Practical Paranoia™ macOS 10.13

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

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Copyright © 2016, 2017 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

Cover design by Ed Brandt

ISBN-10: 1535579323
ISBN-13: 978-1535579322

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 65
5 System and Application Updates 107
6 User Accounts 121
7 Storage Device 153
8 Sleep and Screen Saver 165
9 Malware 171
10 Firewall 211
11 Firmware Password 223
12 Lost or Stolen Device 227
13 Local Network 251
14 Web Browsing 297
15 Email 379
16 Apple ID and iCloud 483
17 Documents 505
18 Voice, Video, and Instant Message Communications 551
19 Internet Activity 575
20 Social Media 631
21 When It Is Time to Say Goodbye 701
22 Miscellaneous 709
23 The Final Word 719
macOS 10.13 Security Checklist 721
Revision Log 727
Index 729
Mintz InfoTech, Inc. when, where, and how you want IT 735
Practical Paranoia Workshops & Books 736

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 26
2.5 About the Author 28
2.6 Practical Paranoia Updates 29
2.7 Practical Paranoia Paperback Book Upgrades 30
2.8 Practical Paranoia Kindle Updates 31
2.9 Practical Paranoia Online Live Student Edition Updates 32
2.10 Notes for Instructors, Teachers, & Professors 33
2.11 Update Bounty 34
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 40
3.1.2 Assignment: Configure Time Machine 43
3.1.3 Assignment: Integrity Test the Time Machine Backup 45
3.1.4 Assignment: Install and Configure Carbon Copy Cloner 47
3.1.5 Assignment: Test Run the First Clone Backup 54
3.1.6 Assignment: Encrypt the Clone Backup. 57
3.1.7 Assignment: Integrity Test the Clone Backup 60
4 Passwords 65
4.1 The Great Awakening 66
4.2 Strong Passwords 67
4.2.1 Assignment: Create a Strong User Account Password 70
4.3 Keychain 75
4.3.1 Assignment: View an Existing Keychain Record 79

4.4 Challenge Questions ... 82
4.4.1 Assignment: Store Challenge Q&A in the Keychain ... 82
4.4.2 Assignment: Access Secure Data from Keychain ... 85
4.5 Harden the Keychain ... 88
4.5.1 Assignment: Harden the Keychain with a Different Password ... 89
4.5.2 Assignment: Harden the Keychain With a Timed Lock ... 91
4.6 Synchronize Keychain Across macOS and iOS Devices ... 94
4.6.1 Assignment: Activate iCloud Keychain Synchronization ... 94
4.7 LastPass ... 99
4.7.1 Assignment: Install LastPass ... 99
4.7.2 Assignment: Use LastPass to Save Website Authentication Credentials ... 103
4.7.3 Assignment: Use LastPass to Auto Fill Website Authentication ... 105
5 System and Application Updates ... 107
5.1 System Updates ... 108
5.1.1 Assignment: Configure Apple System and Application Update Schedule ... 109
5.2 Manage Application Updates With MacUpdate Desktop ... 112
5.2.1 Assignment: Install and Configure MacUpdate Desktop ... 112
5.2.2 Assignment: Application Updates with MacUpdate Desktop ... 117
5.3 Additional Reading ... 119
6 User Accounts ... 121
6.1 User Accounts ... 122
6.2 Never Log in As an Administrator ... 124
6.2.1 Assignment: Enable the Root User ... 124
6.2.2 Assignment: Login as the Root User ... 128
6.2.3 Assignment: Change the Root User Password ... 131
6.2.4 Assignment: Disable the Root User ... 132
6.2.5 Assignment: Create an Administrative User Account ... 132
6.2.6 Assignment: Change from Administrator to Standard User ... 134
6.3 Application Whitelisting and More with Parental Controls ... 136
6.3.1 Assignment: Configure a Managed with Parental Controls Account ... 137
6.3.2 Assignment: View Parental Controls Logs ... 148
6.4 Policy Banner ... 150
6.4.1 Assignment: Create a Policy Banner ... 150

7 Storage Device 153
7.1 Block Access to Storage Devices 154
7.1.1 Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access 154
7.1.2 Assignment: Enable USB, FireWire, and Thunderbolt Storage Device Access 155
7.2 FileVault 2 Full Disk Encryption 156
7.2.1 Assignment: Boot into Target Disk Mode 157
7.2.2 Assignment: Boot into Recovery HD Mode 157
7.2.3 Assignment: Boot into Single-User Mode 158
7.2.4 Assignment: Enable and Configure FileVault 2 158
7.3 FileVault Resistance to Brute Force Attack 162
7.4 Remotely Access and Reboot a FileVault Drive 163
7.4.1 Assignment: Temporarily Disable FileVault 163
8 Sleep and Screen Saver 165
8.1 Require Password After Sleep or Screen Saver 166
8.1.1 Assignment: Require Password After Sleep or Screen Saver 166
9 Malware 171
9.1 Anti-Malware 172
9.1.1 Assignment: Install and Configure Bitdefender (Home Users Only) 176
9.1.2 Assignment: Install and Configure Bitdefender GravityZone Endpoint Security (Business Users) 192
9.2 Additional Reading 209
10 Firewall 211
10.1 Firewall 212
10.1.1 Assignment: Activate the Firewall 213
10.1.2 Assignment: Close Unnecessary Ports 216
11 Firmware Password 223
11.1 EFI Chip 224
11.1.1 Assignment: Create a Firmware Password 224
11.1.2 Assignment: Test the Firmware Password 225
11.1.3 Assignment: Remove the Firmware Password 225
12 Lost or Stolen Device 227
12.1 Find My Mac 228
12.1.1 Assignment: Activate and Configure Find My Mac 228

12.1.2 Assignment: Use Find My Mac From A Computer....234
12.1.3 Assignment: Use Find My Mac From An iPhone or iPad....238
12.2 Prey241
12.2.1 Assignment: Enable the Guest User Account....241
12.2.2 Assignment: Create a Prey Account....242
12.2.3 Assignment: Install Prey....245
12.2.4 Assignment: Configure Prey....247
13 Local Network....251
13.1 Ethernet Broadcasting....252
13.2 Ethernet Insertion....253
13.3 Wi-Fi Encryption Protocols....254
13.4 Routers: An Overview....256
13.4.1 Assignment: Determine Your Wi-Fi Encryption Protocol....257
13.4.2 Assignment: Secure an Apple Airport Extreme Base Station....259
13.4.3 Assignment: Configure WPA2 On a Non-Apple Router....263
13.5 Use MAC Address to Limit Wi-Fi Access....267
13.5.1 Assignment: Restrict Access by MAC Address on an Apple Airport....267
13.5.2 Assignment: Restrict Access by MAC Address to A Non-Apple Router....275
13.6 Router Penetration....284
13.6.1 Assignment: Verify Apple Airport Port Security Configuration....285
13.6.2 Assignment: Verify Non-Apple Airport Router Security Configuration....291
14 Web Browsing....297
14.1 HTTPS....298
14.1.1 Assignment: Install HTTPS Everywhere....300
14.2 Choose a Browser....304
14.3 Private Browsing....305
14.3.1 Assignment: Safari Private Browsing....305
14.3.2 Assignment: Firefox Private Browsing....307
14.3.3 Assignment: Google Chrome Incognito Mode....308
14.4 Secure Web Searches....310
14.4.1 Assignment: Make DuckDuckGo Your Safari Default Search Engine....310

14.4.2 Assignment: Make DuckDuckGo Your Firefox Default Search Engine ... 311
14.4.3 Assignment: Make DuckDuckGo Your Chrome Default Search Engine ... 312
14.5 Clear History ... 314
14.5.1 Assignment: Clear the Safari History ... 314
14.5.2 Assignment: Clear the Firefox Browsing History ... 315
14.5.3 Assignment: Clear the Chrome History ... 316
14.6 Browser Plug-Ins ... 318
14.6.1 Assignment: Install Trafficlight Plug-In for Safari ... 318
14.6.2 Assignment: Install Trafficlight Plug-In for Google Chrome ... 321
14.6.3 Assignment: Install Trafficlight For Firefox ... 323
14.6.4 Assignment: Find and Remove Extensions from Safari ... 325
14.6.5 Assignment: Find and Remove Extensions from Google Chrome ... 326
14.6.6 Assignment: Find and Remove Add-Ons from Firefox ... 327
14.7 Fraudulent Websites ... 329
14.8 Do Not Track ... 333
14.8.1 Assignment: Secure Safari ... 334
14.8.2 Assignment: Secure Firefox ... 335
14.8.3 Assignment: Secure Chrome ... 338
14.8.4 Assignment: Install Ghostery for Safari ... 340
14.8.5 Assignment: Install Ghostery for Chrome ... 340
14.9 Adobe Flash and Java ... 345
14.9.1 Assignment: Configure Oracle Java For Automatic Updates ... 345
14.10 Web Scams ... 349
14.10.1 Recovering From A Web Scam ... 349
14.11 Tor 352
14.11.1 Assignment: Install Tor for Anonymous Internet Browsing ... 354
14.11.2 Assignment: Configure Tor Preferences ... 364
14.12 Onion Sites and the Deep Web ... 375
14.13 Have I Been Pwned ... 376
14.13.1 Assignment: Searching With HaveIBeenPwned ... 376
14.13.2 Assignment: What To Do Now That You Have Been Breached . 378
15 Email ... 379
15.1 The Killer App ... 380

15.2 Phishing 381
15.3 Email Encryption Protocols 383
15.4 TLS and SSL With Mail App 384
15.4.1 Assignment: Configure Mail.app to Use TLS or SSL 384
15.5 HTTPS with Web Mail 389
15.5.1 Assignment: Configure Web Mail to Use HTTPS 389
15.6 End-To-End Secure Email With ProtonMail 390
15.6.1 Assignment: Create a ProtonMail Account 392
15.6.2 Assignment: Create and Send an Encrypted ProtonMail Email 396
15.6.3 Assignment: Receive and Respond to a ProtonMail Secure Email 400
15.7 End-To-End Secure Email With GNU Privacy Guard 405
15.7.1 Assignment: Install GPG and Generate a Public Key 406
15.7.2 Assignment: Add Other Email Addresses to a Public Key 412
15.7.3 Assignment: Install a Friend's Public Key 418
15.7.4 Assignment: Configure GPGMail Preferences 420
15.7.5 Assignment: Encrypt and Sign Files with GPGServices 422
15.7.6 Assignment: Send a GPG-Encrypted and Signed Email 426
15.7.7 Assignment: Receive a GPG-Encrypted and Signed Email 428
15.8 End-To-End Secure Email With S/MIME 431
15.8.1 Assignment: Acquire a Free Class 1 S/MIME Certificate 432
15.8.2 Assignment: Acquire A Class 3 S/MIME Certificate for Business Use 439
15.8.3 Assignment: Purchase a Class 3 S/MIME Certificate for Business Use 448
15.8.4 Assignment: Download and Install a Business S/MIME Certificate 459
15.8.5 Assignment: Exchange Public Keys with Others 463
15.8.6 Assignment: Send S/MIME Encrypted Email 466
15.9 Virtru Email Encryption 469
15.9.1 Create a Free Virtru for Gmail Account 471
15.9.2 Send Encrypted Gmail With Virtru 477
15.9.3 Receive and Reply to a Virtru-Encrypted Email 479
16 Apple ID and iCloud 483
16.1 Apple ID and iCloud 484
16.1.1 Assignment: Create an Apple ID 485

16.1.2 Assignment: Enable 2-Factor Authentication 490
16.1.3 Sign in to Your iCloud Account 499
17 Documents 505
17.1 Document Security 506
17.2 Password Protect a Document Within Its Application 507
17.2.1 Assignment: Encrypt an MS Word Document 507
17.3 Encrypt a PDF Document 510
17.3.1 Assignment: Convert a Document to PDF for Password Protection 510
17.4 Encrypt a Folder for Only macOS Use 513
17.4.1 Assignment: Create an Encrypted Disk image 513
17.5 Encrypt A Folder for Cross Platform Use with Zip 517
17.5.1 Assignment: Encrypt A File or Folder Using Zip 517
17.5.2 Assignment: Open an Encrypted Zip Archive 518
17.6 Cross-Platform Document Encryption 520
17.6.1 Assignment: Download and Install VeraCrypt 520
17.6.2 Assignment: Configure VeraCrypt 526
17.6.3 Assignment: Create a VeraCrypt Container 532
17.6.4 Assignment: Mount an Encrypted VeraCrypt Container 544
18 Voice, Video, and Instant Message Communications 551
18.1 Voice, Video, and Instant Messaging Communications 552
18.2 HIPAA Considerations 554
18.3 Wire 555
18.3.1 Assignment: Install Wire 555
18.3.2 Assignment: Invite People to Wire 560
18.3.3 Assignment: Import Contacts into Wire 565
18.3.4 Assignment: Secure Instant Message a Wire Friend 566
18.3.5 Assignment: Secure Voice Call with A Wire Friend 570
18.3.6 Assignment: Secure Video Conference with a Wire Friend 573
19 Internet Activity 575
19.1 Virtual Private Network 576
19.2 Gateway VPN 577
19.2.1 Assignment: Search for a VPN Host 581
19.3 Perfect-Privacy 583
19.3.1 Assignment: Create a Perfect-Privacy Account 583
19.3.2 Assignment: Configure IKEv2 VPN With Perfect-Privacy 591

19.3.3 Assignment: Advanced Perfect-Privacy Settings ... 596
19.4 Mesh VPN ... 600
19.5 LogMeIn Hamachi ... 601
19.5.1 Assignment: Create a LogMeIn Hamachi Account ... 601
19.5.2 Assignment: Add Users to a Hamachi VPN Network ... 614
19.5.3 Assignment: File Sharing Within a Hamachi VPN Network ... 624
19.5.4 Assignment: Screen Share Within Hamachi VPN ... 626
19.5.5 Assignment: Exit the Hamachi VPN Network ... 628
19.6 Resolving Email Conflicts with VPN ... 630
20 Social Media ... 631
20.1 What, me worry? ... 632
20.2 Protecting Your Privacy on Social Media ... 633
20.3 Facebook ... 634
20.3.1 Assignment: Facebook Security and Login ... 634
20.3.2 Assignment: Facebook Privacy Settings ... 640
20.3.3 Timeline and Tagging Settings ... 643
20.3.4 Assignment: Facebook Manage Blocking ... 646
20.3.5 Assignment: Facebook Public Posts ... 648
20.3.6 Assignment: Facebook Apps ... 650
20.4 LinkedIn ... 660
20.4.1 Assignment: LinkedIn Account Security ... 660
20.4.2 Assignment: LinkedIn Privacy Settings ... 665
20.5 Google–More Than a Search Engine ... 677
20.5.1 Assignment: Manage Your Google Account Access and Security Settings ... 677
20.5.2 Assignment: Enable Google 2-Step Verification ... 694
21 When It Is Time to Say Goodbye ... 701
21.1 Preparing a Computer for Sale or Disposal ... 702
21.2 Secure Erase a Storage Device ... 703
21.2.1 Assignment: Secure Erase a Storage Device ... 703
22 Miscellaneous ... 709
22.1 Date and Time Settings ... 710
22.1.1 Assignment: Configure Date & Time ... 711
22.2 Securing Hardware Components ... 713
22.3 National Institute of Standards and Technology (NIST) ... 715
22.3.1 NIST-Specific Security Settings ... 715

22.4 United States Computer Emergency Readiness Team (US-CERT)..... 717
23 The Final Word..... 719
23.1 Additional Reading..... 720
macOS 10.13 Security Checklist..... 721
Revision Log..... 727
Index..... 729
Mintz InfoTech, Inc. when, where, and how you want IT..... 735
Practical Paranoia Workshops & Books..... 736

Practical Paranoia macOS 10.13 Security Essentials

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

19 Internet Activity

If you go to a coffee shop or at the airport, and you're using open wireless, I would use a VPN service that you could subscribe for 10 bucks a month. Everything is encrypted in an encryption tunnel, so a hacker cannot tamper with your connection.

