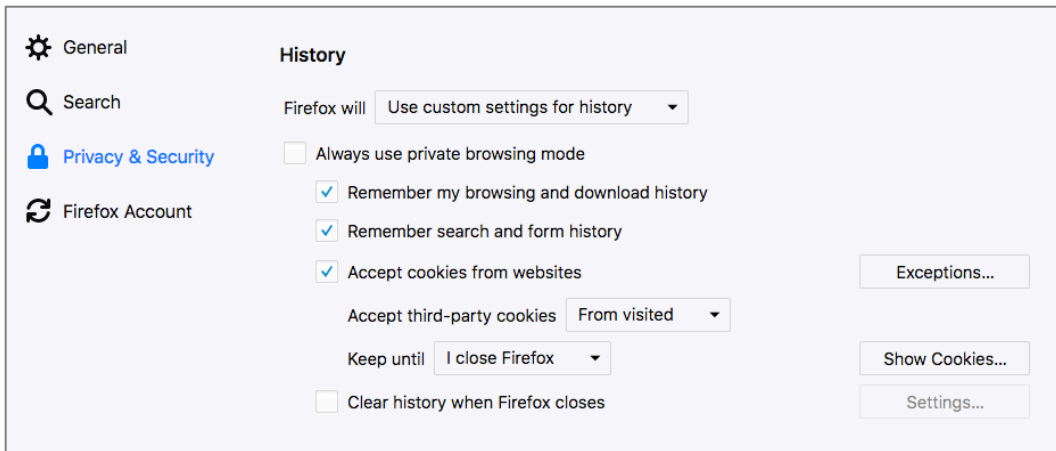
In this assignment, you secure Firefox.

1. Open Firefox, click the *Firefox menu* (three horizontal lines), and then select the *Preferences* button.
2. In the Preferences page, select *General* from the sidebar, and then scroll down to *Firefox Updates*. Set to *Automatically install updates*.

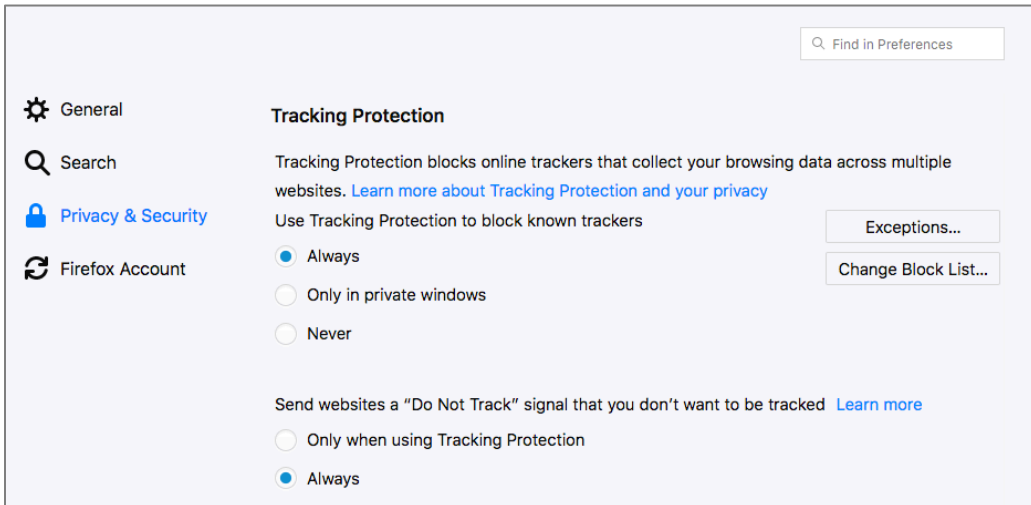


3. In the Preferences window, select on *Privacy & Security* in the left-hand pane, scroll down to *History*, and then select *Firefox will Use custom settings for history*. Configure to your taste, and here are my recommendations:

14 Web Browsing

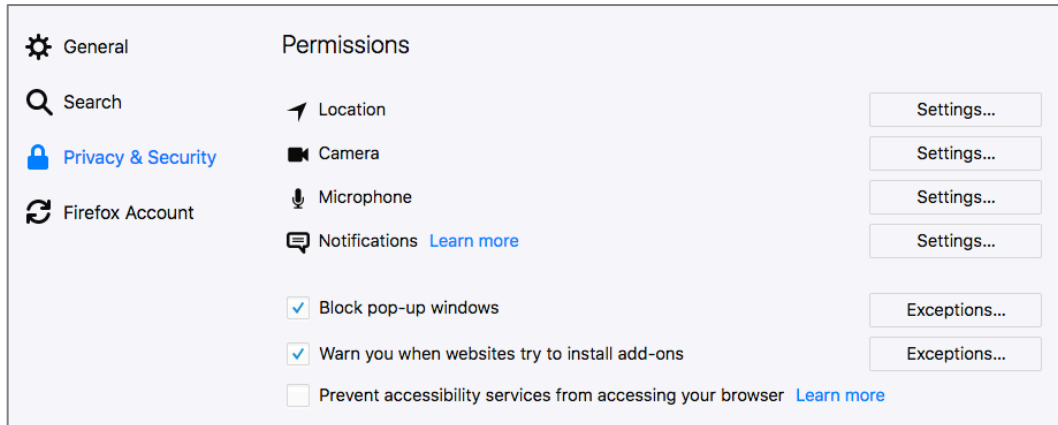


4. Scroll down to the *Tracking Protection* area, enable *Use Tracking Protection* to block known trackers *Always*.
5. Set *Send websites a “Do Not Track” signal* that you don’t want to be tracked to *Always*.



14 Web Browsing

6. Scroll down to *Permissions*. For *Location*, *Camera*, *Microphone*, and *Notifications*, select the *Settings* button. If there are sites listed to have access these services, remove them as desired.



7. Enable *Block pop-up windows* to prevent them.
8. Enable *Warn you when websites try to install add-ons*.
9. Scroll down to *Security*. Enable *Block dangerous and deceptive content*.
10. Enable *Block dangerous downloads*.
11. Enable *Warn you about unwanted and uncommon software*.
12. Close Firefox Preferences.

Congratulations. Your Firefox Browser is now secured from phishing attacks, third-party advertisers and known malware sites.

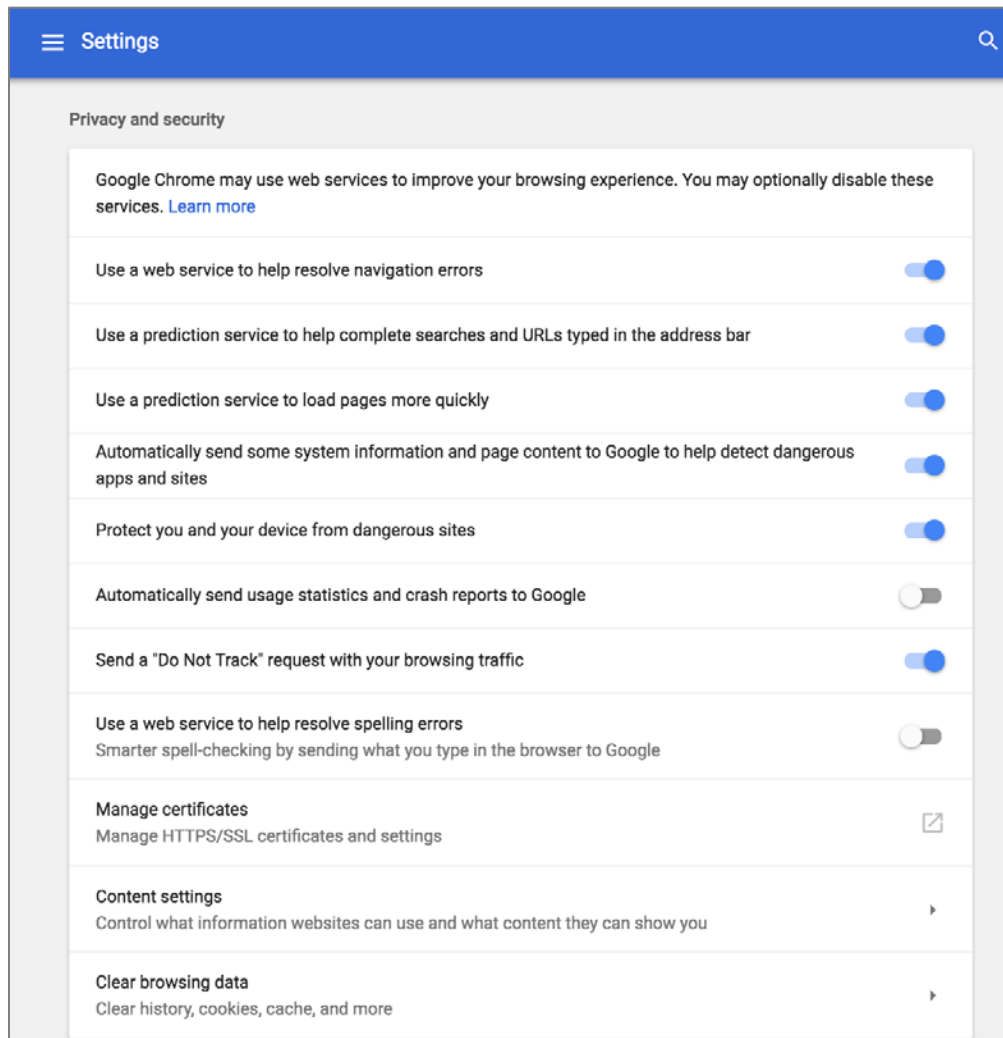
14.8.3 Assignment: Secure Chrome

Just as with Firefox, there are settings within Chrome that will keep you properly secured against the bad guys.

In this assignment, you secure Chrome

1. Open *Chrome*, select the menu item (3 dots), and then click *Settings*.
2. Click the 3 horizontal lines at the top left, select *Advanced*, and then select *Privacy & Security*. Recommended privacy and security settings are shown below:

14 Web Browsing



3. While you are here, have a look around and configure the rest of the *Privacy & Security* area.

Congratulations. Your Chrome Browser is now securing from phishing attacks, third-party advertisers and known malware sites.

14.8.4 Assignment: Install Ghostery For Safari

In this assignment, you install the Ghostery extension for Safari, monitor who is monitoring you, and then block them.

1. Open Safari.
2. Browse to *<https://ghostery.com>*.
3. Select the *Install Ghostery* button. A link will download.
4. In your Downloads folder, locate and then double-click the *Ghostery.safariextz*.
5. In the *Ghostery is from the Safari Extension Gallery* window, select *Visit Gallery*.
6. In the *Safari Extensions* web page, select *Install now*.
7. The *Ghostery Introduction* page will open. Read the information, and then click the *Next* buttons.
8. At the *Notification* page, enable *Click here to enable Alert Bubble*. This will briefly display the trackers at each page visited. Then select *Next*.

14 Web Browsing

- At the *Blocking* page, select which trackers you want blocked, and then select the *Next* button. My recommended settings are shown below:

Blocking

Ghostery can prevent the page elements it detects from running in your browser.

Blocking trackers will prevent them from running in your browser, which can help control how your behavioral data is tracked. Keep in mind that some trackers are potentially useful, such as social network feed widgets or browser-based games ... Blocking may have an unintended effect on the sites you visit.

Please [let us know](#) if you run into any issues.

Trackers that got blocked will be crossed out in the alert bubble and the findings panel.

Blocking **1761** out of **2080** trackers.

When you block a tracker, that tracker is prevented from communicating with its third-party provider.

Show all

Search for

A/B Testing 9 | Affiliate Marketing 47 | Analytics 116 | Audio / Music Player 4 | Behavior Tracking 48 | Commenting System 5 | Device Fingerprinting 4 | [Show more tags...](#)

Select all | Select none | Expand all | Collapse all

>	<input checked="" type="checkbox"/> Advertising	1000 trackers: blocking all
>	<input checked="" type="checkbox"/> Analytics	344 trackers: blocking all
>	<input checked="" type="checkbox"/> Beacons	417 trackers: blocking all
>	<input type="checkbox"/> Privacy	19 trackers: blocking none
>	<input type="checkbox"/> Widgets	300 trackers: blocking none

< Back

Next >

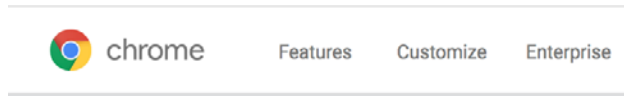
- When complete, click the *Next* button, and then close the Ghostery page.
- To test Ghostery, visit <https://slashdot.com>. Note the purple alerts that appear in the bottom right corner, and the new Ghostery icon in the toolbar.
- Click the Ghostery icon in the toolbar to learn more about Ghostery, and to configure preferences.

From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.

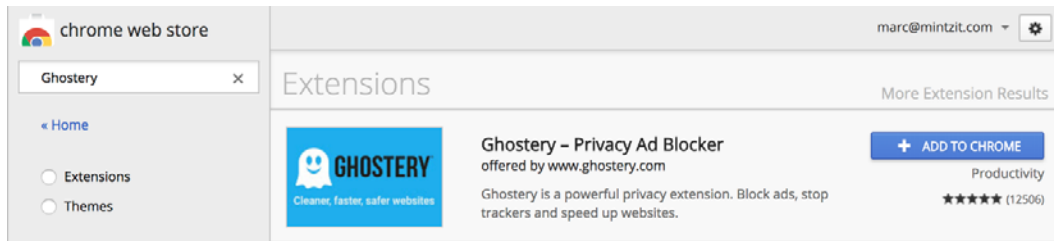
14.8.5 Assignment: Install Ghostery For Chrome

In this assignment, you install the Ghostery extension for Chrome, monitor who is monitoring you, and then block them.

1. Open Chrome.
2. Go to <https://chrome.google.com>.
3. Click *Customize* link at the top center of the window.



4. In the *Search the Store* field, enter *Ghostery*, and then tap the *Enter* or *Return* key. Extensions matching this search term will appear.

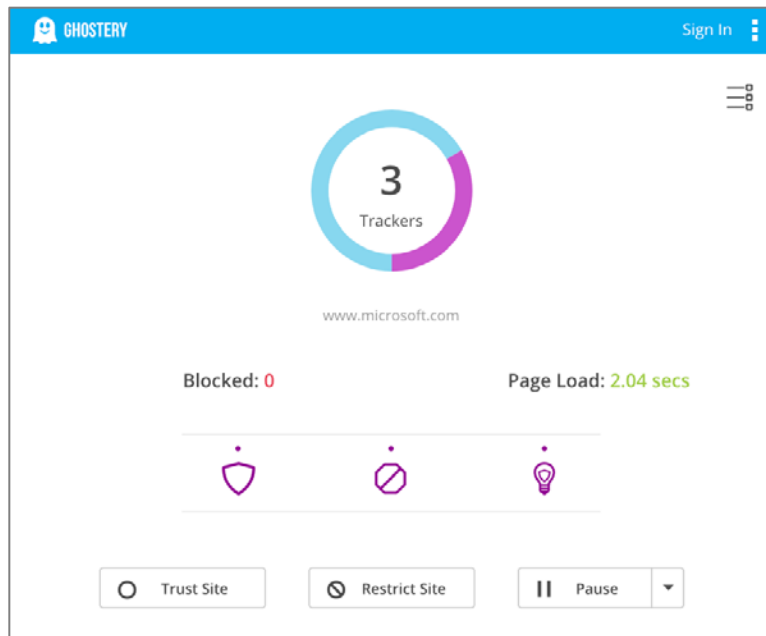


5. When Ghostery is found, click *ADD TO CHROME* button.
6. In the *Add "Ghostery"?* dialog, click *Add extension*.
7. Ghostery will display a few screens asking for your preferences. You may click the *One-Click Setup* button to automatically configure, or click *Custom Setup* to configure to your taste.
8. Notice that you now have the Ghostery icon in the Chrome Tool bar. In this example, it is notifying me that there are 3 trackers on the Ghostery page.



9. Click the Ghostery icon. This will display information about who is tracking you.

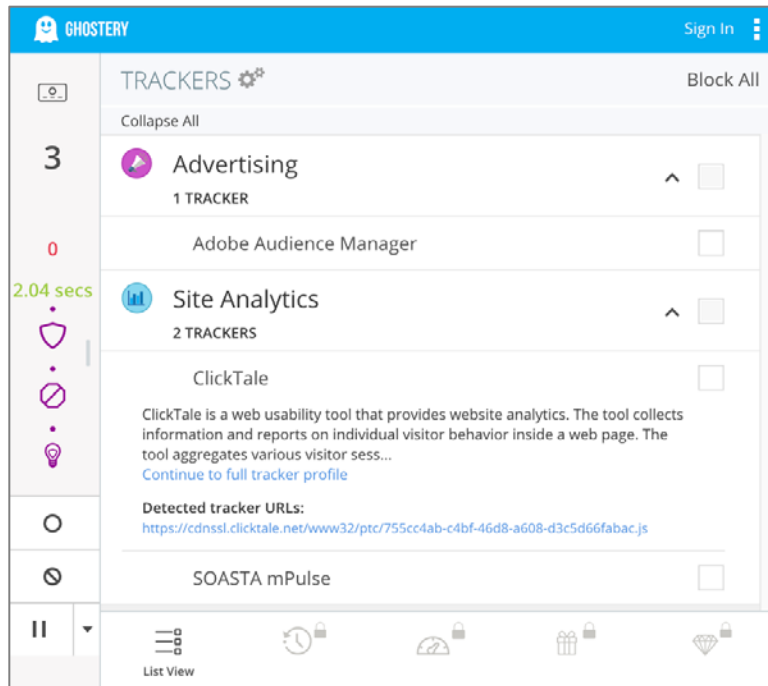
14 Web Browsing



10. Click the *Detail View* icon under the *Sign in* link to display more information.

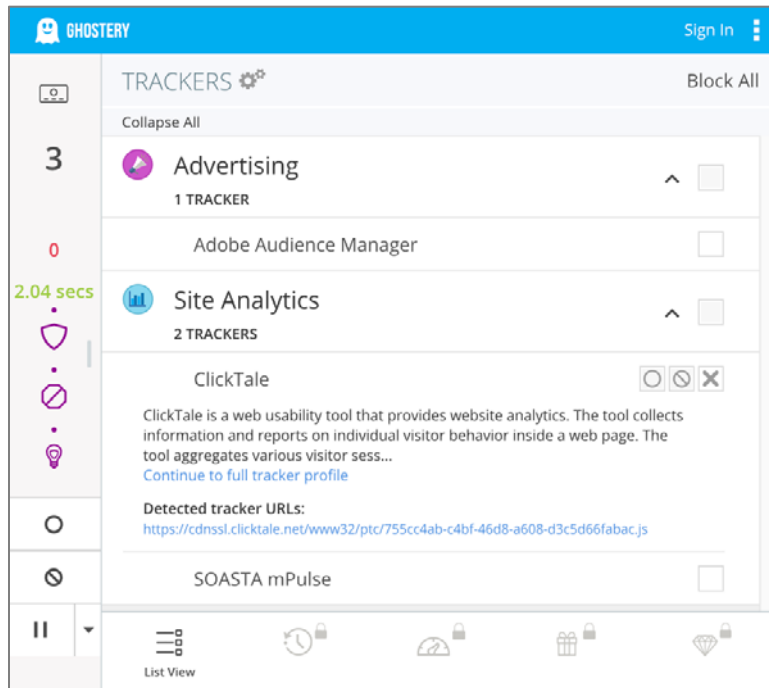
11. Click on one of the trackers to see details on it. In this example, *ClickTale*.

14 Web Browsing



12. Hover your cursor to the right of one of the tracker names (in this example, *ClickTale*), and you now have icons allowing you to *Trust on this site*, *Block on this site*, and *Block on all sites*.

14 Web Browsing



13. Click the 3-dot settings icon at the top right corner of the Ghostery window > *Settings*. Explore the options, and then configure to your taste.

14. Close Chrome.

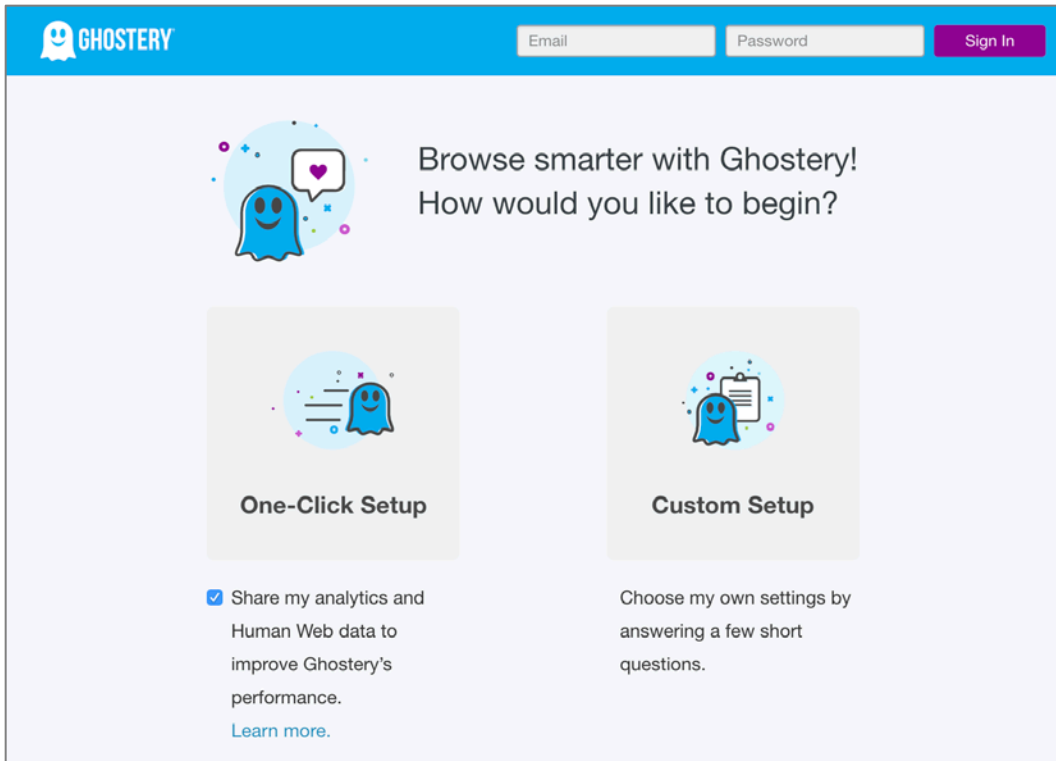
From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.

14.8.6 Assignment: Install Ghostery For Firefox

In this assignment, you install the Ghostery extension for Firefox, monitor who is monitoring you, and then block them.

1. Open Firefox.
2. Click the menu icon (three horizontal lines) > *Add-ons*.
3. From the sidebar, select *Extensions*.
4. In the *Search* field, enter *Ghostery*.
5. Select *Ghostery–Privacy Add Blocker*.

6. Click the *Add to Firefox* button.
7. At the *Add Ghostery Privacy Ad Blocker?* dialog box, click *Add*.
8. Ghostery will display a few screens asking for your preferences. You may click the *One-Click Setup* button to automatically configure, or click *Custom Setup* to configure to your taste.

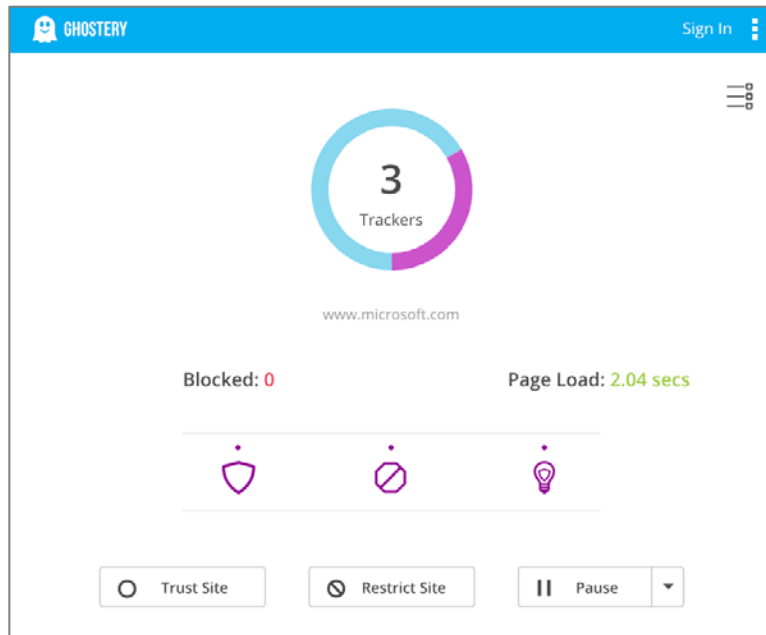


9. You may configure to your taste at this time, or do nothing. You can always configure later.
10. Notice that you now have the Ghostery icon in the Chrome Tool bar. In this example, it is notifying me that there are 3 trackers on the Ghostery page.



11. Click the Ghostery icon. This will display information about who is tracking you.

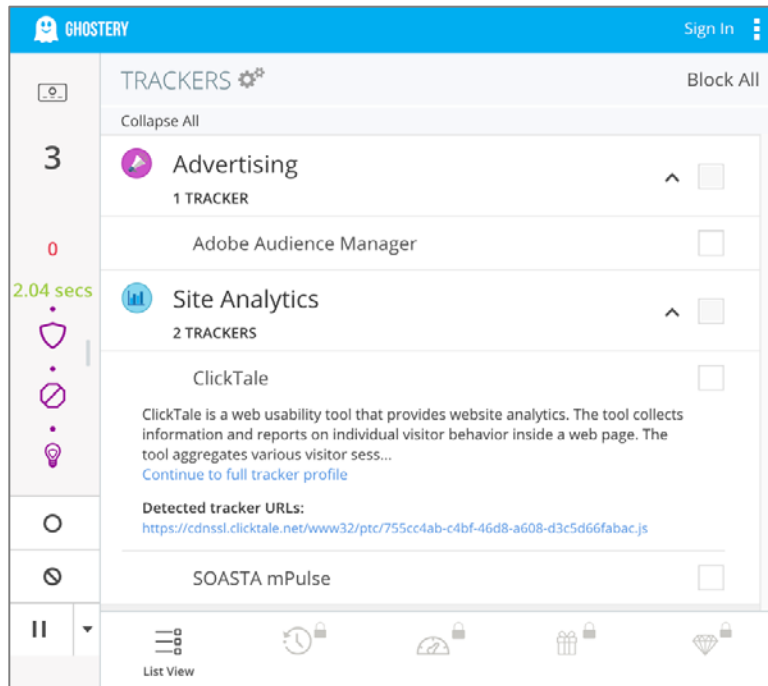
14 Web Browsing



12. Click the *Detail View* icon under the *Sign in* link to display more information.

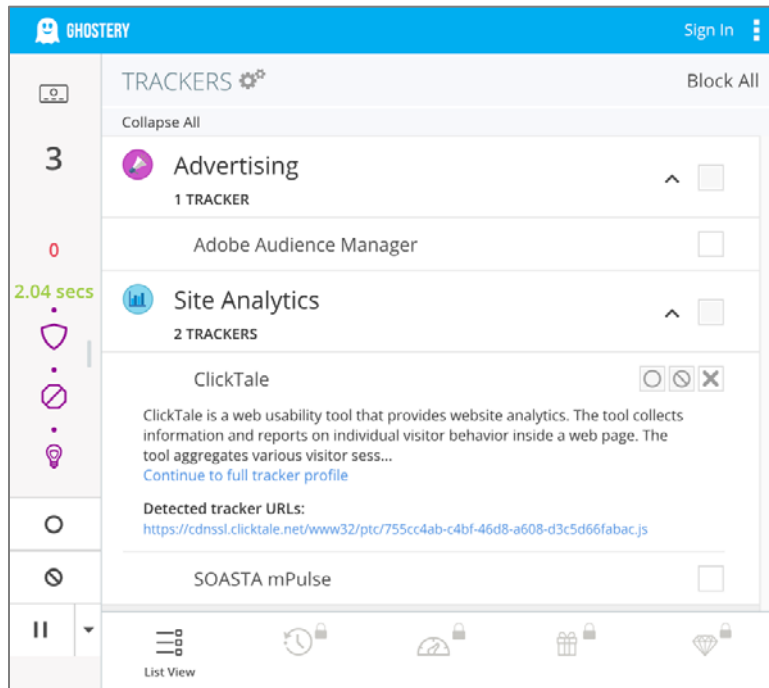
13. Click on one of the trackers to see details on it. In this example, *ClickTale*.

14 Web Browsing



14. Hover your cursor to the right of one of the tracker names (in this example, *ClickTale*), and you now have icons allowing you to *Trust on this site*, *Block on this site*, and *Block on all sites*.

14 Web Browsing



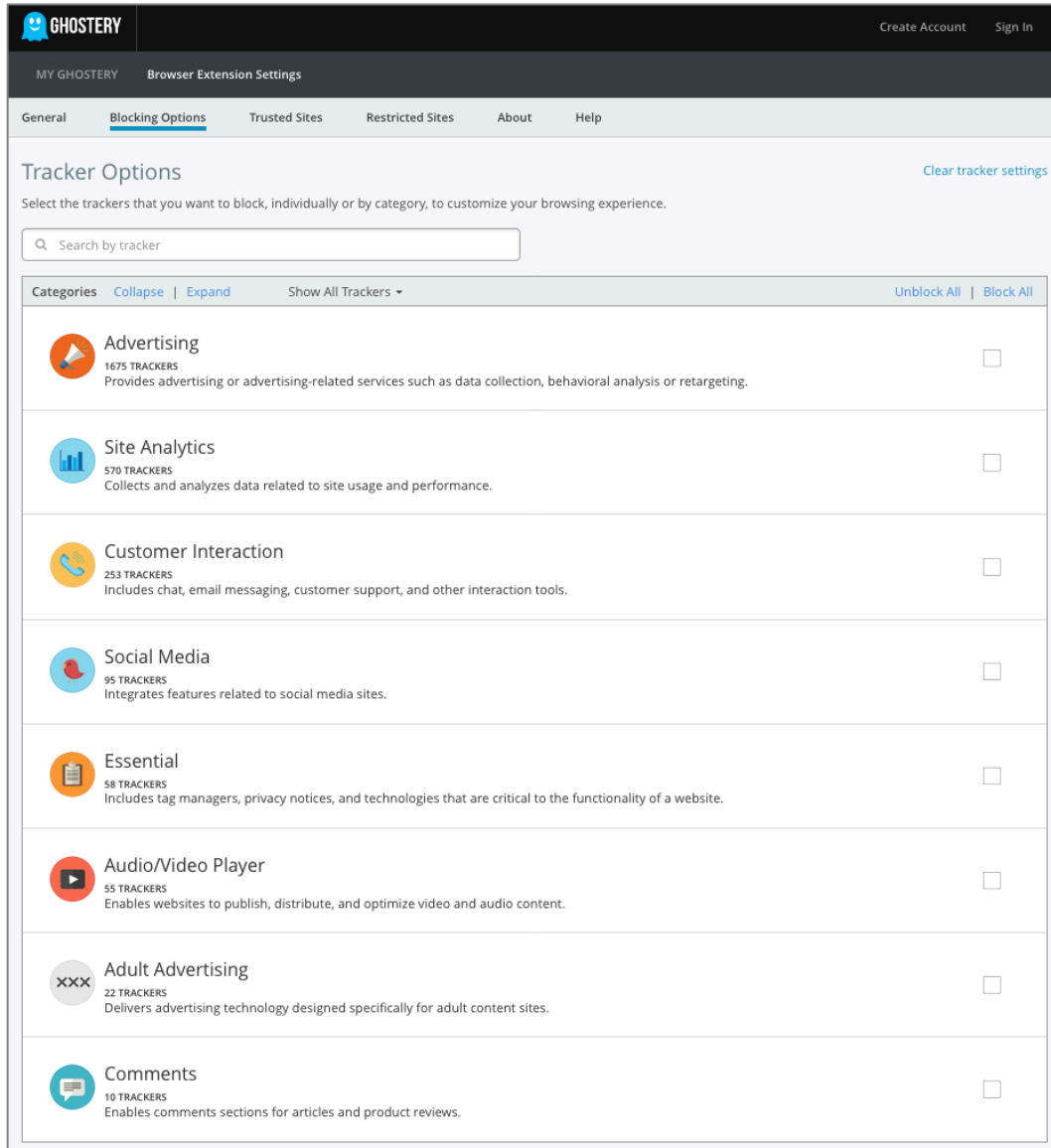
15. Click the 3-dot settings icon at the top right corner of the Ghostery window > *Settings*. Explore the options, and then configure to your taste.

16. Close Firefox.

From now on when visiting sites, you can see who is tracking you, and choose to allow or block this from happening.









14 Web Browsing

17. At the *Tracker Options* page, select the trackers to be blocked.



The screenshot shows the Ghostery browser extension settings page, specifically the "Tracker Options" section. The page has a dark header with the Ghostery logo and navigation links. Below the header, there's a sub-header "MY GHOSTERY" and "Browser Extension Settings". The main navigation bar includes "General", "Blocking Options" (which is active), "Trusted Sites", "Restricted Sites", "About", and "Help".

The "Tracker Options" section has a title and a "Clear tracker settings" link. Below the title is a search bar labeled "Search by tracker". A table-like structure lists various tracker categories, each with an icon, a title, a count of trackers, a description, and a checkbox for blocking.

Categories	Collapse	Expand	Show All Trackers	Unblock All	Block All
 Advertising 1675 TRACKERS Provides advertising or advertising-related services such as data collection, behavioral analysis or retargeting.					<input type="checkbox"/>
 Site Analytics 570 TRACKERS Collects and analyzes data related to site usage and performance.					<input type="checkbox"/>
 Customer Interaction 253 TRACKERS Includes chat, email messaging, customer support, and other interaction tools.					<input type="checkbox"/>
 Social Media 95 TRACKERS Integrates features related to social media sites.					<input type="checkbox"/>
 Essential 58 TRACKERS Includes tag managers, privacy notices, and technologies that are critical to the functionality of a website.					<input type="checkbox"/>
 Audio/Video Player 55 TRACKERS Enables websites to publish, distribute, and optimize video and audio content.					<input type="checkbox"/>
 Adult Advertising 22 TRACKERS Delivers advertising technology designed specifically for adult content sites.					<input type="checkbox"/>
 Comments 10 TRACKERS Enables comments sections for articles and product reviews.					<input type="checkbox"/>

14 Web Browsing

18. Select the *General* tab, and then configure to your taste.

The screenshot shows the Ghostery Browser Extension Settings page. The top navigation bar includes the Ghostery logo, 'MY GHOSTERY', and 'Browser Extension Settings'. On the right, there are links for 'Create Account' and 'Sign In'. Below the navigation bar, the 'General' tab is selected, with other tabs like 'Blocking Options', 'Trusted Sites', 'Restricted Sites', 'About', and 'Help' visible. The main content area is divided into several sections: 'Trackers' with checkboxes for 'Enable automatic updates from the Ghostery tracker library' and 'Show tracker URL patterns'; 'Highlight Interactive Trackers' with checkboxes for 'Show me when I need to allow a tracker to use a site's features' and 'Replace blocked social media buttons with a Ghostery icon'; 'Blocking' with checkboxes for 'Trust and restrict individual trackers', 'Allow trackers created by site owners', and 'Block new trackers added to Ghostery by default'; 'Purple Box' with a checkbox for 'Show the purple box in the corner of my browser', dropdowns for 'Dismiss After' (15 Seconds) and 'Display In' (Bottom Right Corner), and a checkbox for 'Hide the purple box on trusted websites'; 'Notifications' with a checkbox for 'Notify me when Ghostery:' and several sub-options; and 'Support Ghostery' with checkboxes for 'Sharing page and tracker data', 'Sharing extension usage analytics', and 'Sharing Human Web data'.

GHOSTERY Create Account Sign In

MY GHOSTERY Browser Extension Settings

General Blocking Options Trusted Sites Restricted Sites About Help

Trackers

- ☒ Enable automatic updates from the Ghostery tracker library
Auto-updates are highly recommended. [Update now.](#)
- ☒ Show tracker URL patterns ?

Highlight Interactive Trackers ?

- ☒ Show me when I need to allow a tracker to use a site's features
- ☒ Replace blocked social media buttons with a Ghostery icon

Blocking

- ☒ Trust and restrict individual trackers ?
- ☒ Allow trackers created by site owners
(For example, blocking a Facebook tracker on facebook.com might break the site. Turning this feature off might result in some pages breaking.)
- ☐ Block new trackers added to Ghostery by default

Purple Box

- ☒ Show the purple box in the corner of my browser ?
 - Dismiss After: 15 Seconds
 - Display In: Bottom Right Corner
- ☐ Hide the purple box on trusted websites

Notifications ?

Notify me when Ghostery: ?

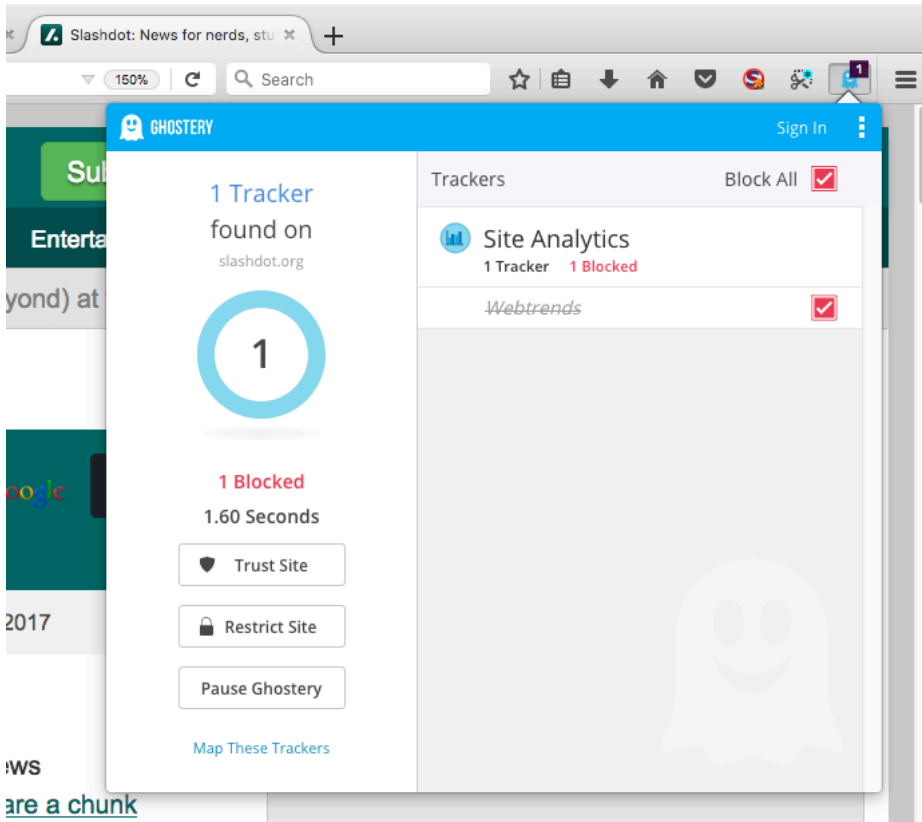
- ☒ Makes announcements
- ☒ Releases new features
- ☐ Releases minor defect fixes
- ☐ Adds new trackers to its tracker library
- ☒ Show page reload banner notifications at the top of the extension
- ☒ Show tracker alert banner notifications at the top of the extension
- ☒ Show tracker count badge on the Ghostery icon in browser toolbar

Support Ghostery

- ☒ Sharing page and tracker data
Ghostery is free because some of our users anonymously and voluntarily opt-in to share data with us about the sites and trackers the browser encounters.
- ☒ Sharing extension usage analytics
We collect usage analytics to better understand what features users like. For example , if you click pause, we will collect a ping letting us know you used that feature.
- ☒ Sharing Human Web data
Ghostery now implements the Human Web by default, a revolutionary technology that uses the wisdom of the crowd to build a more private internet

19. Close the *Ghostery* page.

20. To test, visit <https://slashdot.com>.
21. Select the *Ghostery* icon in the toolbar. The Ghostery window will open, displaying any trackers on this page, and if they were blocked.



22. Close Firefox.

14.8.7 Assignment: View Your Device Fingerprint

Each device on the internet is unique based on its combination of features, traits, fonts, settings, etc. This can be used to identify the device, and then to track it across the internet. This is called a *device fingerprint*¹⁰.

¹⁰ https://en.wikipedia.org/wiki/Device_fingerprint

14 Web Browsing

In this assignment, you view your device fingerprint.

1. Open a browser, and then go to <https://amiunique.org>. You are taken to the site home page.
2. From the sidebar, select *My Fingerprint*. In a minute or two a summary of your unique fingerprint will be displayed.

The screenshot shows the 'Am I Unique?' website interface. On the left is a dark sidebar with a teal header 'Am I Unique?'. The sidebar contains links: Home, My fingerprint (highlighted in teal), My history, My timeline (with a 'New' badge), Global statistics, FAQ, Privacy policy, Privacy tools, Links (with an 'Updated' badge), About, and View on GitHub. The main content area has a teal header with 'Am I Unique?' and tabs for Overview, Details, and Graphs. The 'Overview' tab is active, displaying the title 'Are you unique?' and a large red heading 'Yes! (You can be tracked!)'. Below this, several statistics are listed: 39.97% of observed browsers are Chrome, as yours; 0.54% of observed browsers are Chrome 66.0, as yours; 13.27% of observed browsers run Mac, as yours; 1.74% of observed browsers run Mac 10.13, as yours; 62.57% of observed browsers have set 'en' as their primary language, as yours; and 2.33% of observed browsers have UTC-6 as their timezone, as yours. A note states: 'However, your full fingerprint is unique among the 699543 collected so far. Want to know why?' with a 'Click here' button. At the bottom are two buttons: 'View more details' and 'View graphs'.

Am I Unique?

Home

My fingerprint

My history

My timeline **New**

Global statistics

FAQ

Privacy policy

Privacy tools

Links **Updated**

About

View on GitHub

Overview Details Graphs

Are you unique?

Yes! (You can be tracked!)

39.97 % of observed browsers are **Chrome**, as yours.

0.54 % of observed browsers are **Chrome 66.0**, as yours.