–Kevin Mitnick[1]

What You Will Learn In This Chapter

- Virtual Private Network
- Search for a VPN host
- Install and configure VPN
- Create a mesh VPN
- File share within a Hamachi VPN
- Resolve email conflicts with VPN

[1] *https://en.wikipedia.org/wiki/Kevin_Mitnick*

19.1 Virtual Private Network

In case you have been sleep reading through this book, let me repeat my wake-up call: *They are watching you on the Internet*. *They* may be the automated governmental watchdogs (of your own or another country), government officials (again, of your own or another country), bored staff at an Internet Service Provider or broadband provider, a jealous (and slightly whackadoodle) ex, high school kids driving by your home or office or sitting on a hill several miles away, or criminals.

Regardless, your computer and data are at risk.

Perhaps one of the most important steps that can be taken to protect you is to encrypt the entire Internet experience all the way from your computer, through your broadband provider, to a point where your surfing, chat, webcam, email, etc. cannot be tracked or understood. This is accomplished using a technology called *VPN–Virtual Private Network*[2].

[2] *http://en.wikipedia.org/wiki/Virtual_private_network*

19.2 Gateway VPN

There are two fundamental flavors of VPN. The most common is called a *gateway VPN* (mesh VPN is discussed later.) Historically, gateway VPN involved the use of a VPN appliance resident at an organization. Telecommuting staff can use the gateway so the Internet acts like a very long Ethernet cable connecting their computer to the office network. In addition, all data traveling between the user's computer and the gateway is military-grade encrypted. The downside to this strategy is that these appliances are relatively expensive (from $600 to several thousand dollars), and they require significant technical experience to configure correctly.

In greater detail the concept works like this:

1. Your computer has VPN software installed and configured to connect to a VPN server at the office. This server is connected to your office network. macOS/OS X comes with VPN software built into the Network System Preferences that works with many of the commercially available VPN servers, including the most popular–Cisco. Other VPN servers require their own proprietary client software to be installed.
2. On your computer, you open the VPN software and instruct it to connect to the VPN server. This typically requires entering your authentication credentials of user name and password, along with a long key.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.
4. As you send data from your computer to the network connected to the VPN server (typically the regular business network), all of it is military-grade encrypted. When the data is received at the VPN server or at your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on your organizations network (file server, printer, mail server, etc.)

Although this may sound a bit complex, all a user must do is enter a name, password, and key. Everything else is invisible. The only indicator that anything is

different is that speed slower than normal. This is due to the overhead of encryption/decryption process.

We can use this same strategy so that instead of securely exchanging data with our office server, we can securely surf the Internet. The workflow is just slightly different:

1. Your computer has VPN software configured to connect to a VPN server that is not associated with your office, but is just another server "on the Internet."
2. On your computer, you open the VPN software and instruct it to connect to the VPN server. If you are using our recommended software, it is pre-configured with all the settings necessary–nothing much more to do but launch.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.
4. As you surf the web, all data is military-grade encrypted. When the data is received at the VPN server or your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on the Internet.

Using this strategy (a VPN Internet server), all your Internet traffic is military-grade encrypted between your computer and the VPN server. It is not possible to decipher any of your traffic (user names, passwords, data) or even the type of data coming and going.

One downside is that once the data exits the VPN server, it is readable. However, your data is intermingled with thousands of other user's data, making the process of tweezing out your data a task that perhaps only the NSA can accomplish.

Another concern is that some VPN providers maintain user activity logs. This is law in most countries, so that government agencies can review who is doing what through the VPN. Ideally, you want to work only with a VPN provider operating in a country doesn't require logs, and in fact, do not keep logs.

There are thousands of VPN Internet Servers available. Most of them are free. I don't recommend using the free services for two reasons:

1. You get what you pay for (typically here today, gone tomorrow, unstable, etc.)

2. You don't know who is listening at the server side of things. Remember, your data is fully encrypted up to the server. But once the data reaches the server on the way to the Internet, it is readable. There needs to be a high degree of trust for the administration of the VPN server. I see no reason to have such trust with free services.

There are hundreds of legitimate VPN hosts. Thousands of illegitimate VPN hosts. When determining the best VPN provider for your use, there are some key variables to look for:

- **Privacy Jurisdiction.** Does the VPN host have to comply with US National Security Letters, or other governmental requirements for disclosure of your information? If you don't care about the government access to all of your Internet information, this doesn't apply. If you do care, the geographical location of the host headquarters becomes important.
- **Logs**. Are logs kept on client activities? In many countries, it is required by law that all Internet providers maintain logs of client activities. If so, although the logs may not record *what* you were doing, they keep a record of *where* you traveled. It is ideal to have a VPN provider that keeps no logs whatsoever.
- **Speed**. How fast is your Internet experience? Using VPN introduces a speed penalty due to the encryption/decryption process, as well as the need to process all incoming and outgoing packets through a server instead of point-to-point. VPN providers can reduce this penalty in several ways, including; faster servers, reducing the clients:server ratio, better algorithms, filtering content to remove advertisements and cookies, and faster server internet connections.
- **Support**. VPN adds a layer of complexity to your Internet activities. Should something not work correctly, you don't want to be the one troubleshooting. Ideally, your VPN provider has 24/7/365 chat support. Even better if they offer telephone support.
- **Cross-Platform Support**. Most of us have more than one device. Perhaps a Windows and macOS/OS X computer, an Android phone, and an Apple iPad. It would be madness to have to use a different VPN product for each of these. Look for a provider that supports all your current and potential devices.

- **Multi-Device Support**. Most, but not all, providers now offer from 3-5 concurrent device licensing. This allows your VPN service to be operational on all your devices at the same time. Providers that offer only single-device licensing may be quite costly should you have multiple devices.
- **DNS-Leak Protection**. Although VPN encrypts all data that comes and goes from your device, before you can reach out to the Internet to connect to your email, a website, or text, your device must connect to a DNS server for guidance on where to find the mail, web, or text server. If you are using your default DNS server (typically one by your Internet broadband provider, data between your system and the DNS server is not encrypted *and* is recorded. It is ideal if your VPN provider offered their own DNS servers. Using this strategy, then the data between your device and the DNS server is now either encrypted, or is not logged.
- **VPN Protocol.** There are several network protocols that may be used for encryption. We currently recommend IKEv2. This is the most current, and the only protocol with the ability to automatically activate upon accessing the Internet, and deactivate when not in use.
- **Pricing.** This is sometimes directly related to the quality of service, and occasionally directly related to the greediness of those running the business. Look for reasonable pricing for the services offered, as well as how many concurrent connections you are allowed. Some hosts allow only 1 connection. Others offer 6 or more. This would allow for you to have your computer, phone, tablet connected via VPN, as well as those of a family member.

Right about now you may be asking yourself: *If VPN is so great, why doesn't everyone know about and use it?*

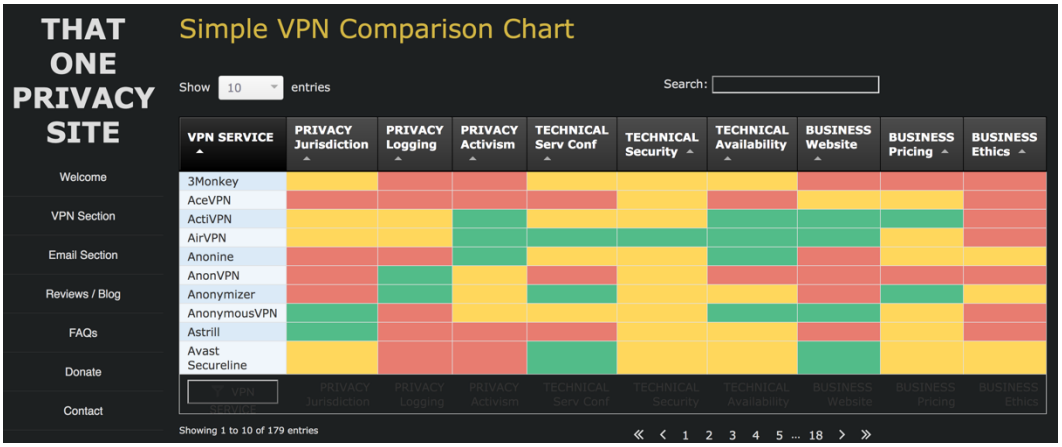
Great question! As with everything else in life, there is bad that comes with the good. Each person needs to weigh the pros and cons for each situation for themselves. I personally *always* have VPN active, but I'm *always* doing work! I hope you don't have that disease. There are two primary downsides to VPN. It slows down your Internet performance. Often by 50% or more. If all I want to do were to stream Netflix to my computer, I'd turn VPN off to reduce the pauses induced by a slow Internet connection. Second, if you have selected a VPN server outside of your home country, you may have unintended consequences due to the

Internet servers thinking you are resident in that other country. For example, Google searches will be displayed in the language native to that country. This is considered a feature of the *Proxy Server* function built into VPN, and is used by those in restrictive countries to view news across the border that are normally filtered out by their home country.

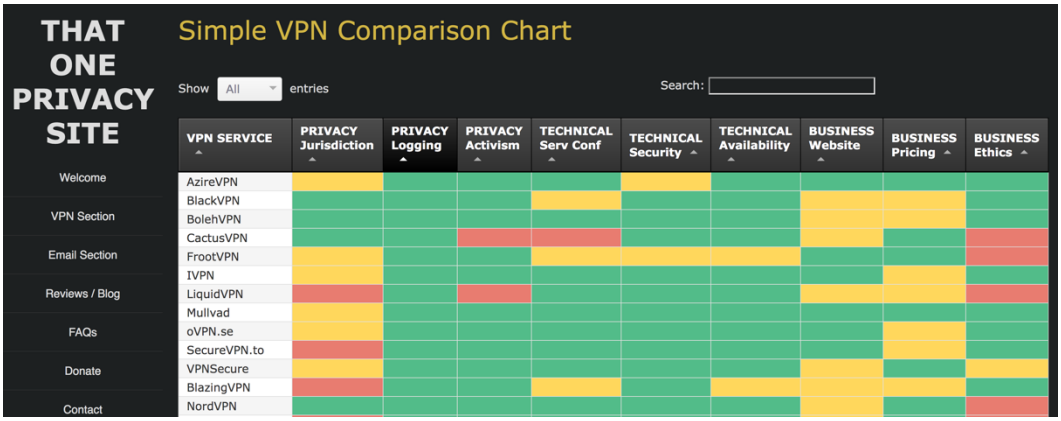
19.2.1 Assignment: Search for a VPN Host

In this assignment, you will search for at least three VPN hosts that best meet your needs.

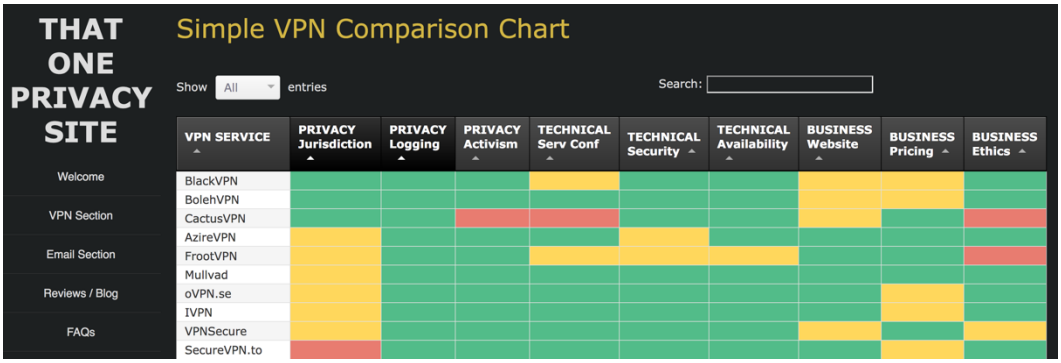
1. Based on the list of criteria listed above, make a list of VPN Host *must-haves,* and *prefer-to-haves.*
2. Open a web browser to *https://thatoneprivacysite.net/simple-vpn-comparison-chart/,* or for a more detailed checklist, *https://thatoneprivacysite.net/vpn-comparison-chart/.*
3. Click the *Show <pop-up menu> entries,* and then select *All.*



4. To sort by your first *must-have,* click in that column header. For this assignment, click on *Privacy Logging.*



5. To sub-sort by a second *must-have* feature, hold down the *Shift* key, and then click on the header matching that must-have. For this assignment, click on *Privacy Jurisdiction.*



6. By performing a sort and sub-sort, we have filtered potential hosts from almost 200, to just a few.

7. From the few hosts meeting these minimum requirements, view their websites to evaluate if any meet your needs.

8. Outside of this course, you may sign-up with one or more of the hosts meeting your needs, put its service through an evaluation, unsubscribe and request a refund if they don't meet with your expectations, or keep them if they meet your needs.

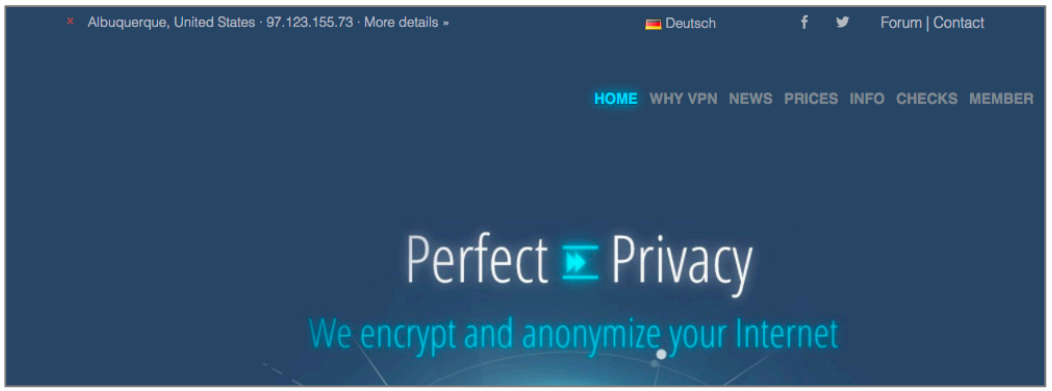
19.3 Perfect-Privacy

One of our favorite VPN providers is *Perfect-Privacy*[3]. Although they do not offer a free or trial option, they offer subscriptions as short as a month, as long as two years. With this you get servers in almost every country you can name, use on multiple devices, unlimited bandwidth, and highly responsive bandwidth. The only major complaint we have with them is that the geolocation reporting of their servers is inconsistent. For example, if you are connected to their Los Angeles, CA, USA VPN server, and then browse to https://google.com, it is likely that Google will see you as being located in a European country, and then reroute your browser to https://google.ru, displaying everything in Russian. However, if you are using DuckDuckGo for web searches, there should rarely be an issue with geolocation.

19.3.1 Assignment: Create a Perfect-Privacy Account

In this assignment, you create a paid account with *Practical-Privacy.com*, and then configure VPN services.

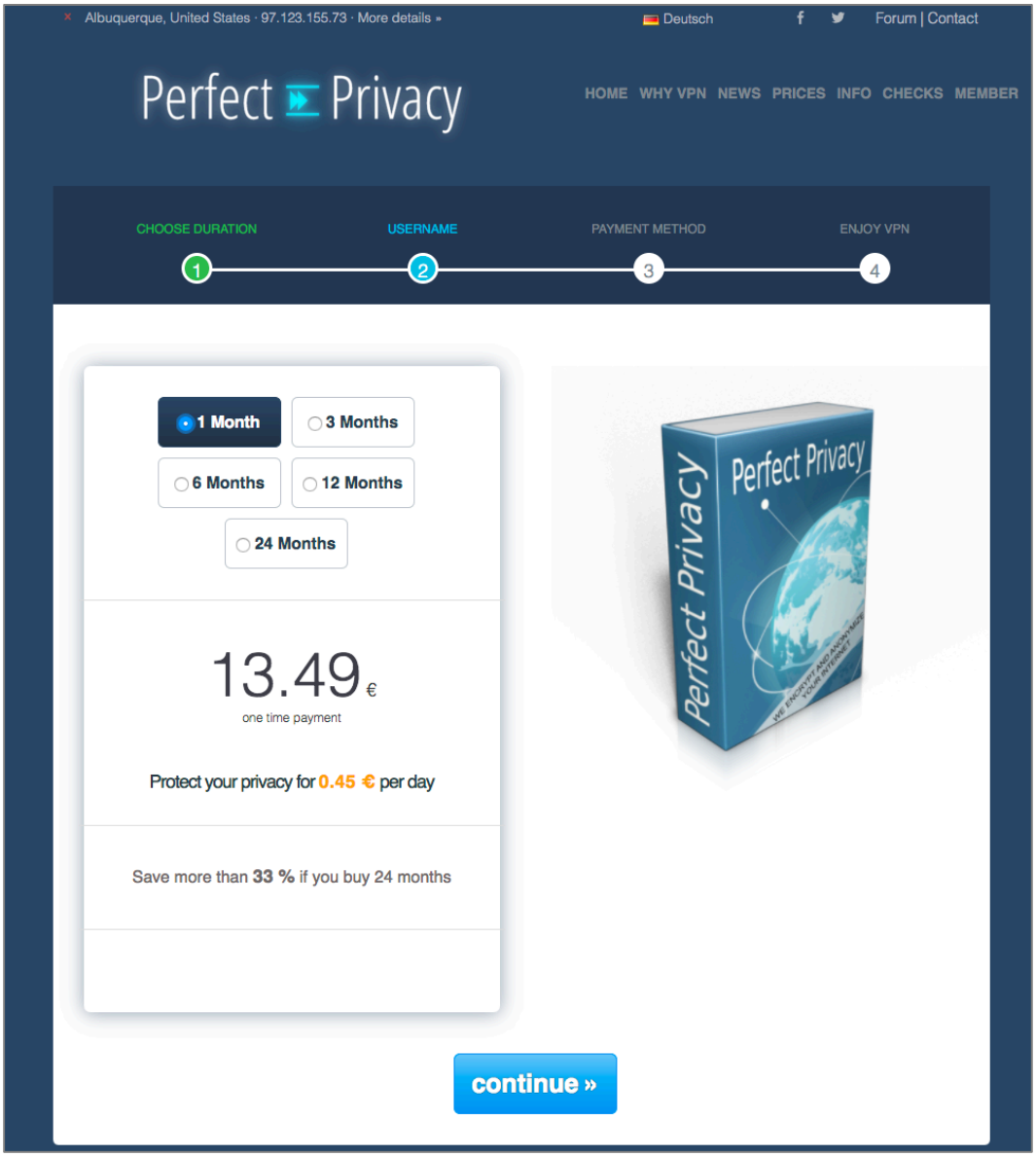
1. Open a browser, visit Perfect-Privacy at *https://perfect-privacy.com,* and then select the *Prices* button.



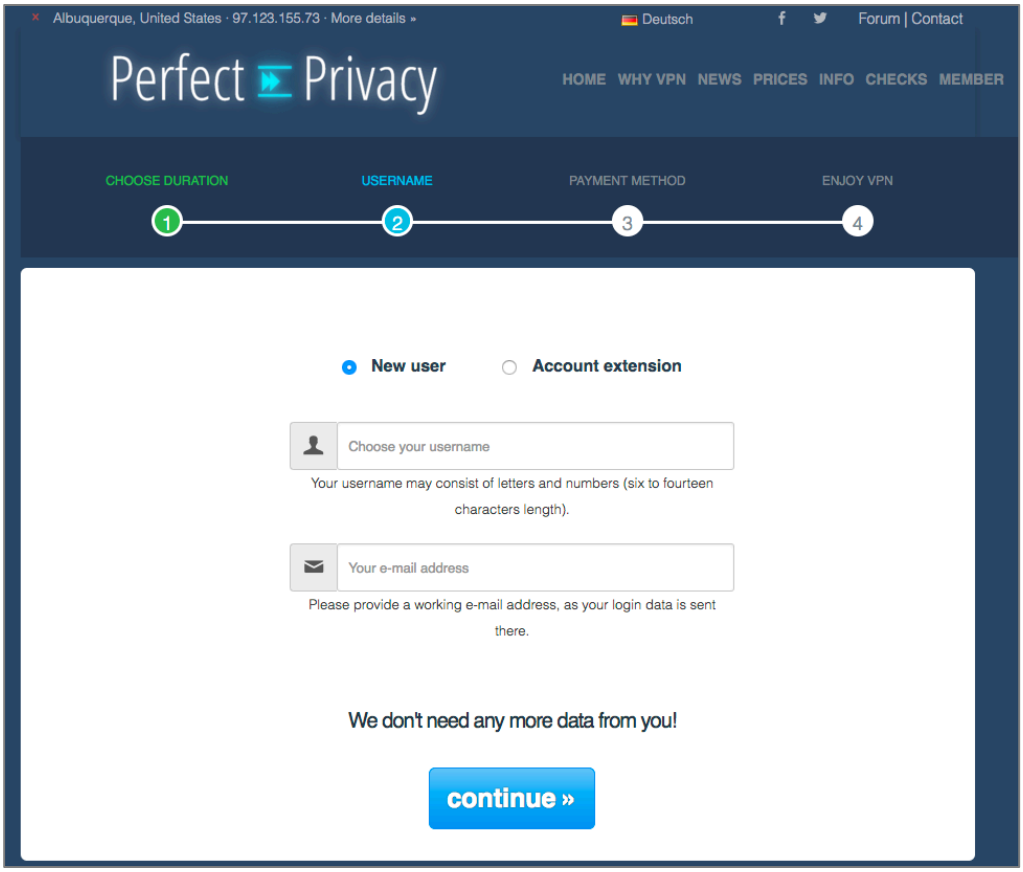
[3] *https://perfect-privacy.com/*

2. Select the *Sign Up Now* button.

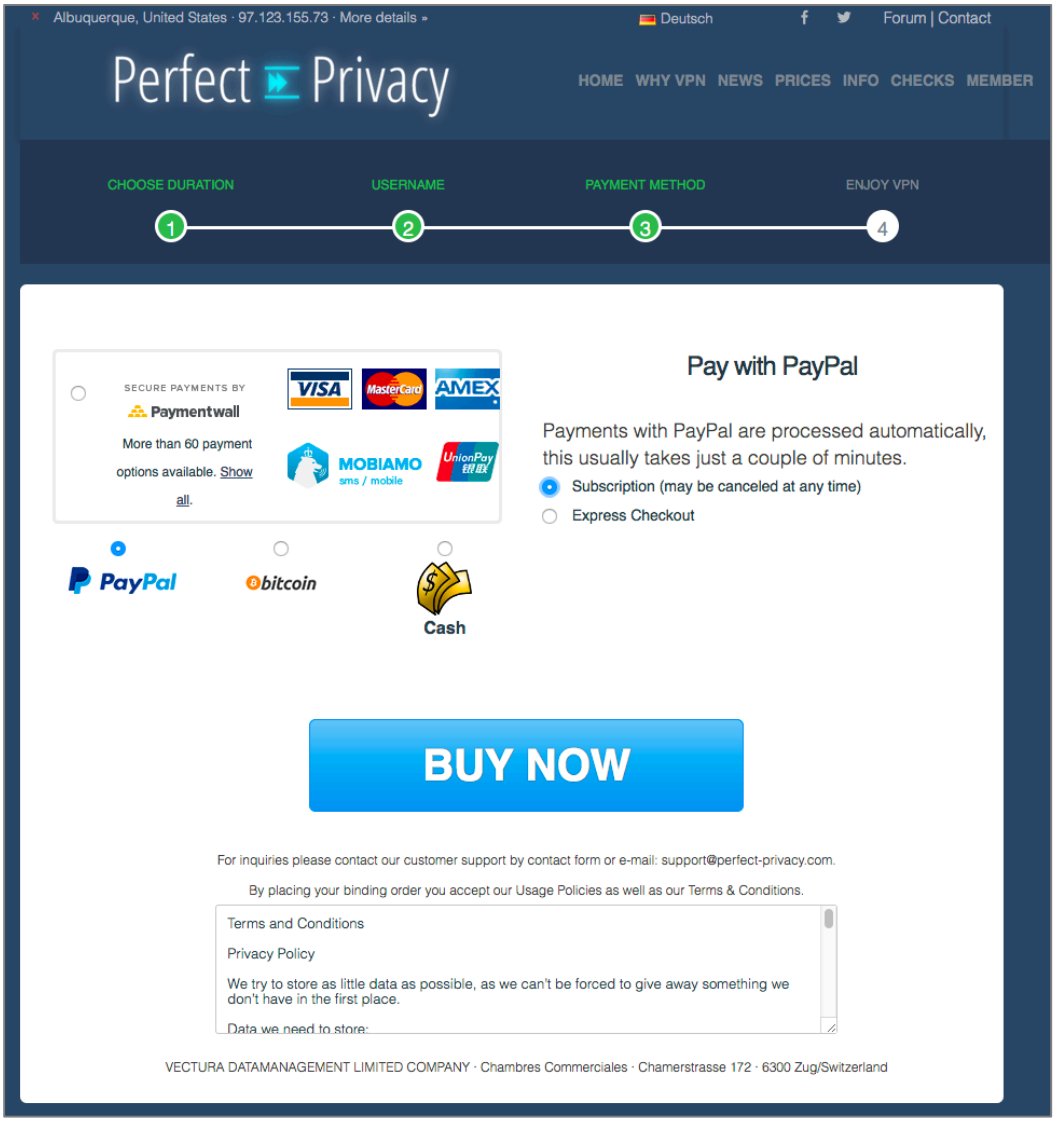
3. At the *Choose Duration* page, select your desired subscription term (the longer, the lower per month cost). Then select the *Continue* button.



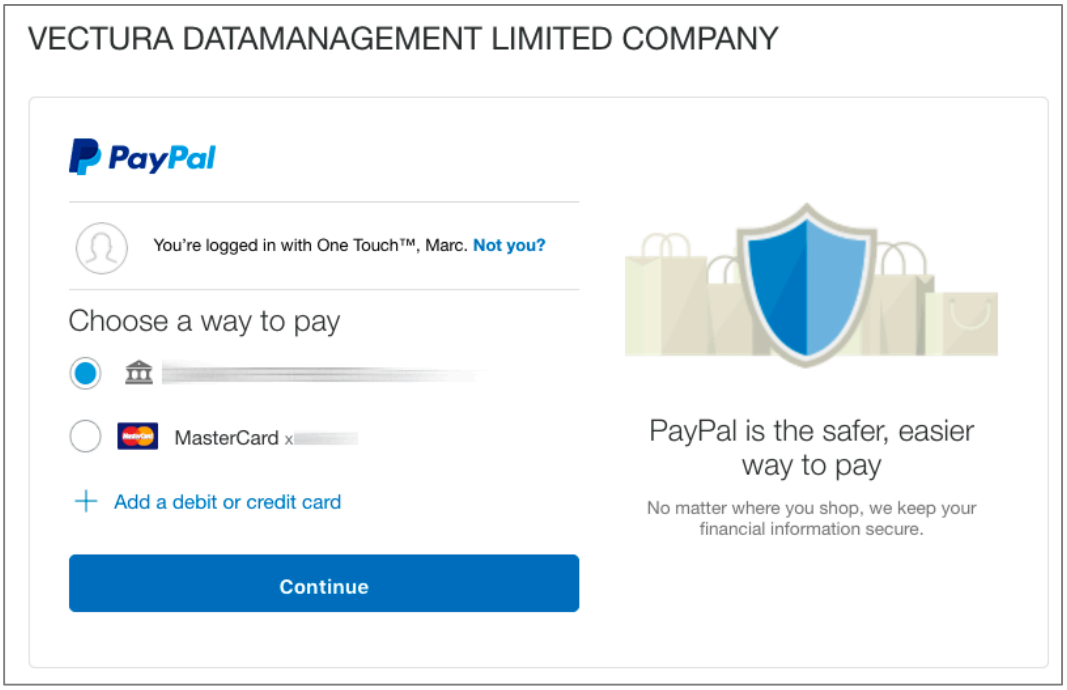
4. At the *Username* page, select *New user*, create a *Username*, enter your *e-mail address*, and then click *Continue*.



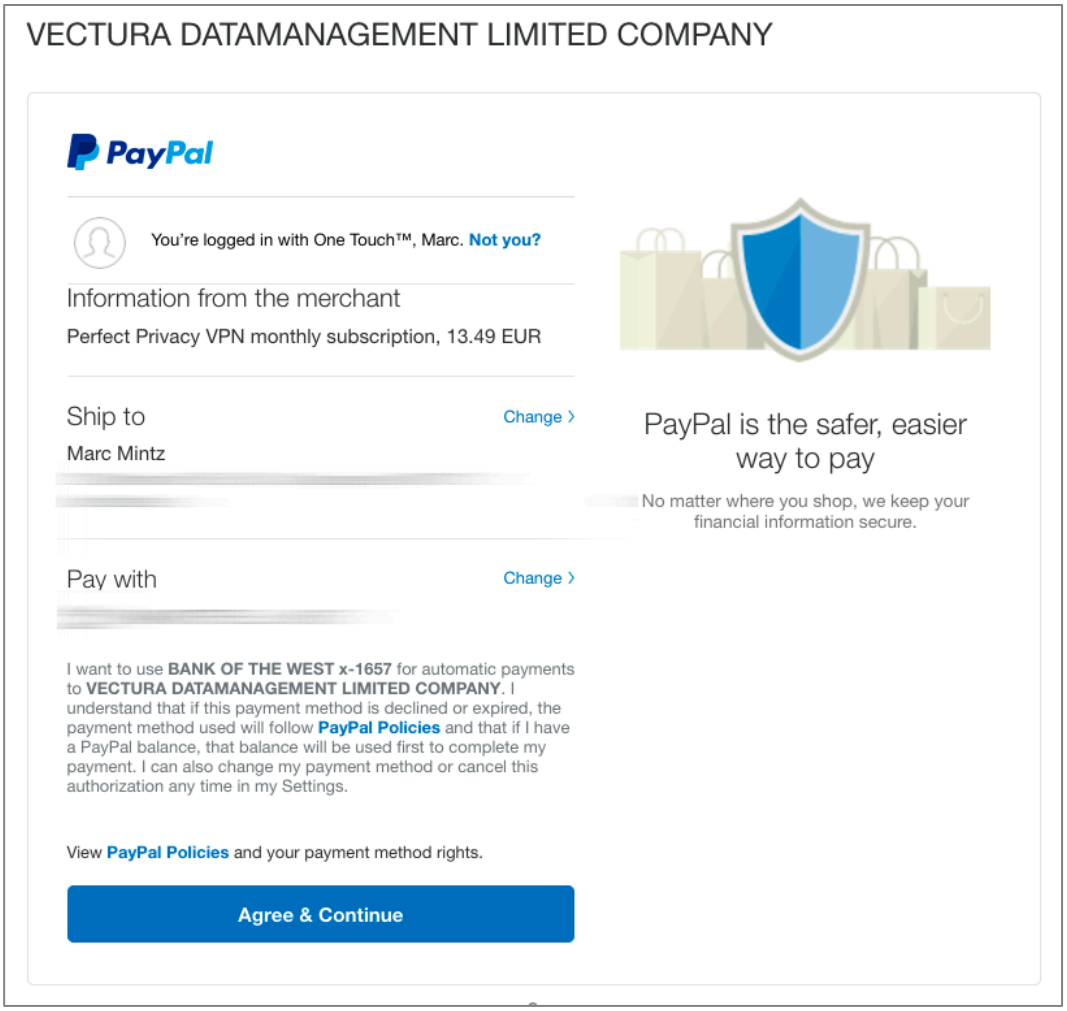
5. At the *Payment Method* page, select your desired method of payment, and then click *Buy Now*. For this assignment, I've select *PayPal*.