13.27 % of observed browsers run **Mac**, as yours.

1.74 % of observed browsers run **Mac 10.13**, as yours.

62.57 % of observed browsers have set "en" as their primary language, as yours.

2.33 % of observed browsers have **UTC-6** as their timezone, as yours.

However, your full fingerprint is unique among the 699543 collected so far. Want to know why?

[Click here](#)

[View more details](#) [View graphs](#)

3. Select the *View more details* button to see all of your fingerprint attributes.

4. Open a new browser window, and then go to <https://panopticlick.eff.org>. This site is similar in function to amiunique.org, and provide some unique information.



5. Enable the *Test with a real tracking company* checkbox.

14 Web Browsing

6. Select the *Test Me* button. After a few minutes, a results summary will appear.

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

Help us defend the Web against tracking:

Twitter Facebook Google+ Email

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your blocker stop trackers that are included in the so-called "acceptable ads" whitelist?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track ?	✗ no
Does your browser protect from fingerprinting ?	✗ your browser has a nearly-unique fingerprint

[Show full results for fingerprinting](#)

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticon does not measure all forms of tracking and protection.

RE-TEST YOUR BROWSER

Thanks to [Fingerprint2](#) for various fingerprinting tests, [Aloodo](#) for portions of the tracker test, [browserspy.dk](#) for the font detection code, and to [breadcrumbs](#) for supercookie help. Send questions or comments to panopticon@eff.org.

7. Select *Show full results for fingerprinting* to display to view all of your fingerprint details.

14.9 Adobe Flash And Java

Both Adobe Flash and Oracle Java are used by many websites to create a more animated or interactive web experience. Flash is no longer supported as a standalone System Preference and should be removed. Its functions are now built into the major web browsers, but will be removed when Adobe discontinues Flash support in 2020. The functions of both will soon be absorbed by HTML 5.

The power these products offer is a double-edged sword. They can also be used to take control of your computer. And often are. There is a vicious cat and mouse game played by hackers who have discovered how to bend Flash and Java to their wills, and Adobe and Oracle patching these vulnerabilities.

The result for users is they have a choice to make:

- Do not install Java, which renders some sites unusable.
- Install Java, and be vigilant with updates.
- Install Java, but don't be vigilant with updates, rendering your system vulnerable

I suspect if you are one who ops for the last option, you aren't taking this course.

Either of the other two options are legitimate strategies. Oracle has tried to make updates automatic, but we have found this process to be less than perfect. Many times, we have found systems with out of date versions, even with their preference settings on *Automatic Updates*.

Associated with the vulnerabilities caused by out of date Java, are malicious or compromised web pages that prompt the visitor to update Flash, Java, or some audio/video codec. In most cases, if you follow the links provided on the site all that gets downloaded is malware.

If a site prompts you do install software, visit the website of the recommended software and download from there, not from the requesting site.

14.9.1 Assignment: Configure Oracle Java for Automatic Updates

In this assignment, you install Java and configure it to automatically update.

Install Oracle Java

1. Open *Apple* menu > *System Preferences*. If you see the Java icon, it is already installed. If so, skip to the next section *Configure Java for Auto-Updates*.
2. Open your browser to surf to *http://www.java.com/*.
3. Click the *Free Java Download* button.
4. Click the *Agree and Start Free Download* button.
5. Once the Java installer has downloaded, launch it, and then follow the on-screen instructions to complete installation.
6. When installation completes, restart your computer.

Configure Java For Auto-Updates

7. Select *System Preferences* > *Java*.
8. Select the *Update* tab, and then enable the *Check for Updates Automatically* checkbox.

At this point, both your Flash and Java are up to date, and configured to automatically update. However, there is a decent chance that they will not do so. It is wise to perform a manual update check at least monthly.

Manually Check For Java Updates

9. Open *System Preferences* > *Java*.
10. Select the *Update* tab.
11. If updates are available, select the *Update Now* button, and then follow the on-screen instructions to download and install.

14.10 Web Scams

Over the past couple of years, a new type of scam has become popular. Instead of directly compromising the user computer, web sites are either compromised, or are deliberately designed to be malicious.

When a user visits such a site, they may receive a pop-up window stating something to the effect of: *Your computer has been found to be infected with XX viruses. Please call Apple at XXX-XXX-XXXX to have this infection removed.*

Upon calling the provided toll-free phone number (which, of course, is not Apple, but that of the scammer), with your permission, they will install remote control software. After looking around your computer, they will assure they can remove the malware for only \$\$\$.

There are two problems here. First, they have installed remote control software that allows the criminal access any time they wish. This gives them access to your usernames, passwords, banking, and other information. The second is that they now have your credit card information.

14.10.1 Recovering From A Web Scam

What to do if this happens to you?

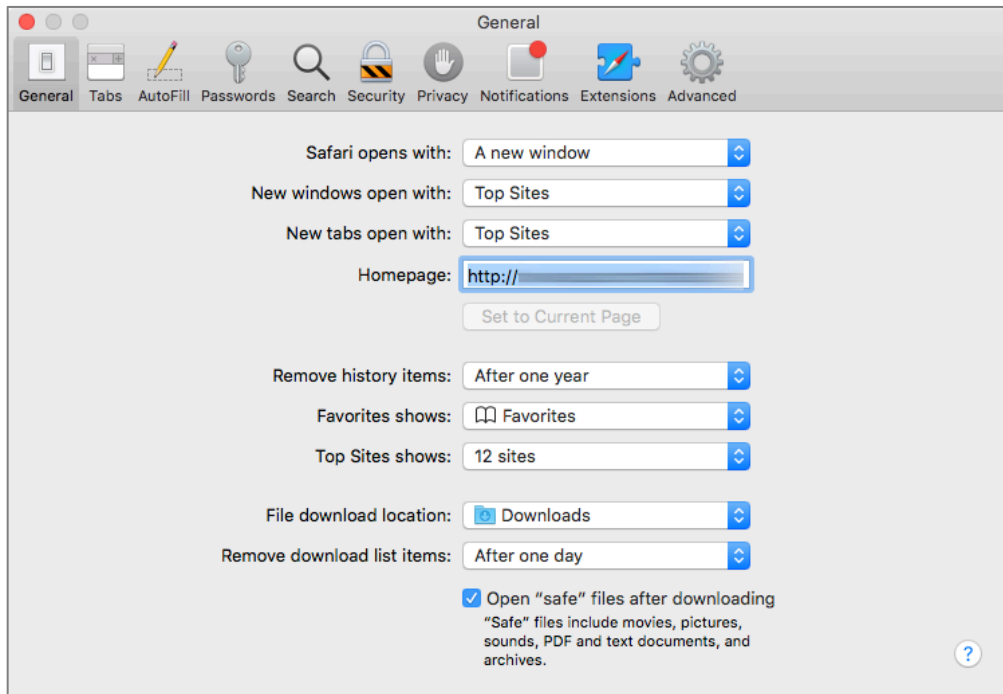
In this assignment, you examine Safari for possible modifications.

1. Don't call!

In most cases, the malicious website has modified your web browser preferences to make the malicious page your home page.

14 Web Browsing

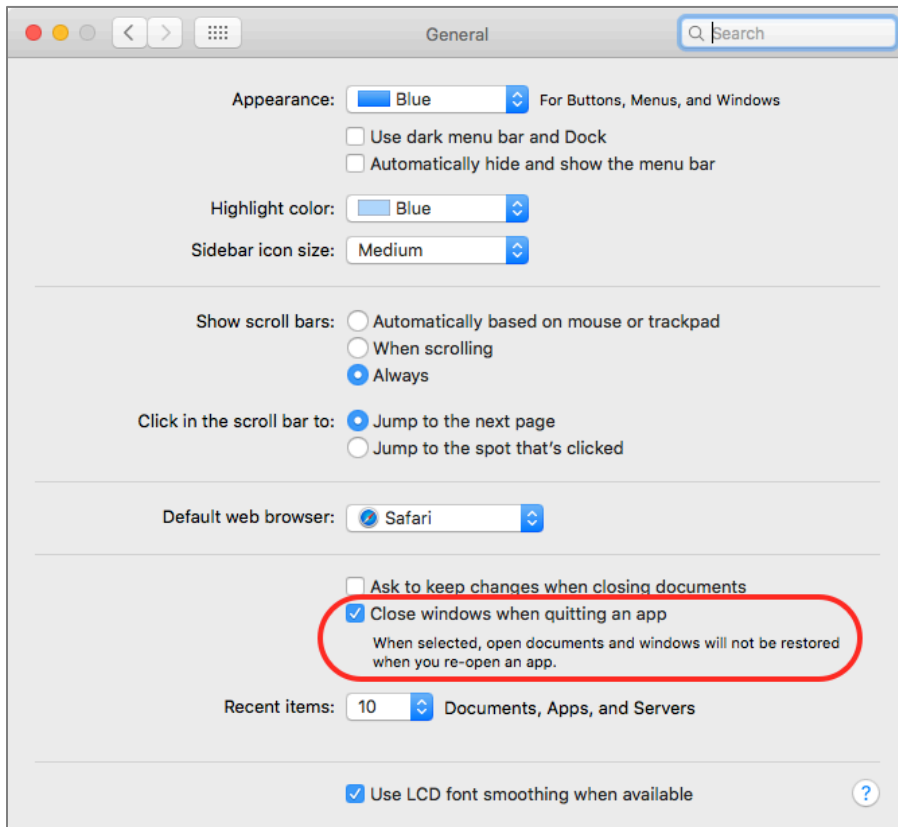
2. Open your browser *preferences* (in this example, Safari) > *General*. If the *Homepage* field is not what you have set, delete the entry.



3. Malicious attacks on a browser often will block access to the browser preferences. If you are not able to access your browser preferences to delete

14 Web Browsing

the homepage setting, open *System Preferences > General*, and then enable *Close windows when quitting an app*.



4. Quit Safari.
5. Open Safari to test. You should no longer have the malicious page open.
Done!

14.11 Tor

Tor¹¹ is a technology developed by the US Department of the Navy that enables anonymous web browsing. It has long since been released to the open source community for the public to use in the form of the *Tor Browser*. Many people within the security community are strong supporters of Tor, including Edward Snowden. Entire books have been written on just Tor. I'm not so sadistic as to subject you to that. What we are going to do is cut to the core of Tor, and learn the basics of how to surf the web anonymously.

The advantages of Tor include:

- Strong anonymity for all activity on the Internet.
- Can be used with Tails¹² which is a bootable, self-contained, flash drive that can run on most Windows, Linux, and Apple computers that leaves no trace behind.
- The bootable Tails flash drive can be immediately disconnected from the host computer, causing the computer to erase memory of all trace of your session, and reboot.

The disadvantages of Tor include:

- It was developed by the US Department of the Navy. It is possible there are back doors only the government knows about.
- The US government has been forthright about having its own Tor relays in place, which enable it to monitor online activity. Not a big deal if you only wish to be anonymous to criminals. It is a big deal if you wish to be anonymous while performing black-market deals for my Aunt Rose's raisin Noodle Koogel recipe.

These features make Tor ideal for those in oppressed countries, journalists working undercover, and anyone who may need to use someone else's computer and leave no trace behind.

¹¹ [http://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](http://en.wikipedia.org/wiki/Tor_(anonymity_network))

¹² <https://tails.boum.org>

Tor works by encrypting your packets as they leave your computer, routing the packets to a Tor relay computer hosted by thousands of volunteers on their own systems, many of which are co-located at ISPs. The relay knows where the packet came from, and the next relay the packet is handed to, but that is all. The user computer automatically configures encrypted connections through the relays. Packets will pass through several relays before being delivered to the intended destination. Tor will use the same relays for around 10 minutes, and then different relays will be randomly selected to create the next path for 10 minutes.

Alas, there is no free lunch. The encryption process and the relay process combine to create *latency*, which means a delay in processing. Most users will experience around a four-fold performance degradation. So, if accessing a web page without Tor normally takes 3 seconds, it may take 12 seconds with Tor.

Even though Tor does as good a job as anything to keep you anonymous on the Internet, you must take precautions to protect your identity. These steps include:

- Don't enable JavaScript when using Tor. This has been used to track users within the Tor network.
- Don't reveal your name or other personal information in web forms.
- Don't customize the Tails boot flash drive. This will create a unique digital fingerprint that can be used to identify you.
- Connect to sites that use HTTPS so your communications are encrypted point to point.

For many security-conscious users, Tor becomes their only tool for defense. However, Tor by itself is at best a partial solution. It can protect your anonymity while surfing the web. At the very least, this still leaves email and messaging to be secured. A bigger issue is what to do when you need to use a computer and leave no trace behind on that system. This is where *Tails* comes into play.

Tails is a Linux Debian fork designed with two primary purposes in mind:

- Provide a highly secure operating system in a format that can be booted from either DVD or thumb drive on almost any PC or Apple computer, and
- Include the tools and applications necessary to provide a secure, anonymous Internet experience

What this means is that you can create a thumb drive that has an operating system capable of booting almost any computer, whereby you can then run Tor for secure anonymous Internet activity, send and receive email that is securely encrypted with GPG/PGP, and message with others in complete privacy. Then, when you remove the Tails thumb drive, there is absolutely no record of your activity on either the computer *or* the thumb drive!

For those of you chomping at the bit to just use Tor, we will start there. When your curiosity has been satisfied, please take the next step to learn Tails¹³.

14.11.1 Assignment: Install Tor For Anonymous Internet Browsing

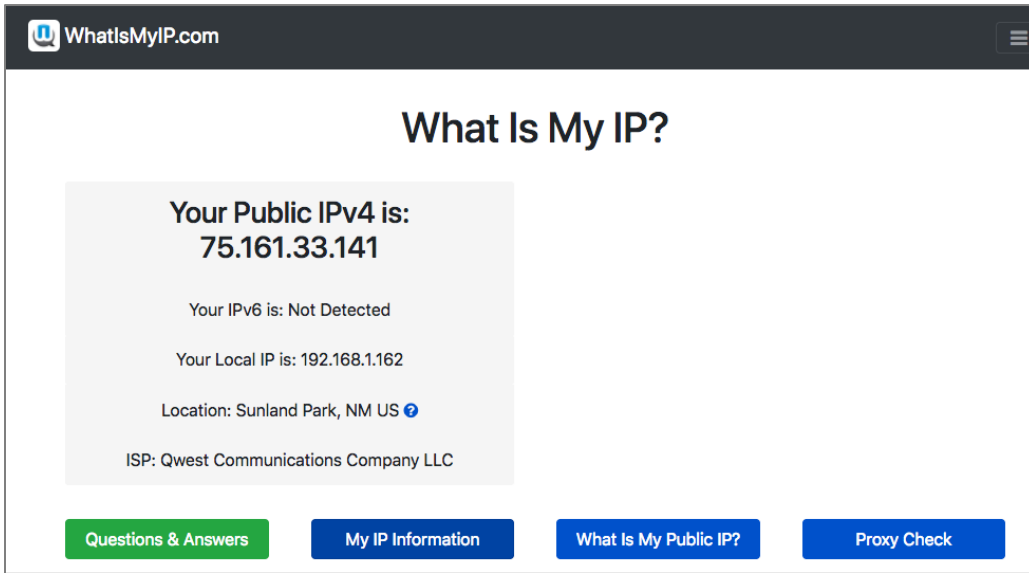
Tor is a stripped down, simplified web browser, designed to provide an encrypted, anonymous browsing experience.

In this assignment, you download and install Tor.

¹³ <https://tails.boum.org>

14 Web Browsing

1. As a first step, we need to know our public IP address. This information will be used a few steps away to verify Tor has hidden our address. Open a web browser to <https://whatismyip.com>. Write down *Your IP*.



2. Open a web browser and then go to <https://www.torproject.org>. Select the *Download Tor* button.

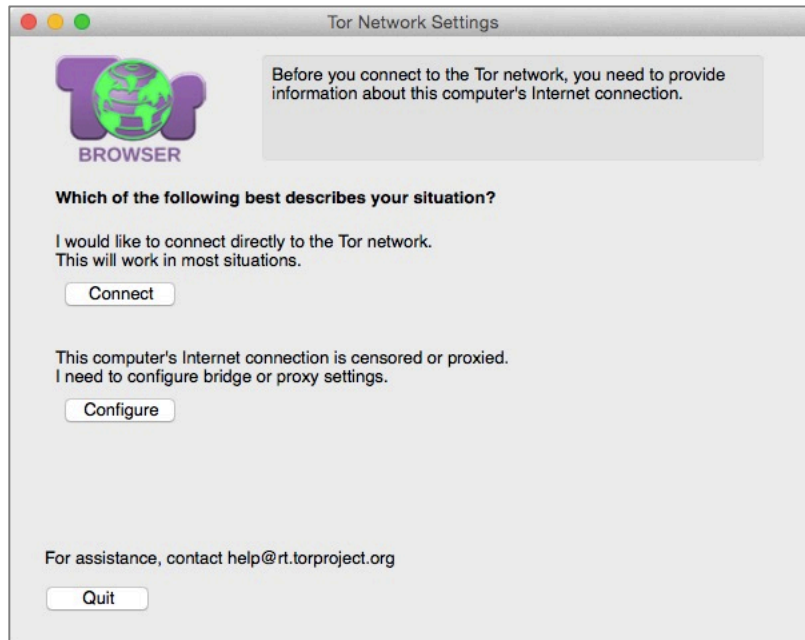


3. Select the *Download Tor Browser* button. The Tor installer will begin to download.
4. While the download is in progress, scroll down the page to read all the other steps that one must take to ensure your privacy is maintained. These include:

- **Use the Tor Browser.** If you are concerned about protecting your privacy and security, do not use other browsers.
- **Don't torrent over Tor.** If you wish to file-share via torrent, don't use Tor. It is painfully slow, it slows down others using the Tor network, and in many cases, torrent software bypasses all the security and anonymity precautions built into Tor.
- **Don't enable or install browser plugins in Tor.** Tor is designed to protect your security and anonymity. Many innocuous-looking plugins break that security.
- **Use HTTPS versions of websites.** Tor has *HTTPS Everywhere* built in (more on HTTPS Everywhere later in this book.) It will force a secure connection if a website has an option for https. This will enable a point-to-point encryption between your computer and the web server.
- **Don't open documents downloaded through Tor while online.** Many documents—particularly .doc, .xls, .ppt, and .pdf—contain links or resources that will force a download when the document is opened. If they are opened while Tor is open, they will reveal your true IP address and you will lose your anonymity and security. If you are concerned about these issues, we strongly recommend that you instead:
 - **Open the documents on a computer fully disconnected from the Internet.** This prevents any malicious files from “phoning home” or infecting your computer.
 - **Install a Virtual Machine (VM) such as Parallels, Fusion, or VirtualBox, configured with no network connection, and open documents within the VM.** This is an alternate way to prevent malicious files from phoning home or infecting your computer.
 - **Or use Tor while within Tails.** This is an alternative way to prevent malicious files from phoning home or infecting your computer.
- **Use bridges and/or find company.** Tor cannot prevent someone from looking at your Internet traffic to discover you are using Tor. If this is a concern for you, reduce the risk by configuring Tor to use a *Tor Bridge relay* instead of a direct connection to the Tor network. Another option is

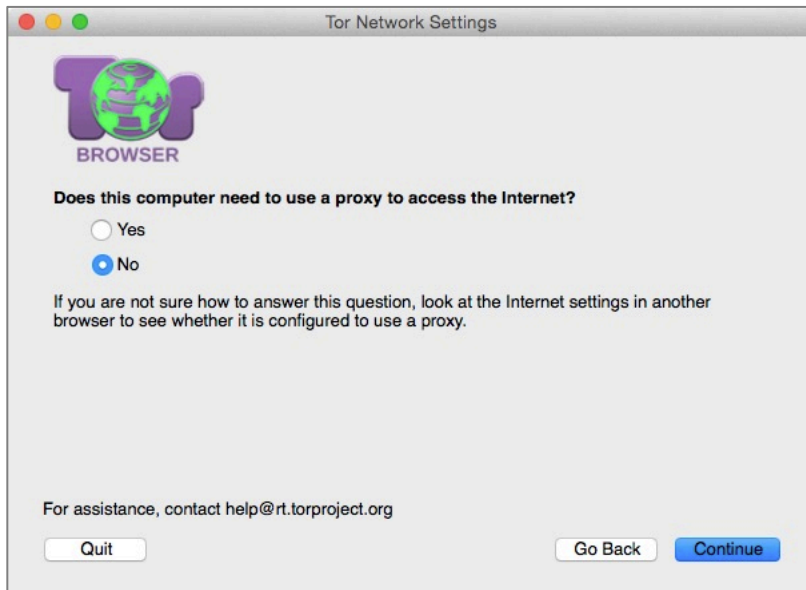
to have many other users running Tor on the same network. In this way, your use of Tor is hidden.

5. Locate the Tor installer, and then double-click to open. It will mount and open a disk image onto the Desktop.
6. Drag the *TorBrowser.app* into your *Applications* folder.
7. Locate the *TorBrowser* in your Applications folder, and then double-click to open it. The *Tor Network Settings* window appears. Select how you would like to connect to the Tor Network
 - *I would like to connect directly to the Tor network.* This will work in most situations. This option provides a faster Internet experience with no additional configuration. The possible downside is that a network administrator or your ISP can see that you are using the Tor Network.
 - *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings.* This option provides a more secure and anonymous Internet experience as a network administrator or ISP is unable to see you using the Tor Network. The downside is a slower Internet experience, and some additional configuration.



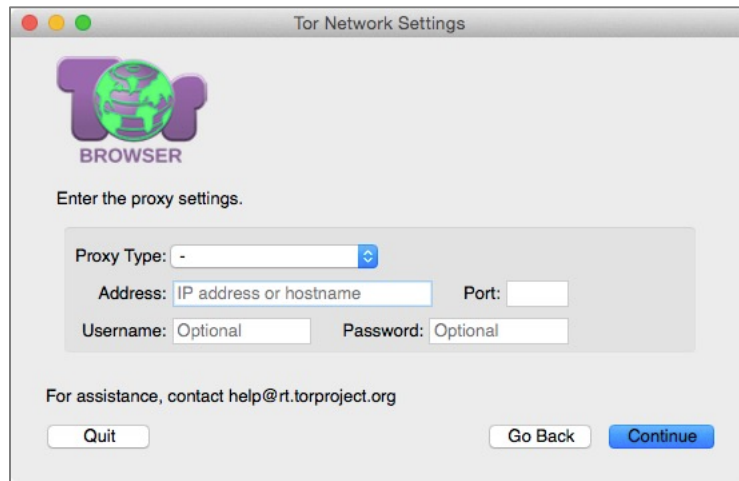
14 Web Browsing

8. If you selected *This computer's Internet connection is censored or proxied. I need to configure bridge or proxy settings*, go to the next step. If you selected *I would like to connect directly to the Tor network*, skip to step 14.
9. If you elected to use a *Tor bridge relay*, the following window appears. If your network requires a proxy to access the Internet, go to the next step and select *Continue*. Otherwise, select *No*, select the *Continue* button, and skip to step 12.



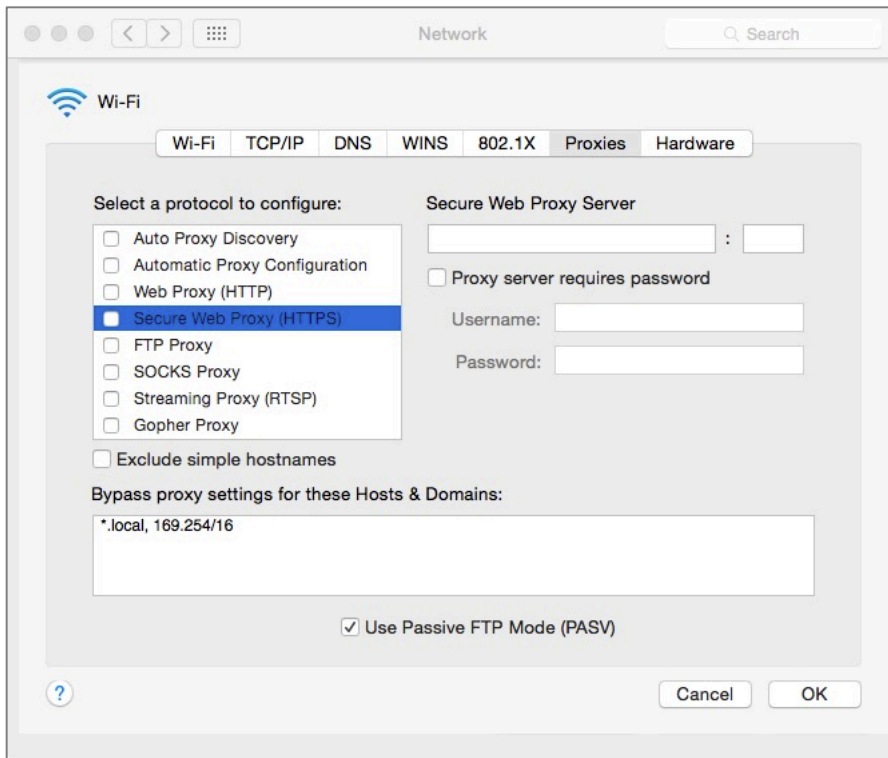
10. If you selected *Yes* to *Does this computer need to use a proxy to access the Internet* you will now see the Enter the Proxy settings window.

14 Web Browsing



11. These will be the same settings your computer requires normally, and if used, will be found in *System Preferences > Network > Advanced > Proxies* tab. Copy your settings from this pane into the Tor window, and then select the *Continue* button. If your ISP blocks or otherwise censor's connections to the Tor network, go to the next step to create a Tor bridge relay. If they do not, skip to step 14 to start using Tor.

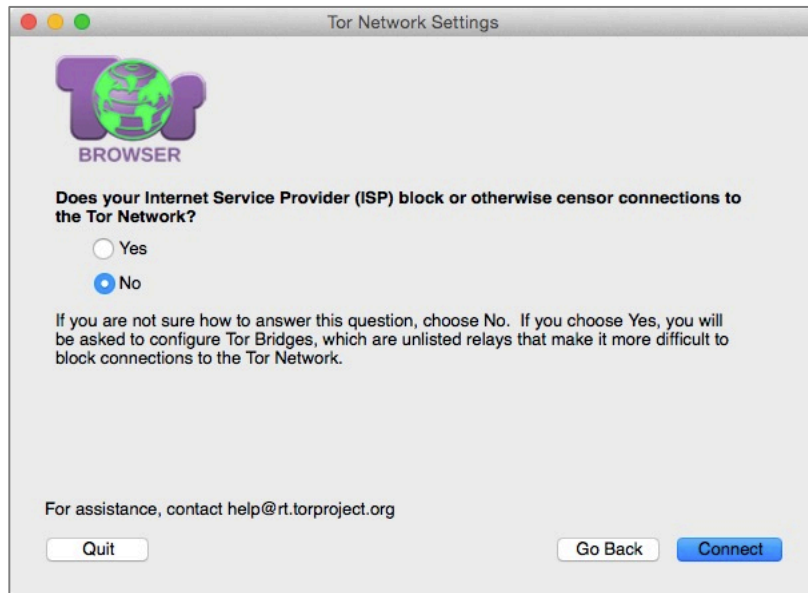
14 Web Browsing



12. At the *Does your Internet Service Provider (ISP) block or otherwise censor connections to the Tor Network* window, for the overwhelming majority of users the answer is *No*, and then select the *Connect* button, and then skip to

14 Web Browsing

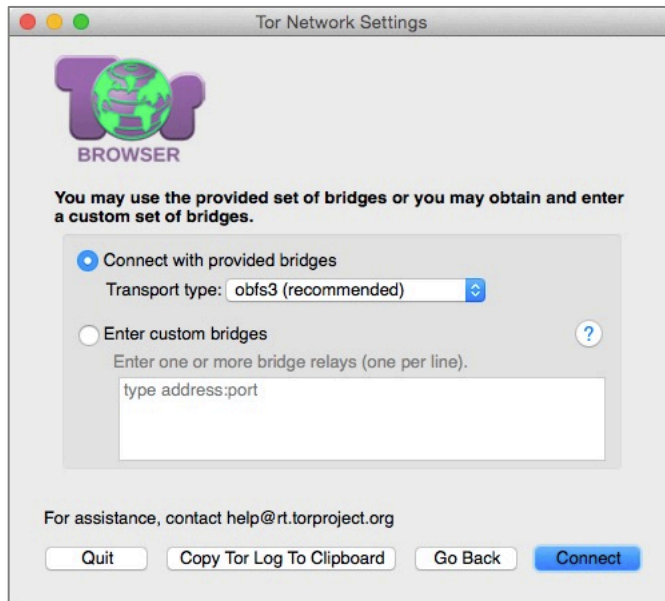
step 14. If your answer is *Yes*, select the *Yes* option, select the *Continue* button, and go to the next step.



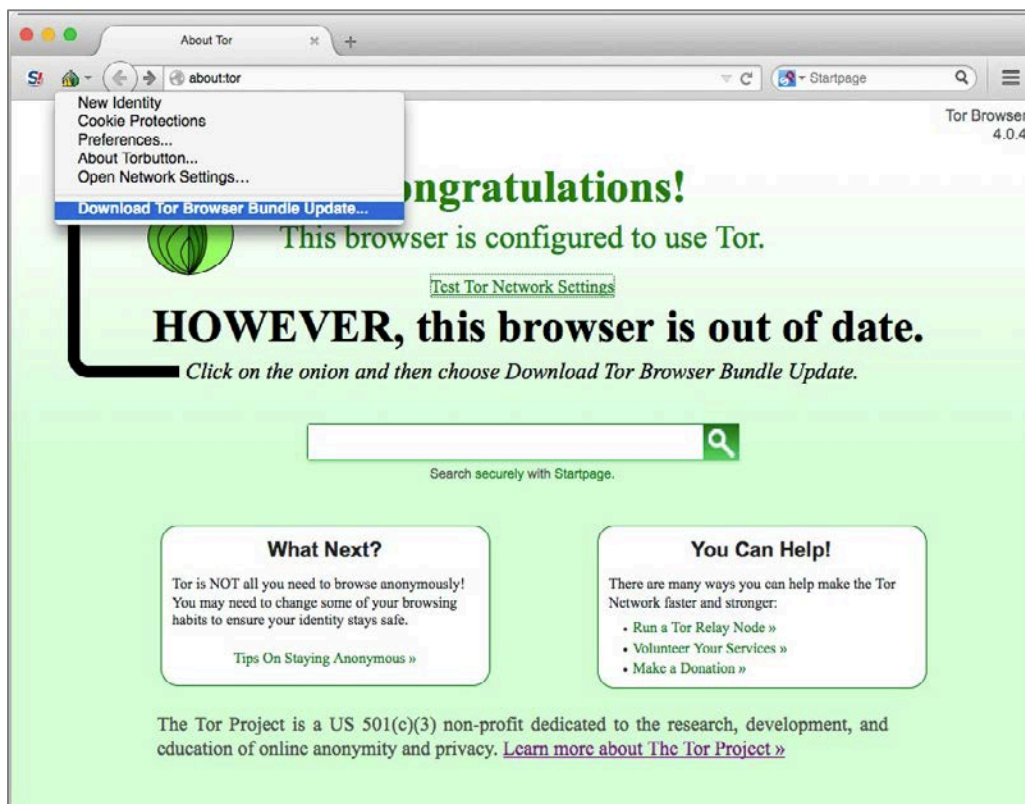
13. If you selected *Yes* to the *Does your ISP block or otherwise censor connections to the Tor Network* window, you now see the *You may use the provided set of bridges or you may obtain and enter a customer set of bridges*

14 Web Browsing


window. Select *Connect with provided bridges*, *Transport type obsf3 (recommended)*, and then select the *Connect* button.



14. The Tor Browser updates often. If your copy is out of date, you will be welcomed by a message asking you to update. Follow the instructions, clicking on the *onion* icon > *Download Tor Browser Bundle Update...* to update. Once the download is complete, Quit Tor Browser, and then replace it with the new version. Otherwise, if you are up to date, skip to the next step.





15. It is vital to test your connection to verify your IP address is hidden/changed. While in Tor, go to <https://check.torproject.org>. You can also return to <https://whatismyip.com> as well.



Congratulations. This browser is configured to use Tor.


Your IP address appears to be: **185.165.168.229**

 WhatIsMyIP.com





What Is My IP?


Your Public IPv4 is:
185.165.168.229

Location: Victoria, 16 SC 

ISP: Flokinet Ltd

Free WAN Optimization  

Boost WAN Speed & Save Costs. Free 2 / 20 Mbps Software License.

wanos.co 

Questions & Answers

My IP Information

What Is My Public IP?

Proxy Check

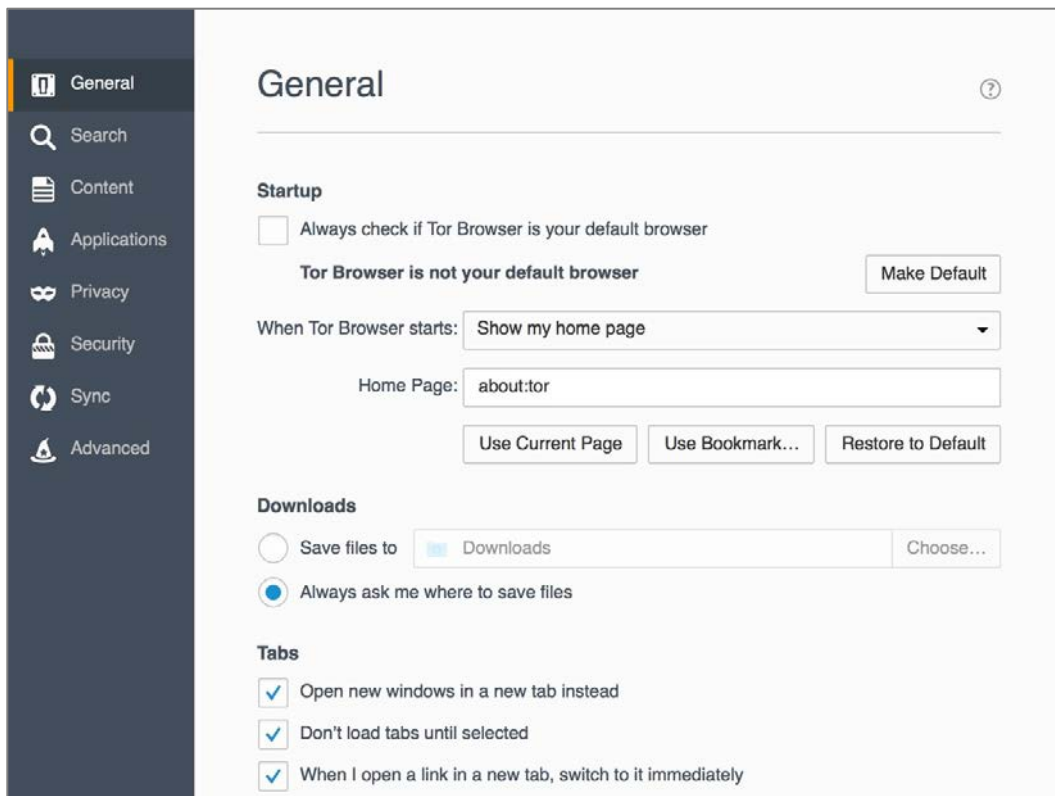
Wahoo! You are now on Tor, completely anonymous and encrypted on the Internet. Next step is to configure Tor.

14.11.2 Assignment: Configure Tor Preferences

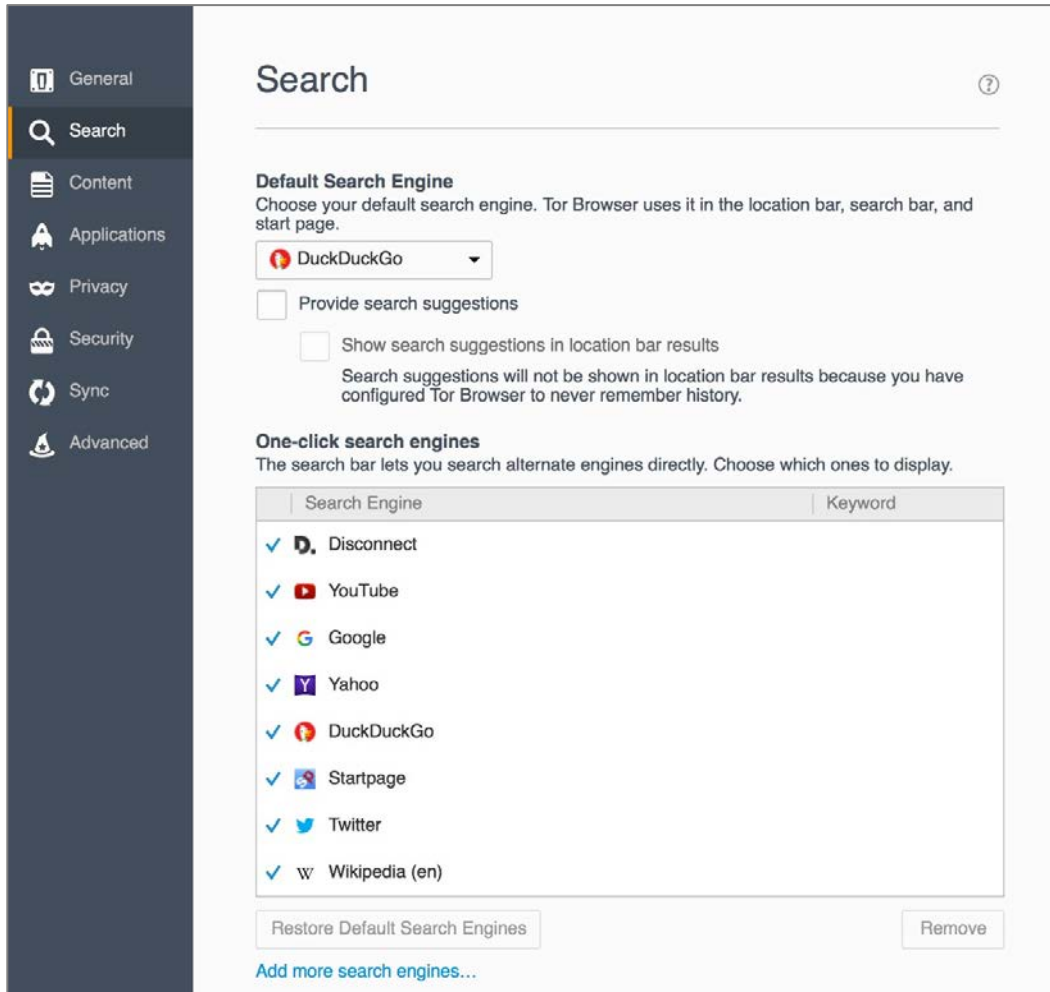
One of the first things one should do when launching an application for the first time is to configure its preferences. No different for Tor.

In this assignment, you configure Tor preferences.

1. Open TorBrowser, and then select the *3 horizontal line* menu (top right) > *Preferences* > *General* tab. This pane may be configured to taste.

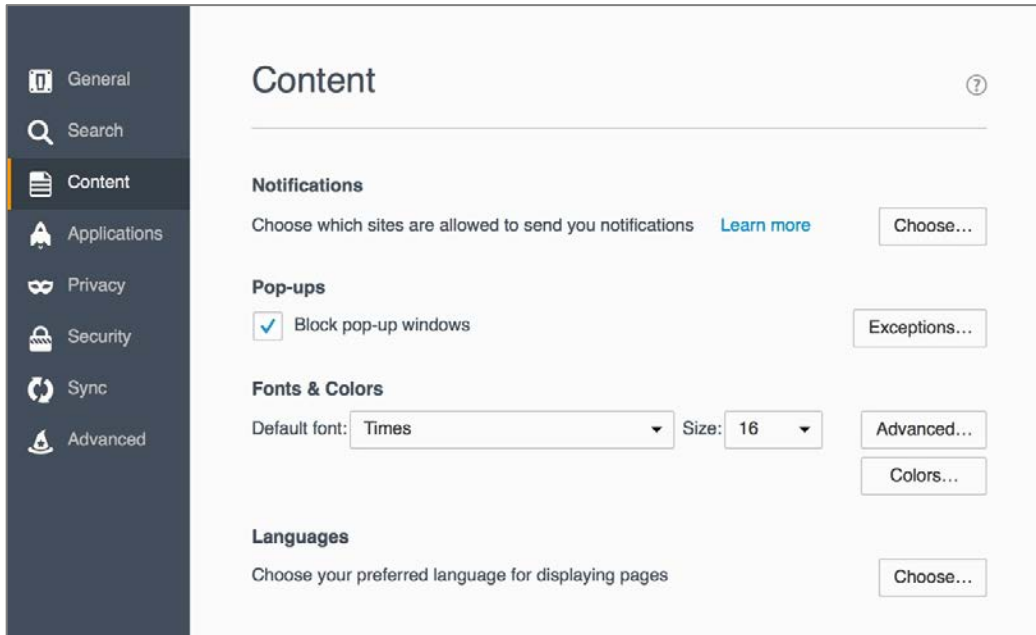


The screenshot shows the 'General' preferences window of the Tor Browser. On the left is a dark sidebar with icons and labels for 'General', 'Search', 'Content', 'Applications', 'Privacy', 'Security', 'Sync', and 'Advanced'. The 'General' tab is selected. The main content area has a title 'General' with a help icon. It is divided into sections: 'Startup', 'Downloads', and 'Tabs'. In the 'Startup' section, there is a checkbox 'Always check if Tor Browser is your default browser' which is unchecked. Below it, the text 'Tor Browser is not your default browser' is displayed, followed by a 'Make Default' button. A dropdown menu 'When Tor Browser starts:' is set to 'Show my home page'. Below that, the 'Home Page:' field contains 'about:tor', with buttons for 'Use Current Page', 'Use Bookmark...', and 'Restore to Default'. The 'Downloads' section has a radio button 'Save files to' (unchecked) with a file explorer icon and the text 'Downloads', and a 'Choose...' button. The second radio button 'Always ask me where to save files' is selected. The 'Tabs' section has three checked checkboxes: 'Open new windows in a new tab instead', 'Don't load tabs until selected', and 'When I open a link in a new tab, switch to it immediately'.