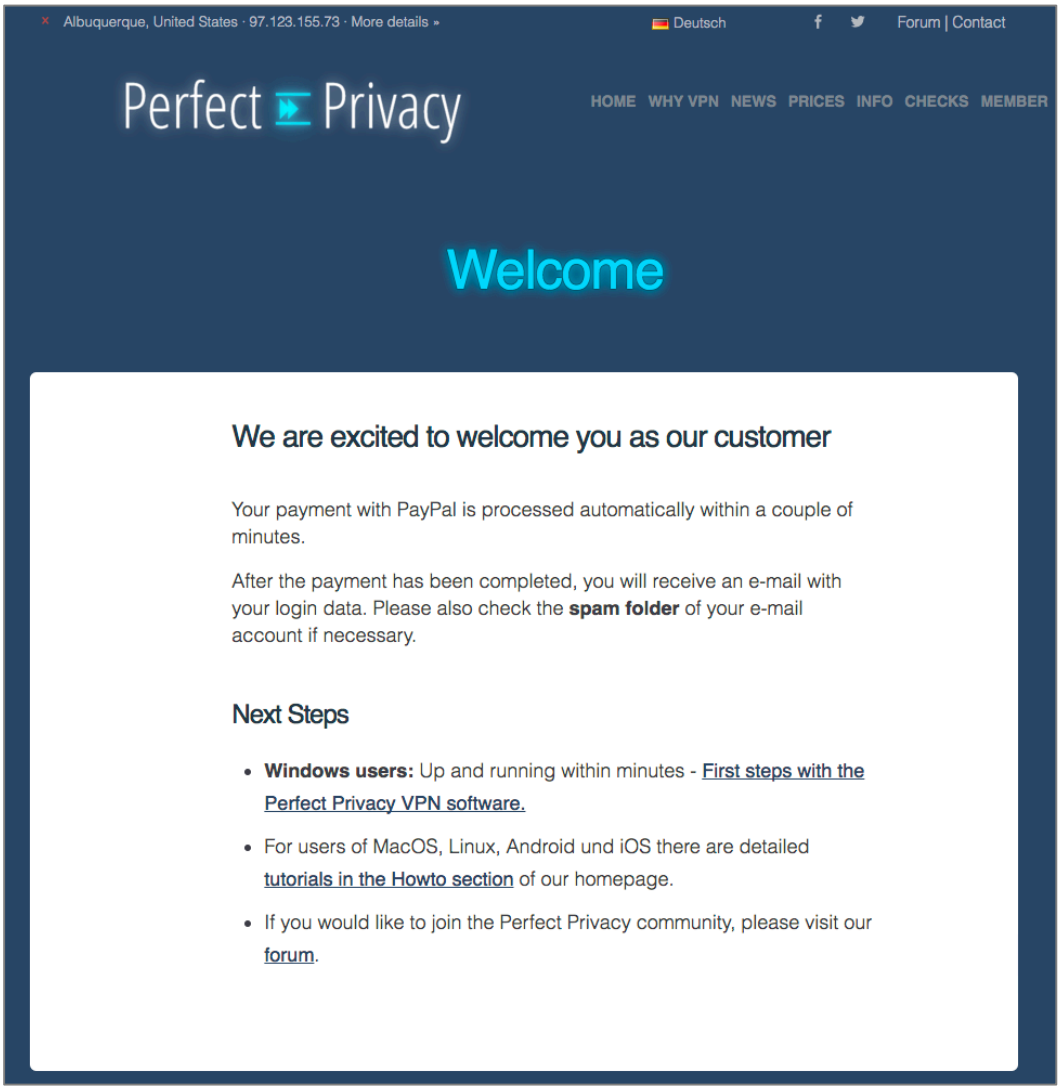
6. Log in to PayPal.
7. At the *PayPal Payment* page, select your *Way to pay,* and then click *Continue.*



8. At the *PayPal* page, verify payment information, and then click *Agree & Continue* to process the payment.



9. You are returned to Perfect-Privacy.

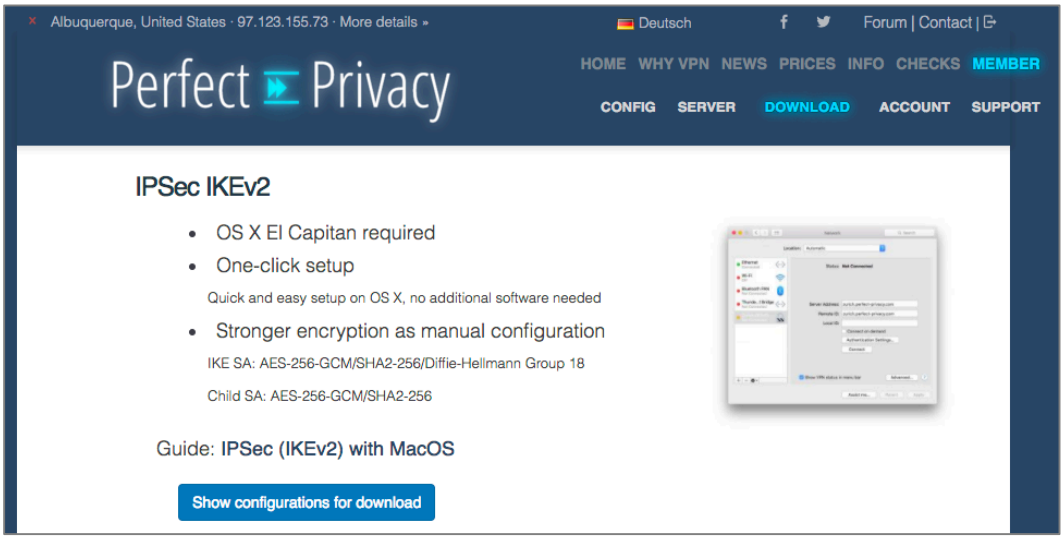


19.3.2 Assignment: Configure IKEv2 VPN With Perfect-Privacy

We recommend using the IKEv2[4] protocol for VPN, both for its strong encryption, and for its automatic activation when accessing the Internet.

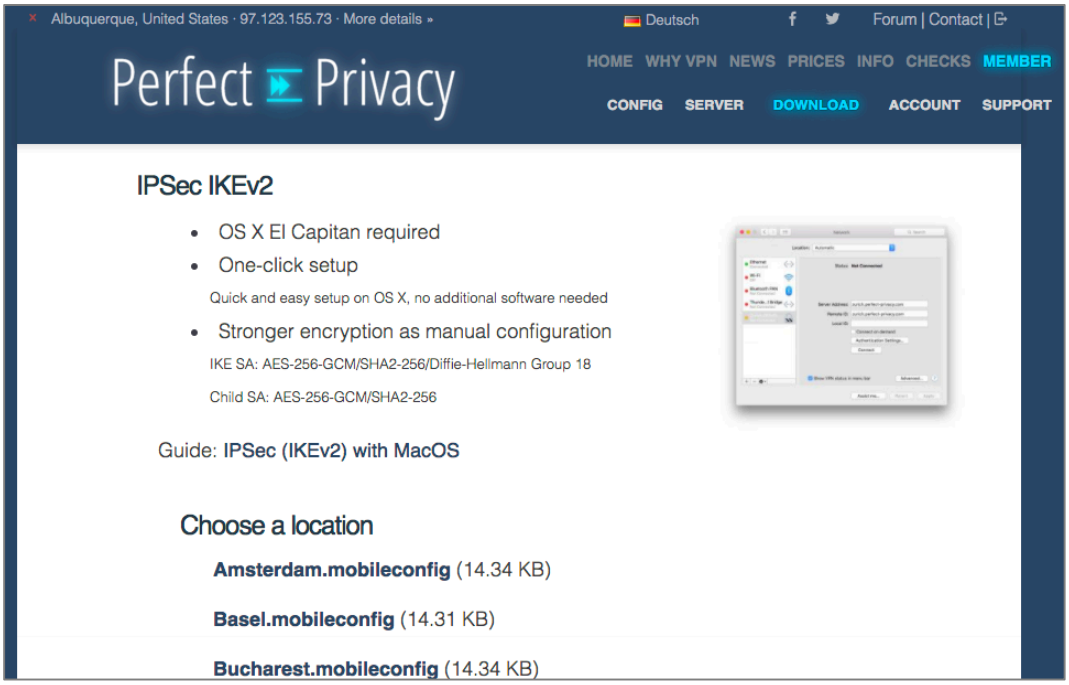
In this assignment, you will configure a VPN connection with Perfect-Privacy using the IKEv2 protocol.

1. Open a browser to the Perfect-Privacy download section[5], and then login with your username and password.
2. Scroll down to the *IPSec IKEv2* section, and then click *Show configurations for download* button.



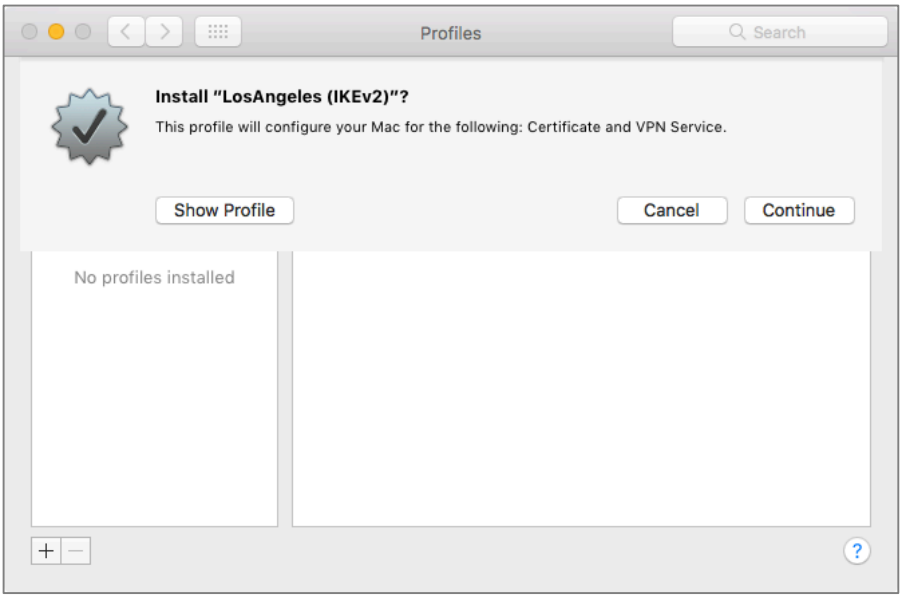
[4] *https://en.wikipedia.org/wiki/Internet_Key_Exchange*
[5] *https://www.perfect-privacy.com/member/download/*

3. Select the location configuration profile to download. For this example, select *LosAngeles.mobileconfig.*.

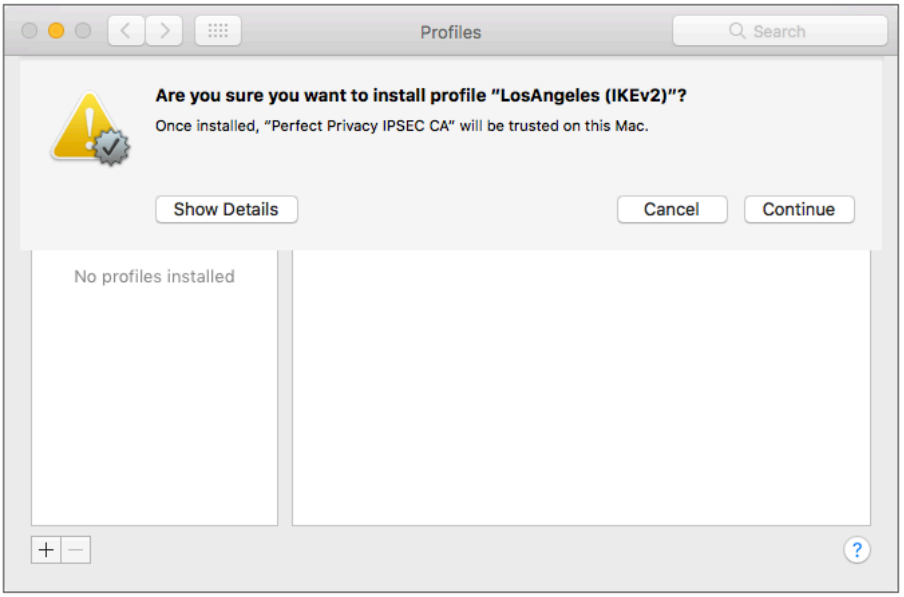


4. Double-click the downloaded profile *LosAngeles.mobileconfig*.

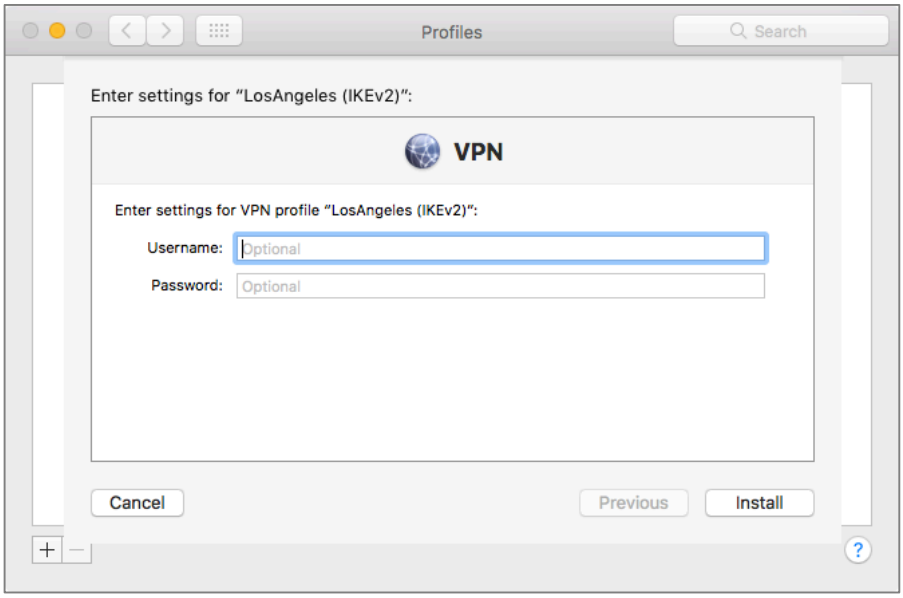
5. The profile installer will launch. Select the *Continue* button.



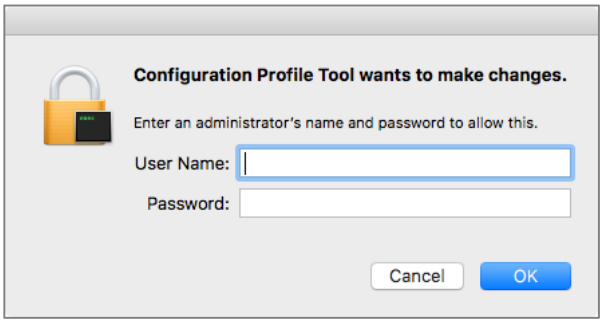
6. At the confirmation window, select *Continue*.



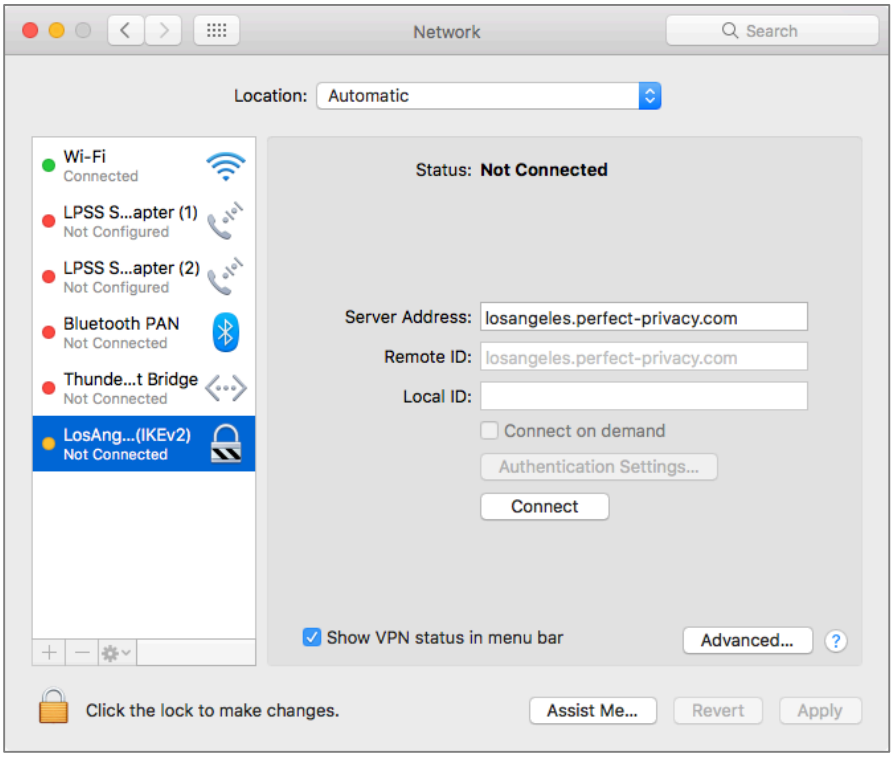
7. In the *Enter Settings for <profile name>* window, enter your *Perfect-Privacy Username* and *Password*, and then click *Install.*



8. At the authorization window, enter an administrator *User Name* and *Password.*

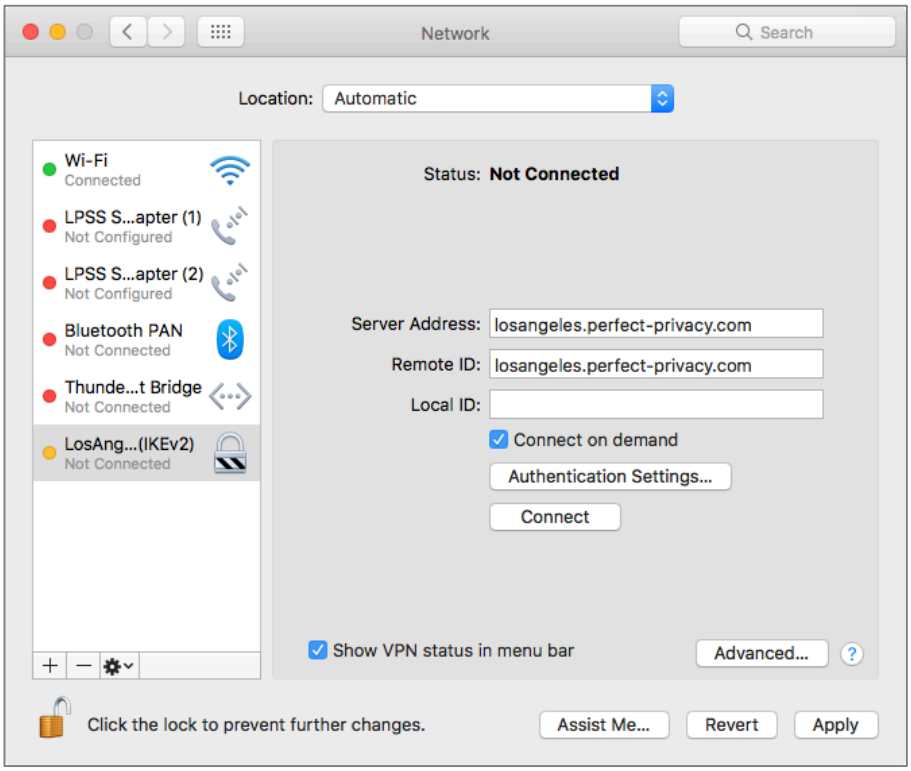


9. The location profile will install.
10. Open *System Preferences* > *Network*. You will see the profile listed.



11. Unlock *System Preferences*.

12. Enable *Connect on demand*, enable *Show VPN status in menu bar*, click *Apply*, and then close System Preferences. With this enabled, whenever you connect to the Internet, the profile will automatically launch, creating a VPN connection with your VPN server.



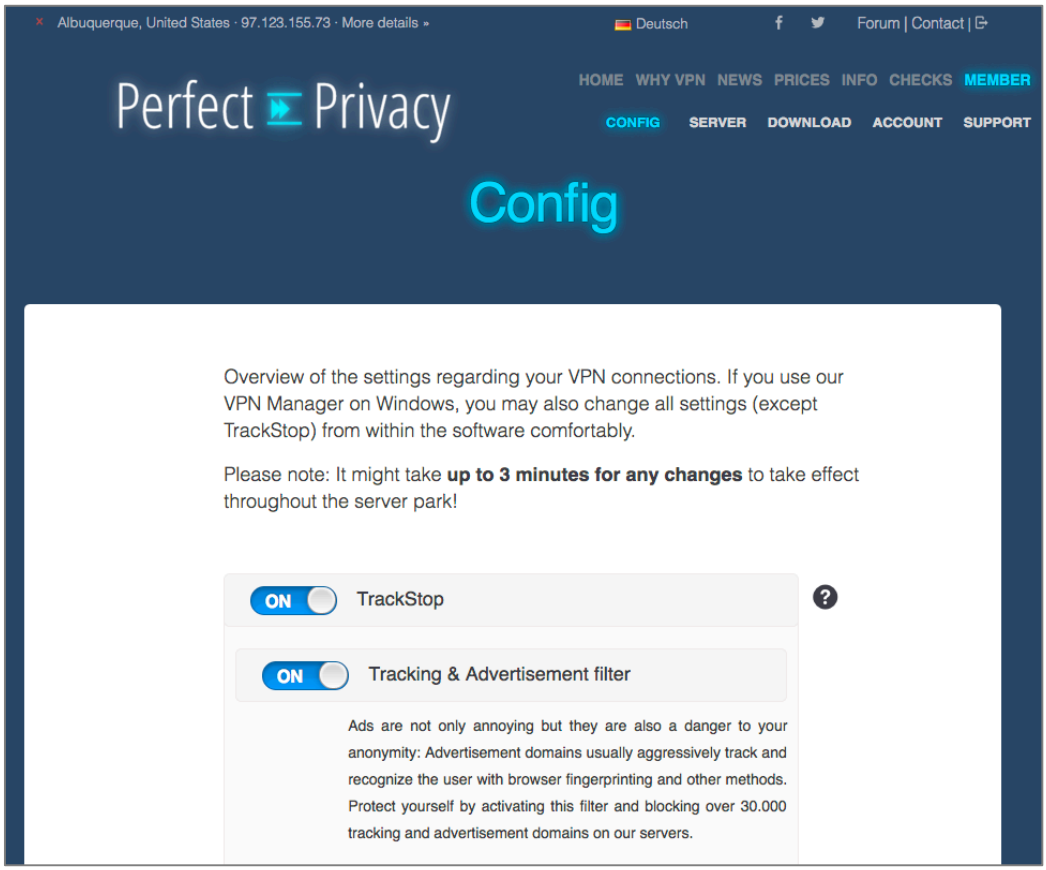
13. A new icon may be found in your menu bar, reporting your connection status.

19.3.3 Assignment: Advanced Perfect-Privacy Settings

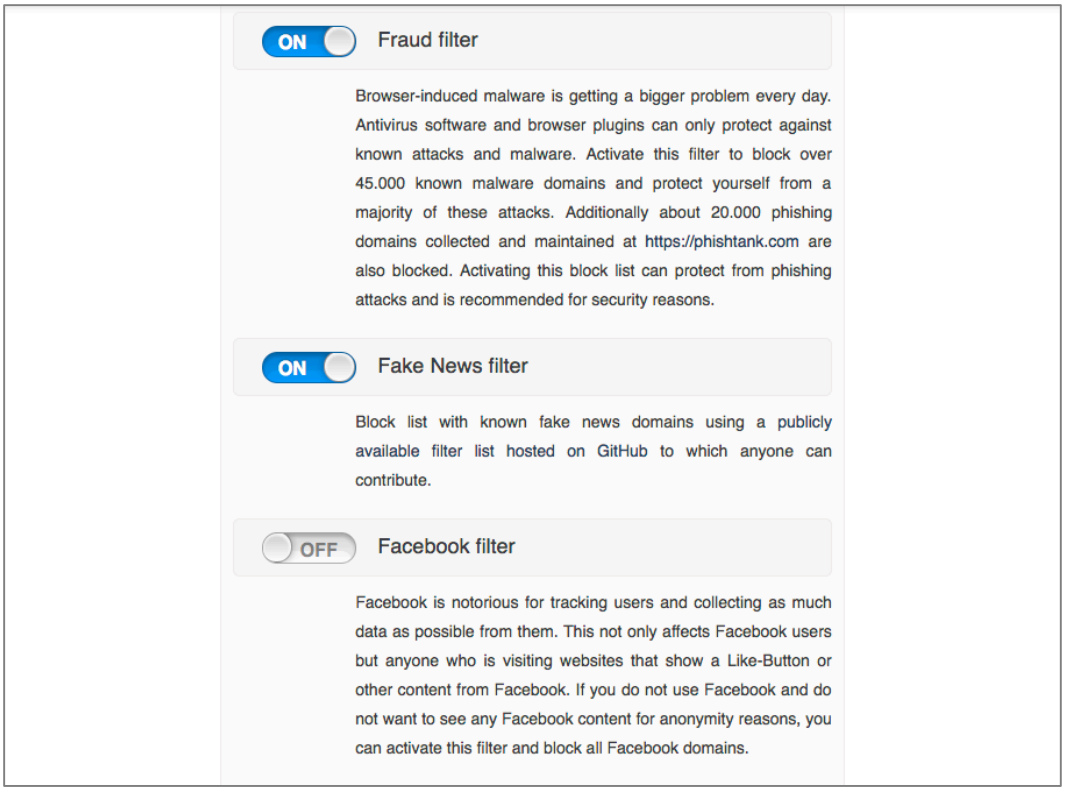
Most quality VPN hosts provide for advanced account configuration. Perfect-Privacy offers several unique options.

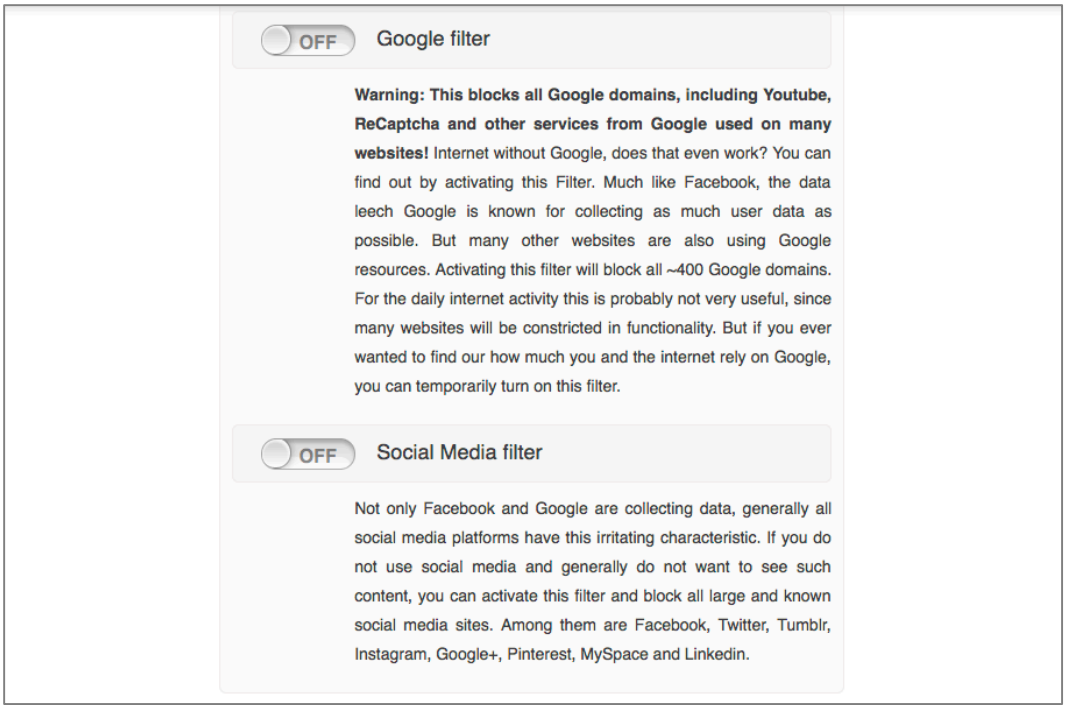
In this assignment, you will configure your advanced Perfect-Privacy settings.

1. Open a browser to the Perfect-Privacy configuration page[6]. If you receive an authentication prompt, enter your Perfect-Privacy *Username* and *Password*.
2. Read each of the options, and then configure to your taste. Listed below are my settings.



[6] *https://www.perfect-privacy.com/member/config/*


ON
Fraud filter
Browser-induced malware is getting a bigger problem every day. Antivirus software and browser plugins can only protect against known attacks and malware. Activate this filter to block over 45.000 known malware domains and protect yourself from a majority of these attacks. Additionally about 20.000 phishing domains collected and maintained at https://phishtank.com are also blocked. Activating this block list can protect from phishing attacks and is recommended for security reasons.
ON
Fake News filter
Block list with known fake news domains using a publicly available filter list hosted on GitHub to which anyone can contribute.
OFF
Facebook filter
Facebook is notorious for tracking users and collecting as much data as possible from them. This not only affects Facebook users but anyone who is visiting websites that show a Like-Button or other content from Facebook. If you do not use Facebook and do not want to see any Facebook content for anonymity reasons, you can activate this filter and block all Facebook domains.