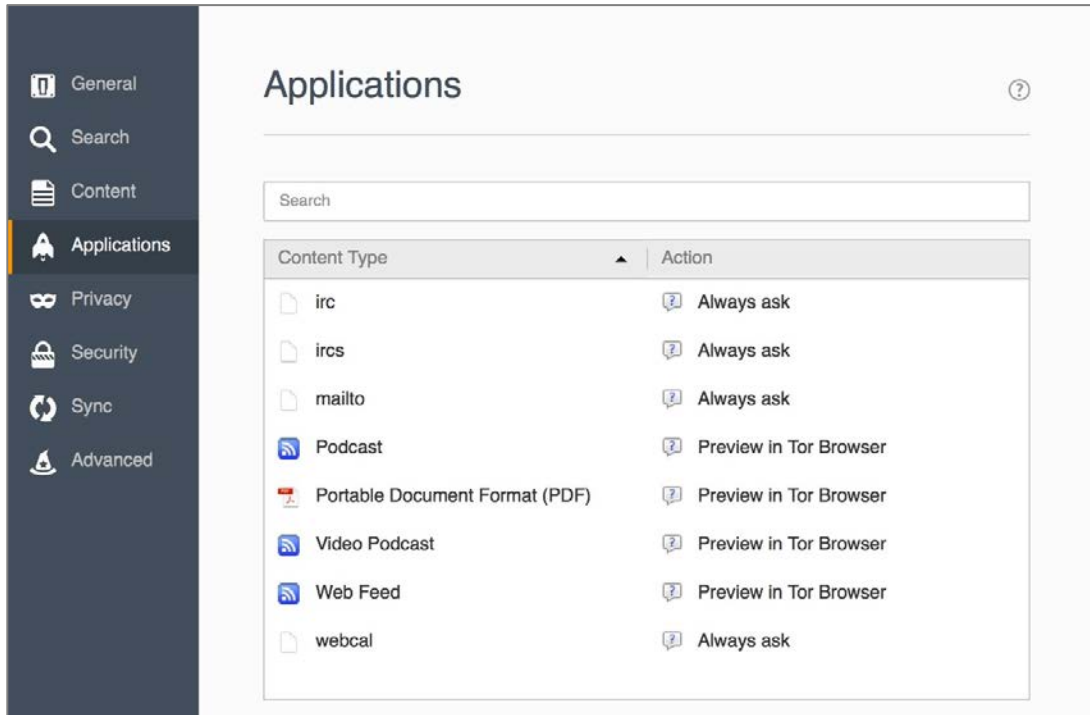
2. Select the *Search* tab.

- For *Default Search Engine*, select *DuckDuckGo*.
- Other settings may be configured to your taste.

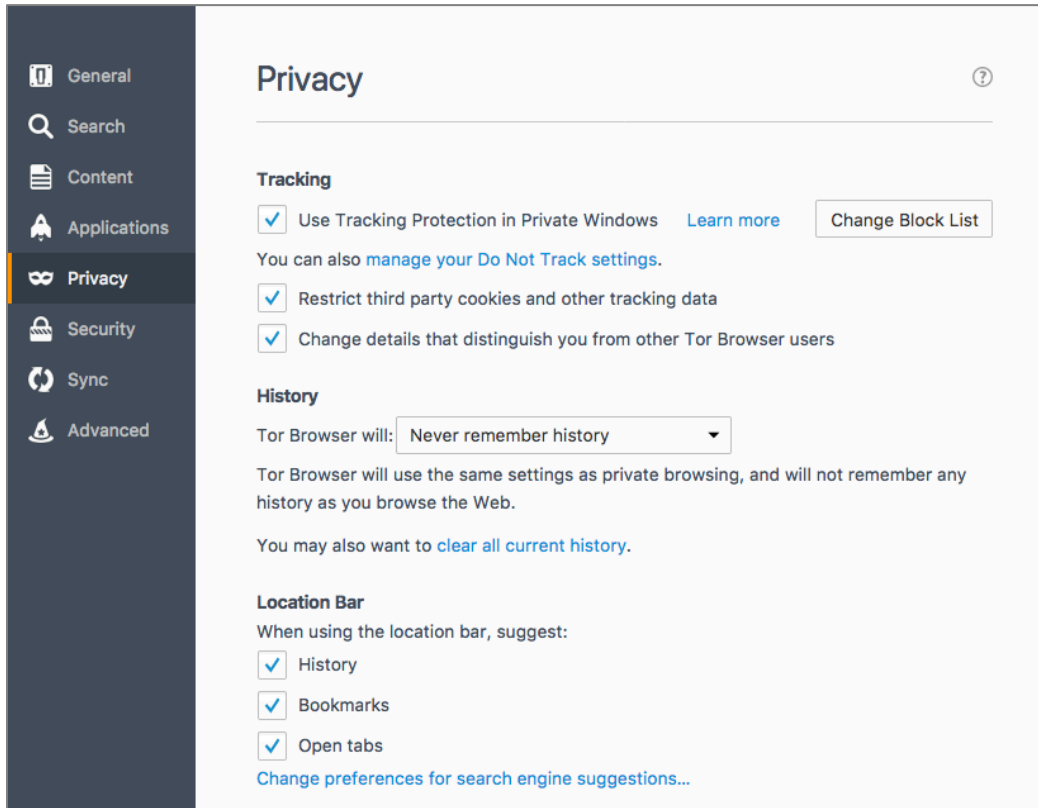
3. Select the *Content* tab. Configure to your taste.



4. Select the *Applications* tab. Configure to your taste.

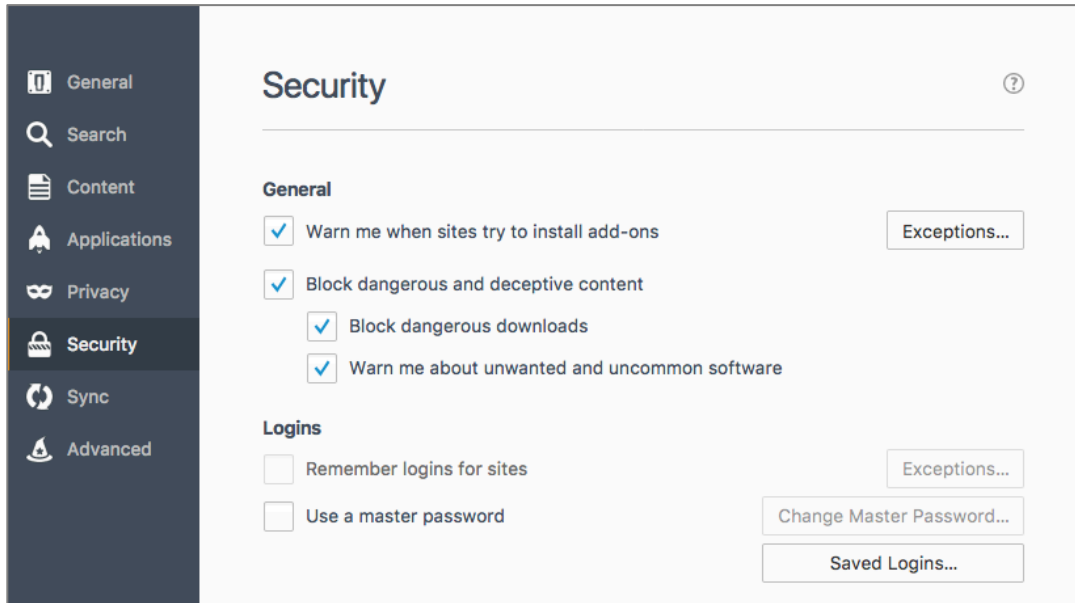


5. Select the *Privacy* tab.



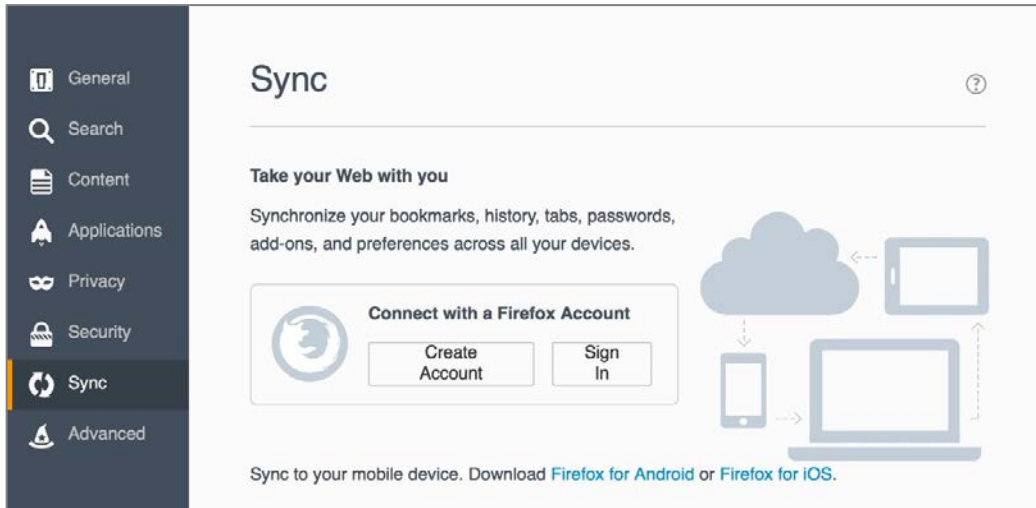
- Enable *Tracking* > *Use Tracking Protection in Private Windows*
- Enable *History* > *Tor Browser will:* > *Never remember history*
- *Location Bar* may be configured to your taste.

6. Select the *Security* tab.



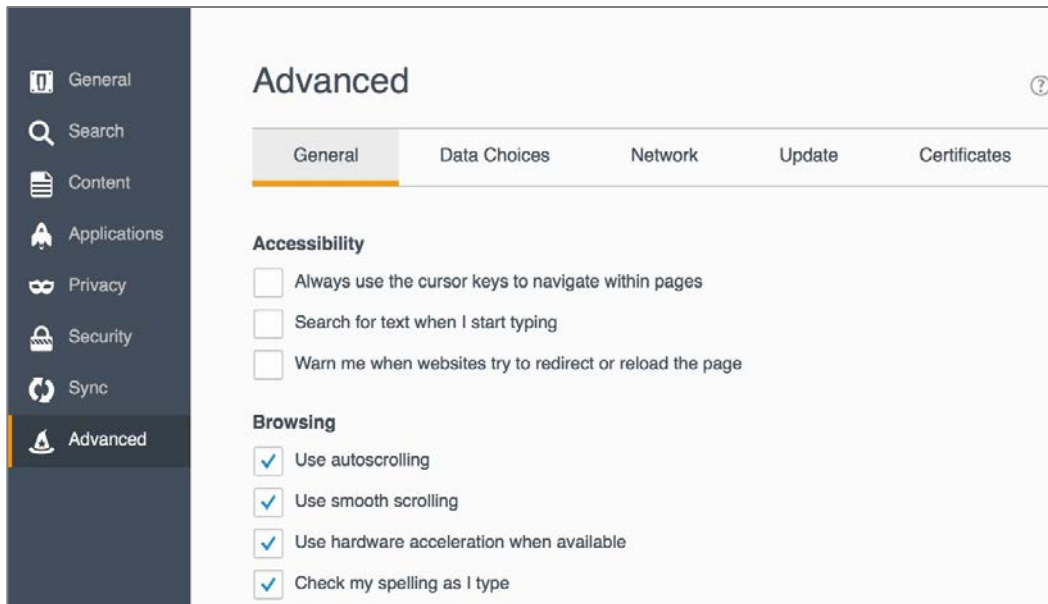
- Enable *General* > *Warn me when sites try to install add-ons*.
- Enable *General* > *Block reported attack sites*.
- Enable *General* > *Block reported web forgeries*.
- Configure other settings to your taste.

7. Select the *Sync* tab.



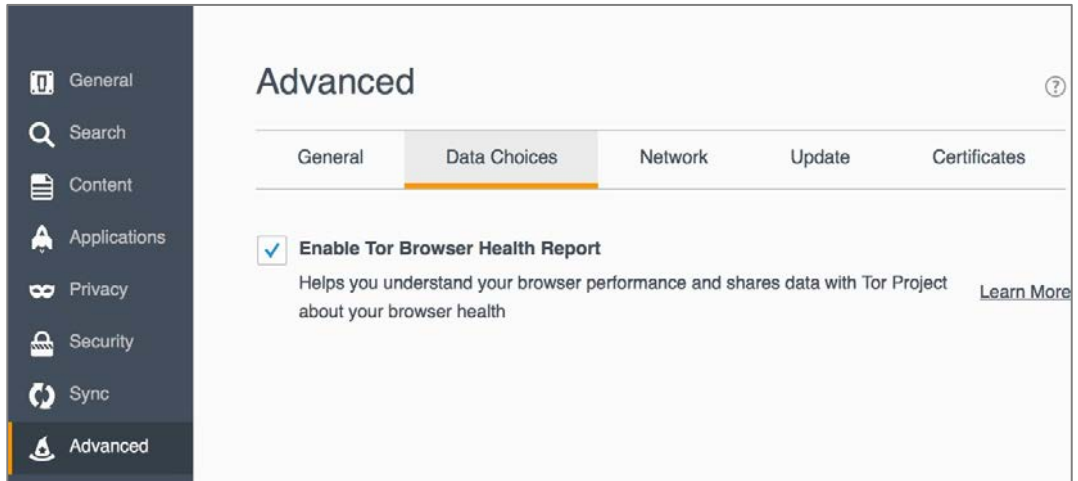
- Configure to your taste.

8. Select the *Advanced* tab, and then select the *General* tab.

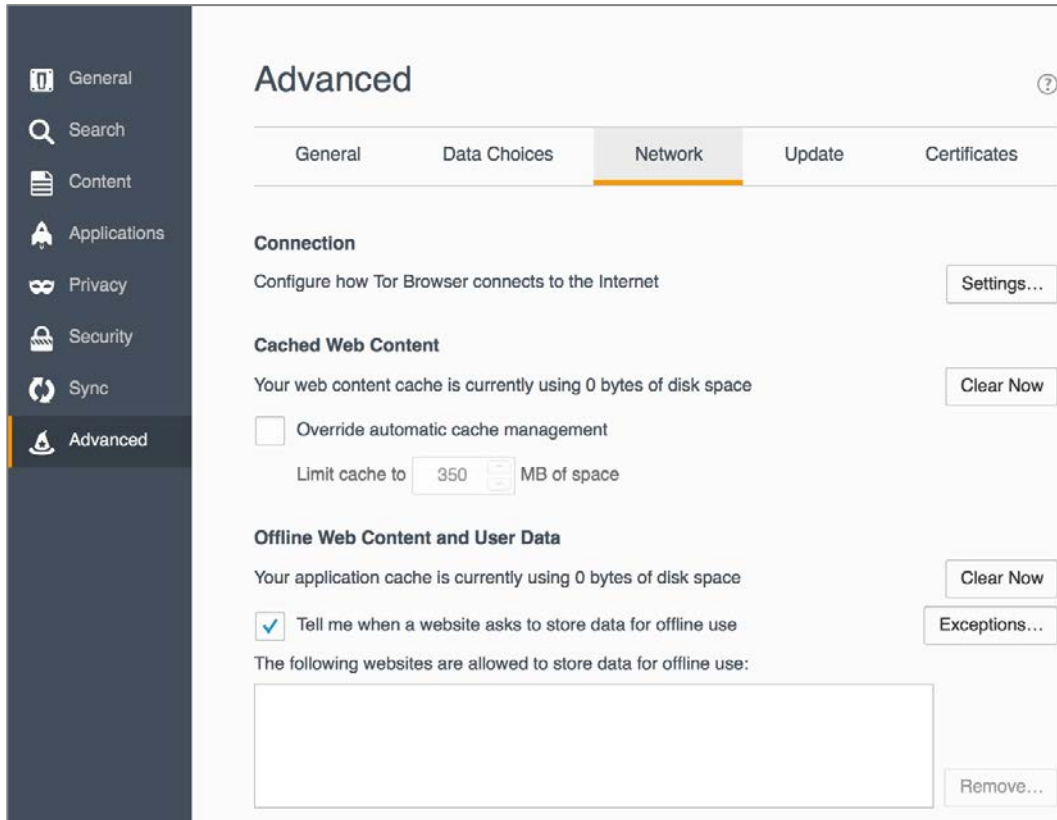


- Configure to your taste.

9. Select the *Data Choices* tab, and then enable *Enable Tor Browser Health Report*.

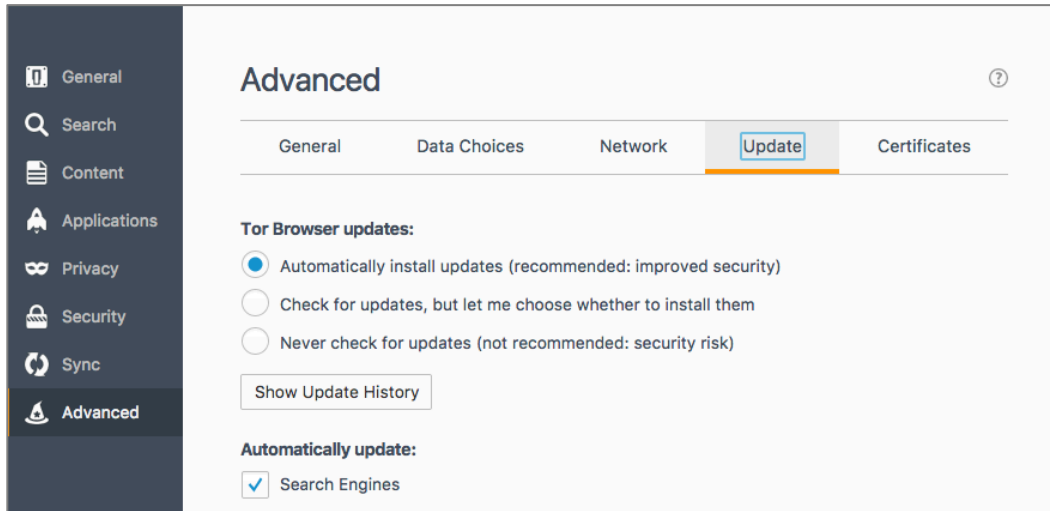


10. Select the *Network* tab.



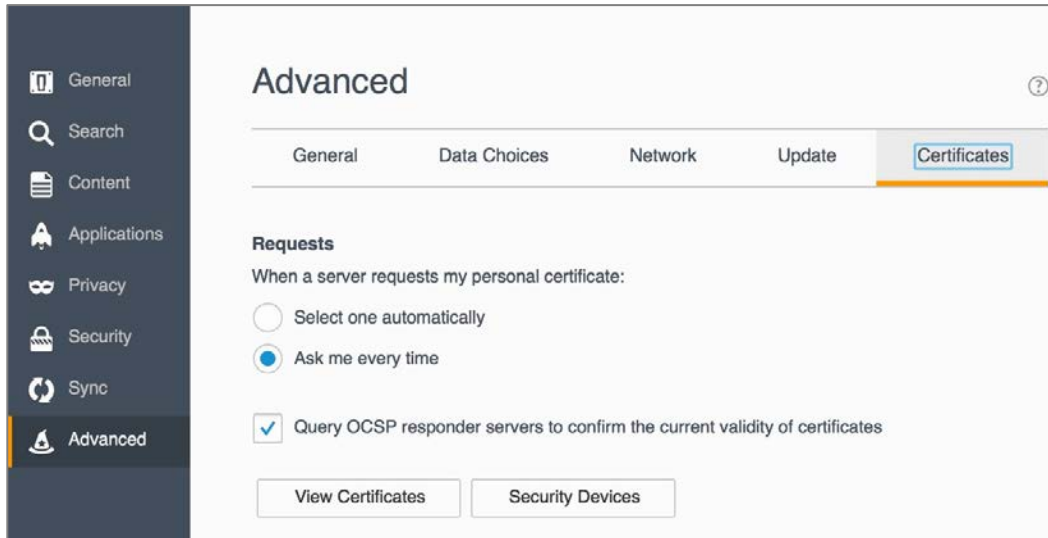
- Enable *Tell me when a website asks to store data for offline use*.
- Configure other settings to your taste.

11. Select the *Update* tab.



- Enable *Automatically install updates (recommended: improved security)*.
- Enable *Warn me if this will disable any of my add-ons*.
- Enable *Automatically update: Search Engines*.
- Configure other settings to taste.

12. Select the *Certificates* tab.



- Enable *Requests* > *Ask me every time*.
- Enable *Query OCSP responder servers to confirm the current validity of certificates*.

13. Close the preferences tab in Tor.

Great work! You are now ready to use Tor to securely and anonymously browse the Internet.

But remember, Tor is just one small part of *real* anonymity and security on the Internet. Many in the Internet Security field (including Edward Snowden) believe that to do this right, you will want a bootable Tails thumb drive. Learn all about it in our upcoming *Practical Paranoia: Tails Security Essentials* book. In the meantime, visit the Tails¹⁴ home page.

¹⁴ <https://tails.boum.org>

14.12 Onion Sites And The Deep Web

Tor not only allows you to have anonymous access to your regular web sites, it is also the only gateway to the *Deep web*¹⁵. The deep web is also known as the *Invisible Web*. It consists of web content deliberately not indexed with standard search engines, and only accessible by Tor. These sites are also called *Onion sites*, as they end with *.onion*.

Although the deep web is primarily thought of as a collection of sites to sell illegal products and services, there are also good and responsible uses for it. For example, in repressive countries such sites provide an avenue for freedom workers to work, for reporters to securely exchange information with sources (Ed Snowden did this), and there are sites to provide resources for whistleblowers.

As the deep web is not indexed by Google, Bing, or any other standard search engine, how do you go about discovering its resources? The list is in constant flux, but as of this writing, here are some good starting points:

- TorLinks¹⁶
- Torch¹⁷
- Torch Tor Search¹⁸

¹⁵ [https://en.wikipedia.org/wiki/Deep_web_\(search\)](https://en.wikipedia.org/wiki/Deep_web_(search))

¹⁶ <http://torlinkbgs6aabns.onion>

¹⁷ <http://xmh57jrznw6insl.onion/>

¹⁸ <http://torchtorsearch.com>

14.13 Have I Been Pwned

“WHAT!?!” is probably the first thing that just went through your mind. No, it’s not a typo. *Pwn*, as defined in the dictionary, is to be totally defeated or dominated. Although most commonly used when trouncing your online game opponent, it is also used to describe when your email or online accounts have been hacked.

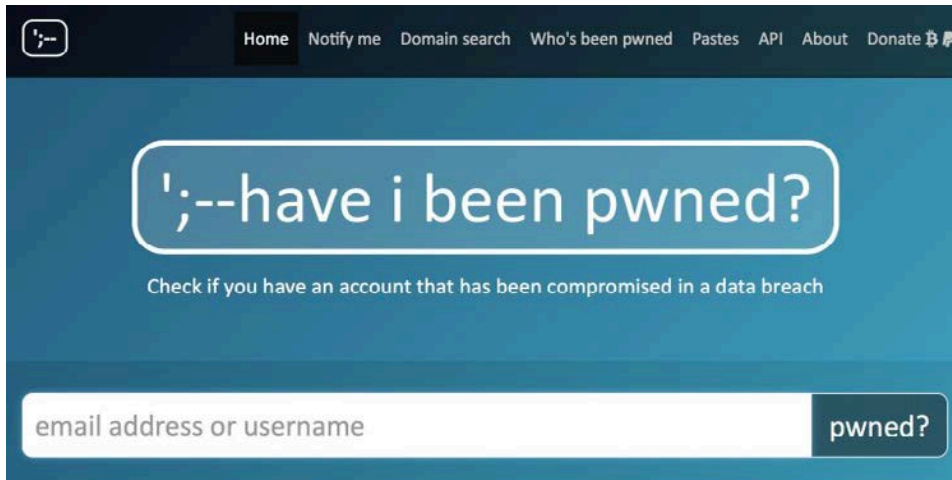
And there is a pretty good chance that you have been pwned!

There are several websites that track email and online account breaches. My favorites are *haveibeenpwned* and *hacked-emails.com*.

14.13.1 Assignment: Has Your Email Been Hacked

In this assignment, you search the *haveibeenpwned.com* and *hacked-emails.com* databases to discover if any of your online accounts have been hacked/pwned.

1. Open a web browser to *https://haveibeenpwned.com*. The home page appears.



2. Enter your email address, and then click the *pwned?* Button.

14 Web Browsing

3. In a few seconds, the results will display.

pwned?


Oh no — pwned!

Pwned on 14 breached sites and found 7 pastes (subscribe to search sensitive breaches)

[Notify me when I get pwned](#) [Donate](#)


Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.




000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed over 13 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.

Compromised data: Email addresses, IP addresses, Names, Passwords




Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords



Final Fantasy Shrine: In September 2015, the Final Fantasy discussion forum known as FFShrine was breached and the data dumped publicly. Approximately 620k records were released containing email addresses, IP addresses and salted hashes of passwords.

Compromised data: Email addresses, Passwords, Usernames, Website activity

4. Make a note of the sites with breaches.
5. In your browser, go to <https://hacked-emails.com>.
6. Enter your email address, and then click *Check*.

14 Web Browsing

7. All found breaches will display.

[HOME](#) [VERIFIED LEAKS](#) [LATEST DATA LEAKS](#) [API](#) [ABOUT THE PROJECT](#)


Has my email been hacked?

CHECK


We have found 46 entries for steve@apple.com


We use the term Data Leak for when a site has been accessed through a vulnerability in its system and information obtained is shared publicly. See the matches we have found and take the suitable measures, such as changing your passwords or asking the site where the information was published to remove the content.

Are you a Google Chrome user? Check our GMail extension!

 available in the chrome web store

Highlighted leaks where your email has been compromised

 **dailymotion.com**
87,164,388 Emails found

 **edmodo.com**
43,219,733 Emails found

8. Close your browser.

14.13.2 Assignment: What To Do Now That You Have Been Breached

In this assignment, you take action to repair any found breaches.

- Prerequisites: Completion of the previous assignment.
- 1. Open a web browser, and then go to the first breach site.
- 2. Change your account password, following best practices:
 - Passphrase is a minimum of 15 characters, in an easy to remember, easy to enter phrase.
 - Use the password/passphrase for only one site. Should a site become compromised and your password harvested, the automated hacking systems will use your credentials at every bank, online store, etc. to see if you are like most folks, using one password for everything.
 - Keep a secure record of your passwords/passphrases. I personally like to use *LastPass* as my password manager. Using a current version of *Excel* to create an encrypted spreadsheet also works well.
 - Only enter a username and password when in a secure web page (https).
- 3. Repeat steps 1 & 2 for each breached site.

15 Email

Human beings the world over need freedom and security that they may be able to realize their full potential.

–Aung San Suu Kyi¹, Burmese opposition leader and chairperson of the National League for Democracy in Burma

What You Will Learn In This Chapter

- Prevent phishing
- Email encryption protocols
- Configure Mail to use TLS and SSL
- Configure web mail to use HTTPS
- End-to-End Secure Email with Proton Mail
- End-to-end Secure Email with GNU Privacy Guard
- End-to-end Secure Email with S/MIME
- End-to-End Secure Email with Virtru

¹ https://en.wikipedia.org/wiki/Aung_San_Suu_Kyi

15.1 The Killer App

It can be rightfully argued that email is the killer app that brought the Internet out of the geek world of university and military usage and into our homes (that is, if you can ignore the overwhelming impact of Internet pornography.) Most email users live in some foggy surreal world with the belief they have a God or constitutionally given right to privacy in their email communications.

No such right exists. Google, Yahoo!, Microsoft, Comcast, or whoever hosts your email service all are very likely to turn over all records of your email whenever a government agency asks for that data. In most cases, your email is sent and received in clear text so that anyone along the dozens of routers and servers between you and the other person can clearly read your messages. Add to this knowledge the recent revelations about PRISM², where the government doesn't have to ask your provider for records, the government simply *has* your records.

If you find this as distasteful as I do, then let's put an end to it!

² [https://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](https://en.wikipedia.org/wiki/PRISM_(surveillance_program))

15.2 Phishing

The act of phishing is epidemic on the Internet. Phishing³ is the attempt to acquire your sensitive information by appearing as a trustworthy source. This is most often attempted via email.

The way the process often works is that you receive an email from what appears to be a trustworthy source, such as your bank. The email provides some motivator to contact the source, along with what appears to be a legitimate link to the source website.

When you click the link, you are taken to what appears to be the trustworthy source (perhaps the website of your bank), where you are prompted to enter your username and password.

At that point, they have you. The site is a fraud, and you have just given the criminals your credentials to access your bank account. In a few moments, your account may be emptied.

The key to preventing a successful phishing attack is to be aware of the *real* URL behind the link provided in the email.

³ <https://en.wikipedia.org/wiki/Phishing>

The link that appears in an email may have nothing at all to do with where the link takes you. To see the *real* link, hover (don't click) your cursor over the link. After 3 seconds, the *real* link will pop-up.



Some of these scams are getting a bit more sophisticated in their choice of URL links, and attempt to make them appear more legitimate. For example, the email may say it is from *Bank of America*, and the link say *bankofamerica.com*, but the actual URL will be *bankofamerica.tv*, or *bankofamerica.xyz.com*.

If you have any doubts at all, it is best to contact your bank, stock broker, insurance agent, etc. directly by their known email or phone number.

15.3 Email Encryption Protocols

There are three common protocols that provide encryption of email between the sending or receiving computer and the SMTP (outgoing), IMAP (incoming), and POP (incoming) servers:

- **TLS**⁴ (Transport Layer Security)
- **SSL**⁵ (Secure Socket Layer), the TLS predecessor
- **HTTPS**⁶ (Hypertext Transport Layer Secure)

Understand that these protocols only encrypt the message as it travels between your computer and your email server and back. Unless you are communicating with only yourself (sadly, as most programmers are prone), this does little good unless you know that the other end of the communication also is using encrypted email. If they aren't, then once your encrypted mail passes from your computer to your email server, it demotes to either the less secure SSL, or if the other end of the communications doesn't support that, demotes to clear text from your email server, through dozens of Internet routers, to the recipient email server, and finally onto the recipient's computer.

⁴ http://en.wikipedia.org/wiki/Secure_Sockets_Layer

⁵ http://en.wikipedia.org/wiki/Secure_Sockets_Layer

⁶ <http://en.wikipedia.org/wiki/Https>

15.4 TLS and SSL With Mail App

Although SSL was originally considered highly secure, it has been broken and should no longer be used for email that is sensitive, secure, or related to the healthcare, legal, government, or military. To use TLS, the following criteria must be met:

- Your email provider offers a TLS. Many do not. If your provider does not offer this, *run*, don't walk, to another provider. If you are not sure which to select, I'm a fan of Google mail.
- You are using an email application as opposed to using a web browser to access your email.
- Your email application supports TLS.
- Your email provider has enabled and configured your email service to use TLS (they may *offer* TLS, but it may not be *enabled* by default).
- You have configured your email application to use TLS (most email applications now do this automatically. Apple Mail.app has gone to the point they have removed the preference setting for both SSL and TLS).
- Lastly, although not a requirement for TLS, a requirement to stall off breaking your password is that your email provider allows for strong passwords, and you have assigned a strong password to your email (many providers still are limited to a maximum of 8 character passwords.)

15.4.1 Assignment: Determine If Sender And Recipient Can Use TLS

In this assignment, you discover if both your own email and that of a recipient can use TLS email encryption.

- Note: If you use a web browser for email, you may skip this assignment and move on to the next where we configure your browser-based email to use https.
1. Open a web browser, and then go to *CheckTLS.com*.

2. Scroll halfway down the home page to the *Internet Secure Email is Easy* section.
3. In the *Just domain or full address* field, enter the domain name of your email address. For example, my email address is *marc@mintzit.com*, so my domain is *mintzit.com*. Then select the *Check It* button.

Internet Secure Email is Easy

Most email systems can encrypt email in compliance with US NIST, HIPAA, HITECH, PCI DSS, S, FINRA, etc. Check yours:

Check It

(we do not keep your address, see [privacy_policy](#))

4. The website will run tests against the domain's mail servers (MX servers), and then report on their level of security.

☰ **Test Results** (scroll up to re-run test)

CheckTLS Confidence Factor for "mintzit.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
aspmx.l.google.com [74.125.29.27]	5	OK (21ms)	OK (91ms)	OK (26ms)	OK (31ms)	OK (292ms)	OK (27ms)	OK (28ms)
alt1.aspmx.l.google.com [64.233.186.27]	10	OK (135ms)	OK (263ms)	OK (457ms)	OK (263ms)	OK (494ms)	OK (266ms)	OK (260ms)
aspmx3.googlemail.com [209.85.202.27]	15	OK (105ms)	OK (104ms)	OK (108ms)	OK (108ms)	OK (377ms)	OK (108ms)	OK (109ms)
aspmx2.googlemail.com [64.233.186.27]	20	OK (129ms)	OK (260ms)	OK (263ms)	OK (268ms)	OK (480ms)	OK (260ms)	OK (271ms)
Average		100%	100%	100%	100%	100%	100%	100%

5. If your *Test Results* are not 100% secure, either discuss this with your email provider for a resolution, or change providers.
6. Repeat steps 1-4 using the domain of your recipient email address.
7. If their *Test Results* are not 100% secure, advise them to discuss this with their email provider, or change providers.

15 Email

- Remember: Email will typically downgrade to lowest common security protocol.

15.5 Require Google Mail To Be TLS Secured

Google mail (Gmail, G-Suite email) uses TLS by default. However, if both the sender and recipient don't support TLS, Google will deliver messages over a non-secure connection. And neither sender nor recipient will know.

However, your Google G-Suite (not Gmail) account can be configured to *only* use TLS. When so configured:

- Your outgoing Google mail (to a non-TLS account) will not be delivered, will bounce back to you, you will receive a non-delivery report (NDR). No additional delivery attempts will be made.
- Your incoming Google mail (from a non-TLS account) will be rejected at entry to Google servers. You will not receive any notification. The sender will receive an NDR.

15.5.1 Assignment: Configure Google G-Suite Mail For Only TLS

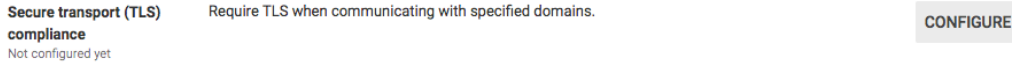
In this assignment, you configure your Google mail account to only allow use of TLS security. This feature is available only with paid G-Suite accounts, not with the free Gmail accounts.

Full details for this operation may be found on the Google *Require mail to be transmitted via a secure (TLS) connection* help page⁷

1. Open a web browser, visit and log in to the Google Admin Console at <https://admin.google.com>.
2. Go to *Apps > G Suite > Gmail > Advanced settings*.
3. If the G-Suite account includes more than one *Organization*, select the desired Organization from the left sidebar.

⁷ <https://support.google.com/a/answer/2520500?hl=en>

4. Scroll down to the *Compliance* section, hover over *secure transport (TLS) compliance*, and then select the *Configure* button.



5. In the *Add setting* page, select *ADD SETTING*.

Add setting

Secure transport (TLS) compliance

Required: enter a short description that will appear within the setting's summary.

1. Email messages to affect

☐ Inbound - all messages
☐ Outbound - all messages
☐ Outbound - messages requiring Secure Transport via another setting

2. Use TLS for secure transport when corresponding with these domains / email addresses.

No lists used yet. [Use existing or create a new one.](#)

3. Options

☐ Require CA signed cert when delivering outbound to the above-specified TLS-enabled domains.

CANCEL

ADD SETTING

6. In the *Secure transport (TLS) compliance* field, enter a description of this setting. For example: *Force TLS with contractors*.
7. In *1. Email messages to effect*, enable both *Inbound* and *Outbound*.
8. In *2. Use TLS for secure transport when corresponding with these domains / email addresses*, add the domain names to be included in forced TLS.
9. In *3. Options*, enable *Require CA signed cert when delivering outbound to the above-specified TLS-enabled domains*. This will prevent man-in-the-middle attacks.
10. Select *Save*.

15.6 HTTPS With Web Mail

We discussed HTTPS in the previous chapter. It is an encryption protocol used with web pages. It also can be used to secure email that is accessed via a web browser. When using HTTPS your user name and password are fully encrypted, as are the contents of all email that you create or open.

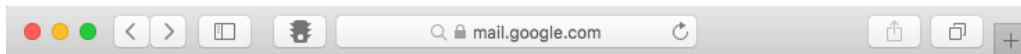
When using a web browser to access email, it is vital that your email site use the HTTPS encryption protocol to help ensure data and personal security.

15.6.1 Assignment: Configure Web Mail To Use HTTPS

If you use a web browser to access your email, it is critical that your web connection use HTTPS. In this assignment, you will verify that your browser-based email uses HTTPS.

In this assignment, you verify your browser-based email uses HTTPS.

- Note: If you do not use browser-based email, you may skip this assignment, and perform the previous assignment.
1. Launch your web browser.
 2. Go to your log in page for your email. In this example, we will be using Google Mail (Gmail).
 3. As in the screen shot below, make sure that the URL field shows either the lock to the left of the URL, or *https://* and not *http://*. This indicates you are communicating over a secure, encrypted pathway.



4. If instead your browser shows the URL to be *http://*, try revisiting your email log in page, but this time manually enter *https://*.
5. If you get to the log in page, all is good. Just bookmark the *https://* URL and use it instead of the previous non-secure URL.
6. If you cannot get to your log in page, change your email provider NOW!

15.7 End-To-End Secure Email With ProtonMail

If you are serious about email security, then you need to use an end-to-end secure email solution. Forcing TLS for incoming and outgoing email is one option (see previous section 15.5). However, it is likely either sender or recipient use email hosts that don't allow forcing TLS.

There are two other options for point-to-point email encryption:

- Use an email encryption utility. This works well if the other end of the communication also is using the same encryption utility. Our next section will cover this strategy using *GNU Privacy Guard* and *S/MIME*.
- Use a cloud-based option. This method makes it every bit as simple to send and receive email as the user is accustomed to. The downside is that instead of using an email client, a website is used to send and receive mail. An example of this is *Sendinc.com*⁸.

An interesting hybrid option is found in *ProtonMail*⁹. ProtonMail includes PGP public key/private key encryption, so that neither you nor the other party need deal with the potential headaches of installing and configuring PGP encryption.

ProtonMail has several advantages for the typical user, including:

- Free with optional monthly/yearly plans.
- Based in Switzerland so all user data is protected by Swiss privacy laws.
- Allows the user to determine the destruction date and includes unlimited retention.
- Allows for encrypted and password protected emailing to non-ProtonMail users.
- Allows for rich text email.

When sending from ProtonMail to a non-ProtonMail user, your recipient receives an email stating that a secure message is waiting. The recipient clicks the link,

⁸ <https://sendinc.com/>

⁹ <https://protonmail.com>

taking the recipient to an authentication page. Upon entering the password the recipient then sees the message. The recipient can directly and securely reply to the message, then you receive their reply in your inbox.

When sending from ProtonMail to ProtonMail, the interface is like other email providers.

Although not quite as convenient as using your own email software, when security, convenience, and cost are taken into consideration against the impacts of data theft, or the potential drama of confidential communications being intercepted, we find ProtonMail to be an easy choice.

15.7.1 Assignment: Create a ProtonMail Account

In this assignment, you create a ProtonMail account.

1. Using your web browser, visit <https://protonmail.com>. Select either the *Sign Up* or *Get Your Encrypted Email Account* button.



2. Scroll down to click the drop-down arrow next to the plan you wish to use (PLUS is selected by default). In this tutorial, we will be making a free

account. If you wish to use a monthly plan, make sure to double check the currency used on the bottom of the page.

The screenshot shows the ProtonMail pricing page. At the top, there is a navigation bar with the ProtonMail logo and links for About, Security, Blog, Careers, Support, and Donate. There are also buttons for LOG IN and SIGN UP. Below the navigation bar, a paragraph states: "users and continue to develop ProtonMail as free and open source software." The main content area displays three pricing plans in a list format, each with a dropdown arrow on the right:

- FREE**
- PLUS** 4.00 € /Month
- VISIONARY** 24.00 € /Month

Below the plans, there is a "change currency" section with a dropdown menu currently set to "EUR". At the bottom, there are logos for various payment methods: VISA, Mastercard, American Express, JCB, Discover, and PayPal.

3. Click the *Select Free Plan* button.

This screenshot shows the ProtonMail pricing page with the "FREE" plan selected and expanded. The navigation bar and introductory text are the same as in the previous screenshot. The "FREE" plan is now highlighted with a grey background and an upward-pointing arrow on the right. The expanded view for the "FREE" plan includes the following text:

We believe privacy is a fundamental human right so we provide free accounts as a public service. You can still support us by telling your friends and family about ProtonMail, or making a donation.

Our **FREE** accounts includes:

- ✓ 500MB storage
- ✓ 150 messages per day
- ✓ Limited Support

At the bottom of the expanded view, the word "FREE" is displayed in large bold letters, followed by "Upgrade Anytime". A blue button labeled "SELECT FREE PLAN" is positioned to the right of this text.

15 Email

4. Enter the *Username* and *Password* you wish to use. We recommend using easy to remember 15 character passphrases.

1

Username and domain
This will be your new ProtonMail email address.

@

Username is available

2

Login password
This is used to decrypt your inbox.

3

Mailbox password
This is used to encrypt and decrypt your messages. Do not lose this password, we cannot recover it.

5. Provide a method of verification.


< Back to protonmail.com

5

Are you human?
To help fight spammers, please verify you are human.