OFF
Google filter
Warning: This blocks all Google domains, including Youtube, ReCaptcha and other services from Google used on many websites! Internet without Google, does that even work? You can find out by activating this Filter. Much like Facebook, the data leech Google is known for collecting as much user data as possible. But many other websites are also using Google resources. Activating this filter will block all ~400 Google domains. For the daily internet activity this is probably not very useful, since many websites will be constricted in functionality. But if you ever wanted to find our how much you and the internet rely on Google, you can temporarily turn on this filter.
OFF
Social Media filter
Not only Facebook and Google are collecting data, generally all social media platforms have this irritating characteristic. If you do not use social media and generally do not want to see such content, you can activate this filter and block all large and known social media sites. Among them are Facebook, Twitter, Tumblr, Instagram, Google+, Pinterest, MySpace and Linkedin.

ON
Use random exit IP address
OFF
Default port forwarding
OFF
Use custom port forwarding

Done!

19.4 Mesh VPN

Another way in which VPN can be configured is a *mesh VPN*. This strategy places multiple computers within the same virtual network regardless of where they are geographically located on the Internet. All the computers operate as if they are on the same physical network, and all traffic between each of the computers is military-grade encrypted. Mesh VPN is ideal for groups of people to exchange files, screen share, and access databases from each other, while maintaining full privacy from the outside world.

We now have software that enables mesh networks for a trivial cost. Keep in mind that VPN is only as secure as the provider, and the vendor of choice is a US company, subject to US federal laws and National Security Letters giving the NSA full access to logs and data crossing the vendor servers.

19.5 LogMeIn Hamachi

LogMeIn[7] is a US-based company with a line of top-grade cloud services. They are best known for their *LogMeIn* remote support software, allowing technical support staff both attended and unattended access to client and server computers.

One of their lesser-known, but game-changing products is *Hamachi*[8]. Hamachi is a cloud-based VPN, eliminating the need for expensive VPN boxes. As if that weren't enough, it also allows for three different types of VPN configurations: Gateway, mesh, and hub & spoke. We will restrict discussion here to the mesh option.

As of this writing, Hamachi is free for use with 5 or fewer nodes (computers). Up to 32 nodes on one network is available for $29/year. Up to 256 nodes on a network is available for $119/year.

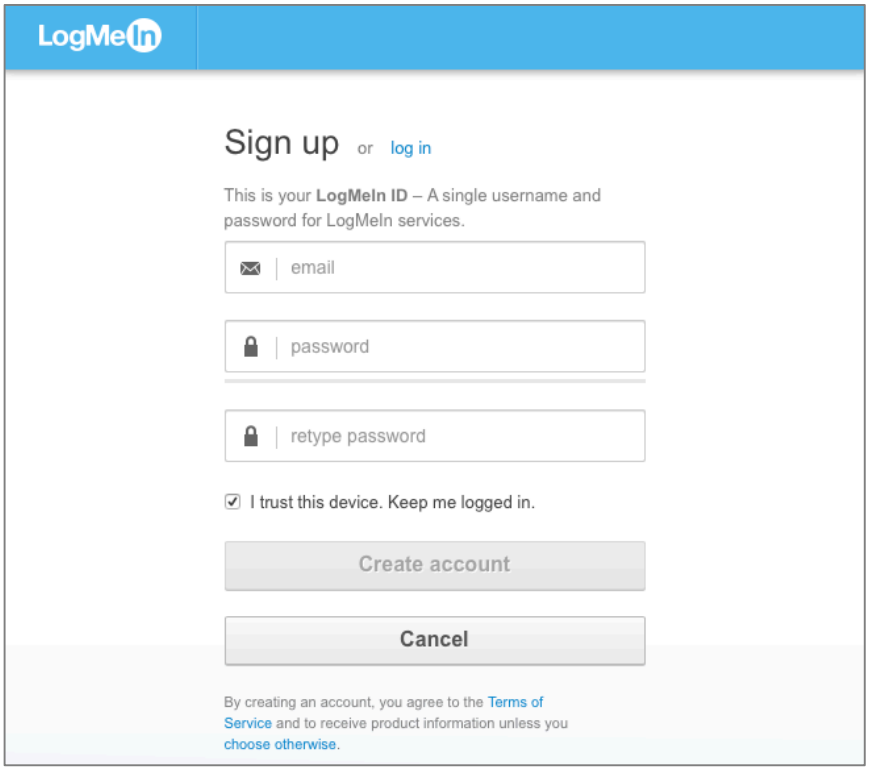
19.5.1 Assignment: Create a LogMeIn Hamachi Account

In this assignment, you create a LogMeIn Hamachi account, so that you can deploy a free Hamachi network for up to 5 computers. Should you eventually need more computers on the network, your account can easily be upgraded at any time.

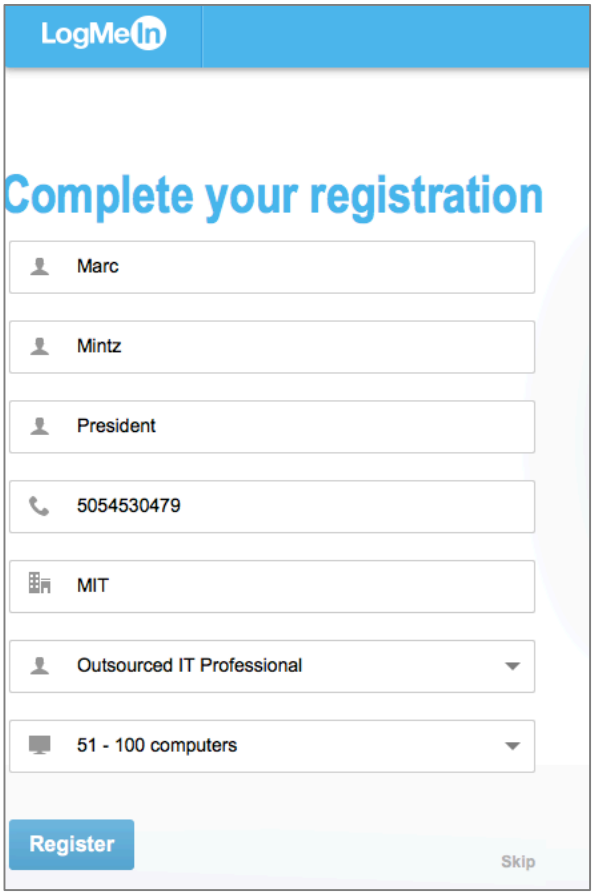
[7] *https://logmein.com*
[8] *https://secure.logmein.com/products/hamachi/*

1. Open a browser, and go to the Hamachi home page at *https://secure.logmein.com/products/hamachi/default.aspx*. The Hamachi home page opens. Click the *Sign up link*.

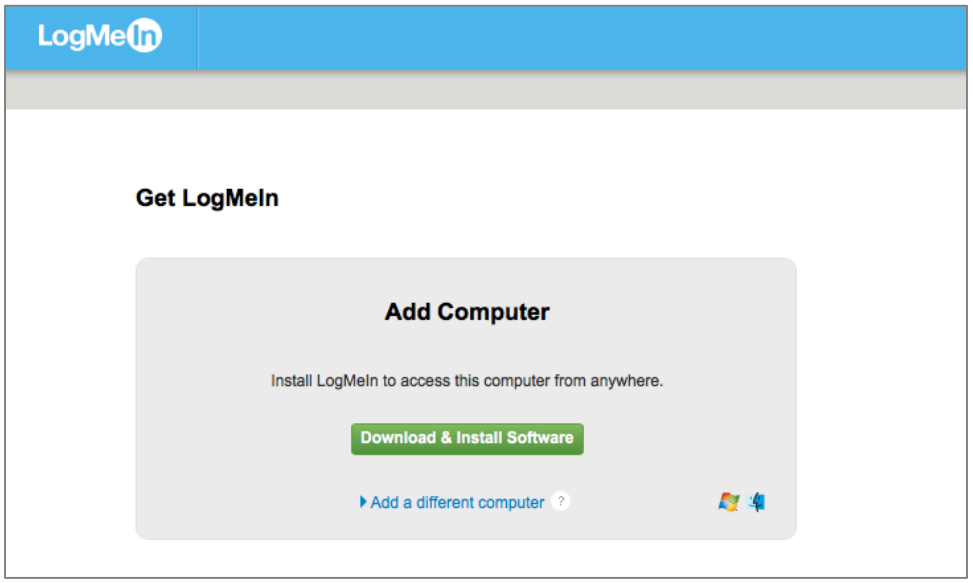
2. Select the *Try it Free* button. In the *Sign Up* field, enter all requested information, and then select the *Create Account* button.



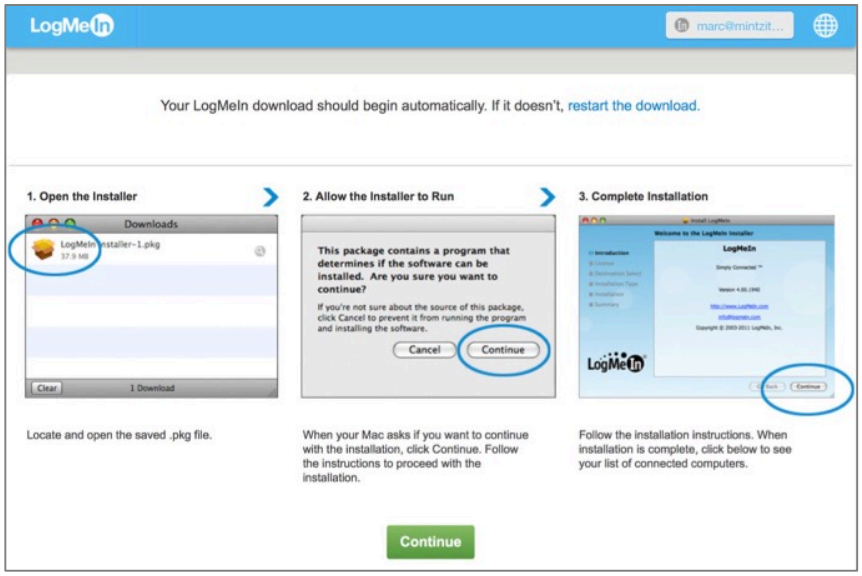
3. In the *Complete Your Registration* page, enter all requested information, and then select the *Register* button.



4. At the *Get LogMeIn* page, select the *Download and Install Software* button to install the software on this computer. If you don't need the software on this computer, but want to install on other computers, click the *Add a different computer link,* and then follow the on-screen instructions.

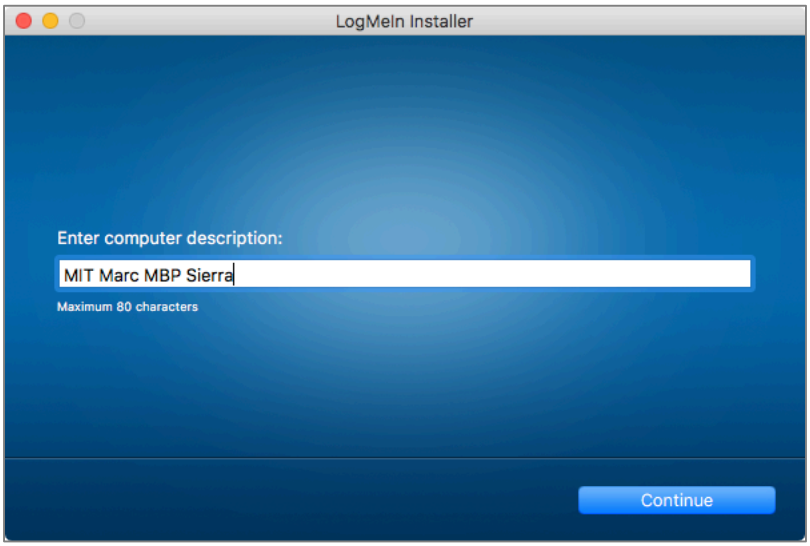


5. The software will begin to download, and the guide page will appear. **Do not** select the *Continue* button quite yet.



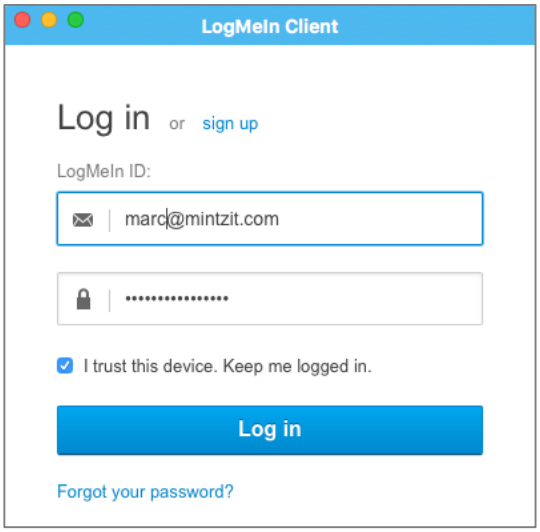
6. Go to your Downloads folder, and open the *LogMeIn Installer.app*. Enable the *I have read and agree…* checkbox, and then select the *Install* button.

7. At the authentication prompt, enter an administrator username and password, and then select the *Install* button.
8. At the prompt, enter a name for your computer, and then select the *Continue* button.

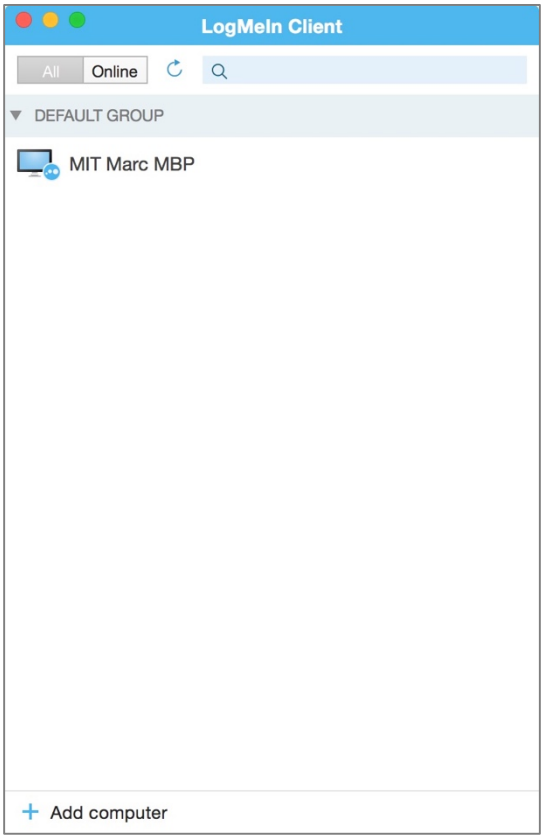


9. At The *Installation Was Successful* pane, select the *Finish* button.

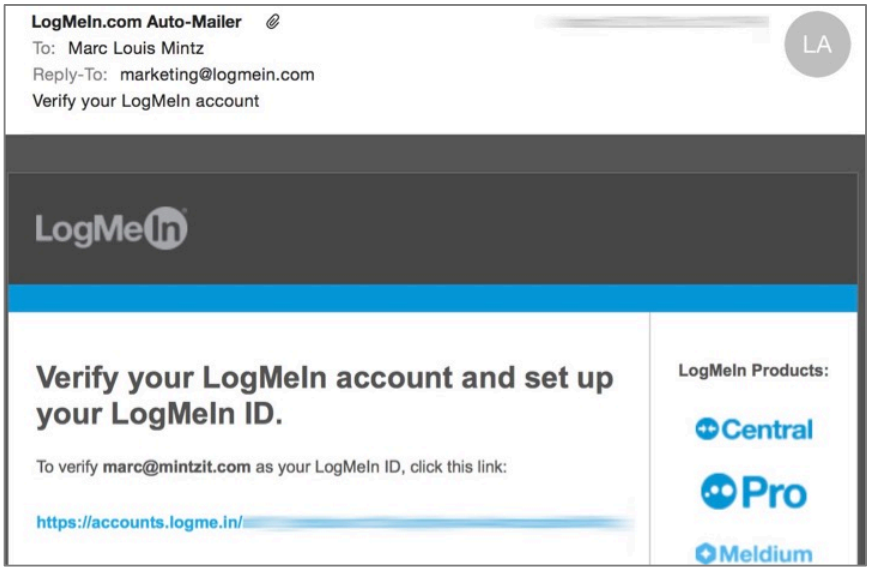
10. The *LogMeIn Client Log In* window appears. Enter the same email and password used to create the account, and then select the *Log In* button.