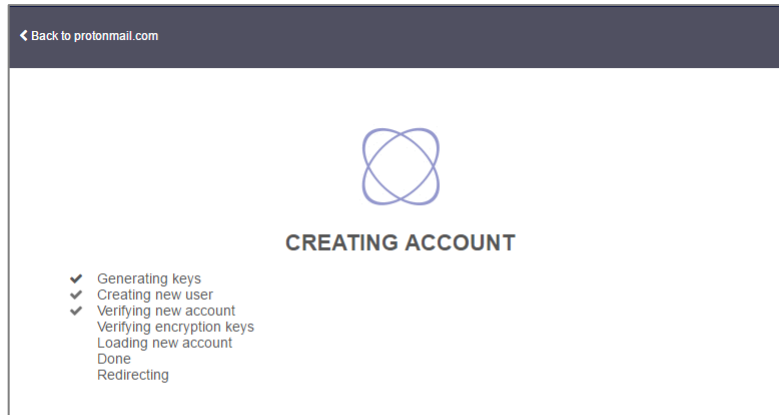
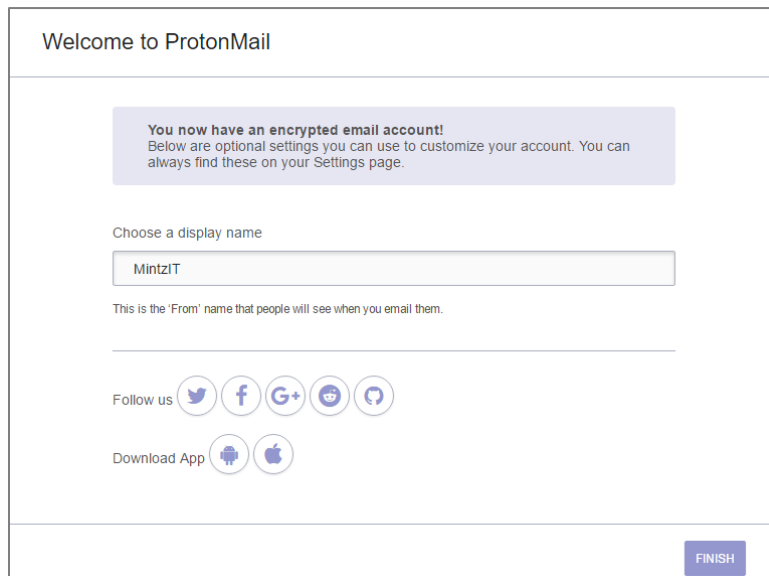
☐ Email
☒ reCAPTCHA
☐ SMS

reCAPTCHA verification

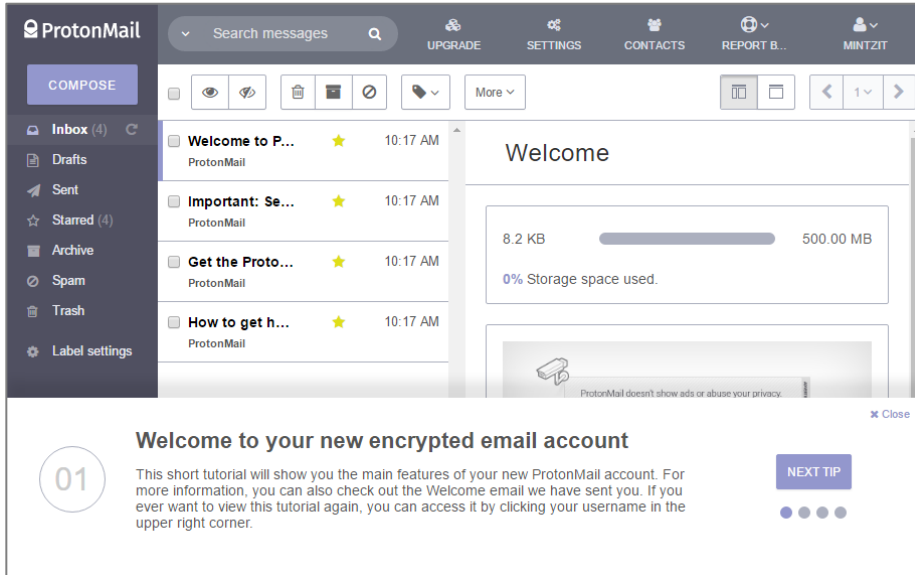
☐ I'm not a robot 
reCAPTCHA
Privacy - Terms

COMPLETE SETUP

6. ProtonMail begins to create your account.

7. At this stage enter the name that will be seen by other users. You also have the option of downloading iOS or Android Apps. Next click on the *Finish* button.

8. You have now finished the setup process. You will see a short tutorial on the bottom of your screen, it is recommended to read through it to understand some more of the features available to you.



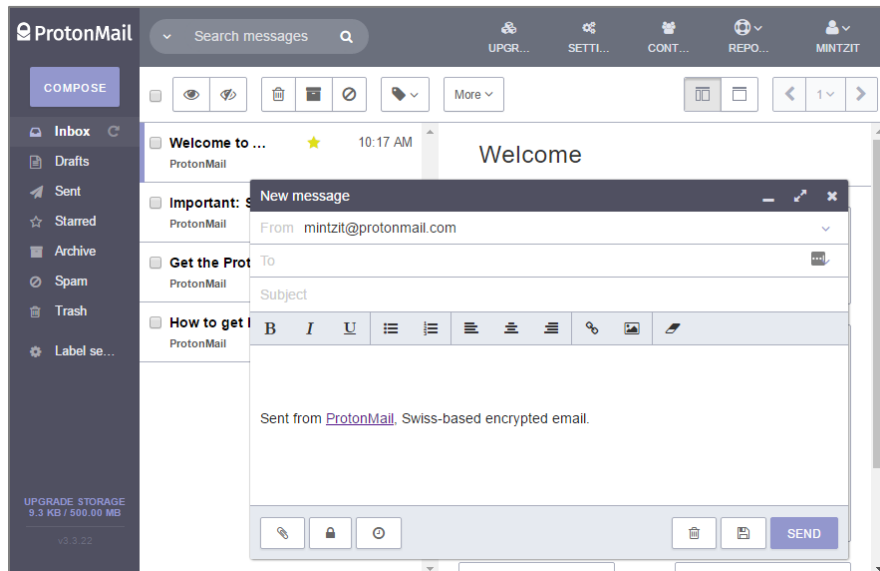
15.7.2 Assignment: Create And Send An Encrypted ProtonMail Email

In this assignment, you send your first fully encrypted email through ProtonMail.

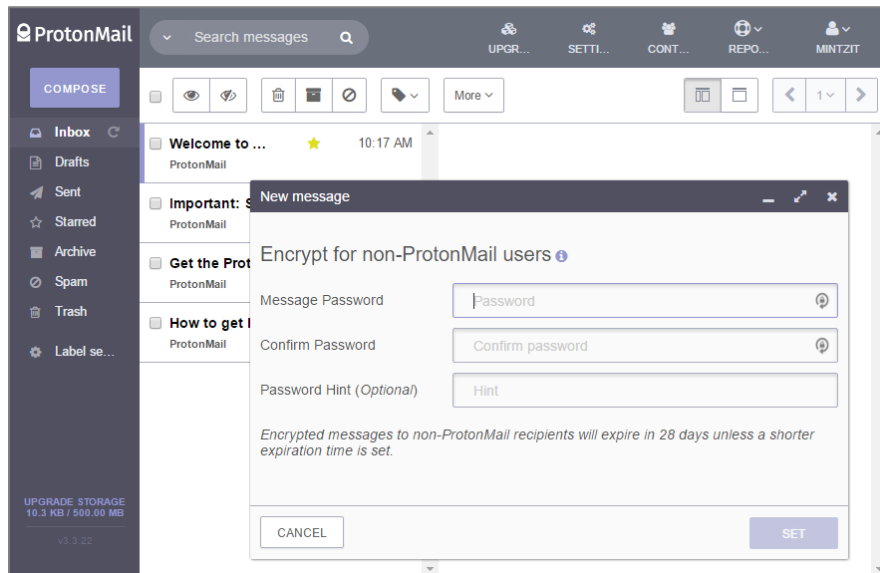
- **Prerequisite:** Completion of the previous assignment, or an existing ProtonMail account.
1. If you have just completed the previous assignment, select the *Compose* button in the top left. If not, use your web browser to visit *ProtonMail* at <https://ProtonMail.com>, select the *Login* link, and then log in.

15 Email

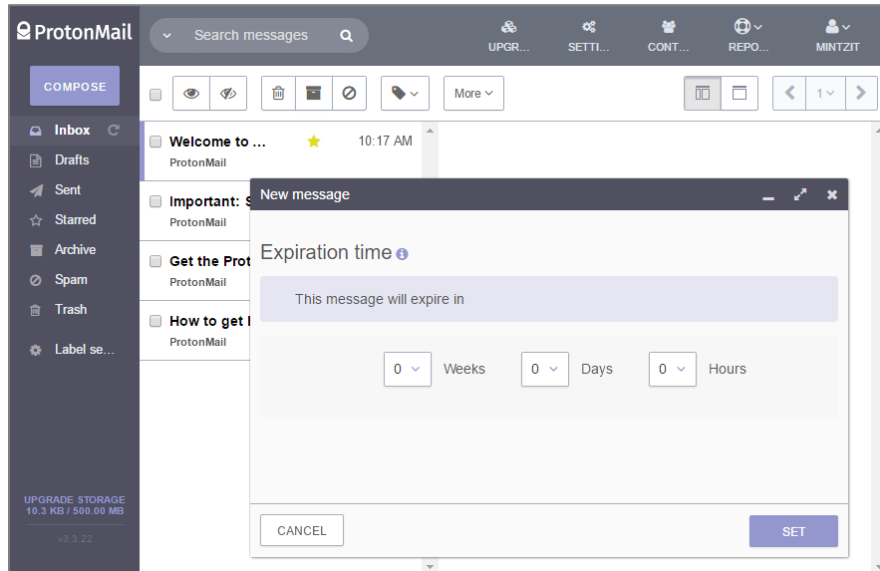
2. The *New Message* window should now be showing, enter the recipient email address, subject and a brief message.



3. Scroll to the bottom of the page, and then configure to your taste. The *Lock* icon allows you to set a password requirement to open the email from a non-ProtonMail account.
 - If you are sending to a recipient who is not a ProtonMail account, you have the option to manually set an encryption password in this screen. If you were sending to another ProtonMail account, the message is automatically encrypted, without need to enter a password.



4. The *Clock* icon allows you to set an expiration time for the email.



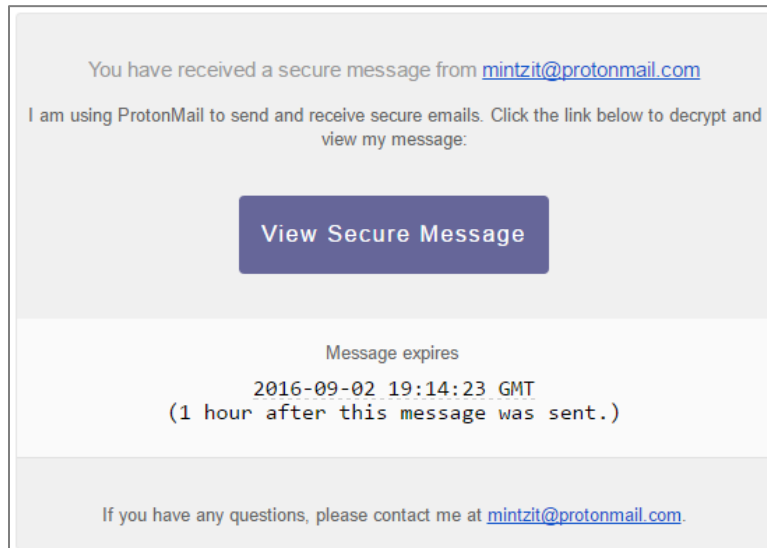
5. Once you have finished configuring your email, click the *Send* button. It will take a moment to encrypt and then send.

Notification of your email has been sent to the recipient.

15.7.3 Assignment: Receive And Respond To A ProtonMail Secure Email

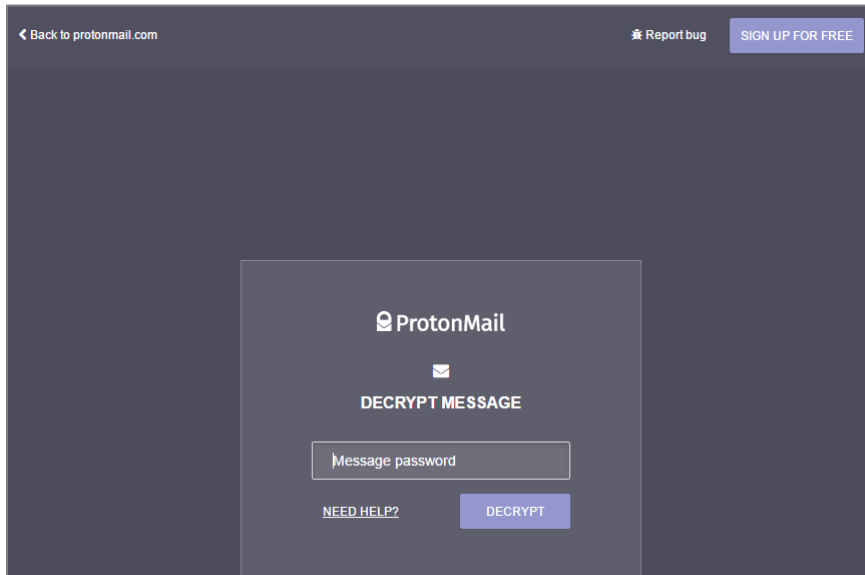
In this assignment, you reply to a ProtonMail secure email.

- Prerequisites: Completion of the previous two assignments.
1. After you have sent an email from your ProtonMail account (previous assignment), the recipient receives the following email. To view the message, the recipient selects the *View Secure Message* button within the email.



15 Email

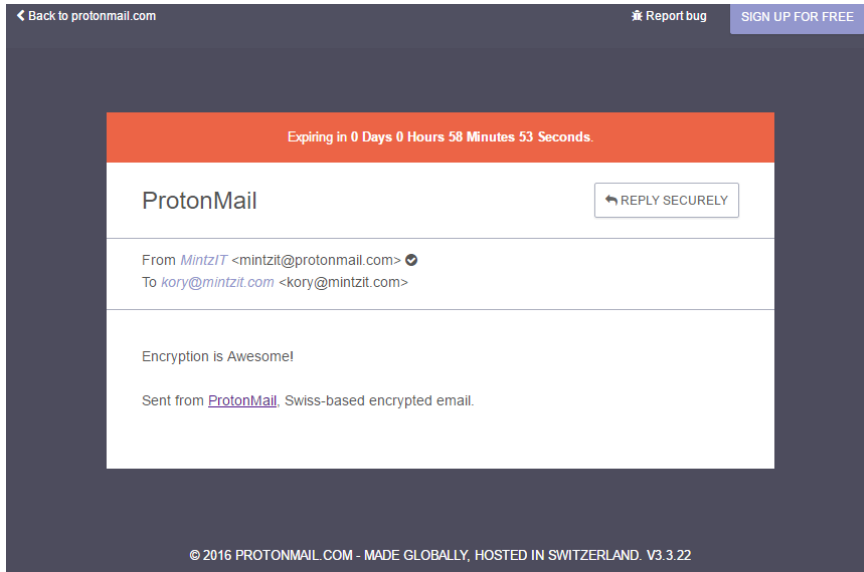
2. If the recipient already has a ProtonMail account, go to step 5. If the recipient does not have a ProtonMail account, they have the option of signing up for ProtonMail in the top right of the webpage. If they do not wish to sign up they may instead enter the required password to access their email on this page.



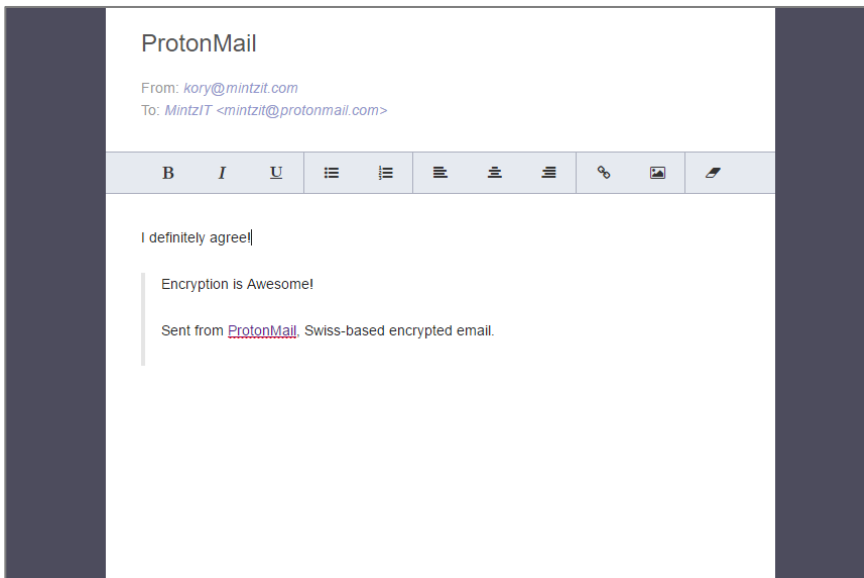
The image shows a screenshot of the ProtonMail 'Decrypt Message' interface. At the top, there is a navigation bar with a link to 'Back to protonmail.com', a 'Report bug' link, and a 'SIGN UP FOR FREE' button. The main content area is dark gray and features a central white box. Inside this box, the ProtonMail logo is at the top, followed by an envelope icon and the text 'DECRYPT MESSAGE'. Below this is a text input field labeled 'Message password'. At the bottom of the white box, there is a 'NEED HELP?' link and a 'DECRYPT' button.

15 Email

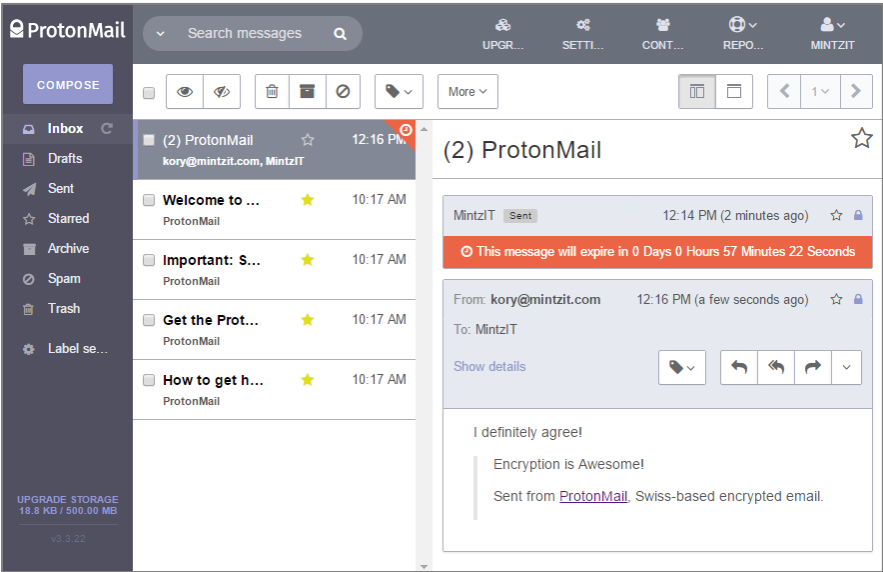
3. After entering the required password, the email is displayed in the recipient's browser. The recipient is also able to reply via this webpage by selecting *Reply Securely*.



4. The recipient then types in their reply and clicks on the *Send* button in the bottom right.



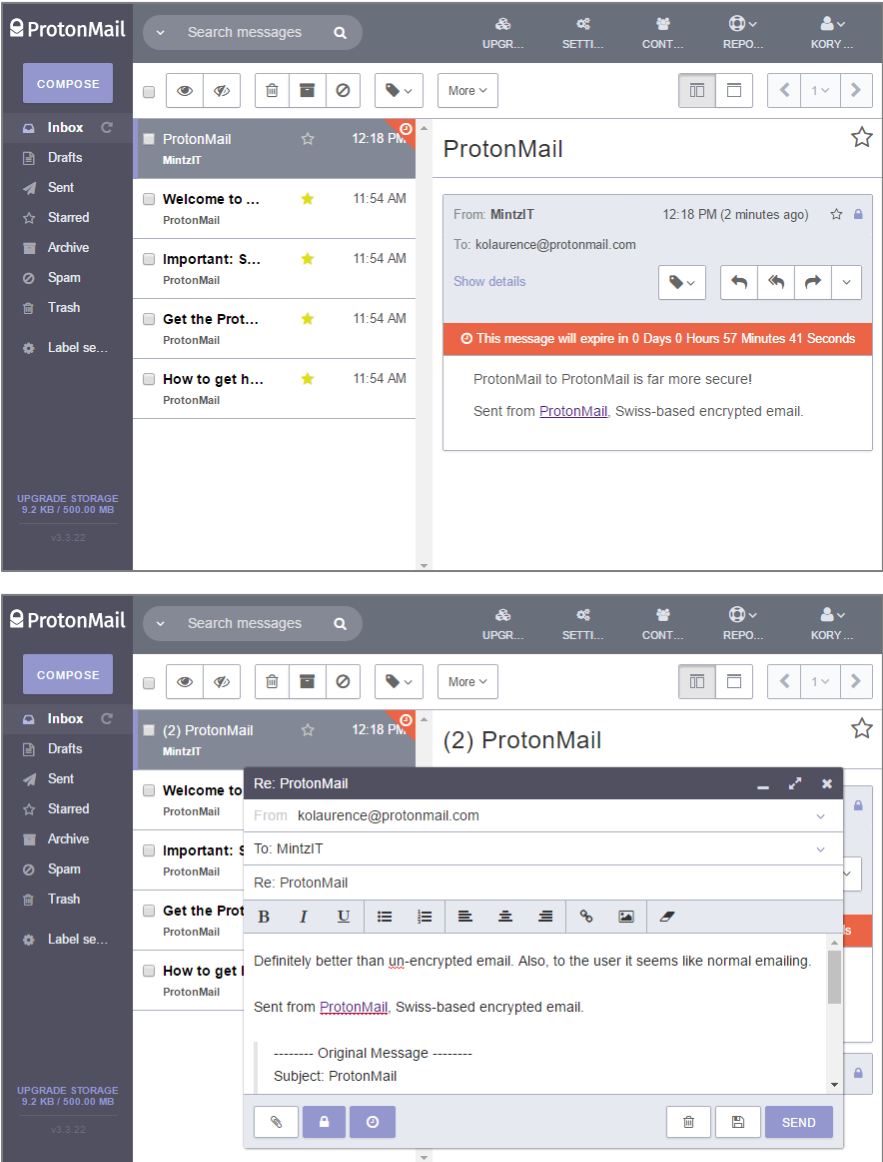
5. The original sender will receive a reply.



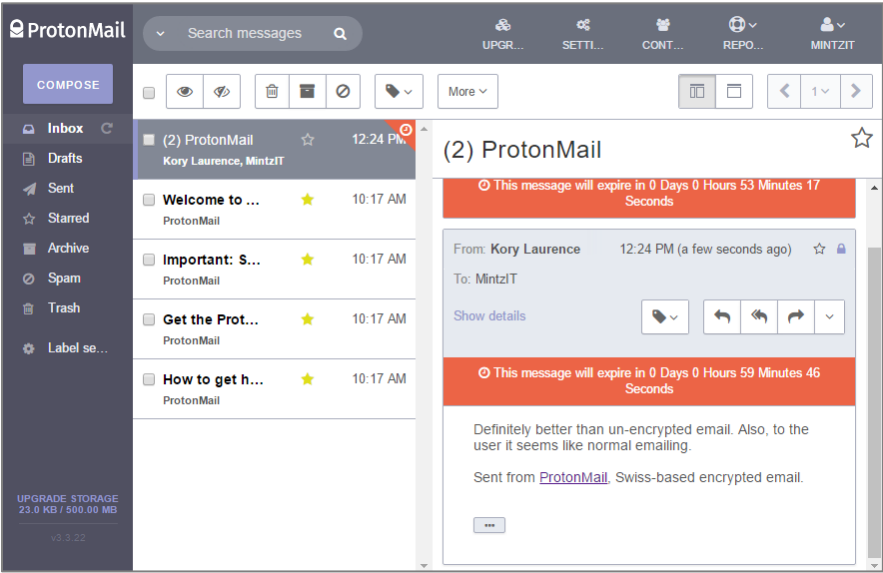
6. For either the original sender or the recipient, if they are using ProtonMail, it will show in their inbox like normal email. The email is decrypted and is fully

15 Email

viewable. Note that at no point is the message transmitted across the internet without encryption.



15 Email



15.8 End-To-End Secure Email With GNU Privacy Guard

The gold standard for email security is to fully encrypt the message at the sender's computer in a format that only the intended recipient can decrypt. This tool also must be capable of alerting the recipient if the message has been tampered with in any way (i.e., a man-in-the-middle attack.) The leader in this arena is PGP (Pretty Good Privacy), now owned and maintained by Symantec. Fortunately, there is an open source utility that provides all the core functionality and security of PGP, for free.

Setting up *GPG*¹⁰ (GNU Privacy Guard)—available for macOS, Windows, and Linux—takes a few more steps than our previous strategies in this section, and those with whom you wish to exchange secure email will need to also install GPG. But once both sender and recipient have their GPG in place, it is effortless to share fully encrypted messages.

Both PGP and GPG use the same strategy to securely encrypt email communications, and can exchange email with each other. Each user creates a *public key* and a *private key*. The Public Key typically is stored at a GPG server in the cloud, which can be found with a search for your name. The Private Key remains only on the user's computer. When sending an email to another person, your email application will automatically use the recipient's Public Key to encrypt the message. When the recipient receives the email, only the recipient's Private Key is able to decrypt and open the message.

If there are shortcomings to PGP and GPG, one is that as of this writing, there are only two iOS apps and one Android app, none of which are well received. Also, GPG is designed to work within an email client application, not a web browser. Although there are plug-ins for Firefox to allow for GPG, you are best to stick with the built-in Mail.app. Another issue is that before one can exchange encrypted email with someone else, both need to manually retrieve each other's public key. This typically is just a two-click process, but still...

¹⁰ <https://gnupg.org/>

Cryptography can quickly become Ph.D.-level material. I will cover everything you are likely to need to fully enable encryption and digital signing using GPG. Should you wish to delve deeper, visit the GPGTools Support site¹¹.

15.8.1 Assignment: Install GPG And Generate A Public Key

To encrypt your email, you need to have GPG installed, and have your recipient's Public Key installed in your GPG keychain. For your intended recipient to decrypt and read your email, the recipient needs to have GPG installed (or Gpg4win¹² if using Windows, or GPA¹³ if using Linux.) The recipient will also need to have your Public Key stored in their computer.

In this assignment, you install GPG on your computer, and upload your Public Key to the *GPG Public Key Server*, making it available to anyone wishing to send encrypted email to you.

¹¹ <http://support.gpgtools.org/kb>

¹² <https://www.gpg4win.org>

¹³ https://www.gnupg.org/related_software/gpa/index.en.html

1. Use your browser to visit *GPGTools* <https://gpgtools.org>, and then select the *Download GPG Suite* button.

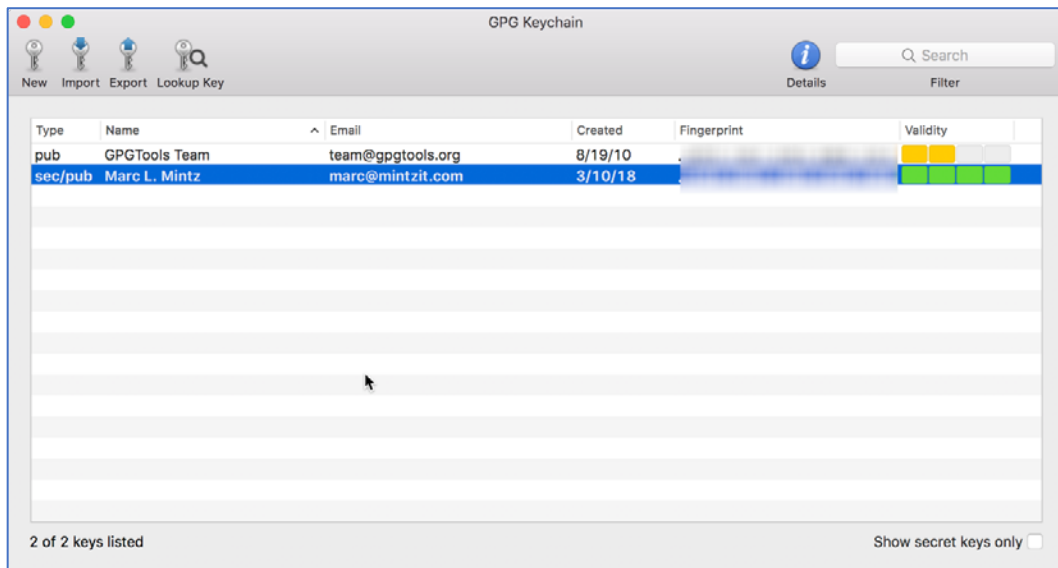


2. The software will begin to download to your computer.
3. Go to your Downloads folder, locate and then double-click on the *GPG Suite.dmg* file. This will mount the GPG disk image to your desktop, and then open the disk image to reveal the GPG Suite window.
4. Double-click the *Install.pkg* icon inside of the GPG Suite window to launch the *Install GPG Suite installer*.
5. Select the *Continue* button.
6. At the *Standard Install on "<Name of hard drive>"* window. Select the *Install* button.
7. The authentication window will appear. Enter an administrator name and password, and then select the *Install Software* button.
8. *The installation was completed successfully* window appears. Click the *Close* button.

9. The *GPG Keychain.app*, located in */Applications* opens.
10. Select the *Advanced Options* link to expand the window, and then complete all fields.

- *Name*: Enter your full name as used in your email.
- *Email*: Enter the email address for which GPG encryption is being configured.
- *Password & Confirm*: This is a password to protect access to this record. As with all passwords, make it strong.
- *Comment*: As you may eventually create many keys, enter a comment to refresh something unique about this key pair.
- *Key type*: Select *RSA and RSA (default)*. This is the strongest option currently available.
- *Length*: Select 4096. The larger the encryption bit depth, the more secure.
- *Expiration Date*: I typically leave this disabled, allowing any of my encrypted email to be accessed (given the proper credentials) forever. However, if you prefer to set your key to self-expire, making any sent emails created with it unreadable after a certain date, then by all means enable this option.

11. Select the *Generate key* button.
12. The new key will start to generate. During this time, the random key generator uses activity on your computer to help create a random key. You should move your cursor, or type some characters in another application during this time.
13. The *Your key was created successfully* window appears. This window gives the option to upload your public key. Remember, the public key allows others to send encrypted email to you—it does not present a security concern if others have access to it. Click the *Upload Public Key* button.
14. When your Public Key generation completes, the *GPG Keychain* window will display your new key.



Congratulations! You have successfully installed GPG to help encrypt your email.

15.8.2 Assignment: Add Other Email Addresses To A Public Key

- Prerequisite: Completion of the previous assignment.

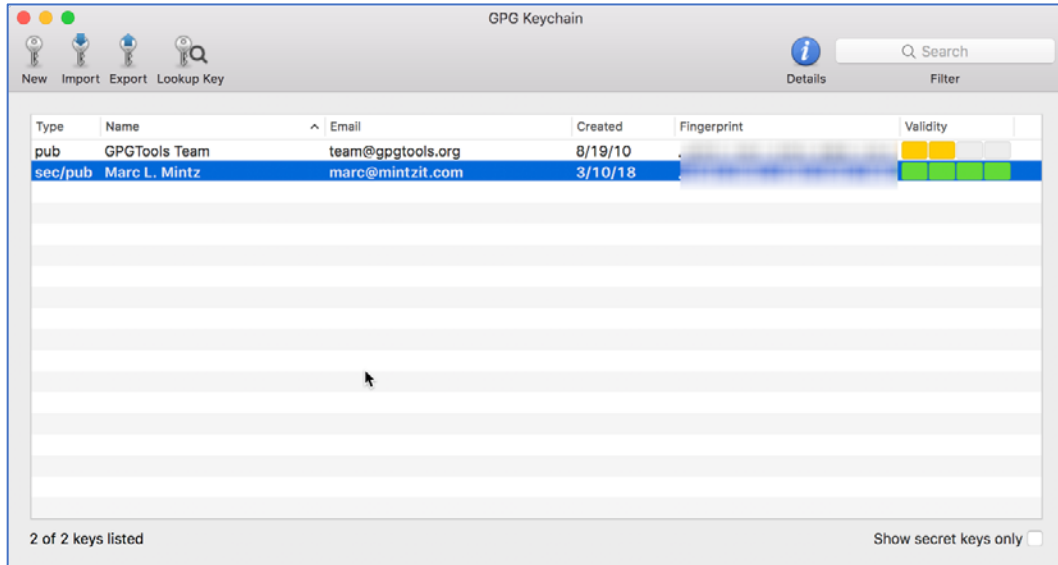
Many people have more than one email address. If you wish, you may create keys for each of your other addresses simply by repeating each of the steps in the

15 Email

previous assignment. However, you may find that both tedious and somewhat redundant. An alternative is to bind all your email addresses together under one key.

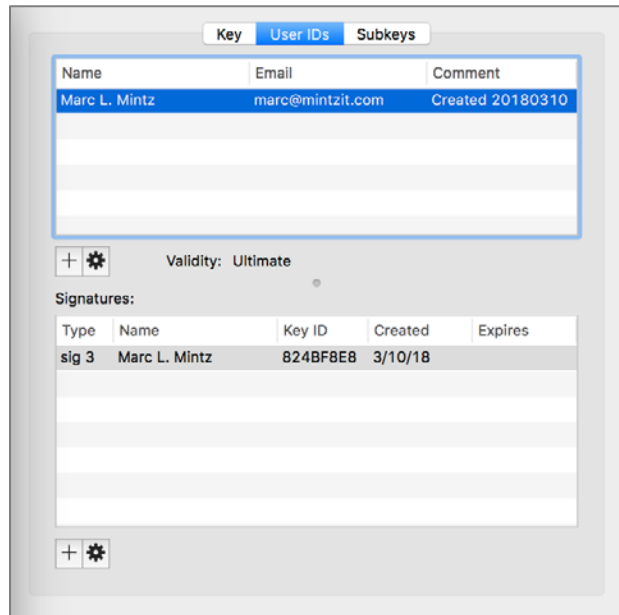
In this assignment, you add your other email.

1. Open *GPG Keychain*, located in your */Applications* folder, and then double-click on your entry from the previous assignment.

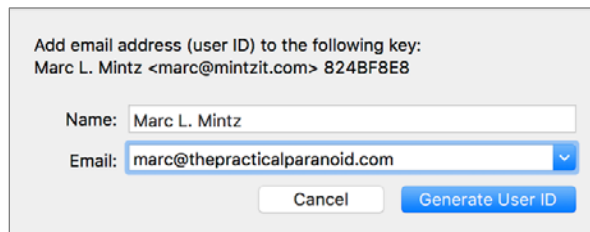


15 Email

2. The *Key Inspector* window will open. Select the *User IDs* tab, from top half of the window, select the account *Name*, and then select the + button.

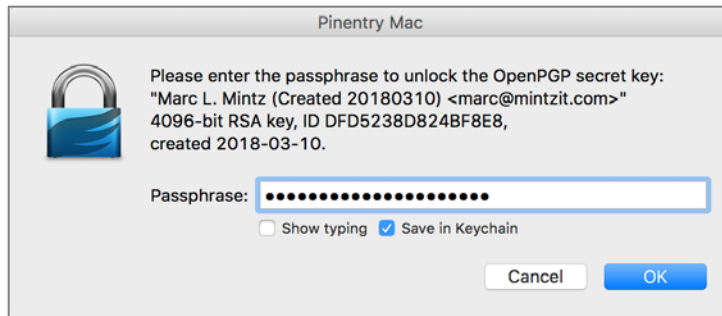


3. In the window that opens, enter your *Full name*, along with the new *Email address* you want to be bound to your original email/key combination, and then select the *Generate user ID* button.

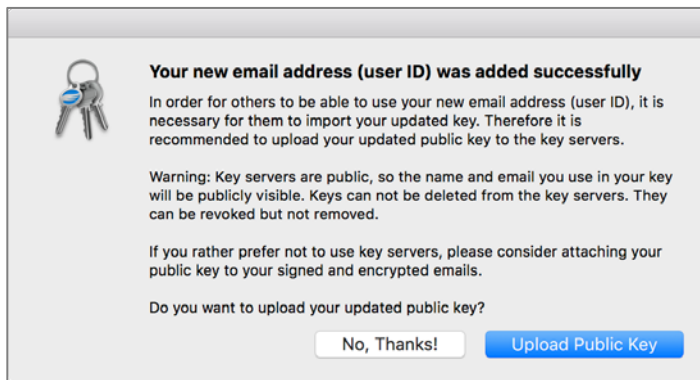


4. In the *Pinentry Mac* window:
 - a. enter the password/passphrase used when creating the original signature.
 - b. Enable *Save in Keychain* checkbox.
 - c. Click the *OK* button.

15 Email



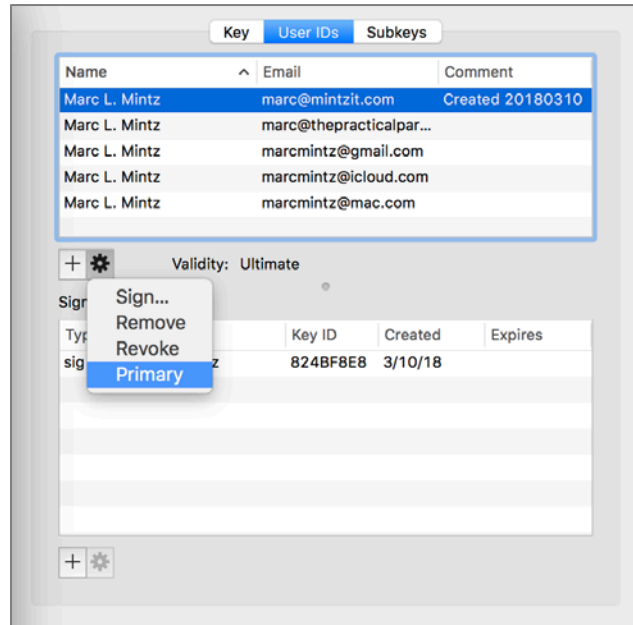
5. The *Your new email address (user ID) was added successfully* window appears. Click *Upload Public Key* button.



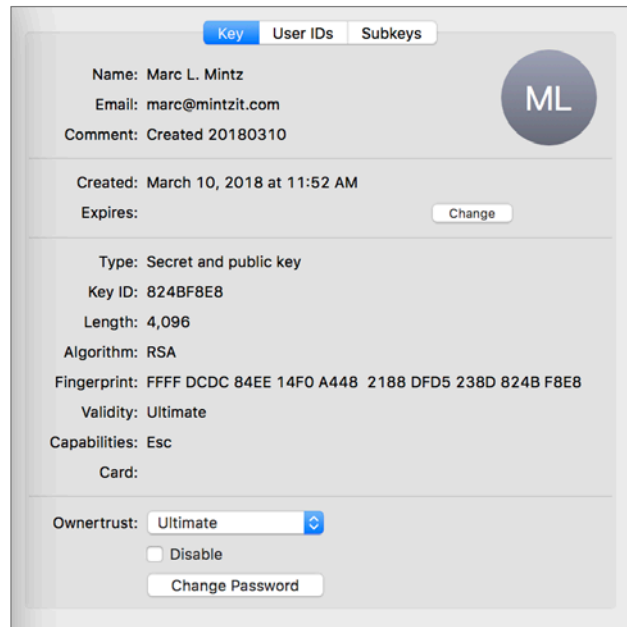
6. Repeat steps 2-5 for each of your email addresses.

15 Email

- When all your email addresses have been added, select the one address you use most often, click the *gear* icon, and then select the *Primary* button to set this as your primary account.



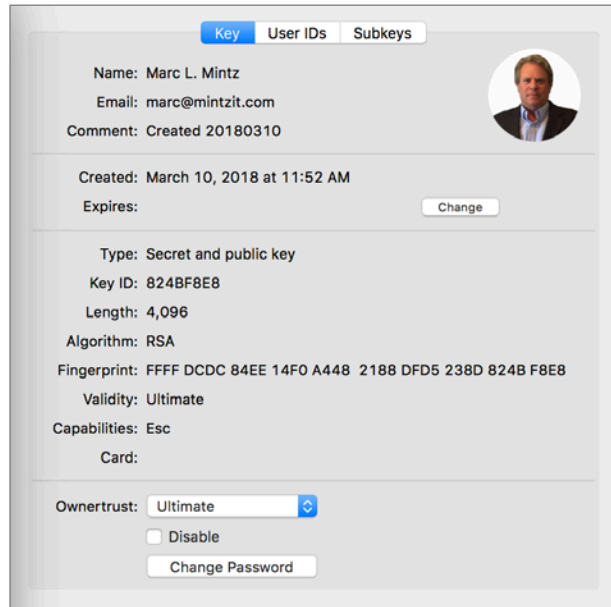
8. Though not required, let's add a photo to better identify you. Select the *Key* tab.



The screenshot shows a web interface for managing GPG keys. At the top, there are three tabs: 'Key' (selected), 'User IDs', and 'Subkeys'. The main content area displays information for a specific key:

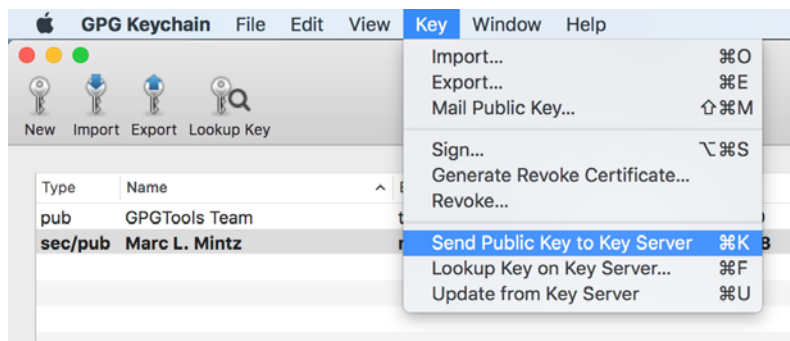
- Name:** Marc L. Mintz
- Email:** marc@mintzit.com
- Comment:** Created 20180310
- Created:** March 10, 2018 at 11:52 AM
- Expires:** (empty) [Change](#)
- Type:** Secret and public key
- Key ID:** 824BF8E8
- Length:** 4,096
- Algorithm:** RSA
- Fingerprint:** FFFF DCDC 84EE 14F0 A448 2188 DFD5 238D 824B F8E8
- Validity:** Ultimate
- Capabilities:** Esc
- Card:** (empty)
- Ownertrust:** [Change](#)
- ☐ Disable
- [Change Password](#)

9. Click the circle with your initials located in the top right corner. This will open a window to locate the desired photo.
10. Navigate your computer to locate the desired photo, and then double-click the photo to add it to your keys.



11. Lastly, upload your changes to the Public Key Server. Select the **Key** menu > *Send Public Key to Server*.

- Note: You may also mail your public key to someone else from the **Key** menu > *Mail Public Key...*

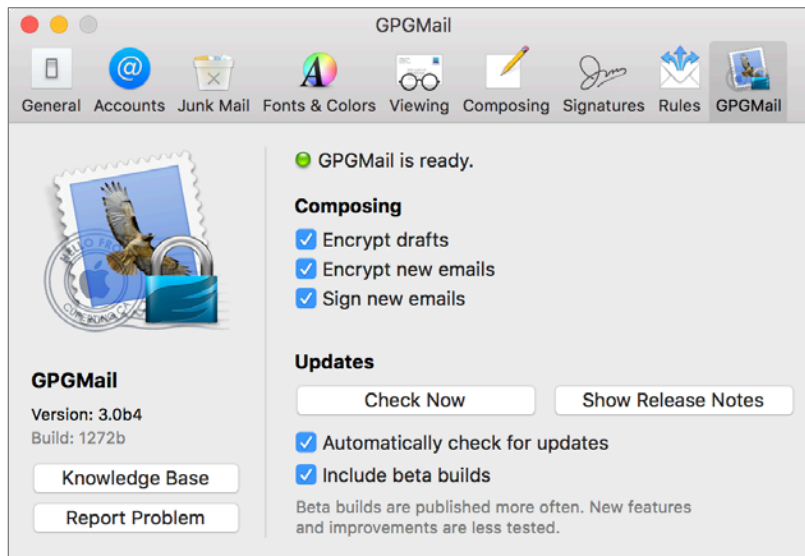


Congratulations! You have successfully added all your email accounts to GPG, allowing encrypted communications with any account.

15.8.3 Assignment: Configure GPGMail Preferences

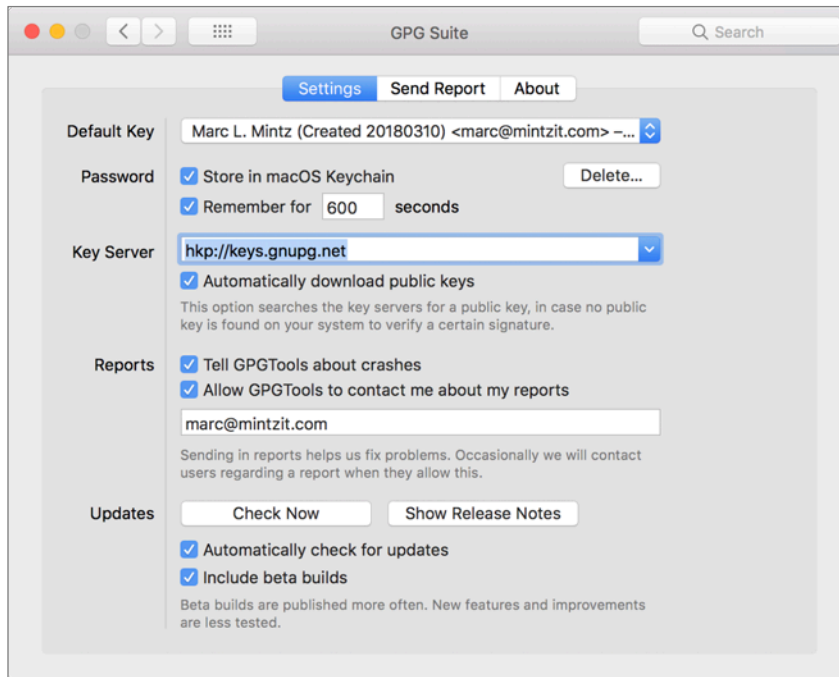
In this assignment, you configure GPGMail Preferences.

1. Open the *Mail.app*, open the *Mail* menu > *Preferences* > *GPG Mail*, and then configure as shown below.



2. Close the *Preferences* window.
3. *Quit* Mail.app.

4. Open the *Apple* menu > *System Preferences* > *GPG Suite*, select the *Settings* tab, and then configure as follows.



- *Default Key*: From the pop-up menu select your primary email account.
- Enable *Password*: *Store in macOS Keychain*.
- Enable: *Password*: *Remember for 600 seconds*.
- *Key server*: Unless your organization prefers using another server, stick with the default of *hkp://keys.gnupg.net*.
- Enable: *Reports Tell GPGTools about crashes*, and *Allow GPGTools to contact me about my reports*. Enter your email address for GPGTools to use when discussing reports.
- Enable: *Updates: Automatically check for updates*, and *Include beta builds*. Normally, I'm not fond of beta builds. But with GPTTools, it appears to be in constant beta.

5. *Quit* System Preferences.

Your GPG is now fully installed, configured, and ready for use!

15.8.4 Assignment: Install A Friend's Public Key

For you to send encrypted mail to someone else, it is necessary to have their *GPG Public Key*.

In this exercise, you find a friend's Public Key and add it to your GPG Keychain.

- Prerequisite: GPGTools must be installed.

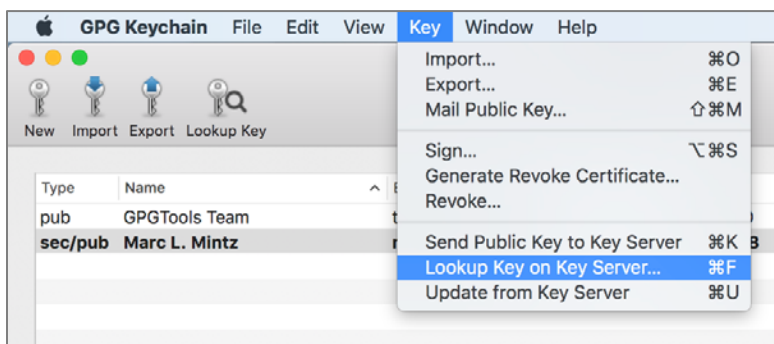
Option A: The No Sweat Strategy

The easiest way to add a friend's Public Key is to have them send to you an email from their GPG-enabled account (signed, but not encrypted.) Once you have their email, you also have their Public Key. But you may be listening a long time to crickets before they send you an email.

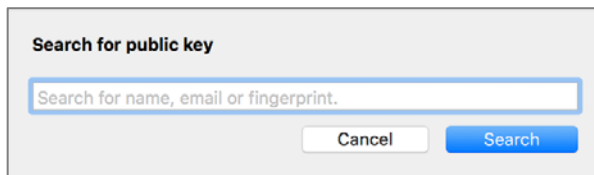
Option B: DIY

The Do It Yourself option is to lookup your friends key on a GPG key server.

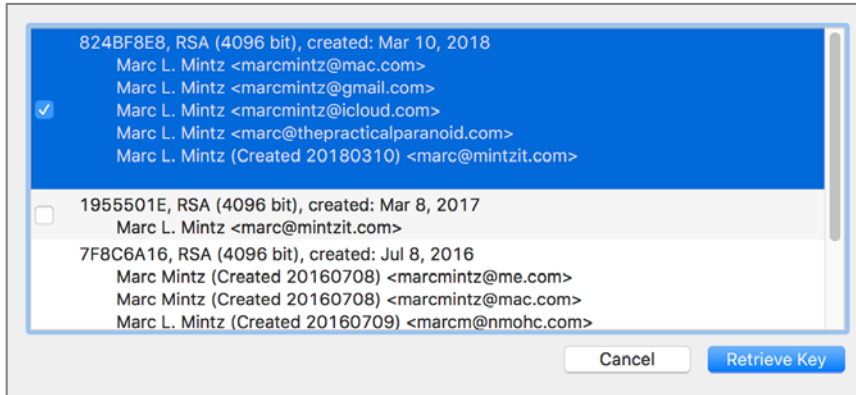
1. Open the *GPG Keychain Access.app* located in your */Applications/* folder.
2. Select *Key* menu > *Lookup key on key server*.



3. The *Search for public key* window opens.



4. Enter the full name of the person you wish to either send encrypted mail to, or receive from, and then select the *Search key* button. A list of possible matches appears. If you don't yet know anyone with a GPG key, feel free to use *Marc L. Mintz*. Shown below are the search results for a *Marc L. Mintz*.



5. the target public key (if you aren't sure which is correct, select all of them), and then select the *Retrieve key* button.
6. The Public Key is now added to your GPG Keychain.

You are now ready to send encrypted email to your friends!

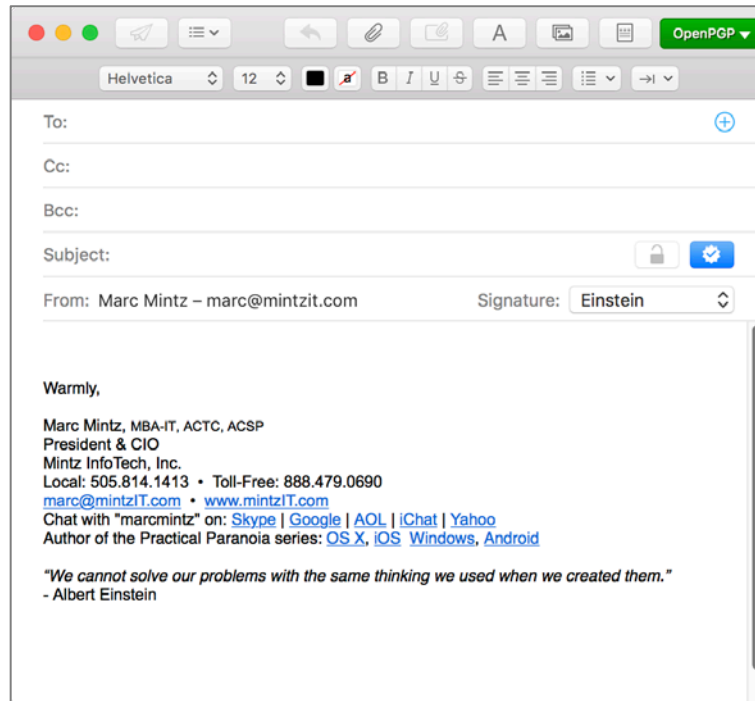
15.8.5 Assignment: Send A GPG-Encrypted And Signed Email

Once you have created your key and have the Public Key of the intended recipient from the previous assignments, you are ready to send your first encrypted and signed email.

In this assignment, you send your first GPG-encrypted and signed email.

1. Open your macOS *Mail.app*.

2. Create a new outgoing mail document. Notice that you have two new icons to the left of the *Subject* line.

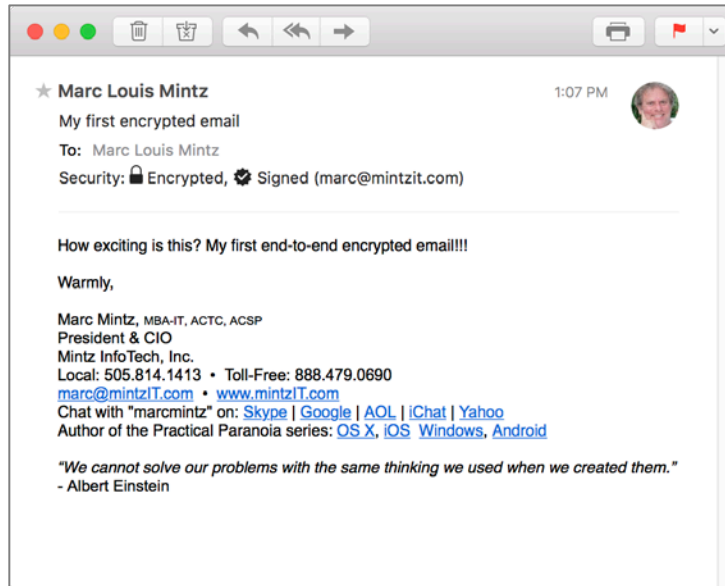


- *Lock* icon: Enables encryption for your document.
 - *Signed* (checkmark) icon: Enables signed emails. A signed email will notify the recipient if the message has been altered in any way between the sender and recipient.
3. In the *To:* field, enter the email address of someone with GPG enabled on their computer (feel free to use my address of marc@mintzit.com for your test). Once you have entered an email address that is registered with GPG (as you have done in the previous assignment), the *Lock* icon will turn blue, allowing selection/enabling.
 4. Verify the *Lock* icon is blue, indicating the email will be encrypted.
 5. Select the *Send* button, and your email is on its way to the recipient, fully secure because only the designated recipient will be able to read the email.
- Wahoo! You have sent your first securely encrypted email.

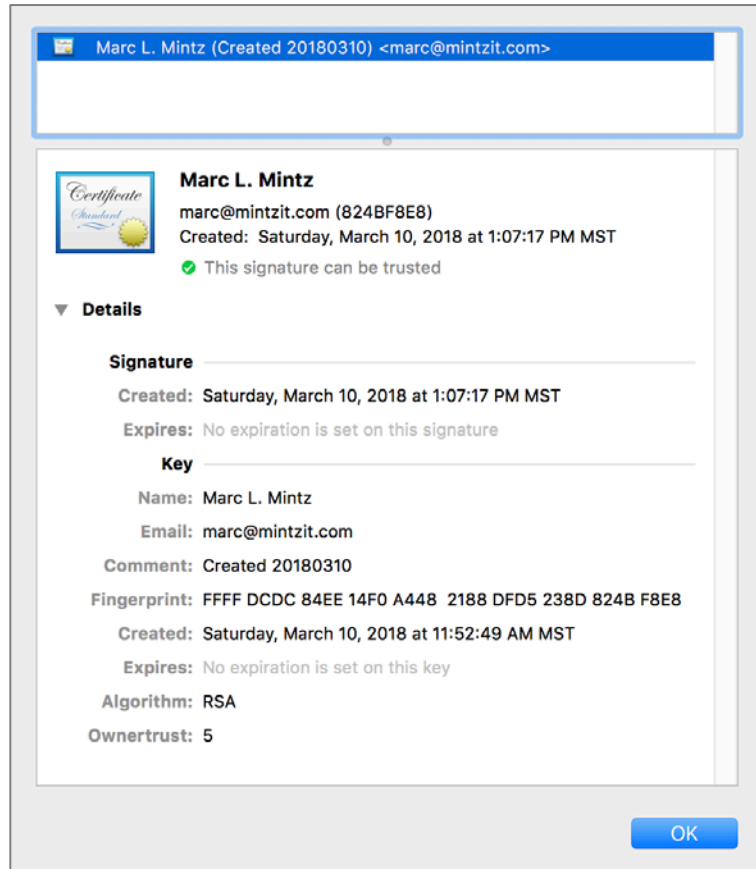
15.8.6 Assignment: Receive A GPG-Encrypted And Signed Email

In this assignment, you receive and read a GPG-encrypted and signed email.

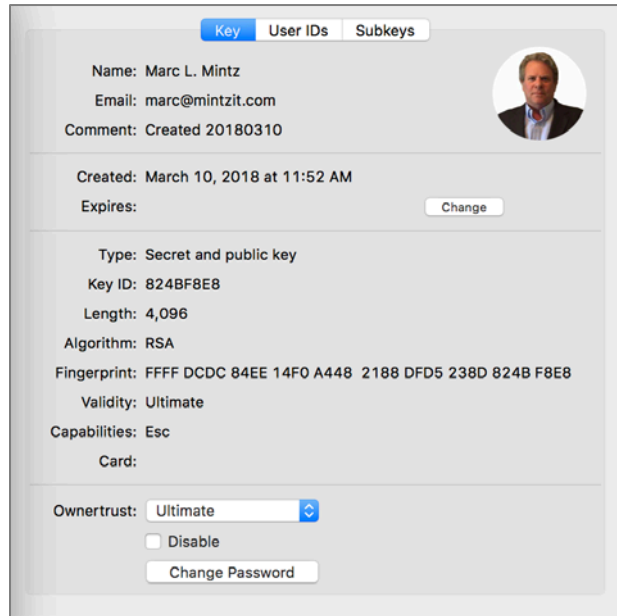
1. When the email arrives at the recipient, it automatically is decrypted (assuming the recipient also has followed the steps detailed in the *Get Your Friend's Public Key* assignment). The message will have an indicator if it is encrypted or signed or both.



2. Should the recipient have any doubts as to the authenticity of the email, click on the *Signed* icon. The certificate will display. Note the Short ID to the right of the sender's email address.



3. This Short ID can be verified. The recipient can open *GPG Keychain Access*, double-click the sender's name, and then view their *Short ID* in the pop-out window.



15.8.7 Assignment: Encrypt And Sign Files With GPGServices

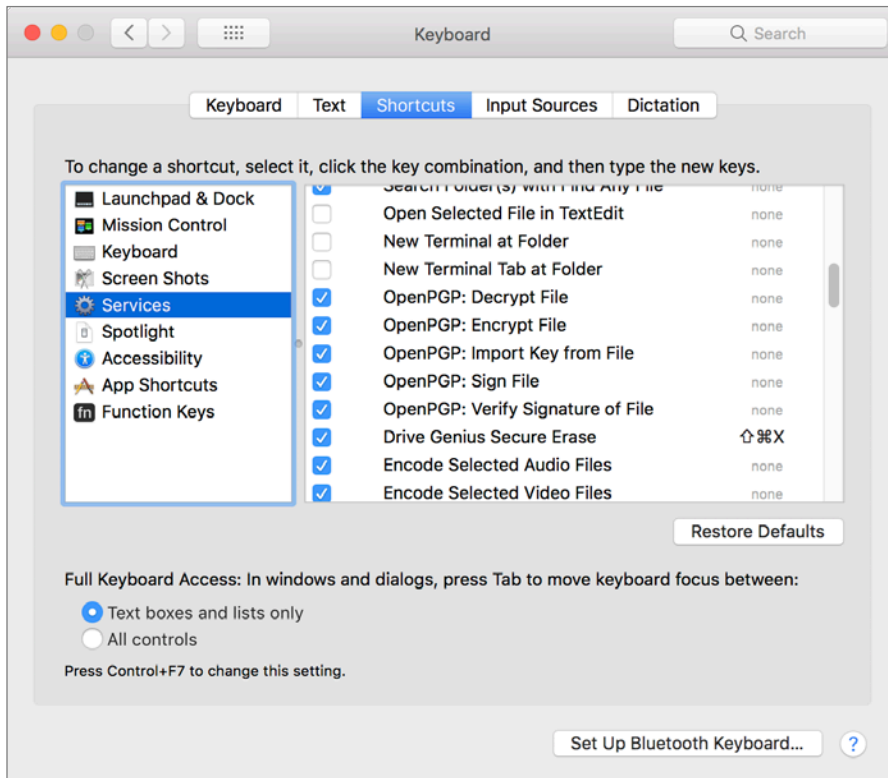
GPGServices allows encryption, decryption, and signing of any type of file for cross-platform use.

In this assignment, you encrypt and sign a file with GPGServices.

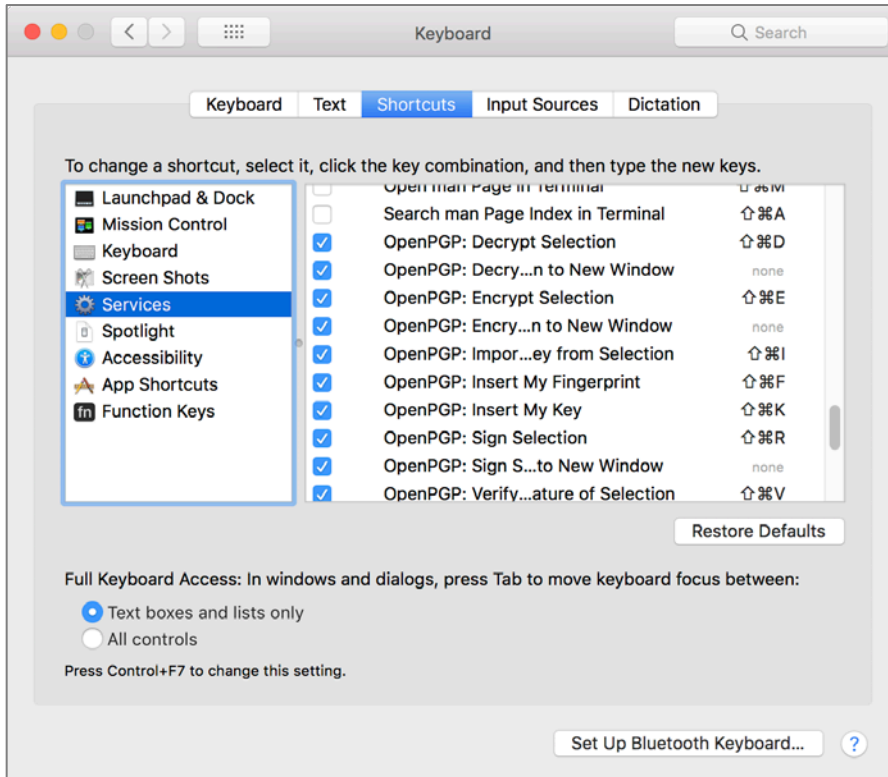
Verify All GPGServices Have Been Activated

1. Open *System Preferences* > *Keyboard* > *Shortcuts* tab > *Services* in sidebar.

- From under the *Files and Folders* group, verify that all *OpenPGP* modules are enabled.

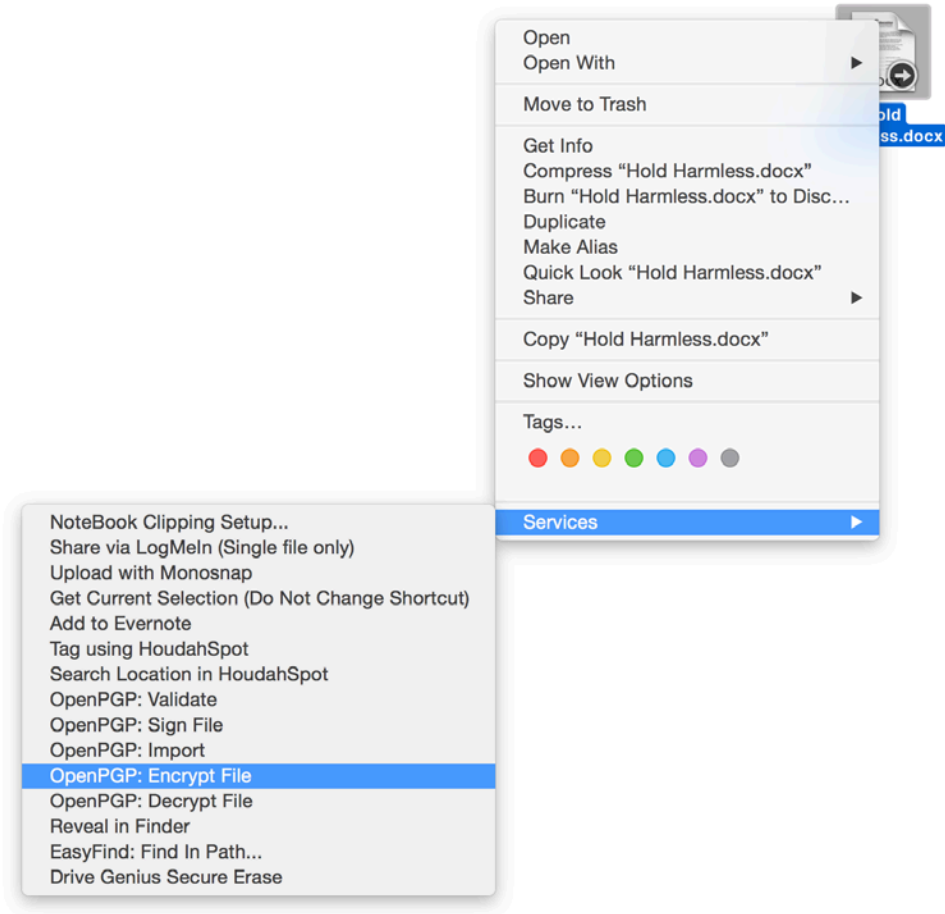


3. While still in the *System Preferences > Keyboard > Shortcuts* tab > *Services*, scroll down to the *Text* group, and then verify that all *OpenPGP* modules are enabled.

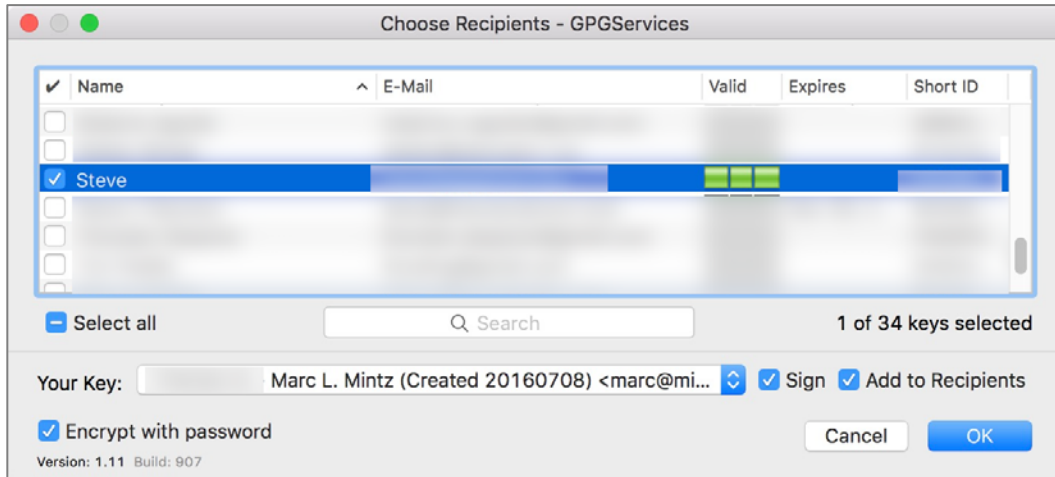


4. Close System Preferences.

5. To sign or encrypt a file or folder, right-click on it. From the pop-up menu, select *Services* > *OpenPGP: Encrypt File*.



6. The *Choose Recipients – GPGServices* window appears. Configure as:



- Enable the checkbox for those you wish to allow to access this encrypted file or folder.
 - Select which *Secret Key* will be used (which of your emails).
 - Enable the *Sign* checkbox so the recipient can validate the file/folder came from you.
 - You can further enhance security by enabling *Encrypt with password*. This will require the recipients to know a password in order to open the file.
7. Select the *OK* button.
 8. If you have enabled *Encrypt with password*, at the *Pinentry Mac* window, enter the desired password in the *Passphrase* field, and then select the *OK* button.
 9. You will be prompted a second time to enter the passphrase, do so, and then select the *OK* button.
 10. In a few seconds, the *Encryption Finished* window appears. Select the *OK* button.
 11. Your encrypted file will be found next to the original, with a *.gpg* file extension.

15 Email

This encrypted file can now be attached to an email, uploaded to a server, or placed on a storage device. Only the selected recipients will be able to open and view the file.

15.9 End-To-End Secure Email With S/MIME

*S/MIME*¹⁴ (Secure/Multipurpose Internet Mail Extensions) uses the same fundamental strategy of employing both Public and Private Keys to secure email as do PGP and GPG. Each person has a Private Key to decrypt a received email, and a Public Key that others may use to encrypt email to send out. An advantage of S/MIME over GPG is that S/MIME is built right into both the macOS/OS X and the iOS Mail.app. No need to install another application.

Unlike GPG, you will need to acquire an *email certificate* from a *Certificate Authority (CA)*. There are many Certificate Authorities available. Your Internet Provider or Web Host may be able to do this for you. Free certificates for personal use, which are valid for one year, are available. However, using these can become tedious, as you will need to repeat all the steps below every year. Purchasing a commercial certificate will set you back \$10 to \$100 per year, but you will only have to go through the process once.

Because your keys are stored with a CA, if that CA resides in a country that complies with USA National Security Letters, then it is possible for the US Government agencies to gain access to your private key, giving them full access to your email. Should you have concerns over the government having access to your communications, you should use either PGP/GPG, or S/MIME with a CA located in a country that does not comply with National Security Letters.

S/MIME offers three certificate classes:

- **Class 1:** This level of certificate is acquired without any background check or verification that the person requesting it has anything to do with the email address it will be assigned to. In fact, it is even possible to roll your own certificate! That said, it will verify that the email address in the *From* field is the address that sent the email, and do the job of encrypting email so that only the intended recipient can decrypt and read it.
- **Class 2:** This level takes it a step further, validating that not only is the email address in the *From* field the one that sent the email, but that the name in the *From* field is tied to that email address.

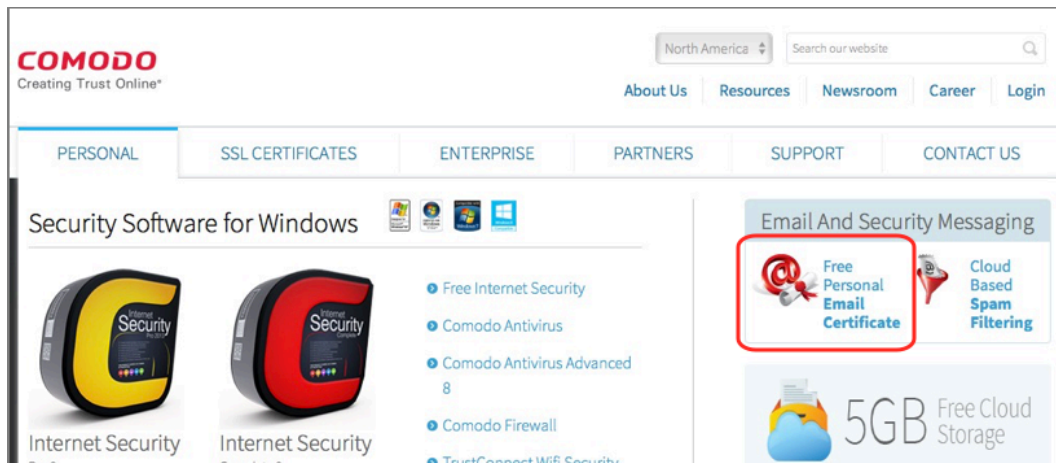
¹⁴ <http://en.wikipedia.org/wiki/S/MIME>

- **Class 3:** This is the highest-level validation, with a background check performed to verify not only the name of the individual or company, but physical address as well. **This is the only class suitable for healthcare (HIPAA), financial, legal, and business use.**

15.9.1 Assignment: Acquire A Free Class 1 S/MIME Certificate

In this assignment, you sign-up for a free 1-year free S/MIME certificate for personal use from a leading Certificate Authority, Comodo. This can be converted into a long-term commercial certificate.

- Note: A Class 1 certificate is appropriate for home users only. For business use, see the assignment to *Acquire a Class 3 S/MIME Certificate*.
1. Open your web browser and surf to Comodo at <https://comodo.com>.
 2. From the navigation bar, select the *Personal* tab > *Free Personal Email Certificate*.



3. This takes you to the *Email Security & Messaging* page. Select the *Free Email Certificate* > *Free Download* button.

4. The *Application for Secure Email Certificate* page opens. Complete the form, specifying *2048 (High Grade)* for your *Key Size*, and then select the *Next* button.

Application for Secure Email Certificate

Your Details

First Name

Last Name

Email Address

Country

United States

Private Key Options

Key Size (bits):

2048 (High Grade)

Note: Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)

Revocation Password

If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate:

Revocation Password

Comodo Newsletter

☒ Opt in?

Subscriber Agreement

Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.

Email Certificate Subscriber Agreement

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

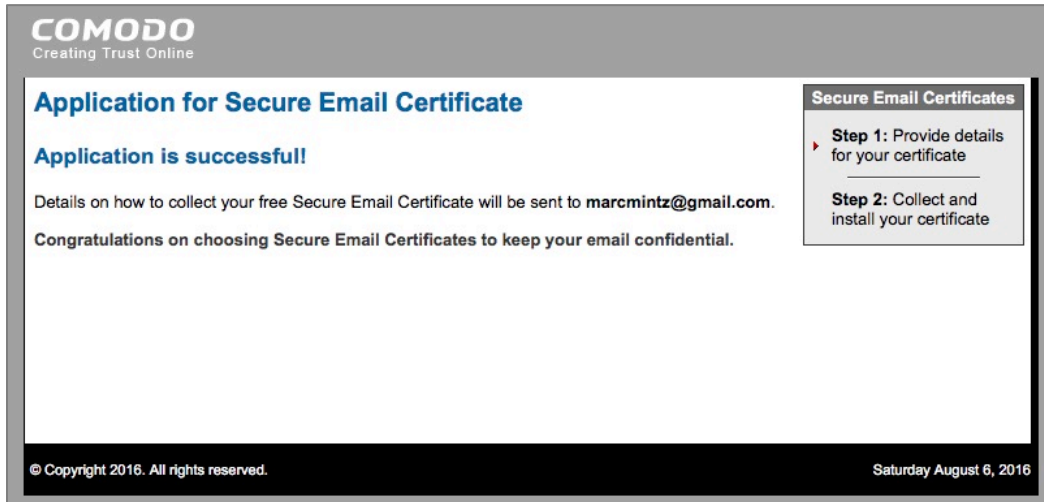
IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU ACCEPT THE TERMS AS PRESENTED, AND AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO EMAIL CERTIFICATE AND CLICK "DECLINE" BELOW.

1. Application of Terms

☐ I ACCEPT the terms of this Subscriber Agreement.

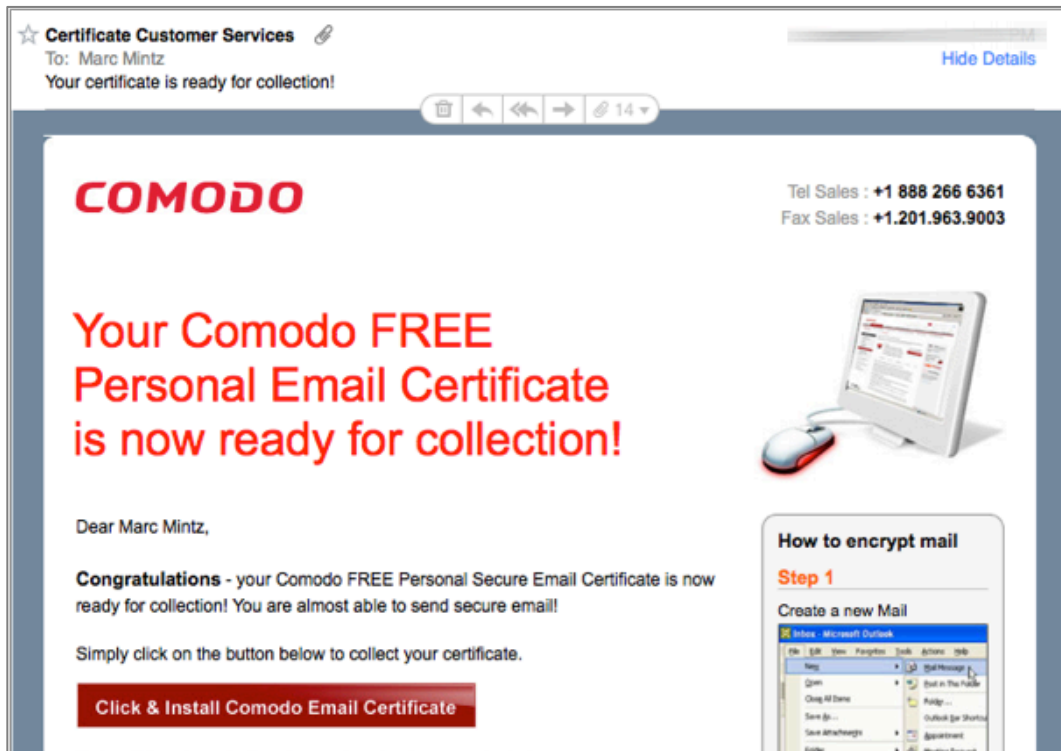
Next >

5. If all was completed correctly, you will see the *Application is Successful* page!



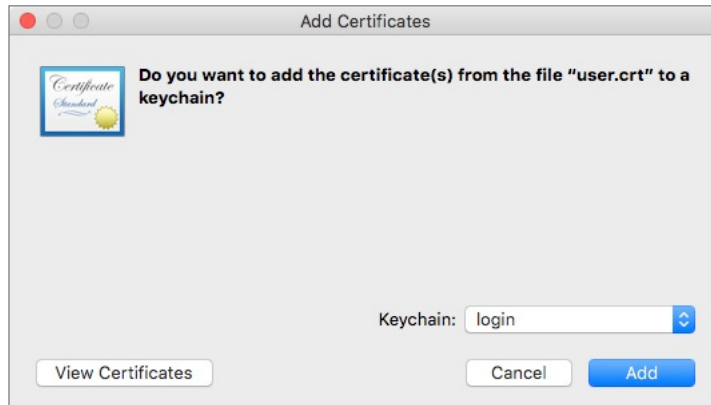
6. The certificate will be sent to the email address you specified.

7. Open your Mail.app to find the email, and then select the *Click & Install Comodo Email Certificate* button.



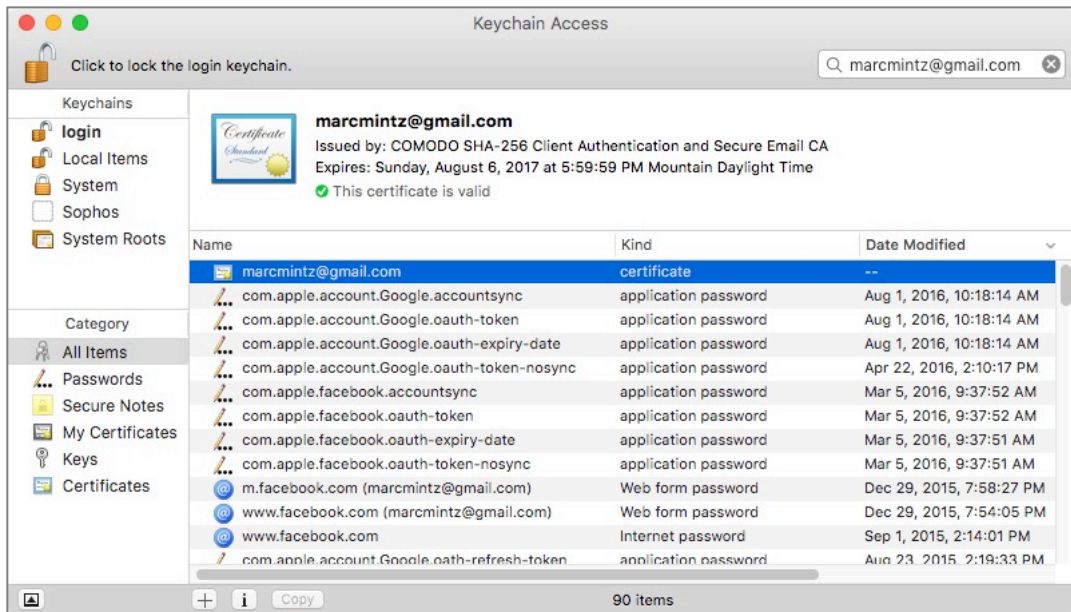
8. Although the button says *Click & Install Comodo Email Certificate*, all it does is download the certificate. You will need to manually install the certificate.
9. Once downloaded, the certificate will be found in your *Downloads* folder, named something like *user.crt*. Navigate in the Finder to your *Downloads* folder to find this certificate file.

10. Double-click the *CollectCCC.p7s* certificate. An *Add Certificates* window will open asking if you want to add the certificate to your Keychain. From the *Keychain* pop-up menu, select *Login*, and then select the *Add* button. This will add the certificate to your own default Keychain database,



Validate Certificate Installation

11. To quickly find the new certificate, in the Keychain Access utility, in the *Search* field, enter the email address for the new certificate, and then tap the *Return* or *Enter* key.



12. Double-click on the new certificate. This will open the certificate info window.
13. Quit the Keychain Access application.
14. Repeat steps 1-10 for each of your email addresses for which you need secure communications.

Wahoo! The hard part is over. You now are the proud owner (at least for a year) of email certificates for each of your email accounts. Next step is to migrate the certificate to your iOS device.

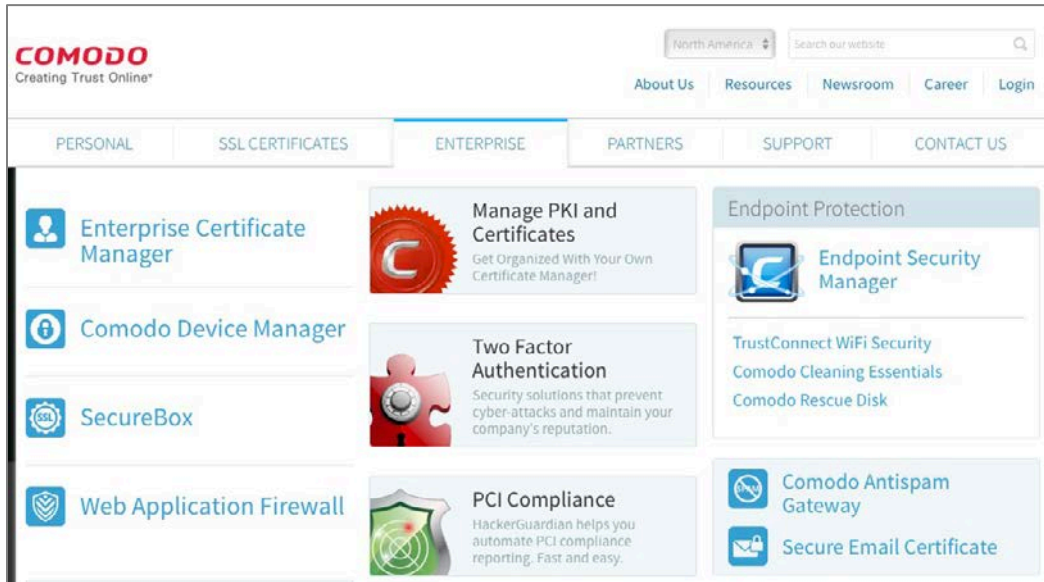
15.9.2 Assignment: Acquire A Class 3 S/MIME Certificate For Business Use

Getting a Class 3 certificate is significantly more involved than that of a Class 1. This is due to the need for identity verification, but also to the need for an infrastructure to help with managing potentially thousands of email addresses within an organization.