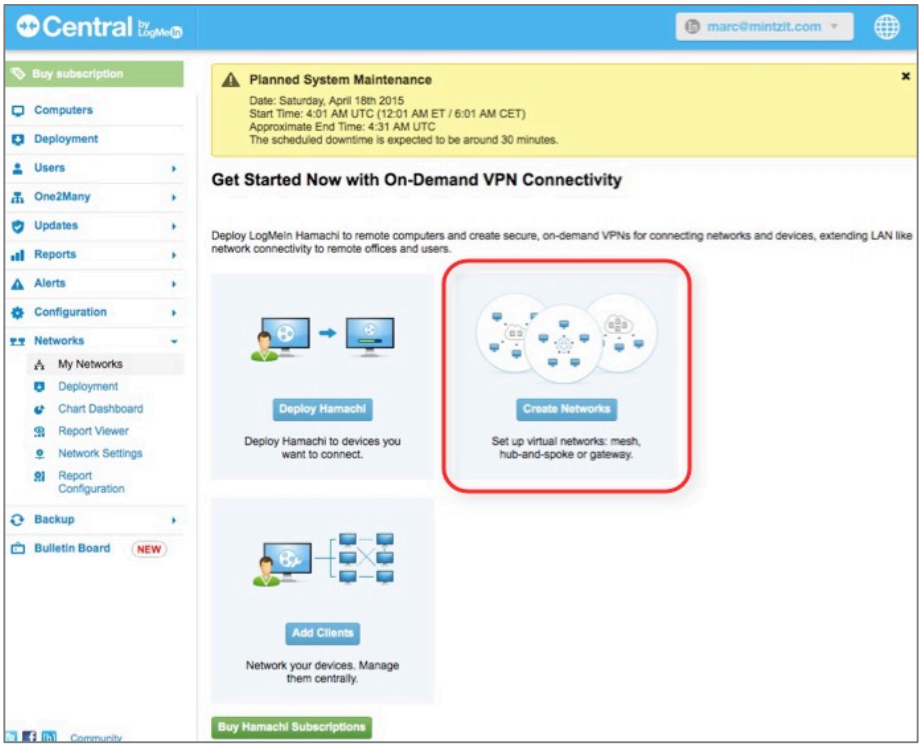
11. The *LogMeIn Client* window will now display all users who are members of this network (currently, just yourself.) To add additional users, skip to step 13.



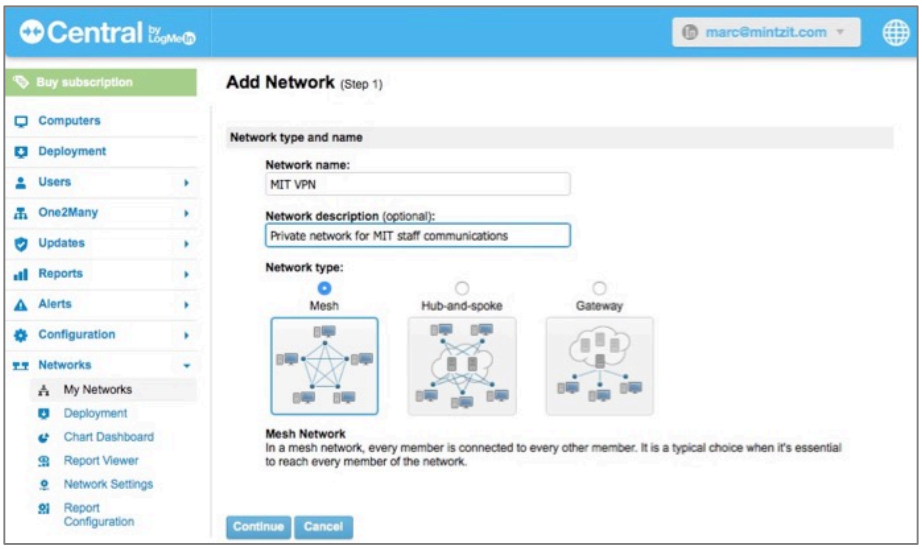
12. Open your email to check for a verification message from LogMeIn. Click the reply link.



13. Returning to your browser, in the *Hamachi* screen, select *Networks* > *My Networks*, and then select *Create Networks.*



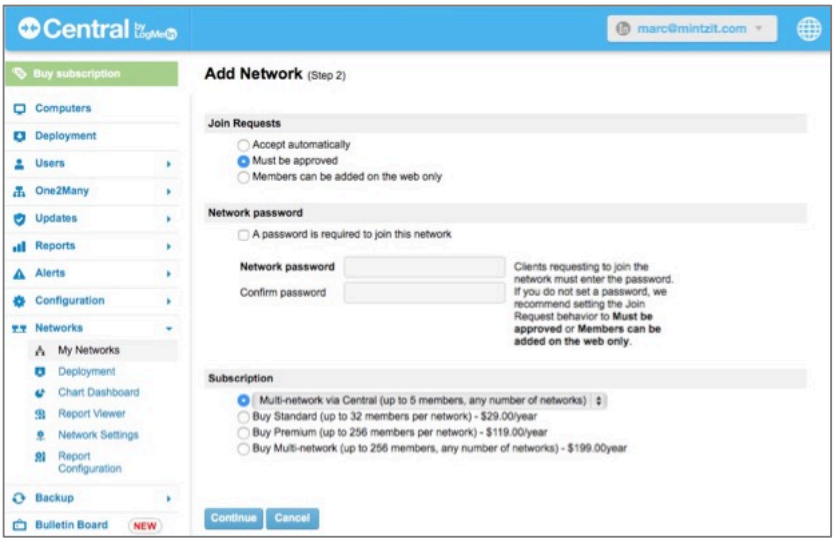
14. In the *Add Network* page, in the *Network Name* field, give your network a human-readable name, select the *Network Type* (in this example, we are creating a *Mesh* network), and then select the *Continue* button.



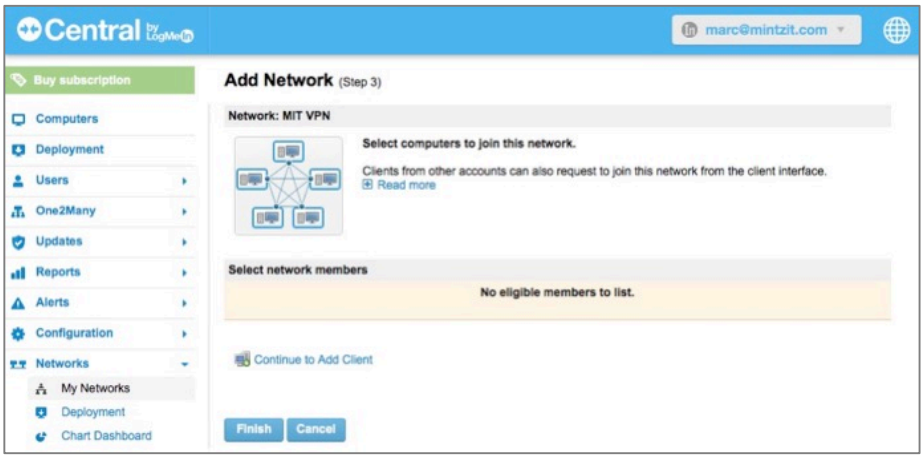
15. In *Add Network (Step 2),* in *Join Requests*:

    - In *Join Requests,* specify how users will be able to join the VPN network. If security is a concern, we recommend *Must be approved* to keep strangers out.
    - In *Network password,* configure if a password is required to join the network. Assuming all user computers have strong passwords, and full-disk encryption, it would be extremely unlikely anyone other than the authorized user would be attempting network connection. However, if security is a concern, enable the password requirement, and then set a strong password.
    - In *Subscription,* specify what subscription level is requested. For the purposes of this assignment, select *Multi-network via Control (up to 5 members, any number of networks.)*

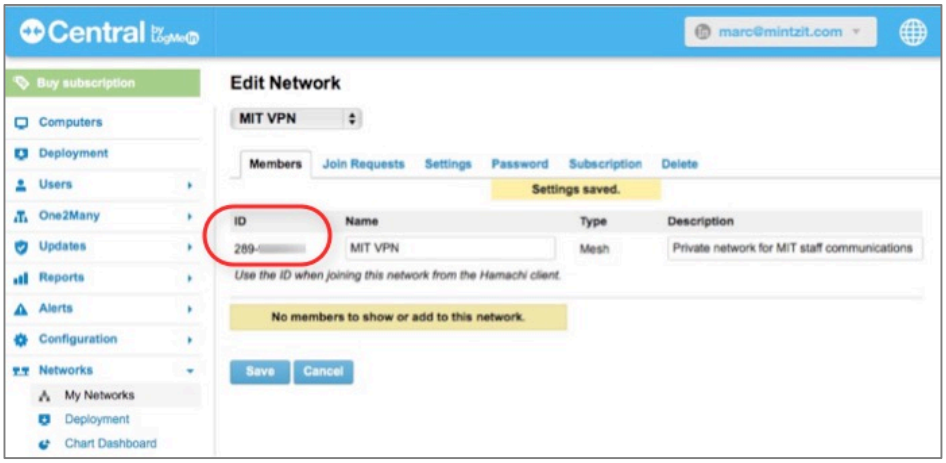
16. Select the *Continue* button.



17. The *Add Network (Step 3)* appears. Select the *Finish* button.



18. In the *Edit Network* page, make note of your network *ID,* as this will be used when joining the network. Select the *Save* button.



Congratulations, your account is created and you are ready to add users to your mesh VPN network.

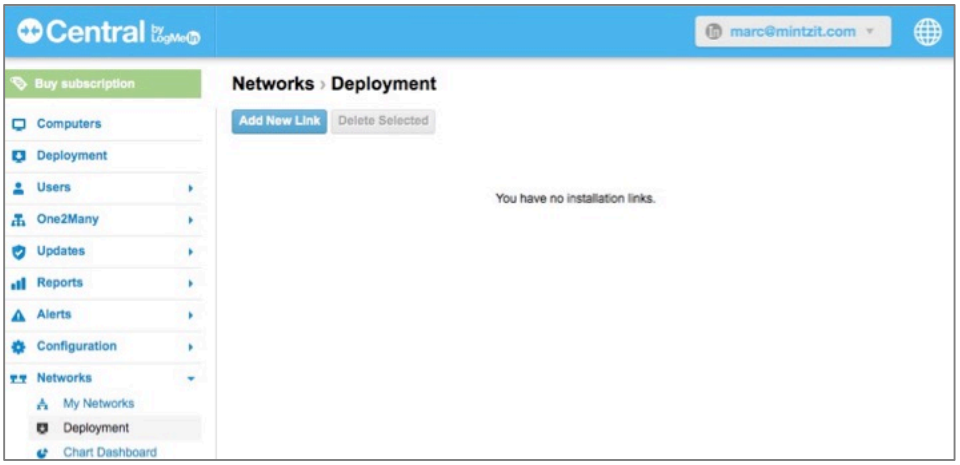
19.5.2 Assignment: Add Users to a Hamachi VPN Network

In this assignment, you add users to the Hamachi VPN network created in the previous assignment.

- Prerequisite: Completion of the previous assignment.

1. Open a browser and go to *https://secure.logmein.com*, and then login with your username and password. The *LogMeIn Central* page appears.

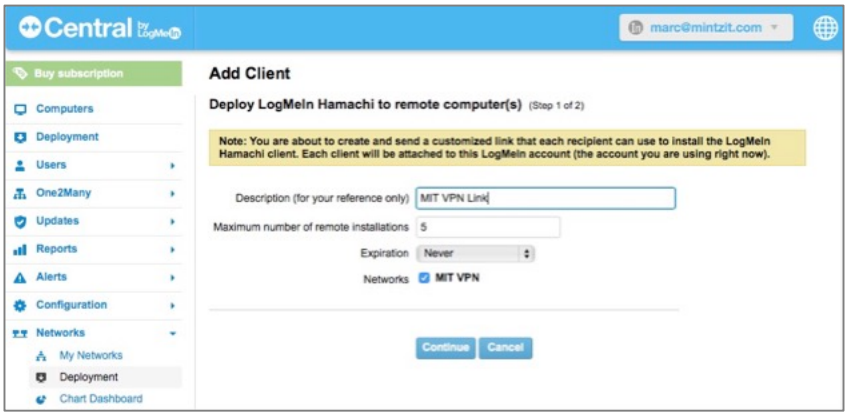
2. Select the *Networks* > *Deployment* link, and then select the *Add New Link* button.



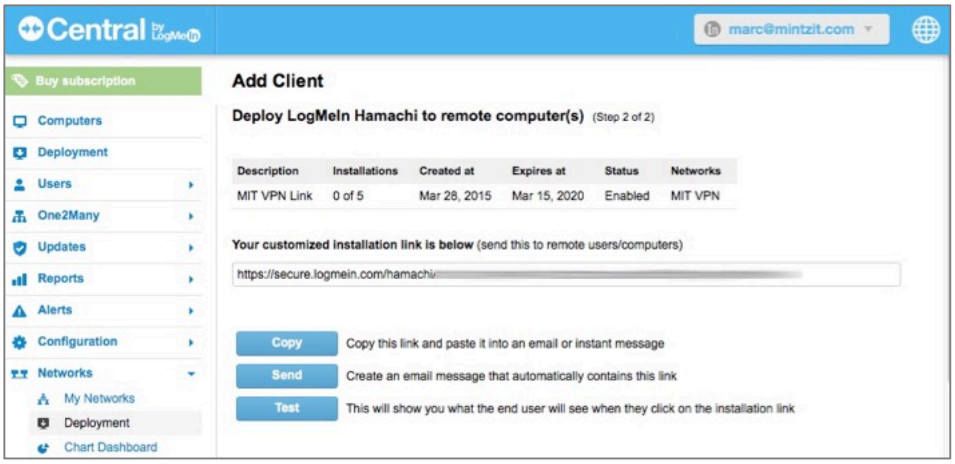
3. In the *Add Client* page, you will create a link that can be used to allow a custom installation of Hamachi.

    - In the *Description* field, enter information for your own reference.
    - In the *Maximum number of remote installations* field, enter, well, the maximum number of installations permitted (with a free account, this is 5.)
    - In the *Expiration* pop-up, specify when the link expires.
    - In *Networks,* enable the checkbox for the network this link will be used.