In this assignment, you acquire and configure a Class 3 S/MIME Certificate from Comodo.

- Note: A Class 3 S/MIME Certificate is appropriate for business use, but may also be used by home users
1. Using your web browser, visit *Comodo.com*

2. From the Navigation bar, select *Enterprise > Secure Email Certificate*.



3. In the *Secure Email Certificates* page, select the *Buy Now* button.

4. In the *Purchase Corporate Secure Email Digital Certificate* page, enter your desired *Term* and *Quantity*. And then select the *Next* button.

COMODO
Enterprise SSL

Country Region: North America
Fully validated, Enterprise SSL Certificates
[Secure Account Login](#)

[Products](#)
[Resellers](#)
[Comparisons](#)
[Corporate](#)
[Support](#)
[Contacts](#)

Products

Latest News: Mon, 28 Jul 2014 08:00:00 EST Comodo Strengthens Endpoint Security Capabilities with Comodo SecureBo...

Contact us to learn more
Contact us to learn how Comodo can further support your security needs, or to obtain **volume discount pricing**

Comodo Enterprise Sales
US: +1-888-256-2608
Int'l: +1-703-637-9361
Monday-Friday 9-5 EST

or email
EnterpriseSolutions@comodo.com

Purchase Corporate Secure Email Digital Certificate

Comodo email certificates are a proven way to secure all email communications in your organization.

By digitally signing and encrypting every email message, your business can ensure: Private Communications, Authenticated Communications and Message Integrity.

[Watch a video](#) on how to apply, install and use S/MIME Certificates.

Certificates as low as \$7 per year.
Purchase certificates and issue them as needed. Unused funds remain available.

Certificates as low as \$7 per year.
Contact us today or download our SecureEmail and PKI Certificate Management Made Easy to find out how Comodo SecureEmail and PKI Certificate Management can benefit your organization.

Certification Authorities

Certification Authorities

Per Certificate	1 Year	2 Year	3 Year
1 - 25	\$12.00	\$21.50	\$29.00
26 - 100	\$11.20	\$20.40	\$27.00
101 - 250	\$10.50	\$18.90	\$25.20
250 +	CALL	CALL	CALL

Term
Three Years

Quantity

Total Price

5. In the *Open an Enterprise S/MIME Enterprise PKI Manager (E-PKI) Account* window. Enter a domain name for your certificates, and then select the *Next* button.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Certification Authorities
Certification Authorities
Let's Encrypt

Enterprise PKI Manager (E-PKI)

Open an Enterprise S/MIME Enterprise PKI Manager (E-PKI) Account

Welcome to the Enterprise S/MIME E-PKI signup pages. Please complete the following steps to apply to open an Enterprise S/MIME E-PKI Account.

Email Domain Name (optional)
e.g. @acme.com

mintzit.com

Initial Prepayment Amount (USD)
Please refer to the below table to learn how prepayment amounts will determine your banding and in turn your discounts on Enterprise S/MIME products

Select Band	Deposit Amount	Prices
E-PKI S/MIME 1 - 25 Certs	\$12.00	View

Next >

Signup
1: Your E-PKI Details
2: Your Corp Details
3: Payment
4: Management

6. In the *Step 2: Your Corporate Details* page, enter all requested information, and then select the *Next* button.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Corporate Details

Step 2: Your Corporate Details
Required fields are displayed in RED.

Company Details - These must be your Registered Address

Company Name	<input type="text"/>
Dept	<input type="text"/>
PO Box	<input type="text"/>
Address 1	<input type="text"/>
Address 2	<input type="text"/>
Address 3	<input type="text"/>
City / Town	<input type="text"/>
State / Province / County	<input type="text"/>
Zip / Postcode	<input type="text"/>
Country	<input type="text" value="United States"/>
Company Number	<input type="text"/>
DUNS Number	<input type="text"/>
VAT Details <small>Please note that advertised prices are exclusive of Value Added Tax (VAT). VAT is only payable by EU companies:</small>	Enter VAT number, if applicable <input type="text"/>

Your Contact Details

If the following Admin Contact Details are incorrect, please amend with the correct details:

Title	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email Address	<input type="text"/>
Telephone Number	<input type="text"/>

☐ Click if you would like to provide additional Admin Contact details
☐ Click if your Billing Contact is different to your Admin Contact
☐ Click if you would also like to provide an Organisational Contact
☐ Click if your Trading Address is different to the Address provided in the Company Details

Choose your Admin Contact's Management Details

Username (min 6 characters)	<input type="text"/>
Password (min 8 characters)	<input type="password"/>
Confirm Password (re-enter)	<input type="password"/>

Rules Password

Cancel & Start Again Next >

7. At the *Agreement* page, select the *I ACCEPT* button.

8. In the *Secure Payment Page*, enter your credit card information, and then select the *Make Payment* button.
9. You will receive an email from Comodo informing you of receipt of your order, and stating that you will soon be receiving another email requesting documents to validate your identity.
10. Soon you will receive an email requesting the validation documents. Submit the requested documents and information.
11. You will receive an email informing you that your account has been created, with a link to their *Getting Started Guide*. Although the steps outlined in this book will take you through the process, it is not a bad idea to download and read the Guide as well. Download the *Getting Started Guide*.
12. Register for Comodo technical support by clicking the link provided in the email, and then follow the on-screen instructions. This will save you significant time and headache if you ever need technical support from Comodo.

15.9.3 Assignment: Purchase A Class 3 S/MIME Certificate For Business Use

Once you have set up your Class 3 business account with Comodo, you are able to order S/MIME certificates for you and your staff at any time.

In this exercise, you purchase your first certificate.

1. From your web browser, go to the Comodo home page at <https://comodo.com>.
2. Select the *Login* link, and then login. This opens the *SSL CA Providers Comodo Account Management* page.

3. In the *Comodo Certificate Authority* area, enter your *Username* and *Password* used to start your account with Comodo, and then select the *Log on* button.

COMODO
Creating Trust Online®

SSL CA Providers Comodo Account Management

SSL provider Comodo Member Login

Comodo Certificate Authority

Log in to your Comodo Account to manage your subscriptions and services for **SSL** and E-mail Certificates, PCI Compliance, Authentication and PKI Management products.

Username:
marc@mintz.it.com

Password:

Log on

Comodo Security Solutions

Click the button below to log in to your Comodo Account to manage your subscription and services for Comodo Internet Security, Antivirus Advanced, TrustConnect, Online Storage, GeekBuddy, LivePCsupport, System Utilities, Antispam Gateway and Endpoint Security Manager.

Click Here

4. The *Account Options: Management* window opens. Select the *E-PKI Manager* link.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Logout

Account Options: Management

Welcome:
Marc Mintz
Mintz InfoTech, Inc.

My Account Areas:

- E-PKI Manager**
Place orders through your E-PKI Manager
- IdAuthority**
Add / Update details of your website(s) in the IdAuthority

My Account Summary:

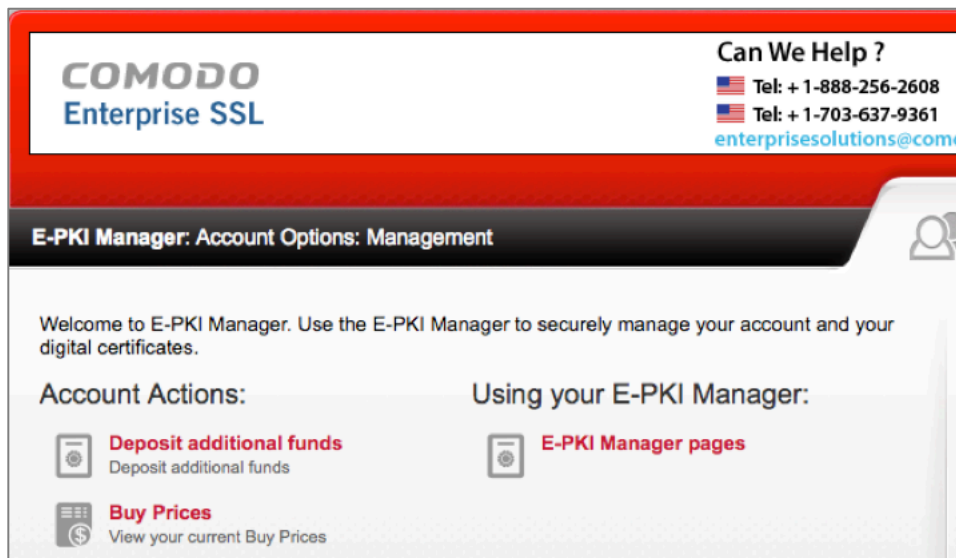
Last Login Time
21-NOV-2014 04:33:40 (UTC)

Status
Active

Verification Level
Class 3

5. This will take you to the *E-PKI Manager: Account Options: Management* page. With Comodo, you pay for certificates not directly, but by pulling from

monies on deposit with Comodo. If there are inadequate funds on deposit, you will need to deposit money now. To do so, select the *Deposit additional funds* link.



6. In the *Deposit Funds: Account Options: Management* page, enter at least the amount needed to purchase your S/MIME certificates. Rates per certificate as of this writing are.

Per Certificate	1 Year	2 Year	3 Year
1 - 25	\$12.00	\$21.50	\$29.00
26 - 100	\$11.20	\$20.40	\$27.00
101 - 250	\$10.50	\$18.90	\$25.20
250 +	CALL	CALL	CALL

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Deposit Funds: Account Options: Management

Welcome:
Marc Mintz
Mintz InfoTech, Inc.

Your Current Credit is: **\$0.00**

How much would you like to deposit (US Dollar)?

Cancel Next >

7. In the *Secure Payment* page enter your credit card information, and then select the *Make Payment* button.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Secure Payment

Secure Payment Page
Your Order Number: [blurred]
Total Amount: [blurred]

Required fields are displayed in RED.

Card Details

Card Number: [input]
Card Code (3 or 4 digits): [input]
Expiry Date: [date picker]
Cardholder's Name: Marc Mintz

Cardholder Address and Contact Details

Company Name: Mintz InfoTech, Inc.
Address 1: 7000 Phoenix Ave NE
City / Town: Albuquerque
State / Province / County: NM
Zip / Postcode: 87110
Country: United States
Phone: 888.479.0690
Email: marc@mintzit.com

Cancel & Start Again Make Payment

8. Return to the *Account Options: Management* page, and then select the *E-PKI Manager* link.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Account Options: Management

My Account Areas:

E-PKI Manager
Place orders through your E-PKI Manager

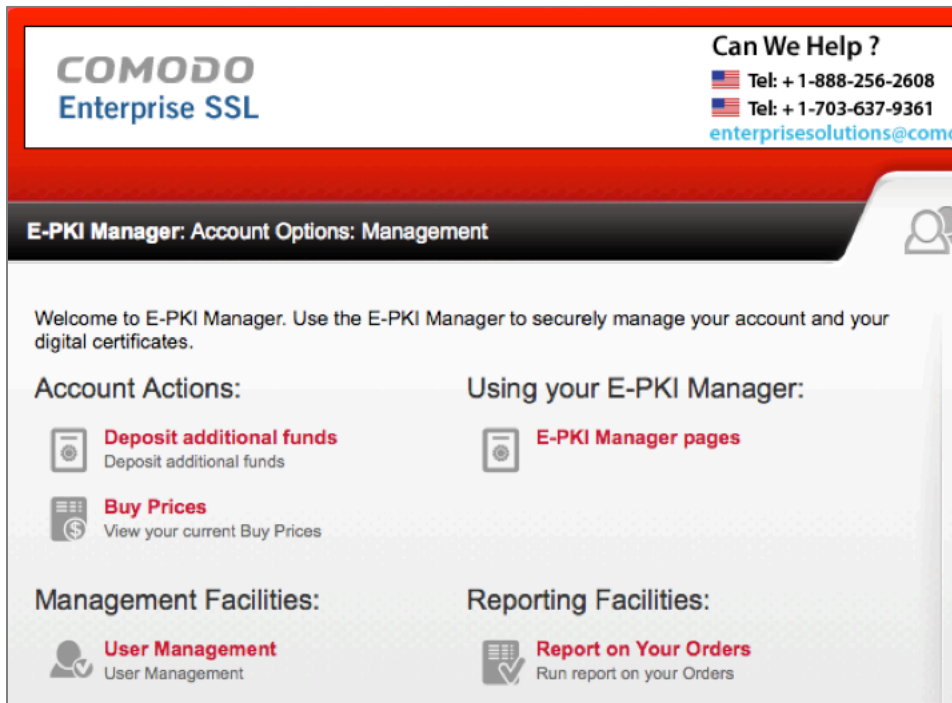
IdAuthority
Add / Update details of your website(s) in the IdAuthority

My Account Summary:
Last Login Time
21-NOV-2014 04:33:40 (UTC)
Status
Active
Verification Level
Class 3

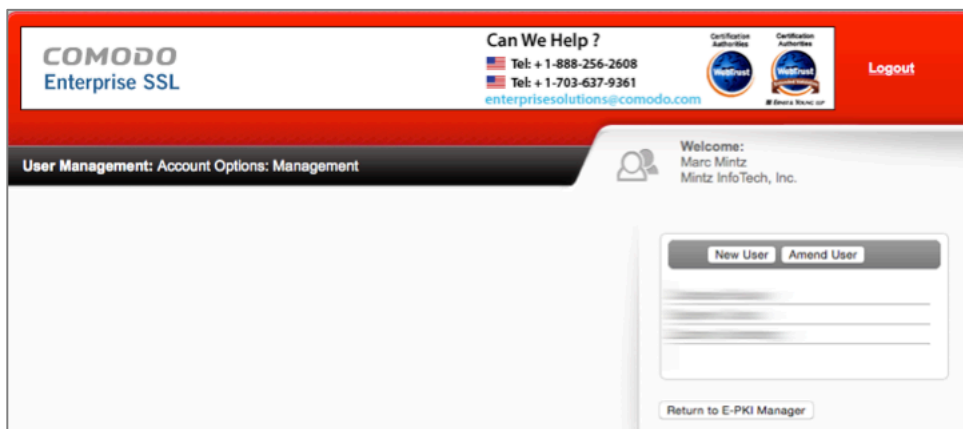
Welcome:
Marc Mintz
Mintz InfoTech, Inc.

Logout


9. In the *E-PKI Manager: Account Options: Management* page, select the *User Management* link.



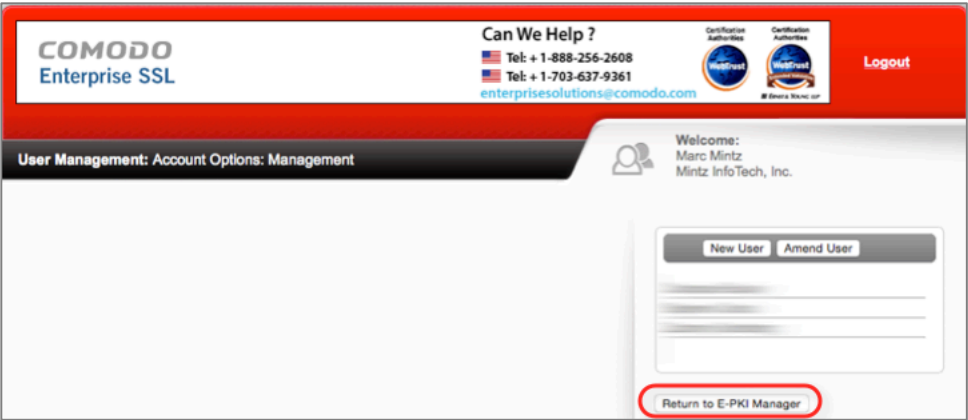
10. In the *User Management: Account Options: Management* page, select the *New User* button.



11. In the *New User* window, enter all information for your new user, and then select the *Save Changes* button.

User Details	
Title	<input type="text"/>
First Name	<input type="text"/>
Surname	<input type="text"/>
Email Address	<input type="text"/>
Telephone No.	<input type="text"/>
Fax No.	<input type="text"/>
Is Active?	<input checked="" type="checkbox"/>
Login Name	<input type="text"/>
Password	<input type="password"/>
Password Confirmation	<input type="password"/>
Is Api User? Enabling this will disable the users Order Management Link.	<input type="checkbox"/>
User Address	
Department	<input type="text"/>
PO Box	<input type="text"/>
Street Address 1	7000 Phoenix Ave NE
Street Address 2	310
Street Address 3	<input type="text"/>
City	Albuquerque
State / Province / County	NM
Postal / Zip Code	87110
Country	United States 
<input type="button" value="Cancel"/> <input type="button" value="Save Changes"/>	

12. Repeat steps 7-10 to enable each user/email account to have an S/MIME certificate.
13. When all certificates have been requested, return to the *User Management: Account Options: Management* window, and then select the *Return to E-PKI Manager* button.





14. In the *E-PKI Manager: Account Options: Management* page, scroll to the bottom, and then select the *Corporate Secure Email Certificate Buy* button.


E-PKI Manager: Account Options: Management

Welcome to E-PKI Manager. Use the E-PKI Manager to securely manage your account and your digital certificates.


Account Actions:

-  **Deposit additional funds**
Deposit additional funds
-  **Buy Prices**
View your current Buy Prices


Using your E-PKI Manager:

-  **E-PKI Manager pages**

Management Facilities:

-  **User Management**
User Management

Reporting Facilities:


-  **Report on Your Orders**
Run report on your Orders

Customer Order Options:

Apply for a new product through your E-PKI Manager:

Product	
Corporate Secure Email Certificate	BUY
Personal Authentication Certificate	BUY

15. In the *Corporate Secure Email Certificate: E-PKI Manager: Management* page, complete the information for the user/email address you wish to assign an S/MIME certificate, and then select the *Submit* button.




Can We Help ?

Tel: + 1-888-256-2608


Tel: + 1-703-637-9361

enterprisesolutions@comodo.com




[Logout](#)

Corporate Secure Email Certificate: E-PKI Manager: Management



Welcome:
Marc Mintz
Mintz InfoTech, Inc.

Your Current Credit is: 

User Details

1. Email Address	<input type="text" value="marc@mintzit.com"/>
Example: username@	<p>You may only apply for Corporate Secure Email Certificates containing domain names for which your right of use has been validated. If your required domain name does not appear in the above list, you may submit it for validation by clicking here to register an IdAuthority Website.</p>
2. First Name	<input type="text" value="Marc"/>
3. Last Name	<input type="text" value="Mintz"/>
<input checked="" type="checkbox"/>	I confirm that the above individual is an employee / authorized representative of Mintz InfoTech, Inc. and is permitted to use the above email address for email communication.

Advanced Security Options

(Only applicable if the User will obtain their Certificate using Internet Explorer)

4. Cryptographic Service Provider	<input type="text" value="Microsoft Enhanced Cryptographic Provider v1.0"/>
5. Is Private Key "User-Protected"?	<input type="checkbox"/>
6. Is Private Key "Exportable"?	<input checked="" type="checkbox"/>

Certificate validity period

7. Select the validity period for your Certificate:	<div>1 year</div> <div>2 years</div> <div>3 years</div>
---	---

Total Cost: **\$12.00**

16. At the *Order Confirmation: E-PKI Manager: Management* page, print your receipt, and then select the *Management Area...* button.

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Order Confirmation: E-PKI Manager: Management

We advise you to print this page for your records.
Thank you for placing your order. Your Order Number is 15552626. Please quote this Order Number in all correspondence. You have purchased:

Product	Value
Corporate Secure Email Certificate for marc@mintztl.com	\$12.00
Total Value	\$12.00

Your Account has been debited by \$12.00.
A collection email will shortly be sent to marc@mintztl.com.
A confirmation email will shortly be sent to marc@mintztl.com.
Comodo Contact Details:
Support Telephone: +1.888.266.6361 / +1.703.581.6361
Support Website: <http://support.comodo.com>
Validation Docs Fax: US and Canada +1.866.831.5837 / Worldwide +1.801.303.9291

We now operate a registration-based system for support.
Please submit your ticket at the [support website](http://support.comodo.com).

Comodo Group, Inc. - US Office
1255 Broad Street
Clifton, NJ 07013-3398
United States

Comodo CA Limited - European Office
26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom

Comodo offers essential infrastructure to enable e-merchants, and other Internet-connected companies, software providers, and individual consumers to interact and conduct business via the Internet safely and securely. Our PKI solutions, including [SSL Certificates](#), [EV SSL Certificates](#), [Code Signing Certificates](#) as well as [Secure E-Mail Certificates](#), increase consumer trust in transacting business online, secure information through strong SSL encryption, and satisfy many industry best practices or security compliance requirements.
You may now go to the Management Area for further options. Or you may log into your account at any time to use the Management Area.

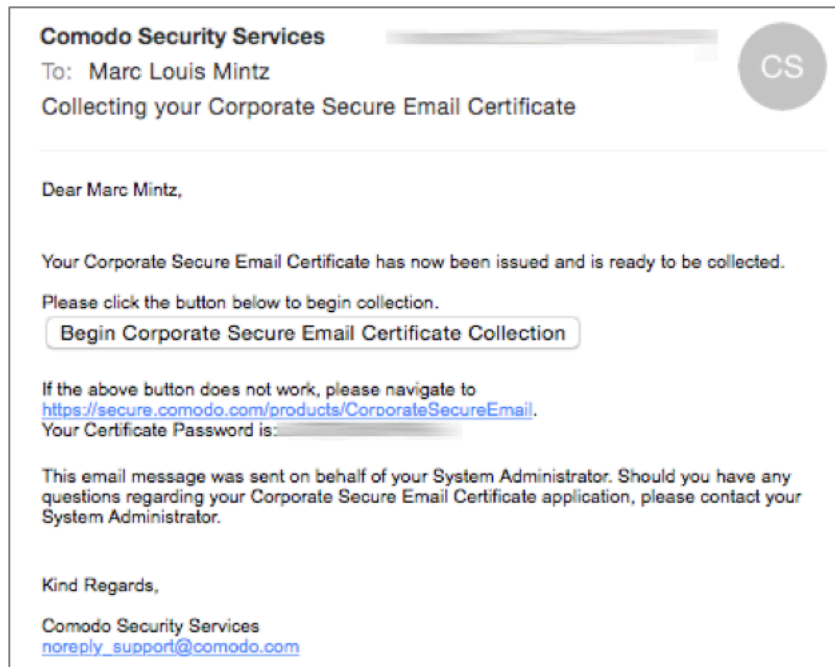
[Management Area...](#)

17. Repeat steps 13-15 for each user/email account to be assigned an S/MIME certificate.

15.9.4 Assignment: Install A Business S/MIME Certificate

In this assignment, you download and install a Class 3 S/MIME Certificate.

1. At the user's computer, check email for a message from Comodo, select and copy the *Your Certificate Password*, and then select the *Begin Corporate Secure Email Certificate Application* button.



2. In the *Corporate Secure Email Certificate Center*:

- Enter the **exact same email address** as used during the certificate creation.
- Paste in the *Certificate Password* that was included in the Comodo email sent to the email address.
- Enable the *I Accept* checkbox.
- Select the *Submit & Continue* button.

Corporate Secure Email Certificate Center

User Details:

Please enter the following details:

Email Address

Certificate Password

Subscriber Agreement

Please read this Subscriber Agreement before applying for your certificate. If you do not agree to the terms of this Subscriber Agreement, do not click the "I ACCEPT" tickbox.

Email Certificate Subscriber Agreement

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

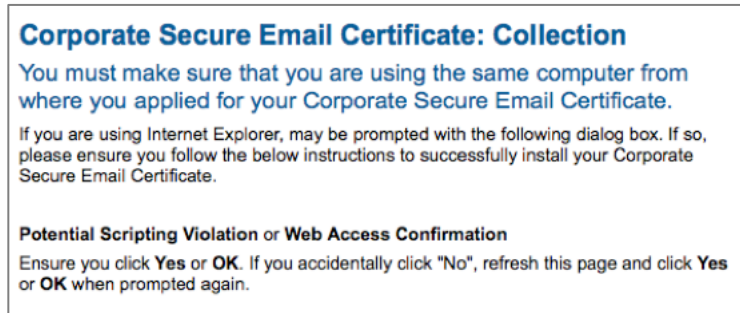
IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, THAT YOU ACCEPT THE TERMS AS PRESENTED, AND AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO EMAIL CERTIFICATE AND CLICK "DECLINE" BELOW.

1. Application of Terms

☐ **I ACCEPT** the terms of this Subscriber Agreement.

Submit & Continue

3. The *Corporate Secure Email Certificate: Collection* page will open; your certificate will be generated and begin to download.



4. When the certificate has been generated, it will start downloading. When downloaded, you will find it in your *Downloads* folder named something like *CollectCCC.p7s*.
5. Open your *Downloads* folder and locate the *CollectCCC.p7s* file.
6. To install your S/MIME certificate into the *Keychain Access.app*, double-click on the *CollectCCC.p7s* file.
7. The *Add Certificates* window may open. Select *Keychain: login*, and then select the *Add* button.
8. *Quit* Keychain Access.
9. Quit the Mail.app.
10. *Open* the Mail.app. This forces the Mail application to search for new certificates.
11. If you use multiple computers, place a copy of your *CollectCCC.p7s* file on each of your computers, and repeat steps 6-10.

Your S/MIME certificate, which includes both your *Public Key* (used by others to encrypt email to you) and *Private Key* (used by you to decrypt email received by you) is now installed.

15.9.5 Assignment: Exchange Public Keys With Others

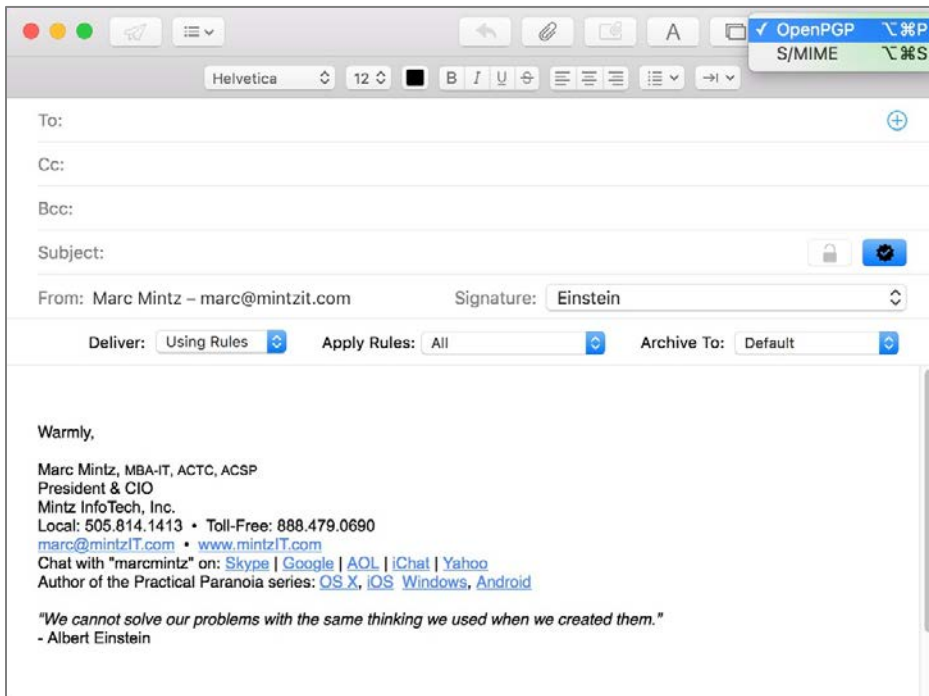
Before you can send or receive encrypted email with others, you need to exchange Public Keys with each other. This is as simple as sending a signed email to each

other. To start, you send a signed email to a friend. This gives this recipient your Public Key, as well as instructions for the recipient to set up S/MIME on their own system.

In this assignment, you send a friend your public key.

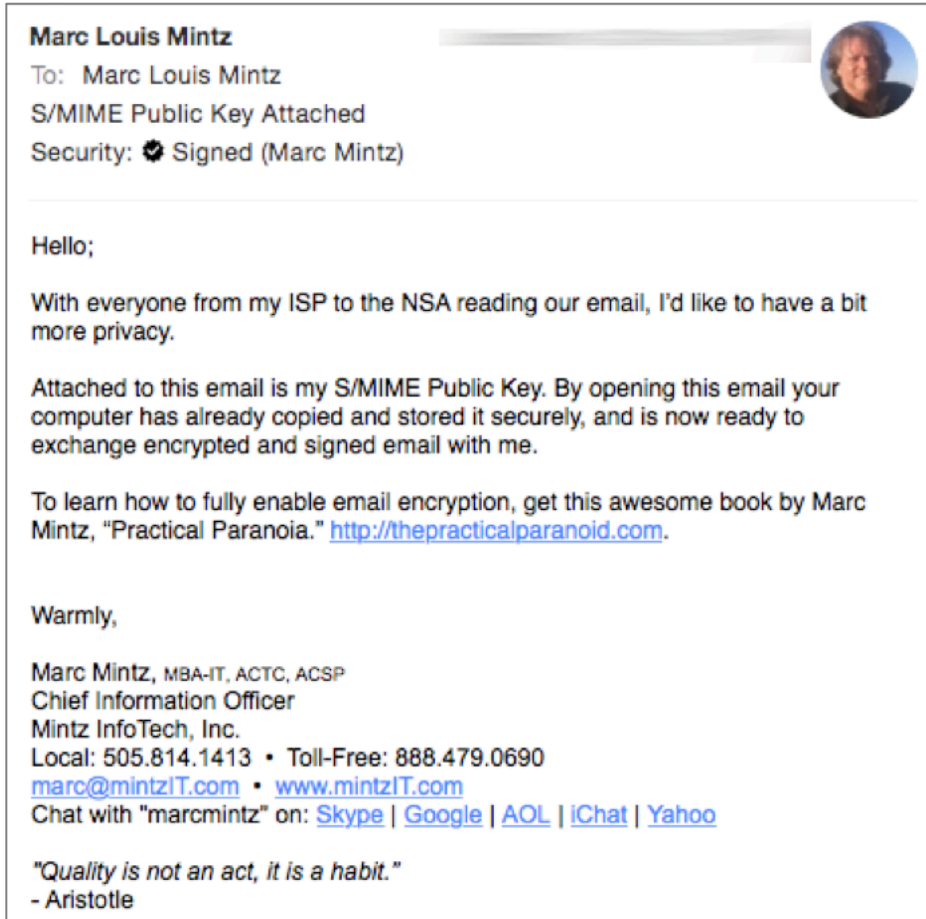
1. From a computer that now has your newly acquired email certificates, *Open the Mail.app*. This process forces *Mail.app* to look for new certificates.
2. Select the *File* menu > *New Message*.
3. From the *From:* pop-up menu, select the email account with the new certificates. (If you have only one email account, the *From* field typically does not appear.)
4. At the bottom right of the header area, note the two new icons—an encryption lock and signed check. If you have performed the earlier GPG assignments, these are the same and are shared between the two systems. The lock becomes available when you have the Public Key of the recipient, allowing for encryption. The check is available for anyone once you have your certificate. It will verify that the sender (you) are who you say you are.
5. If you have performed the earlier GPG assignments, the drop-down menu at the top right corner allows you to select either GPG or S/MIME as your

encryption protocol. If you have not performed the earlier GPG assignments, this menu is absent.



6. Address your email to an associate with whom you would like to be able to exchange encrypted email. Feel free to address the email to me at *marc@mintzit.com*.
7. If you have installed both PGP and S/MIME, ensure the *S/MIME* is the selected protocol, and that the *S/MIME signed check* is enabled (it should be by default.) This will ensure your Public Key is sent to your designated recipient.
8. In the Subject line, be clear about the intent of the email by noting something like: *S/MIME Public Key Attached*.
9. In the body area, you may want to include instructions for how to acquire an email certificate—or better yet—point to this book at its website *http://thepracticalparanoid.com*.

10. When the recipient receives and opens the email, that recipient now has your Public Key and can determine that the email truly did come from you due to your signing the email with your certificate.



11. The recipient then needs to repeat the steps in this and the previous assignments to acquire an email certificate, and then send a signed email to you. Once this is done, the two of you may exchange encrypted email.

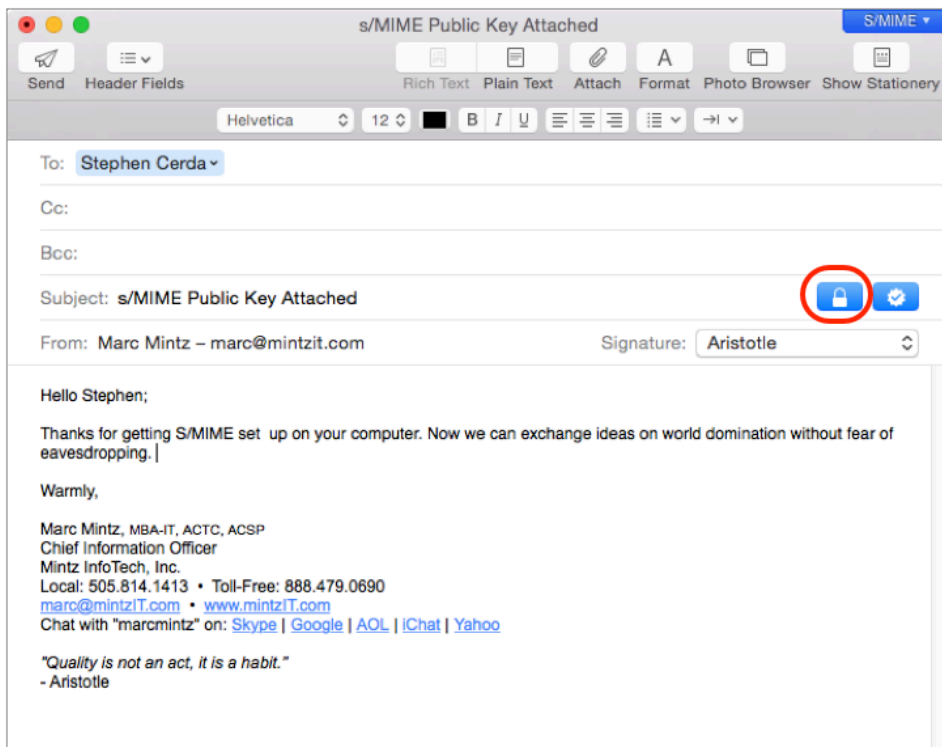
15.9.6 Assignment: Send S/MIME Encrypted Email

To exchange encrypted email using S/MIME, the previous assignments must be completed by yourself and at least one other person with whom you wish to have

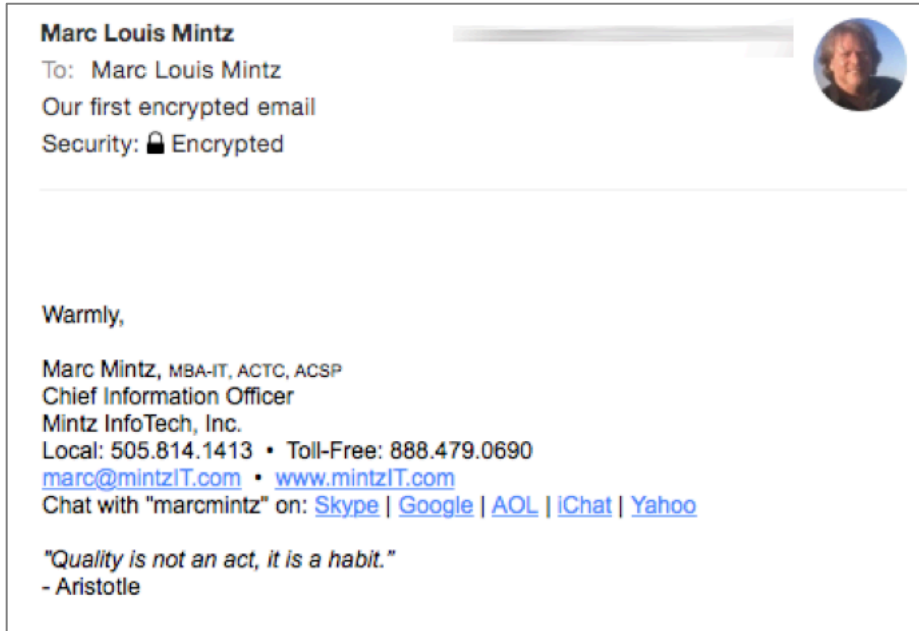
secure communication. Once done, each has an email certificate, a private key, and a public key that is embedded in the other's computer.

In this assignment, you send your first S/MIME encrypted email.

1. Open your *Mail.app*.
2. Create a new message, addressed to someone with whom you share public keys.
3. If you have also installed GPG, set the *GPG-S/MIME* menu in the top right corner of the message to *S/MIME*.
4. Enable the *encrypted* lock icon in the bottom right area of the message header.



5. Send the message. When received by the recipient, the message is instantly and automatically decrypted, and the recipient gets a notice that the message is encrypted as well as signed.



Congratulations! You are now able to send and receive securely encrypted email using the S/MIME protocol.

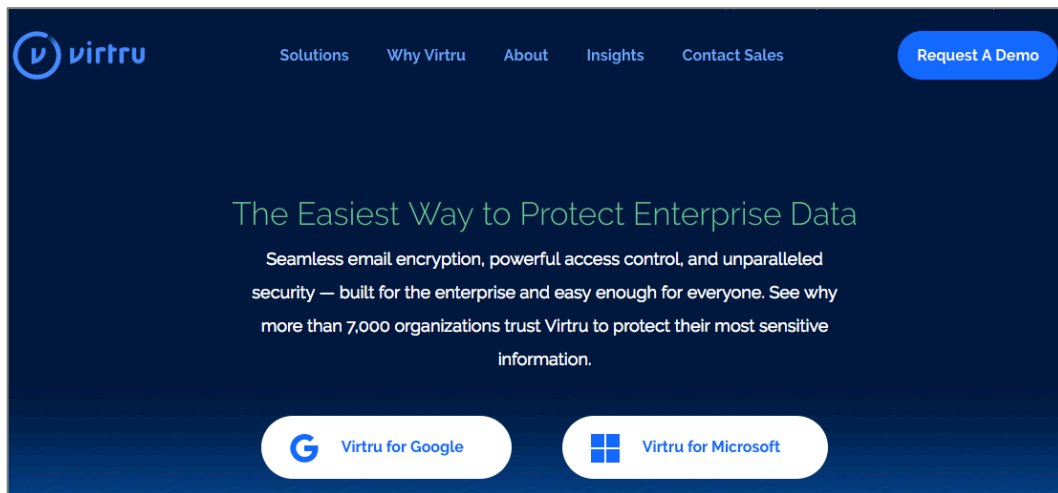
15.10 Virtru Email Encryption

Although PGP/GPG and S/MIME are excellent, highly secure options, they do need some expertise and time to install and configure, and require that both the sender and recipient have the same protocol installed.

For many businesses, that is simply a deal breaker.

If you or your organization use Gmail, Google G-Suite (previously Google Apps for Work) or Microsoft Outlook (currently Windows only), another excellent, highly secure option is *Virtru*¹⁵. Virtru only requires that the sender have a Virtru account, the recipient still can read the encrypted email, as well as any attached encrypted documents.

Virtru offers free accounts for personal use, and for-fee business accounts. The free account works with Gmail and G-Suite mail through the web interface. The business accounts work with Gmail, Google mail, and Microsoft Outlook.



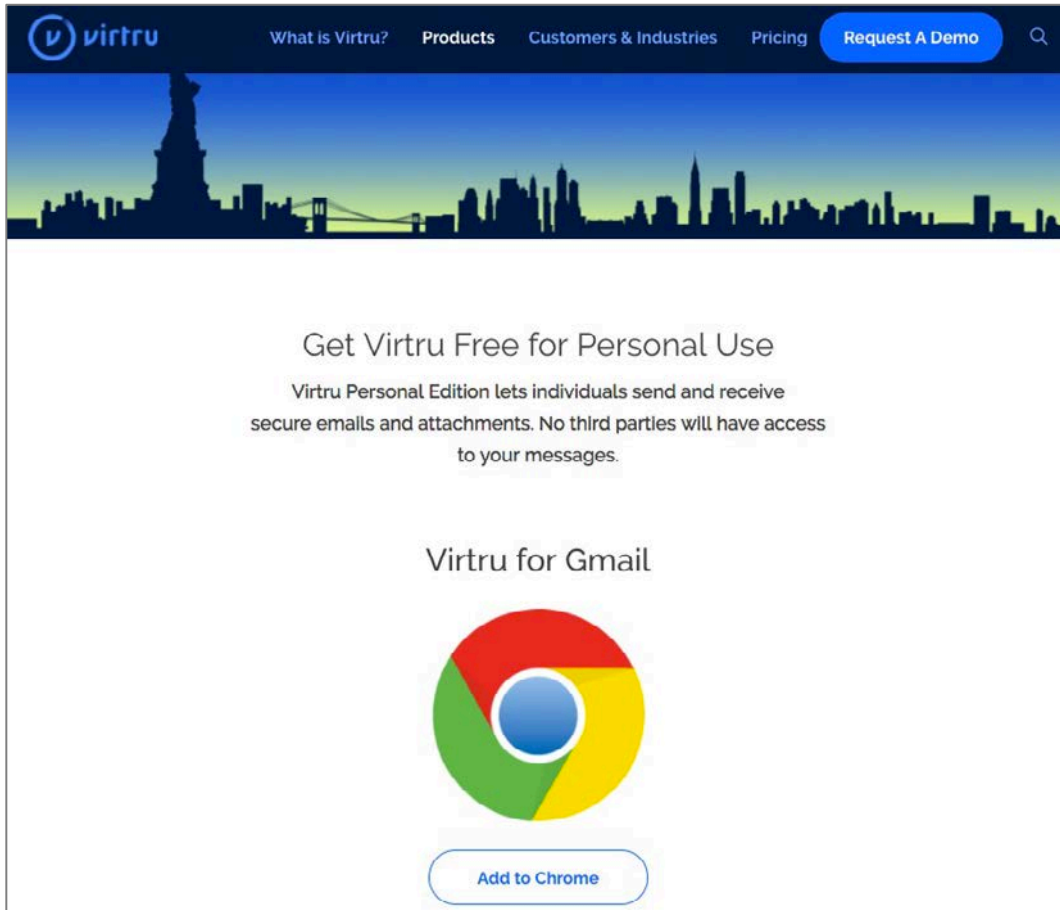
¹⁵ <https://virtru.com/>

15.10.1 Assignment: Create A Free Virtru For Gmail Account

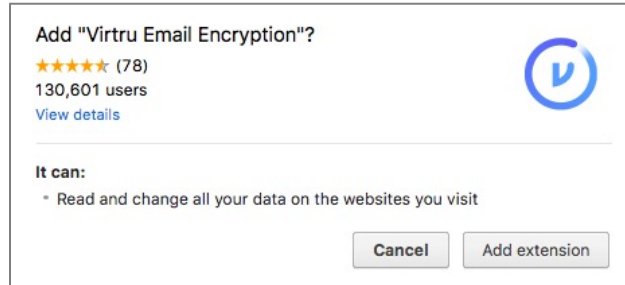
A free Virtru account is perfect for personal use with your existing Gmail account. You will immediately be able to send fully encrypted email and attachments to friends and family, without a need for them to do any additional work!

In this assignment, you create a free Virtru account.

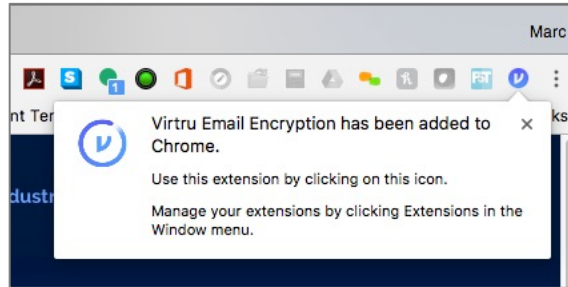
- Prerequisite: Must have a Gmail or Google G-Suite account, and use Google web mail.
1. Open Google Chrome, and visit <https://www.virtru.com/secure-email/>.



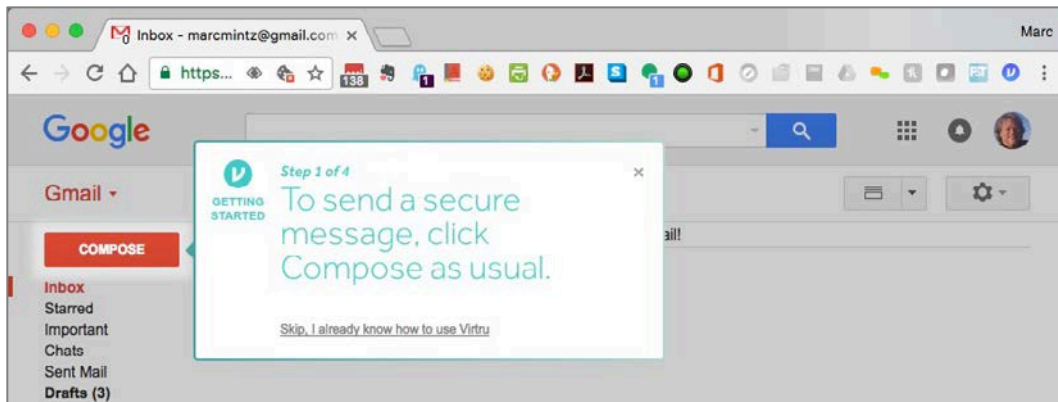
2. Click the *Add to Chrome* button.
3. The *Add "Virtru Email Encryption"* window appears. Click the *Add extension* button.



4. A pop-up will appear, showing the new Virtru Chrome icon.

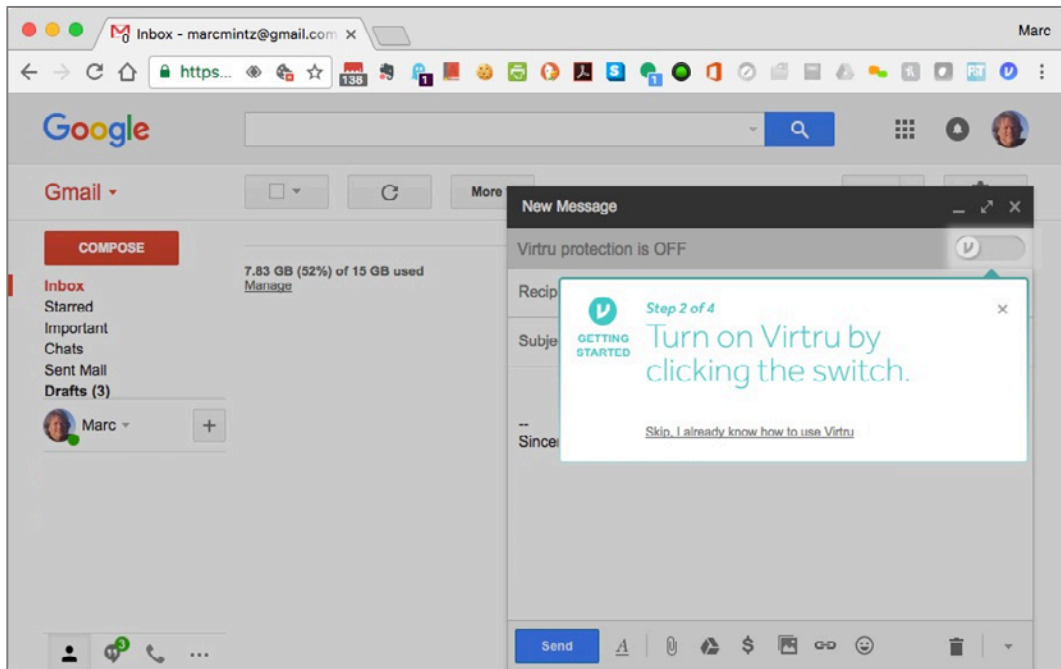


5. In Chrome, go to your Gmail account at <https://mail.google.com>, and then sign in.
6. You will see a *Step 1 of 4* alert. Following the instructions of the alert, click the *Compose* button.

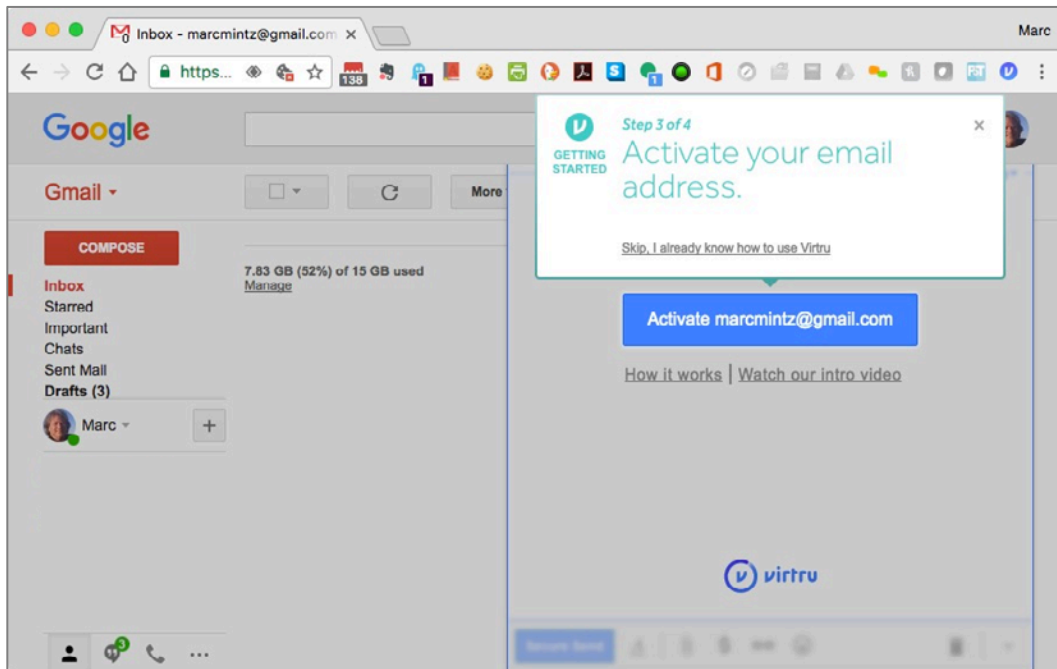


15 Email

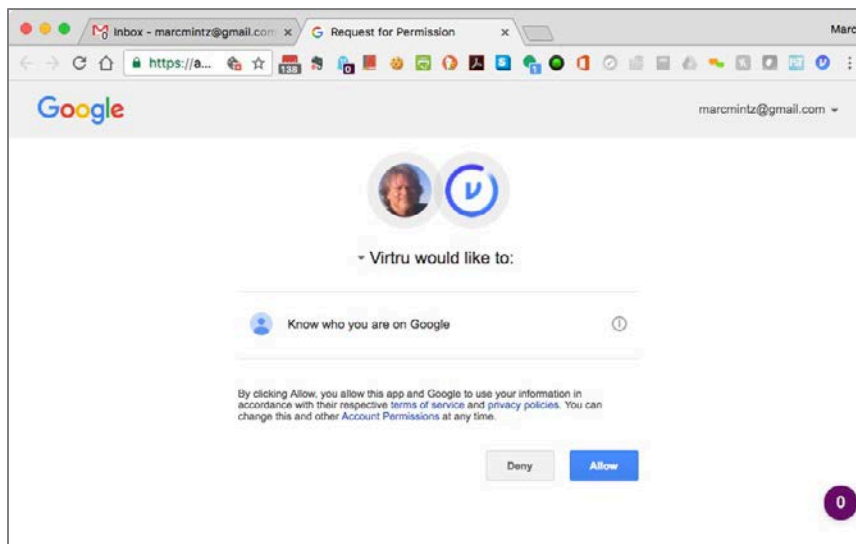
7. The *Step 2 of 4* alert appears. Following the instructions, click the Virtru switch to enable Virtru encryption.



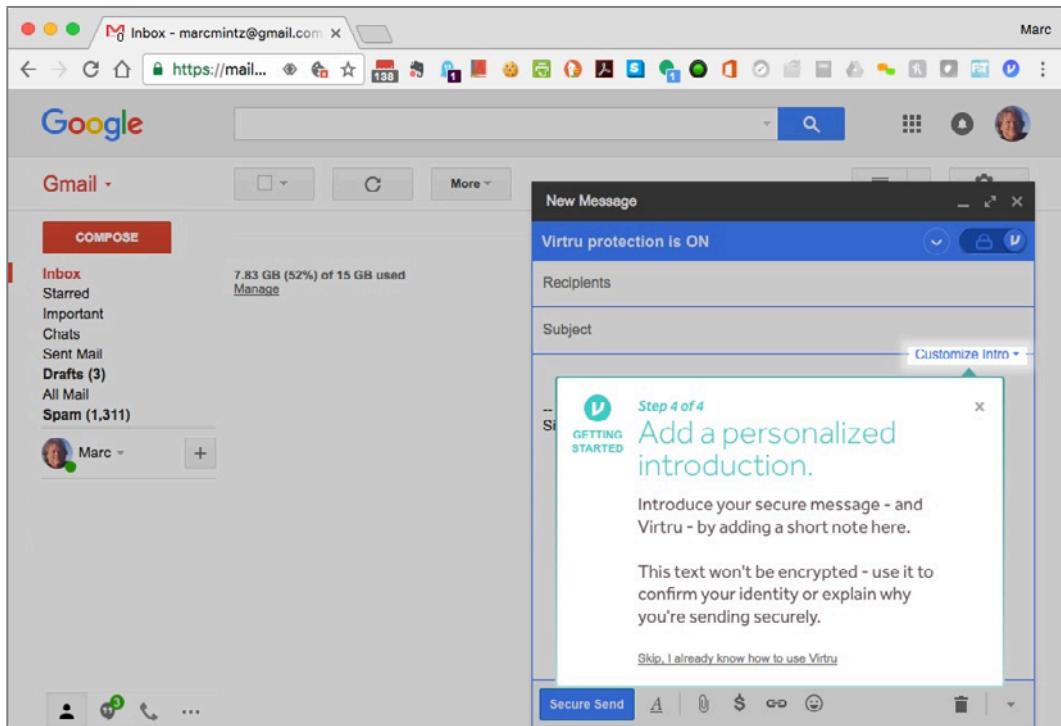
8. The *Step 3 of 4* alert appears. Following the instructions, click the *Activate <your email address>* button.



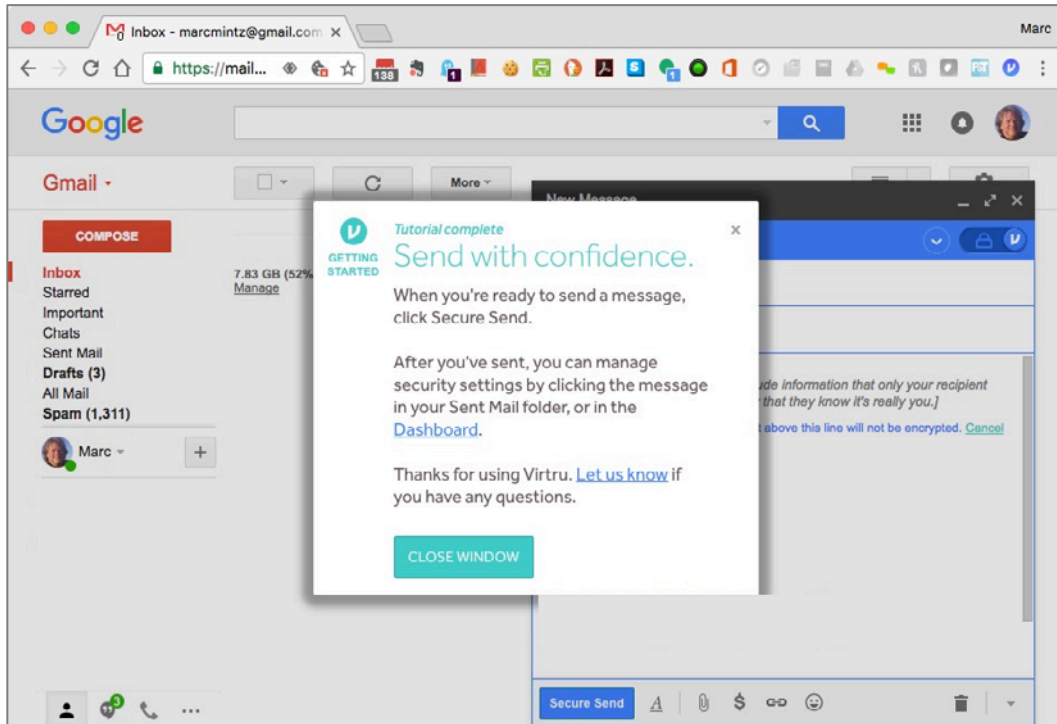
9. In the *Virtru would like to:* window, click the *Allow* button.



10. The *Step 4 of 4* alert appears. As you aren't really sending an email yet, click the *Customize Intro* button to move to the last alert.



11. The *Send with confidence* alert appears. Click the *Close Window* button.



You are now ready to send your first Virtru encrypted email.

15.10.2 Assignment: Send Encrypted Gmail With Virtru

In this assignment, you send your first encrypted Gmail or G-Suite email with Virtru.

- Prerequisite: A Gmail or G-suite account.
1. Open Google Chrome to *http://mail.google.com*.
 2. Click the *Compose* button to create a new email.

3. A *New Message* window appears. Click the *Virtru* switch in the top right corner to enable Virtru encryption.

The screenshot shows a 'New Message' window with a dark header bar. Below the header, a blue bar indicates 'Virtru protection is ON' with a dropdown arrow and a lock icon. The main area contains fields for 'Recipients' and 'Subject'. Below these fields is a large text area containing the following text:

Warmly,

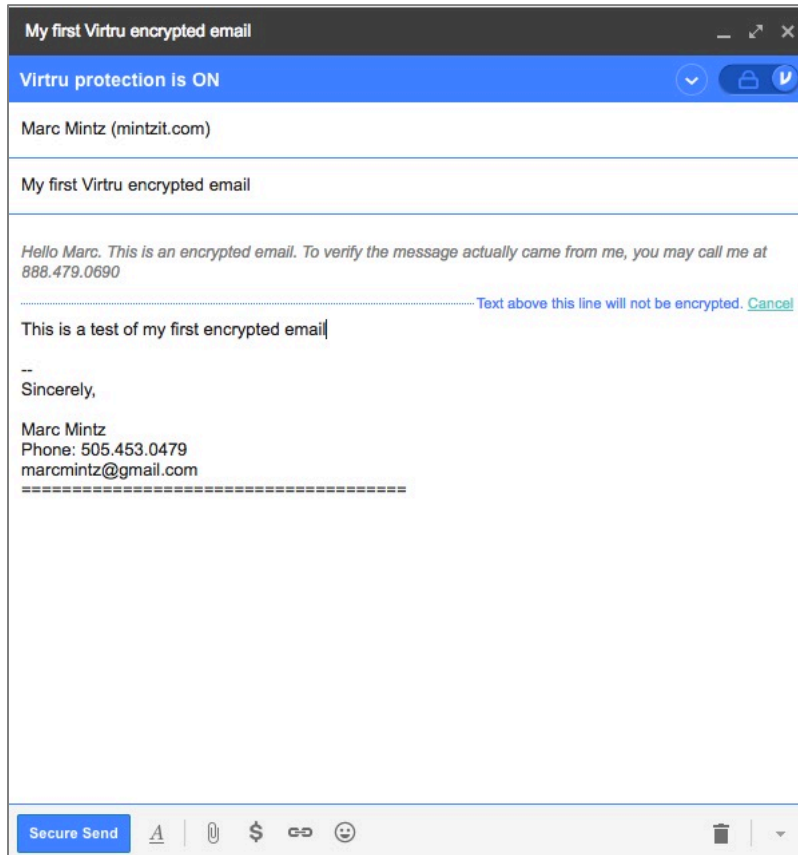
Marc Mintz, MBA-IT, ACTC, ACSP
 President & CIO
 Mintz InfoTech, Inc.
 505.814.1413 | 888.479.0690
marc@mintzit.com | www.mintzit.com

"Quality is not an act, it is a habit."
 - Aristotle

At the bottom right of the text area is a 'Customize Intro' link. The bottom of the window features a 'Secure Send' button and a toolbar with icons for text formatting, attachments, currency, links, and emojis.

- Enter the name of a friend in the *Recipients* field. If you are in a classroom, send to your classmate. If you are self-study, either send to one of your other email account, or to a friend.
 - Enter a subject in the *Subject* field.
 - Enter some text in the *Message* area.
4. Click the *Customize Intro* button.
 5. Enter a way that the recipient may verify the email is from you.

6. Click the *Secure Send* button to send the email.



Your Virtru-encrypted email is on its way!

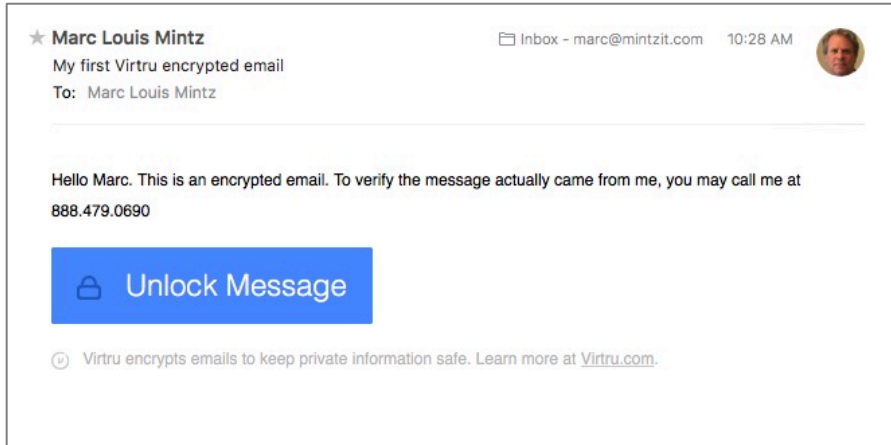
15.10.3 Receive and Reply To A Virtru-Encrypted Email

In this assignment, you receive and reply to a Virtru-encrypted email.

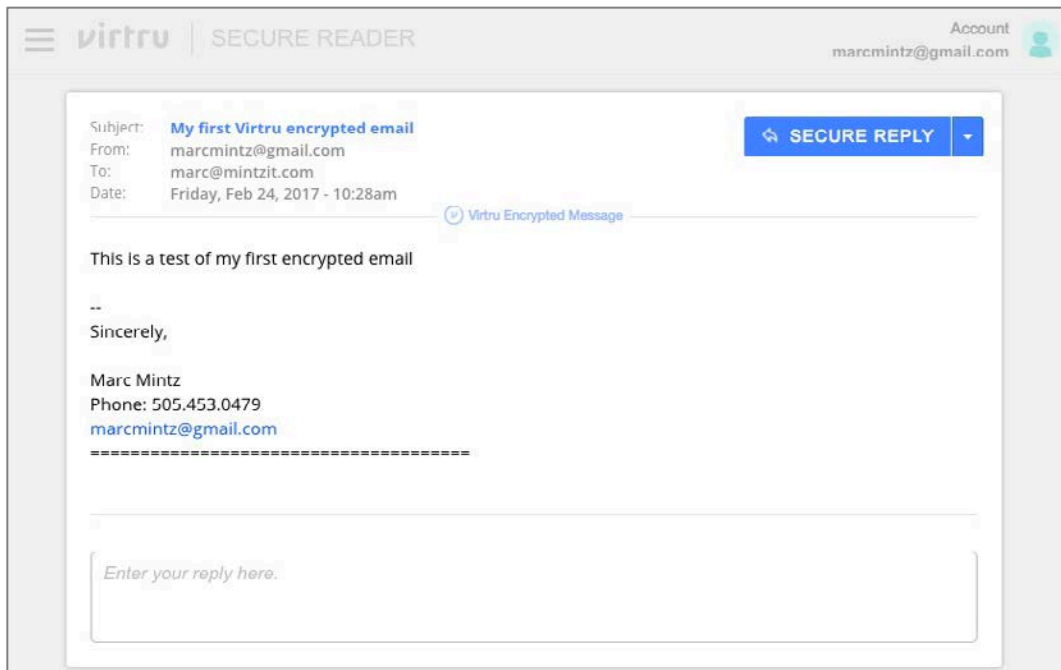
- Prerequisite: Completion of the previous assignment.

15 Email

1. As the recipient of a Virtru-encrypted email, open your email to find the encrypted message sent from the previous assignment. Click the *Unlock Message* button.



2. A browser will open to the *Virtru Secure Reader* site, with the message decrypted.



3. To send an encrypted reply to the original sender (from the previous assignment), click the *Secure Reply* button.
4. Within the same window, a *Reply* field will appear. Enter your message, and then click *Send Secure*. The encrypted reply is on its way.

The screenshot shows the Virtru Secure Reader interface. At the top, the Virtru logo and 'SECURE READER' text are on the left, and the user's account 'marcmintz@gmail.com' with a profile icon is on the right. The main content area displays an email from Marc Mintz with contact information and a redacted body. Below the email, a 'Reply' button with a dropdown arrow is shown next to the 'To: marcmintz@gmail.com' field. A text input box contains the message 'Hey, Marc. Very cool. I'm signing up for Virtru right now.' Below the input box is an 'Add Attachment' button. At the bottom, a warning message states: 'You're using the Virtru secure send functionality. For maximum security, we recommend you download the free Virtru plugin for client-side email encryption.' To the right of the warning are 'Cancel' and 'SEND SECURE' buttons.

Virtru | SECURE READER Account marcmintz@gmail.com

Sincerely,

Marc Mintz
Phone: 505.453.0479
marcmintz@gmail.com
=====

Reply To: marcmintz@gmail.com

Hey, Marc. Very cool. I'm signing up for Virtru right now.

Add Attachment

⚠ You're using the Virtru secure send functionality. For maximum security, we recommend you download the [free Virtru plugin](#) for client-side email encryption.

Cancel SEND SECURE

15.11 Email Validation with SPF, DKIM, and DMARC

*Sender Policy Framework (SPF)*¹⁶ is an email-validation system. It provides a mechanism to allow receiving mail exchangers (mail servers) to verify that incoming mail from a domain is actually coming from a host authorized to do so. When a criminal hacker sends email to you with fake “from” information (for example, a vendor submitting an invoice for payment), your email server is able to validate or invalidate the sender as authentic.

If the sender of an email is validated, the email comes on through just as it always has. If the sender is invalidated, the spoofed/fake/junk email simply never makes it to your inbox.

*Domain Keys Identified Mail (DKIM)*¹⁷ is an email authentication system to detect spoofing. It provides a mechanism for the receiver to verify that an email stating to have come from a specific domain was authorized by that domain. The intent is to prevent forged sender addresses.

DKIM works by attaching a digital signature to each outgoing email. The recipient’s email system validates the signature. These signatures are normally not visible to the user.

*Domain-based Message, Authentication, Reporting & Conformance (DMARC)*¹⁸ is the configurable policy detailing how to deal with email that has failed the DKIM validation. The options are to take no action, quarantine the email, or reject the email.

15.11.1 Assignment: Configure SPF

In this assignment, you configure SPF for your email domain.

- Note: Creating SPF records is only possible if your email is on its own Fully Qualified Domain Name (such as *thepracticalparanoid.com*). If you are using

¹⁶ https://en.wikipedia.org/wiki/Sender_Policy_Framework

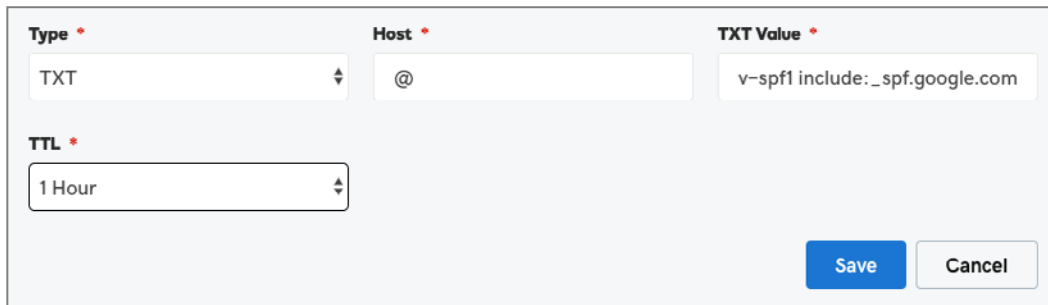
¹⁷ https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail

¹⁸ <https://en.wikipedia.org/wiki/DMARC>

a public domain such as *gmail.com*, you do not have the ability to edit your DNS records, and therefore cannot create your own SPF records.

In this assignment, I will be using the domain *mintzit.com* which is hosted with Google G-Suite, with DNS hosting at *GoDaddy.com* as the example. If your email or DNS hosts are different, the necessary steps may be different as well.

1. Open a web browser to your DNS Control Panel.
2. Select *Edit*.
3. Create a new *TXT* record with the following values:
 - a. For *Name/Host/Alias* enter *@*
 - b. For *Time to Live* enter *3600*
 - c. For *Value/Answer/Destination* enter *v=spf1 include:_spf.google.com ~all*



The screenshot shows a form for creating a new DNS record. It has four main sections: 'Type', 'Host', 'TXT Value', and 'TTL'. The 'Type' dropdown is set to 'TXT'. The 'Host' field contains '@'. The 'TXT Value' field contains 'v=spf1 include:_spf.google.com'. The 'TTL' dropdown is set to '1 Hour'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Type *	Host *	TXT Value *
TXT	@	v=spf1 include:_spf.google.com

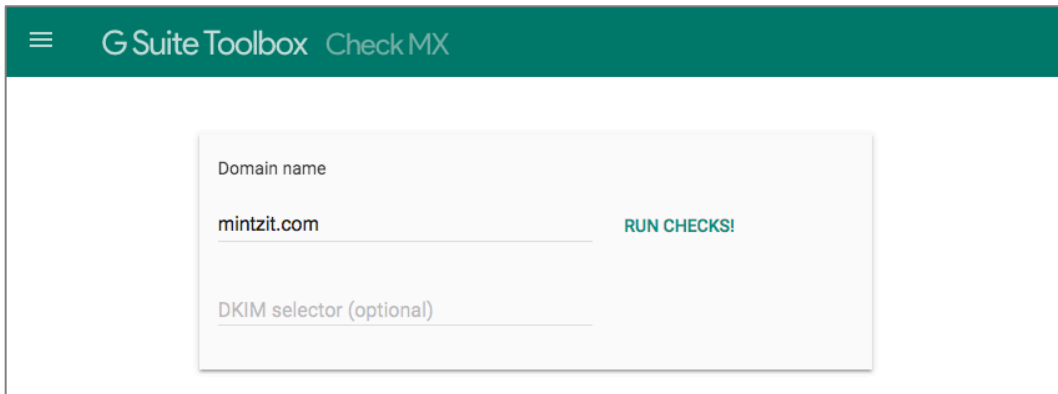
TTL *

1 Hour

Save Cancel

4. Save the DNS changes.


5. Verify the DNS changes. This is done in Google from <https://toolbox.googleapps.com/apps/checkmx/>


The image shows a screenshot of the Google Suite Toolbox 'Check MX' page. The header is a dark teal bar with a hamburger menu icon on the left and the text 'G Suite Toolbox Check MX' on the right. Below the header is a light gray rectangular box containing the form. The form has two input fields: 'Domain name' with the text 'mintzit.com' entered, and 'DKIM selector (optional)' which is currently empty. To the right of the 'Domain name' input is a teal button labeled 'RUN CHECKS!'.

6. Enter your domain name, and then select *Run Checks!*
7. When the check completes, select *Effective SPF Address Ranges* link. The results should include:
_spf.google.com
_netblocks.google.com followed by several IP addresses


_netblocks2.google.com followed by several IP addresses

_netblocks3.google.com followed by several IP addresses


G Suite Toolbox
Check MX


mintzit.com

No problems were found with the configuration of this domain.


Effective SPF Address Ranges.

The following IP addresses are taken from the includes and IP4/IP6 directives within this domains SPF record.

mintzit.com.

52.42.192.149

_spf.google.com

_netblocks.google.com

64.233.160.0/19

66.102.0.0/20

66.249.80.0/20

72.14.192.0/18

74.125.0.0/16

108.177.8.0/21

173.194.0.0/16

209.85.128.0/17

216.58.192.0/19

216.239.32.0/19

_netblocks2.google.com

2001:4860:4000::/36

2404:6800:4000::/36

2607:f8b0:4000::/36

2800:3f0:4000::/36

2a00:1450:4000::/36

2c0f:fb50:4000::/36

_netblocks3.google.com

172.217.0.0/19

172.217.32.0/20

172.217.128.0/19

172.217.160.0/20

172.217.192.0/19

108.177.96.0/19

servers.mcsv.net

205.201.128.0/20

198.2.128.0/18

148.105.8.0/21

15.11.2 Assignment: Configure DKIM

Note: Creating DKIM records is only possible if your email is on its own Fully Qualified Domain Name (such as *thepracticalparanoid.com*). If you are using a public domain such as *gmail.com*, you do not have the ability to edit your DNS records, and therefore cannot create your own DKIM records.

In this assignment, I will be using the domain *mintzit.com* which is hosted with Google G-Suite, with DNS hosting at *GoDaddy.com* as the example. If your email or DNS hosts are different, the necessary steps may be different as well.

Generate a *public domain key* for your domain

1. Open a browser to *admin.google.com*.
2. Select *Apps > G-Suite > Gmail > Authenticate email*.
3. Select the target domain for which you want to generate a domain key.
4. Click *Generate New Record*.
5. Click *Generate*.
6. A text box opens to display a 2048-bit key.
7. Select and then copy this key.

Create a DKIM record

8. Open a new web page, and then go to your DNS Control Panel.
9. Select *Create a new TXT record*.
10. In the *TXT Value* field, *paste* in the key created in step 6 above.
11. In the *Host* field, enter *google._domainkey*.



The screenshot shows a form for creating a new TXT record. The title is 'TXT'. There are three main fields: 'Host', 'TXT Value', and 'TTL'. The 'Host' field contains the text 'google._domainkey'. The 'TXT Value' field contains the text 'v=DKIM1; k=rsa; p=MIIBIjANBg'. The 'TTL' field is a dropdown menu currently showing '1 Hour'. At the bottom right of the form are two buttons: 'Save' (in blue) and 'Cancel' (in light gray).

12. Save the changes made to your DNS records.

15.11.3 Assignment: Sign Email With The Domain Key

In this assignment, you configure your mail server to automatically attach the DKIM key to all outgoing email.

- Prerequisite: Completion of the previous assignment.
- 1. Open a browser to *admin.google.com*.
- 2. Select *Apps > G-Suite > Gmail > Authenticate email*.
- 3. Select the target domain for which you want to attach a domain key.
- 4. Select *Start authentication*.

15.11.4 Assignment: Configure DMARC

Once DKIM is in place, a decision must be made what to do with incoming email found to be spoofed or fake. A general recommendation is this:

1. Configure DMARC to do nothing with failed validations, and to notify the administrator. Leave on this setting for a week or two to make sure no false positives are found.
2. Reconfigure DMARC to place failed validations in quarantine, and to notify the administrator. Leave on this setting for a week or two. If false positives are found in quarantine, research the reason, and resolve.
3. Reconfigure DMARC to reject failed validations.

In this assignment, you configure your mail server to do nothing with failed validations, and to notify the administrator.

1. Open a browser to your DNS control panel.

2. Create a new TXT record with the following attributes:
 - a. For *Record Name/Host* enter *_dmarc.mintzit.com*
 - Substitute your domain name in place of *mintzit.com*
 - b. For *Value* enter *v=DMARC1; p=none; rua=mailto:webmaster@mintzit.com.*
 - Substitute your administrator email address in place of *webmaster@mintzit.com.*
 - To send failed validations to quarantine, substitute *p=quarantine.*
 - To reject failed validations, substitute *p=reject.*

TXT

<p>Host *</p> <input style="width: 90%;" type="text" value="_dmarc"/>	<p>TXT Value *</p> <input style="width: 90%;" type="text" value="v=DMARC1; p=quarantine; rua="/>	<p>TTL *</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> 1 Hour ⌵ </div>
<div style="display: inline-block; margin-right: 10px;"> <input style="background-color: #007bff; color: white; padding: 5px 15px; border: none;" type="button" value="Save"/> </div> <div style="display: inline-block;"> <input style="border: 1px solid #ccc; padding: 5px 15px;" type="button" value="Cancel"/> </div>		

3. Save your changes.

Refer to the *DMARC Tag Registry*¹⁹ for other available options.

¹⁹ https://dmarc.org/draft-dmarc-base-00-01.html#iana_dmarc_tags

16 Apple ID And iCloud

Even in the common affairs of life, in love, friendship, and marriage, how little security we have when we trust our happiness in the hands of others!

–William Hazlitt¹, English writer and philosopher

What You Will Learn In This Chapter

- Create an Apple ID
- Implement Apple ID Two-Factor Authentication
- Remove a Device from Two-Factor Authentication

¹ https://en.wikipedia.org/wiki/William_Hazlitt

16.1 Apple ID And iCloud

In 2012 a well-known journalist had his Apple ID hacked, allowing the hacker full access to the victim's Apple ID, and through that, his iCloud account, including calendar, contacts, and email. This was accomplished not by traditional black hat hacking, but with a bit of social engineering. All the hacker needed was to discover the victim's birthdate and email address associated with his Apple ID. With a quick email to Apple saying something like, *I've forgotten my Apple ID password and would like to reset it. Here is my birthdate and my email address*, the hacker could reset the Apple ID password. With this, he could access the victim's iCloud website as if he were the victim himself.

I have had several clients whose iTunes accounts have been compromised in a similar fashion, one to the tune of \$1,400 in music purchases.

As of March 21, 2013, Apple has implemented an optional 2-Factor Authentication (2FA) process to harden your Apple ID security. With macOS 10.13, 2FA is mandatory for your Apple ID. Adding this security layer makes it extremely difficult for anyone to hijack your Apple ID and make fraudulent purchases.

Remember that every password can be broken. Your defense is to make it so difficult and time consuming to break that the hacker moves on to an easier target. Also, most security questions can be accurately guessed or broken through social engineering (*What is your birthday? In what city did your parents marry? What is the name of your first pet?* etc.) Both types of security are based on what you know. And if there is something that you know, someone else can know it as well. Unfortunately, even those you love and trust may occasionally use this information against you.

Apple has implemented 2-Factor Authentication for Apple ID so that whenever you sign in to your Apple ID on the web to manage your account, purchase something from iTunes, App Store, or iBooks Store from a new (unknown) device, or attempt to get Apple ID-related support from Apple, a code (either SMS or phone call) is sent to your previously verified device. You are prompted to provide this code before the purchase or support can be made.

If your device has been stolen or lost, you can log in to <https://appleid.apple.com> to remove that device from the verified device list, so that no code will be sent to that device.

- Note: As of August 2016, NIST has stopped recommending Two-Factor Verification that involves SMS/text messaging as the second factor². This is due to the ease of which this can be intercepted. However, *any* verification that is received via cellular signal (SMS, voice, etc.) is subject to the same vulnerabilities. Currently, the best solution is to use a digital token (a keychain-sized device that displays random number strings), or an *Authenticator* app, which serves the same purpose. At this time, Apple does not use digital tokens or an authenticator app, but can use a phone to provide verification codes.

16.1.1 Assignment: Create An Apple ID

Although it is possible to have a different Apple ID for the iTunes Store, iCloud, App Store, etc., life soon becomes far more complex than necessary. Unless you have a solid case to do otherwise, I strongly recommend having a single Apple ID (email address and password) for all your various Apple accounts.

If you already have an Apple ID, skip this assignment. If you do not already have an Apple ID, no better time than the present to create one!

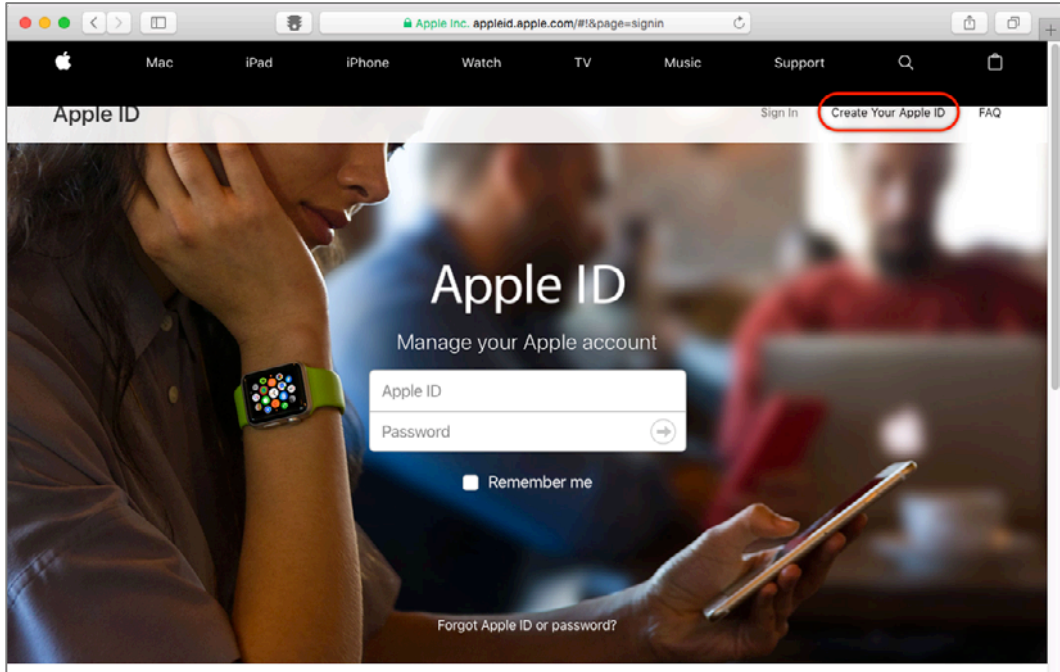
In this assignment, you create an Apple ID.

1. Open a browser, and then go to <https://appleid.apple.com>.

² <https://pages.nist.gov/800-63-3/sp800-63-3.html>

16 Apple ID And iCloud

2. Click on *Create Your Apple ID* link.



16 Apple ID And iCloud

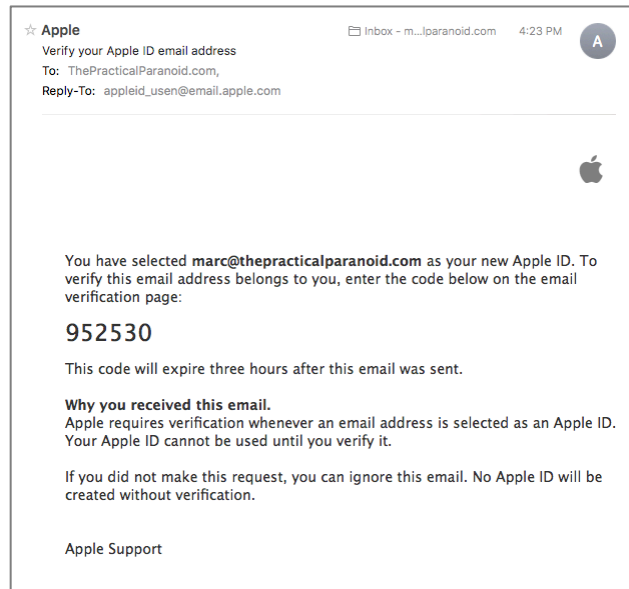
3. In the *Create Your Apple ID* page, complete the form, and then click the *Continue* button. Do securely record all information, particularly the security questions. These will be required should you ever need to validate your identity with Apple.

The screenshot shows the 'Create Your Apple ID' page in a web browser. The browser's address bar shows 'appleid.apple.com/account#'. The page has a dark header with the Apple logo and navigation links: Mac, iPad, iPhone, Watch, TV, Music, Support, and a search icon. Below the header, the page title 'Create Your Apple ID' is centered. The main content area is white and contains the following sections:

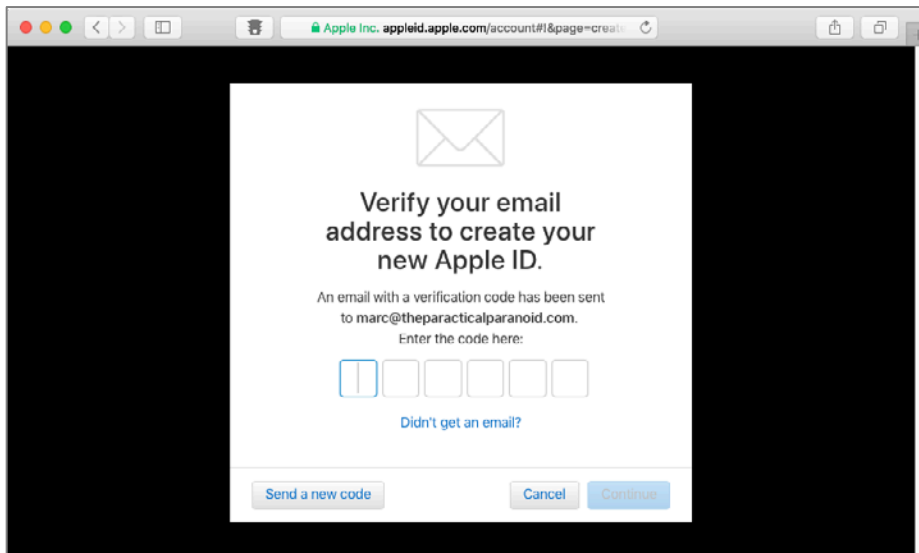
- Introduction:** 'One Apple ID is all you need to access all Apple services. Already have an Apple ID? [Find it here](#)'
- Personal Information:** Fields for 'first name', 'last name', a country dropdown menu (currently showing 'United States'), and 'birthday'.
- Email:** A field for 'name@example.com' with the note 'This will be your new Apple ID.'
- Password:** Fields for 'password' and 'confirm password'.
- Security Questions:** Three sections, each with a dropdown menu for a question and a text field for the answer.
 - Security Question 1: dropdown, answer field
 - Security Question 2: dropdown, answer field
 - Security Question 3: dropdown, answer field
- Verification:** A note: 'These questions will be used to verify your identity and recover your password if you ever forget it.'
- Service Selection:** Three checkboxes, all of which are checked:
 - ☒ **Announcements**: Get announcements, recommendations, and updates about Apple products, services, software updates, and more.
 - ☒ **Apple Music, New Apps and More**: Get recommendations, the latest releases, special offers, and exclusive content for music, apps, movies, TV, books, podcasts and more.
 - ☒ **Apple News Updates**: Get the best stories and recommendations from Apple News delivered directly to your inbox.
- Captcha:** A box with the characters 'BEG' and a field 'Type the characters in the image'. Below it are links for 'New Code' and 'Vision Impaired'.
- Footer:** A note 'Apple is committed to protecting your privacy. [Learn more...](#)' and a blue 'Continue' button.

16 Apple ID And iCloud

4. Go to your email for the verification code.



5. Return to the Apple web page, enter the code, and then click the *Continue* button.



You now have an Apple account. The next step is to continue with the next assignment to harden your account security.

16.1.2 Assignment: Enable 2-Factor Authentication

Any password can be broken. And even if it isn't broken, a website's entire user database can be harvested. Apple has implemented *2-Factor Authentication* (2FA) to prevent such events from breaking your Apple security.

With 2FA, if an attempt to access your Apple account is made from an unknown device, each of the known devices will receive a prompt asking if this is ok, and providing a security code that can be entered on the unknown device to permit access.

Assuming the criminal doesn't have access to your mobile device or computer, without knowing the security code, they can't access your account-even if they have your password.

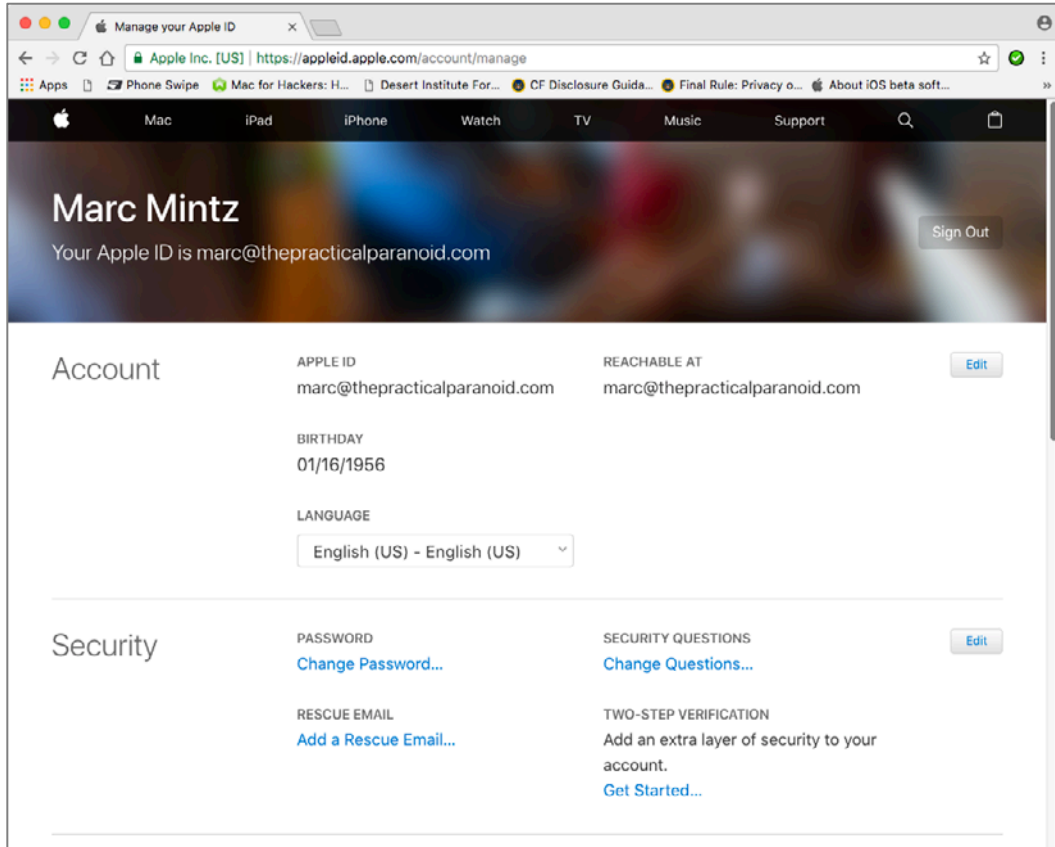
As of this writing, with macOS 10.13, Apple defaults to setting up *Two-Step Authentication*, not *2FA*. Two-Step Authentication is an older technology that Apple has replaced with 2FA (I know, it gives me a headache as well).

In this assignment, you will enable Apple Two-Step Verification, which will then be converted to 2FA.

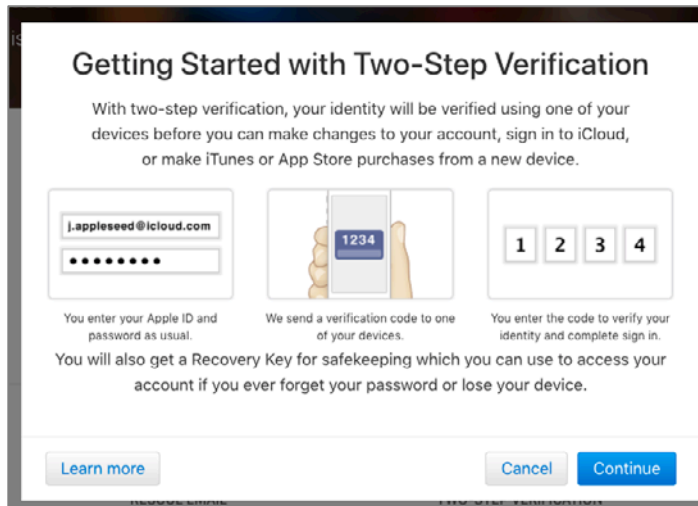
- Prerequisite: Completion of the previous assignment.

16 Apple ID And iCloud

1. Open a browser to *https://appleid.apple.com*. Your Apple ID Account page opens. Scroll to the *Security* section > *Two-Step Verification*, and then click the *Get Started* link.

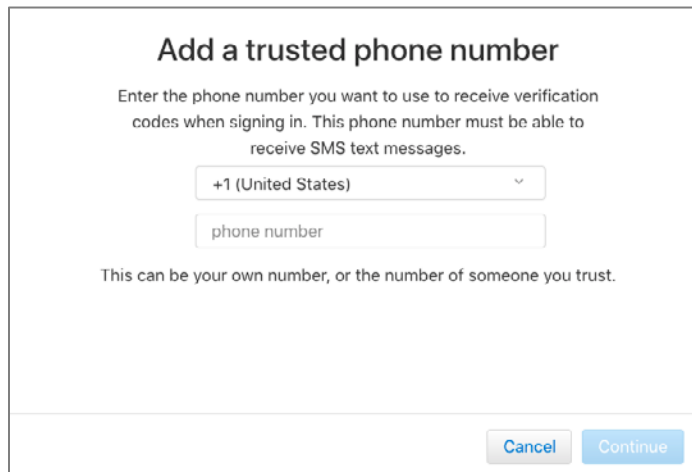


2. At the *Getting Started with Two-Step Verification* prompt, click the *Continue* button.



The screenshot shows a window titled "Getting Started with Two-Step Verification". The text inside explains that two-step verification uses a device to verify identity before making account changes. It shows three steps: 1. Entering Apple ID and password (example: j.appleseed@icloud.com). 2. Receiving a verification code (example: 1234) on a device. 3. Entering the code to verify identity. Below these steps, it mentions a Recovery Key for safekeeping. At the bottom, there are "Learn more", "Cancel", and "Continue" buttons.

3. At the *Add a trusted phone number* prompt, enter your mobile phone number, and then click the *Continue* button.

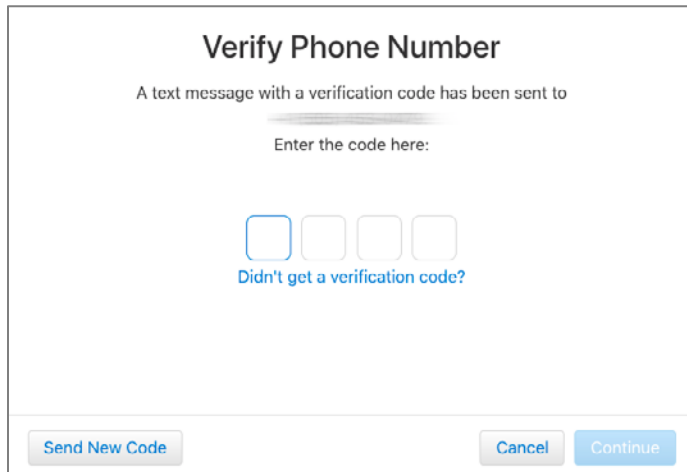


The screenshot shows a window titled "Add a trusted phone number". The text asks for a phone number to receive verification codes. It includes a dropdown menu for the country code (currently "+1 (United States)") and a text input field for the phone number. A note states: "This can be your own number, or the number of someone you trust." At the bottom, there are "Cancel" and "Continue" buttons.

4. Check your phone for a text from Apple with a *Verification Code*.

16 Apple ID And iCloud

5. Enter this code at the prompt on the Apple web page, and then click the *Continue* button.



Verify Phone Number

A text message with a verification code has been sent to

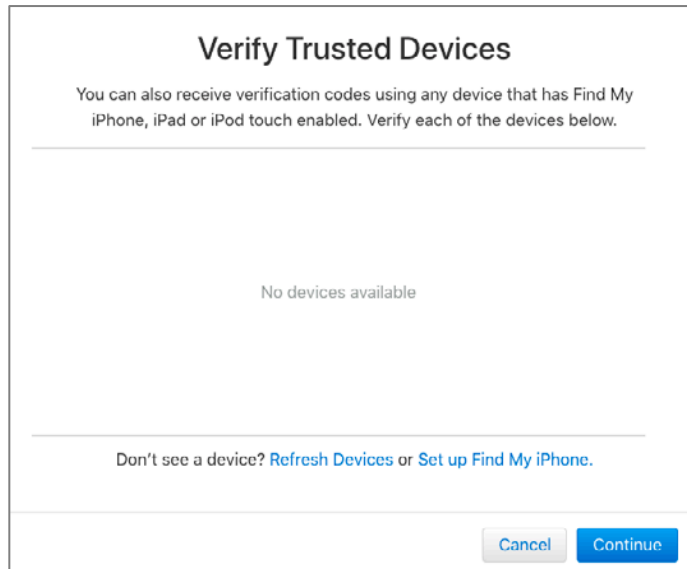
Enter the code here:

Four empty square boxes for entering the verification code.

[Didn't get a verification code?](#)

[Send New Code](#) [Cancel](#) [Continue](#)

6. At the *Verify Trusted Devices* window, click the *Continue* button.



Verify Trusted Devices

You can also receive verification codes using any device that has Find My iPhone, iPad or iPod touch enabled. Verify each of the devices below.

No devices available

Don't see a device? [Refresh Devices](#) or [Set up Find My iPhone](#).

[Cancel](#) [Continue](#)

16 Apple ID And iCloud

7. At the *Print Your Recovery Key* window, securely record your recovery key, and then click the *Continue* button. This code will be required if you ever forget your Apple ID password, or lose access to your trusted devices.



Print Your Recovery Key

You will need your Recovery Key to access your account if you ever forget your password or lose your trusted devices.

Recovery Key:

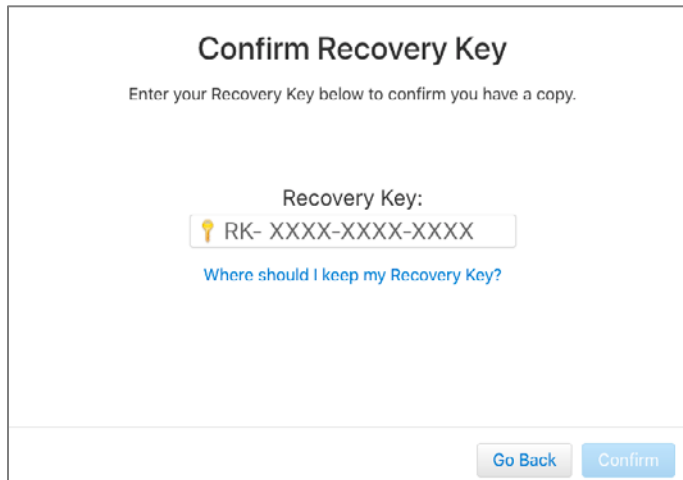
 [Redacted]

Print or write down your Recovery Key. Keep at least one copy in a safe place.
Do not save it on your computer.

[Where should I keep my Recovery Key?](#)

[Print Key](#) [Cancel](#) [Continue](#)


8. At the *Confirm Recovery Key* window, enter your recovery key. (Yes, the one from the previous step. Apple wants to make sure you actually recorded it).



Confirm Recovery Key

Enter your Recovery Key below to confirm you have a copy.

Recovery Key:

 RK- XXXX-XXXX-XXXX

[Where should I keep my Recovery Key?](#)

[Go Back](#) [Confirm](#)

9. At the *Enable Two-Step Verification* window, Apple wants to triple-check that you know what you are doing. Read the requirements, enable the *I understand* checkbox, and then click the *Enable Two-Step Verification* button.

Enable Two-Step Verification

Before you enable two-step verification, you must agree to the following conditions:


When Two-Step Verification is enabled:

- You will always need two of the following to manage your Apple ID: your password, a trusted device, or your Recovery Key.
- If you forget your password, you will need your Recovery Key and a trusted device to reset it. Apple will not be able to reset your password on your behalf.
- App-specific passwords will be required to sign in to any apps and services not provided by Apple.
- You are responsible for storing your Recovery Key in a safe place.

☐ I understand the conditions above.

[Cancel](#) [Enable Two-Step Verification](#)

10. The *Two-Step Verification Enabled* window opens. Click the *Done* button.



Two-Step Verification Enabled

[Done](#)

11. The *Two-Step Verification Enabled* window opens. Click the *Done* button.
12. In your browser, visit <https://icloud.com>. Sign in with your Apple ID and password.
13. Follow any on-screen instructions to verify your identity and activate iCloud for this Apple ID.

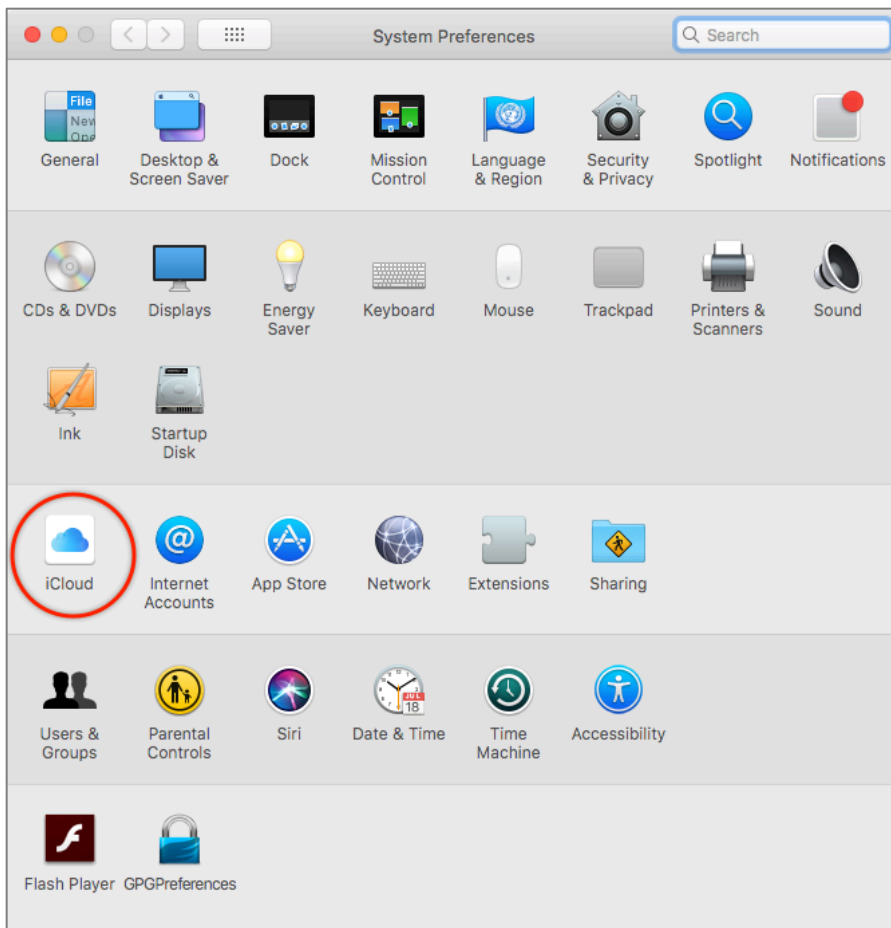
14. When done, you may quit the browser.

16.1.3 Assignment: Sign In To Your iCloud Account

Once you have created an Apple ID, you may sign in to your iCloud account in System Preferences. iCloud's primary function is to act as a server with which you can share your Contacts, Calendar, Keychain, and other services with your other Apple devices.

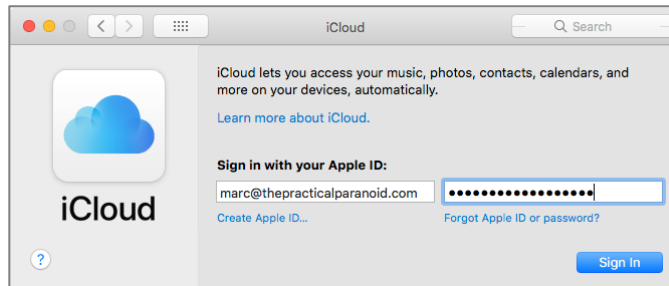
In this assignment, you sign in to your iCloud account in System Preferences.

1. Open *Apple* menu > *System Preferences* > *iCloud*.



16 Apple ID And iCloud

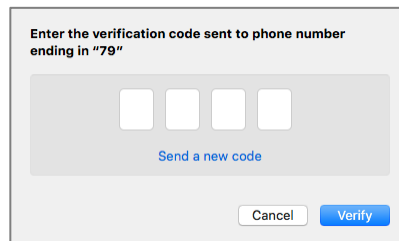
2. In the iCloud pane, enter your *Apple ID* and *password*, and then click the *Sign In* button.



6. As mentioned earlier, for reasons only Apple understands, the default is to create your Apple ID with Two-Step Verification (an older technology). With your first attempt to login to iCloud in System Preferences, Apple will convert your Two-Step Verification to 2-Factor Authentication (the current technology). Click the *Done* button.

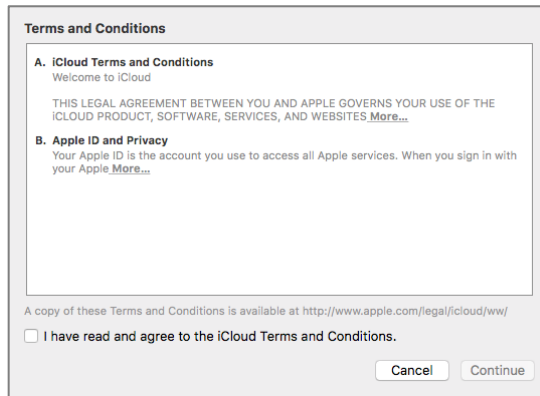


7. Check your mobile device for an SMS message from Apple.
8. On your Mac, enter the code, and then click the *Verify* button.

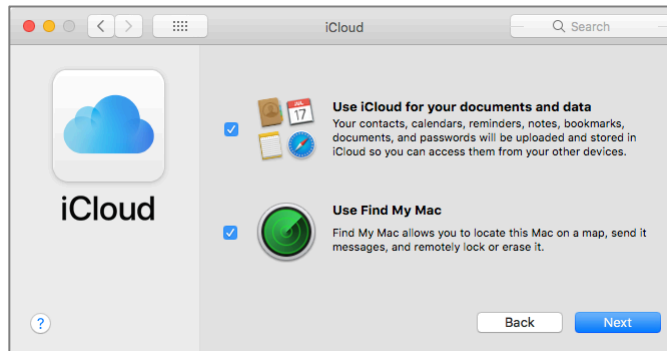


16 Apple ID And iCloud

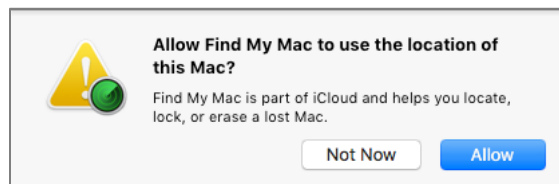
9. In the *Terms and Conditions* window, enable the *I have read and agree* checkbox, and then click the *Continue* button.



10. In the *iCloud* pane, configure to your taste, and then click the *Next* button. You can change these settings at any time.



11. At the *Allow Find My Mac to use the location of this Mac*, configure to your taste. You can change this setting at any time.



12. The iCloud Preferences window opens (finally).



Congratulations! You have successfully created a new Apple ID, and have secured your identity with 2-Factor Authentication.

16.1.4 Assignment: Remove A Device From Two-Factor Authentication

All the devices (computers, iPads, iPhones, Apple TVs, etc.) on which you have signed in to your Apple account will receive *Apple ID Verification Codes* when an attempt is made to access your Apple account on any device. Should one of your devices become lost, stolen, sold, or given to someone, the person who takes possession of it may be able to see your verification codes, presenting a security vulnerability.

To prevent this from happening, you must remove the device from your Apple ID device list.

In this assignment, you remove a device from your Apple ID device list.

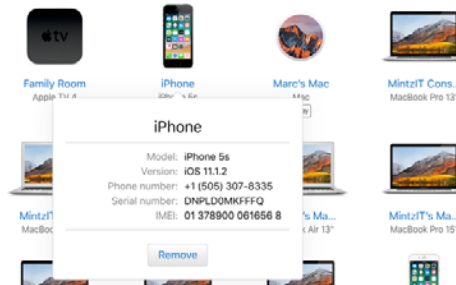
- Note: Unless you really do wish to remove the device, skip this assignment.
1. Open a browser to <https://appleid.apple.com>.
 2. At the prompt, enter your *Apple ID email address* and *Apple ID password*.

16 Apple ID And iCloud

3. If you have set up 2-Factor Authentication, your devices will display an alert that someone is attempting to access your account. Select *OK*. An *Apple ID Verification Code* will appear.
4. Enter the *Apple ID Verification Code* in the alert window in your browser.
5. Scroll down to the *Devices* area.



6. Click on the device to be removed.
7. A pop-up window will appear. Click on *Remove <device type>*.



The device is detached from your Apple ID, and will no longer receive Apple ID Verification Codes.

Revision Log

20180513, v2.1b

- *Chapter 14.8 Do Not Track* has been edited to include browser fingerprinting.
- *Chapter 14.8.6 Assignment: View Your Device Fingerprint* added.
- *Chapter 15.11 Email validation with SPF, DKIM, and DMARC* added
- *Security Checklist* updated

20180505, v2.1a

- *Chapter 13.4 Routers: An Overview*, added information regarding Intrusion Detection Systems and Intrusion Prevention Systems.
- *Chapter 14.2.1 Assignment: Secure Browsing With Brave* added.
- *Chapter 16.1.5 Assignment: Remove A Device From Two-Factor Authentication* added.

20180422, v2.1

- Reduced page count by 62 pages by removing superfluous images.
- *Chapter 3.1 The Need for Backups* added recommendation of Spinbackup for use with Google G-Drive.
- *Chapter 12.2 Prey* removed all but introductory paragraph on Prey.
- *Chapter 22.6 International Organization for Standardization (ISO)* added, with specific reference to the ISO 27001 standard for IT security.

20180420, v2.0

- The majority of chapters have been edited for updated information.
- *Chapter 2.6* renumbered for readability.
- *Chapter 4.5.1 Assignment: Harden the Keychain with a Different Password* removed. As of macOS 10.13.4 the login keychain password cannot be changed from the user account login password.

Revision Log

- Chapter 19.3 *NordVPN* revised to create a free trial account.
- Chapter 20.3 *Facebook* heavily edited to reflect the revised privacy and timeline settings.
- Chapter 20.4 *LinkedIn* heavily edited to reflect the revised privacy settings.
- Chapter 20.5 *Google* heavily edited to reflect the revised privacy and Takeout options.

20180325, v 1.3

- Chapter 4.8 *Password Policies* added.
- Chapter 12.1 *Find My Mac* has been slightly edited.
- Chapter 14.8 *Do Not Track* has been edited to reflect changes in Ghostery, and the Chrome extension installation process.
- Chapter 15.7 *End-To-End Secure Email With GNU Privacy Guard* rewritten to reflect the major update of GPGTools.
- Chapter 19.3 *NordVPN* is rewritten from scratch from our previous recommended VPN host.

20171022, v1.2

- Chapter 14 *Web Browsing* is rewritten.
- Chapter 15 *Email*, added *hacked-emails.com* for checking if your email account was included in site breaches.
- Chapter 16 *Apple ID and iCloud*, added that Two-Factor Authentication can use either text messaging or voice call.
- Chapter 19 *Internet Activity*, changed the recommended VPN provider to *Perfect-Privacy.com*.

20171001, v1.1

- Updated chapter *Documents > Encrypt A Folder for Cross Platform Use With Zip* to use Keka, instead of the depreciated macOS built-in tools.

20170923, v1.01

Revision Log

- Updated chapter *When It Is Time To Say Goodbye*

20170918, v1.0

Initial release

Index

- 2-Factor Authentication..... 462, 686
- 2-step verification89, 650, 655
- 802.1x..... 227, 229
- access point..... 231
- administrative ... 118, 126, 127, 128, 195
- administrator58, 118, 126, 128, 211, 214, 234
- Administrator..... 116, 118, 127, 129
- AES 75, 229, 507, 513
- Airport.. 37, 38, 233, 234, 236, 241, 246, 248
- Al Gore..... 527
- Andrew S. Tanenbaum..... 671
- Android..... 498, 553
- Anonymous Internet Browsing.. 335
- antenna..... 226
- anti-malware 106, 129, 164, 165
- Antivirus... 164, 168, 169, 174, 177, 188
- App Store..... 106, 107, 221, 462
- Apple ID71, 89, 106, 217, 221, 461, 462, 463, 476
- Application Updates..... 108, 112
- Assignment ... 41, 44, 46, 47, 53, 56, 59, 68, 75, 79, 82, 85, 88, 92, 96, 98, 99, 105, 108, 112, 118, 122, 125, 126, 127, 130, 141, 143, 146, 147, 149, 150, 155, 158, 168, 180, 195, 198, 206, 207, 210, 217, 221, 231, 233, 237, 241, 249, 259, 265, 274, 277, 281, 283, 284, 286, 287, 288, 290, 291, 292, 294, 295, 297, 299, 300, 307, 308, 310, 312, 314, 317, 324, 328, 335, 346, 358, 361, 368, 371, 373, 375, 379, 383, 390, 393, 400, 402, 403, 405, 407, 414, 419, 424, 433, 436, 439, 443, 448, 453, 457, 458, 463, 467, 473, 476, 481, 484, 487, 490, 496, 498, 501, 508, 520, 531, 535, 540, 541, 544, 547, 555, 557, 560, 568, 581, 590, 592, 593, 598, 603, 605, 606, 608, 609, 619, 626, 632, 635, 650, 660, 664, 669, 673, 689
- Aung San Suu Kyi 363
- AV Comparatives 164
- Avira 166
- Backblaze 40
- backup36, 37, 38, 39, 46, 59, 220
- Ban Ki-moon 145
- Benjamin Franklin 115, 271
- Bitdefender 165, 168, 169, 177, 180, 188
- Blog..... 30
- Boot Camp..... 164, 165
- broadcasting.....210, 226
- Broadcasting..... 226
- Carbon Copy Cloner .38, 41, 47, 48, 49, 53, 54, 57
- Carbonite 40
- Certificate Authorities..... 413
- Challenge Question..... 79
- Cisco 67

Index

- CISPA..... 25
- Clear History..... 290
- clone 38, 39, 58, 59, 60
- Clone ..51, 52, 53, 54, 56, 57, 58, 59
- Comodo 414, 417, 419, 424, 425, 433, 435
- Computer theft..... 36
- Cookies..... 286
- crack 65
- Criminal activities..... 36
- Deep Web 357
- Disk Decipher 498
- Disk Utility 41, 487
- DKIM 453, 457, 458, 689
- DMARC 453, 458, 459, 689
- DMZ..... 258
- Do Not Track 306
- DoD 664, 665, 669
- DoE 664, 669
- Dr. Seuss..... 659
- DuckDuckGo 286, 287, 288
- Ed Snowden..... 357
- EDS 498
- EFI Chip 206
- Elayne Boosler..... 205
- Elbert Hubbard..... 157
- email..... 379
- Email ...97, 363, 367, 374, 383, 389, 392, 393, 395, 403, 405, 413, 414, 415, 417, 420, 421, 431, 432, 433, 435, 436, 566, 690
- Encrypt 58, 273, 407, 410, 411, 481, 484, 487, 490
- Encrypted Data Store 498
- encrypted email. 367, 389, 390, 436, 438, 439
- encryption..... 58, 59, 148, 152, 153, 226, 228, 272, 367, 373, 374, 480, 481, 484
- Encryption .148, 228, 231, 367, 411, 488
- Entropy..... 36
- Erase..... 220
- Ethernet 217, 226, 227
- Facebook 30, 67, 96, 97, 98, 117, 129, 528, 596, 598, 603, 604, 605, 609, 610, 626
- Facetime 528
- FAT 517
- FBI 25
- FileVault..56, 58, 59, 148, 150, 151, 153, 210, 480, 664, 665, 684
- FileVault 2..... 56, 58, 59, 148, 150, 210, 480
- Find My iPhone 218, 219, 221, 222, 223
- Find My Mac 210, 211, 217, 219, 221
- Find My Mac? 210
- Fire 36
- firewall 194, 195, 196, 230
- Firewall 195, 196, 197, 199, 200, 201
- FireWire 37, 41, 146, 147
- Firmware ...205, 206, 207, 210, 259, 684
- firmware password..... 207
- Firmware Password... 153, 206, 207, 208, 684
- Flash..... 25
- Gateway VPN..... 551
- General Douglas MacArthur 225
- George Carlin 35

Index

- Ghostery ... 306, 312, 314, 317, 318, 321
- GNU Privacy Guard...374, 389, 690
- Google Hangouts 528, 529
- GPA..... 390
- GPG...389, 390, 391, 393, 394, 402, 403, 404, 405, 407, 413, 437, 440
- GPG Keychain Access 393, 394, 402, 407
- GPG Public Key..... 390
- Gpg4win 390
- GPGMail..... 400
- GPGTools390, 391, 402
- Gravity Zone..... 165
- GravityZone..... 180, 181, 184, 187
- G-Suite 40
- Guest .117, 129, 210, 213, 215, 217, 684
- Hamachi.... 568, 569, 581, 582, 583, 584, 586, 589, 590, 592, 593
- HaveIBeenPwned..... 358
- haystack 66, 69
- HIPAA..... 40
- Honore de Balzac..... 163
- Hot Corners..... 161
- https 66, 69, 272, 273, 368, 373
- HTTPS..... 273, 274, 367, 373, 685
- HTTPS Everywhere...273, 274, 337
- Hypertext Transport Layer Secure 367
- iCloud..70, 71, 88, 89, 91, 151, 210, 217, 218, 461, 462, 463, 473, 474, 475, 686
- Incognito Mode..... 281
- infected 65
- Insertion..... 226, 227, 238, 250
- Integrity Test..... 46
- Integrity Testing 59
- International Organization for Standardization 679
- iOS 88, 389, 413, 498
- ipconfig 244, 245, 253, 254
- ISO 679
- iTunes..... 463
- Java 25
- Joseph Heller 21
- Keka ... 490, 491, 492, 493, 494, 496
- Keychain .70, 72, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 232, 392, 394, 402, 403, 418, 419, 436, 683
- LAN230, 231
- LastPass..... 67, 92, 93, 96, 98
- LinkedIn 626
- Linux ..333, 334, 389, 390, 498, 517
- Local Area Network..... 230
- LogMeIn....568, 572, 573, 575, 576, 577, 581, 583, 585, 586, 588, 589, 593
- MAC Address241, 248
- Mac OS Extended488, 517
- MacKeeper 305
- MacUpdate 108, 111, 112
- MacUpdate Desktop.....108, 112
- maintenance.....38, 118
- malware118, 164
- Malware.....36, 164
- Managed with Parental Controls 117, 129, 130
- Marc L. Mintz..... 21, 28, 29, 63
- Mintz's extrapolation of Sturgeon's Revelation..... 24
- modem..... 230
- Newsletter..... 30

Index

- NIST..... 23, 513, 676, 677, 678
- NIST SP 800-171..... 676
- NordVPN..... 557, 560
- NSA..... 23, 64, 206, 207, 513, 552, 567, 664, 681
- NTP..... 672, 673
- Onion sites..... 357
- Onion Sites..... 357
- Parallels..... 165, 337
- Parental Controls..... 117, 129, 130, 141, 142
- passphrase..... 66
- password..... 25, 58, 65, 66, 68, 118, 126, 128, 148, 152, 206, 207, 210, 220, 221, 227, 228, 234, 236, 368, 373, 375, 462, 481, 487, 488, 489
- Password..... 65, 68, 206, 236, 481
- Password Policies..... 99, 677
- permissions..... 118
- PGP..... 389, 413
- phishing..... 25, 164
- Phishing..... 365
- port..... 194, 258
- Port forwarding..... 258
- Ports..... 198
- Power surges..... 36
- Practical Paranoia Book Upgrades..... 30
- Practical Paranoia Updates..... 30
- Pretty Good Privacy..... 389
- Prey..... 224
- private browsing..... 281
- profile keys..... 99
- ProtonMail 374, 375, 379, 381, 383, 384
- public key..... 393
- Public Key..... 389, 390, 393, 399, 402, 403, 405, 437, 438, 439, 440
- pwpolicy..... 99
- RADIUS..... 227
- RAM-Resident Malware..... 258
- Recovery HD . 53, 56, 206, 207, 666
- Recovery Key..... 58
- Root..... 116, 118, 122, 125, 126
- router..... 230, 231, 258, 259
- Router..... 237, 258, 265
- S/MIME..... 413, 414, 419, 424, 426, 429, 432, 433, 436, 437, 438, 439, 440
- Sabotage..... 36
- Screen Saver..... 158, 161
- screensaver..... 162
- SEC..... 40
- Secure Socket Layer..... 272
- Sender Policy Framework..... 453
- Seneca..... 103
- Server..... 37, 38, 226, 227
- SHA..... 513
- Sharing Only..... 117
- Single User Mode..... 206
- Skype..... 528, 529
- sleep..... 54, 59, 159, 160, 162, 241, 281, 550
- Sleep..... 153, 158, 161
- software..... 37, 40, 65, 66, 118, 164, 226, 375
- SPF..... 453, 455, 689
- Spinbackup..... 40
- SSL..... 272, 368
- Standard..... 117, 128, 129, 391, 510
- Static electricity..... 36
- stealth..... 198
- switch..... 231

Index

- Symantec 25, 389
- System Updates..... 103
- Tails...333, 334, 335, 337, 356, 686, 687
- Takeout..... 655, 690
- Target Disk Mode 206
- Terrorist activities 36
- theft 25, 36, 37
- Theodore Roosevelt 193
- Theodore Sturgeon..... 24
- thepracticalparanoid..... 438
- Thomas Jefferson..... 63
- Thomas Sowell 209
- Thunderbolt 37
- Time Machine37, 38, 39, 41, 44, 45, 46, 47, 683
- TKIP..... 229
- TLS..... 367, 368
- Tor.....333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 344, 345, 346, 356, 357, 685, 686
- TorBrowser.....338, 344, 346
- Trafficlight..... 295
- TrafficLight 177, 178, 188, 189
- Trojan horses 25, 164
- TrueCrypt 498, 504
- Two-Step Verification..... 476
- USB..... 37, 41, 146, 147
- US-CERT 104
- User Accounts..... 115
- VeraCrypt..498, 501, 502, 503, 507, 508, 509, 510, 520, 521, 523, 524
- Virtru.442, 443, 444, 445, 446, 448, 449, 450, 451
- virtual machine 164
- Virtual Machine.....165, 337
- Virtual Private Network....228, 273, 550
- viruses 25
- VMware Fusion 165
- VPN...228, 233, 273, 550, 551, 552, 553, 554, 557, 566, 567, 568, 579, 581, 586, 589, 590, 592, 593, 686
- war driving 25
- Water damage 36
- Web Mail..... 373
- WEP228, 231
- Whitelisting 129
- Wi-Fi...25, 210, 217, 226, 227, 228, 231, 232, 233
- William Blum 479
- William Hazlitt 461
- Windows ...146, 164, 165, 166, 244, 253, 333, 389, 390, 498, 517, 553, 591
- Wire.....531, 540, 541, 543, 544
- worms.....25, 164
- WPA.....228, 229, 231
- WPA2.....228, 229, 231, 233, 236
- zero-day exploits..... 27

Mintz InfoTech, Inc.

when, where, and how you want IT

Technician fixes problems.

Consultant delivers solutions.

Technician answers questions.

Consultant asks questions, revealing core issues.

Technician understands your equipment.

Consultant understands your business.

Technician costs you money.

Consultant contributes to your success.

Let us contribute to your success.

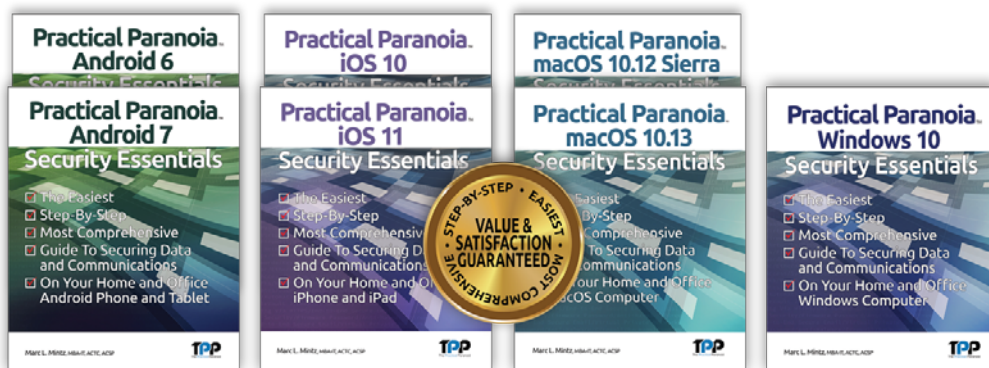
Mintz InfoTech, Inc. is uniquely positioned to be your Virtual CIO and provide you and your organization comprehensive technology support. With the only MBA-IT consultant and 100% certified staff in New Mexico, our mission is to provide small and medium businesses with the same Chief Information and Security Officer resources otherwise only available to large businesses.

Mintz InfoTech, Inc.

Toll-free: +1 888.479.0690 • Local: 505.814.1413
info@mintzIT.com • <https://mintzit.com>

Practical Paranoia Workshops & Books

4 Years Undisputed #1 Best, Easiest, & Most Comprehensive Cybersecurity Series



This is an age of government intrusion into every aspect of our digital lives, criminals using your own data against you, and teenagers competing to see who can crack your password the fastest. Every organization, every computer user, everyone should be taking steps to protect and secure their digital lives.

The *Practical Paranoia: Security Essentials Workshop* is the perfect environment in which to learn not only *how*, but to actually *do* the work to harden the security of your macOS and Windows computers, and iPhone, iPad, and Android devices.

Workshops are available online and instructor-led at your venue, as well as tailored for on-site company events.

Each Book is designed for classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, and security checklist. Available from Amazon (both print and Kindle format), and all fine booksellers, with inscribed copies available from the author.

Call for more information, to schedule your workshop, or order your books!

The Practical Paranoid, LLC
+1 888.504.5591 • info@thepracticalparanoid.com
<https://thepracticalparanoid.com>