4. Select the *Continue* button.



5. The *Add Client* link page appears. You have the option to *Copy* or *Send* the link. For our assignment, select *Send.*

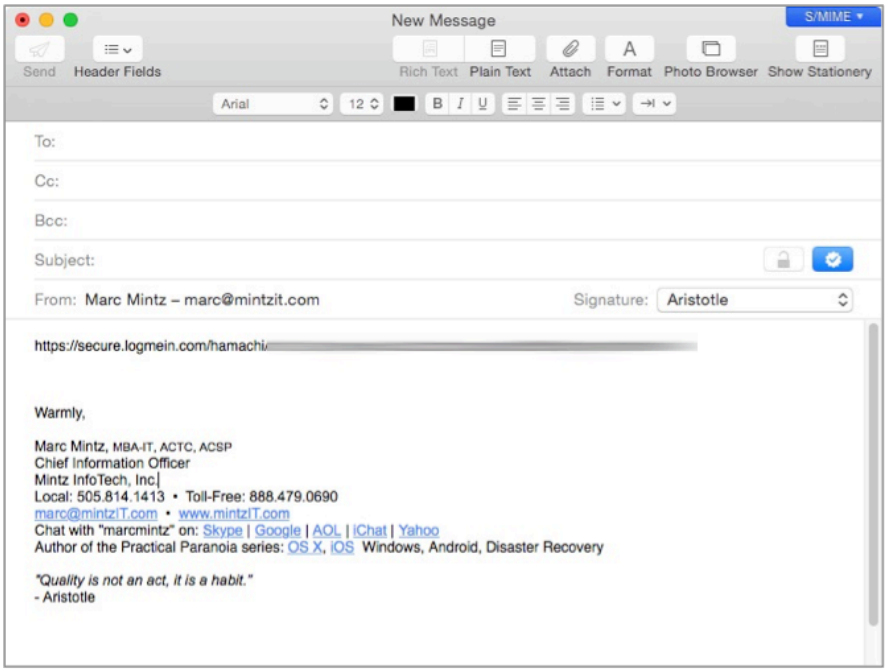


The default email client will open, with the link pre-entered in the body area, awaiting entry of recipient(s) and a message.

6. Enter recipient address(es).
7. Enter a subject.
8. Enter additional information in the body area explaining what to do next. Something like: *Listed below is a link to download LogMeIn Hamachi. This*

software will allow all of us to create a private encrypted network within which we may continue our plans for world domination.

9. Send the email.



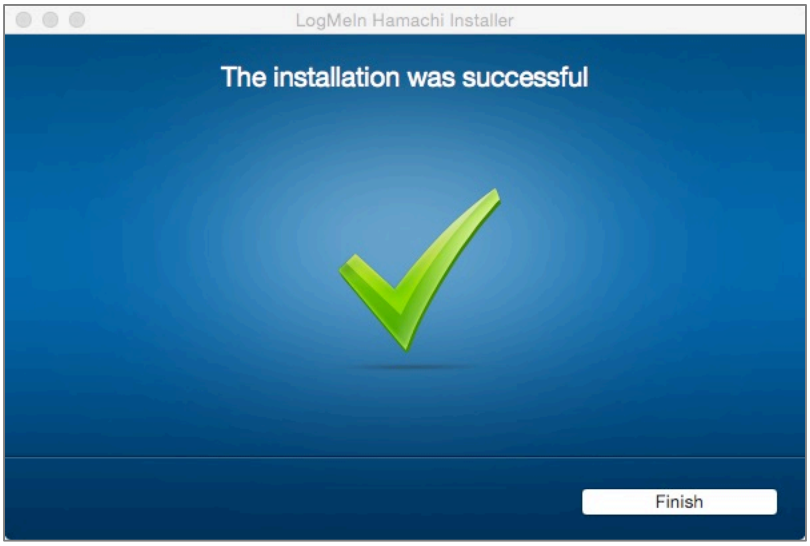
10. When the recipient clicks the link, they are taken to the *Hamachi Installer* page. Enable the *I have received this link from a trusted source* check box, and then select the *Continue* button.

11. At the *Download* page, select the *Download Now* button.

12. The *LogMeIn Hamachi Installer* will download. Once complete, launch the installer, enable the *I have read…* check box, and then select the *Install* button.

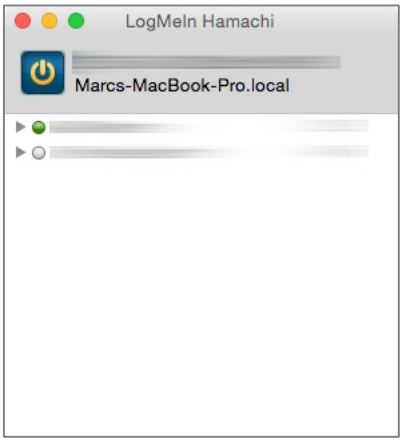
13. The *Attach client to LogMeIn account* screen appears. Select the *Next* button.

14. When the installation completes, select the *Finish* button.

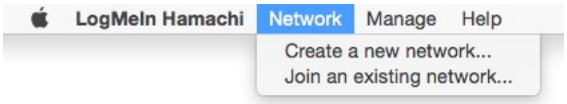


15. Open *LogMeIn Hamachi.app,* located in */Applications/LogMeIn Hamachi.* In my case, there are networks that I currently belong to listed, one of which I am connected (the green button), and one I am not connected with (white button). Neither of which is the MIT VPN network (yet).

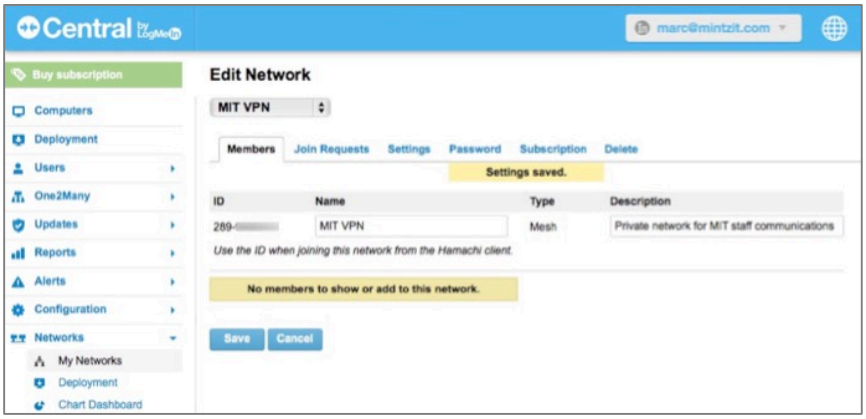
    - If your target network appears in the *LogMeIn Hamachi* window with a green button, all is done!
    - If your target network doesn't appear in the *LogMeIn Hamachi* window, we have a few more steps to complete.

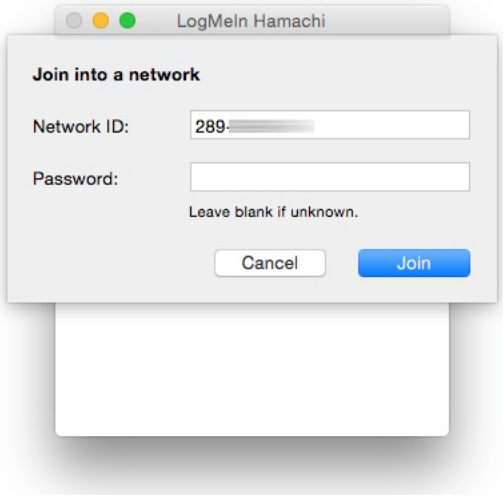


16. In LogMeIn Hamachi select *Network* menu > *Join an existing network*…

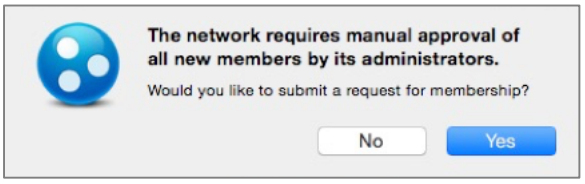


17. Enter the *Network ID* as displayed in step 18 of the previous exercise, and then select the *Join* button.

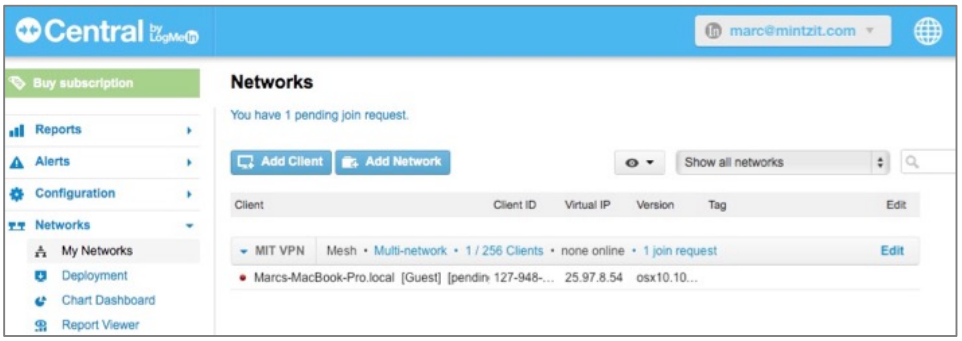




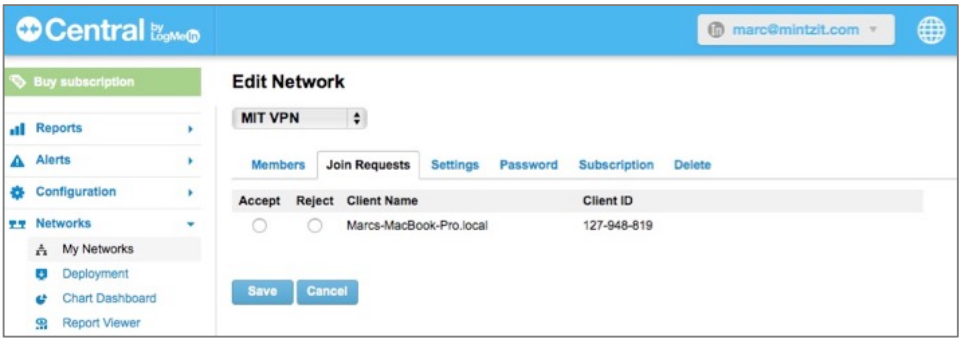
18. At the dialog box asking *Would you like to submit a request for membership?* Select the *Yes* button.



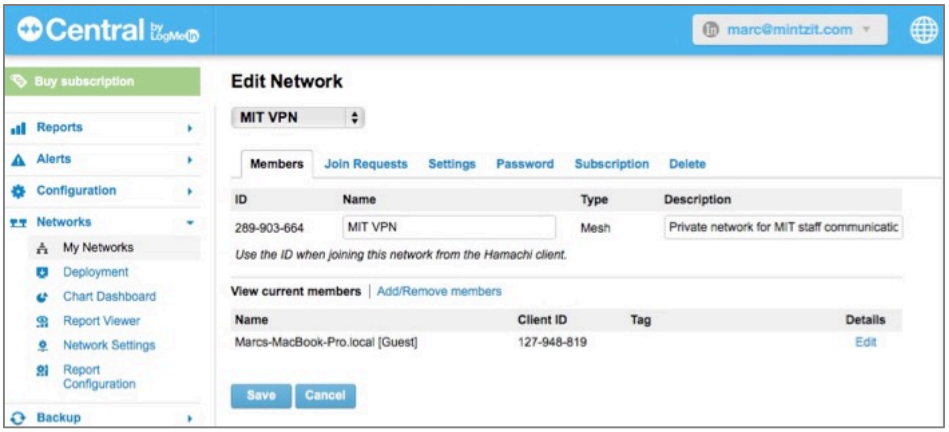
19. Back at your computer, or the computer used to administer this network, in the *LogMeIn Central* page > *Networks* > *My Networks* will be found all the users who have received and responded to their links from the previous steps. Select the *Edit* link.



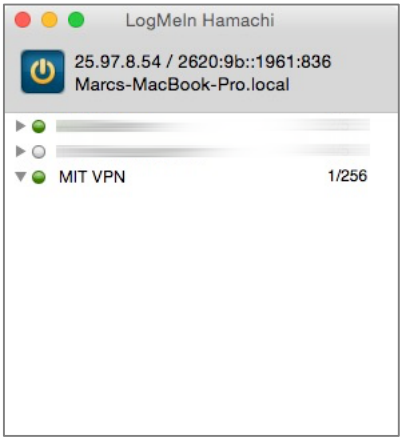
20. In the *Edit Network* page, select *Join Requests*. If the pending join request is from someone who should join the network, select the *Accept* radio button. If they are someone who should not join the network, select the *Reject* radio button, and then select the *Save* button.



21. In the *LogMeIn Central* page > *Networks* > *My Networks* > *Members* you will see that this user is now part of the group.



22. Returning to the user who has just been accepted into the group, their Hamachi window will now reflect they are part of the network (the network appears in the window) and that they are actively joined to the network (green button next to the network name.)



Awesome! You have your first member of the VPN network. Of course, you can't do anything with just one person. The value of VPN comes with additional members. Repeat the steps in this assignment to have at least one more computer part of your network, and then move on to the next assignment.

19.5.3 Assignment: File Sharing Within a Hamachi VPN Network

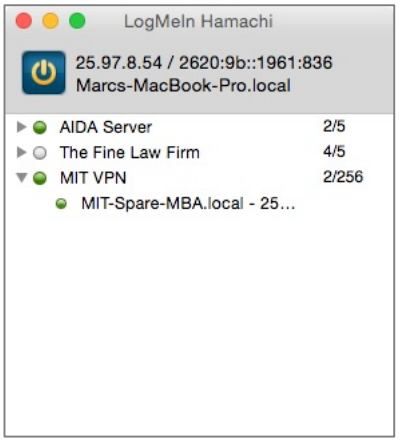
In this assignment, you file share within a Hamachi VPN network.

- Prerequisite: Completion of the previous assignment.

In the typical macOS network environment, one Mac can see another Mac over the network using an automatic discovery protocol, *Bonjour*. This protocol isn't in effect over a VPN connection, so we will need a different method of accessing other computers for file sharing and other network activities.

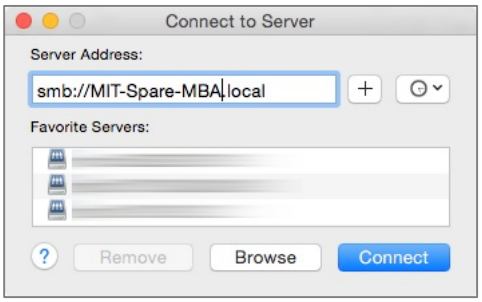
Before we begin, please make sure the other computer has *System Preferences* > *Sharing* > *File Sharing* enabled, that SMB file sharing is enabled, and that you know a username/password allowed to file share.

1. Launch *Hamachi*, and verify the target computer is showing as *Online*. In this example, the other computer is named *MIT-Spare-MBA.local*.



2. On your macOS/OS X computer, in the *Finder,* select the *Go* menu > *Connect to Server*. Enter *afp://<name of computer>* (to create an *Apple Filing Protocol* connection), or *smb://<name of computer>* (to create a *Server Message Block* connection) and then select the *Connect* button.

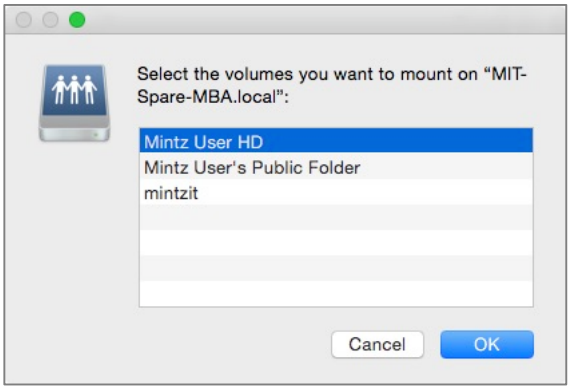
    - Although AFP[9] is the legacy standard of communication between Apple computers. As of OS X 10.10, Apple is moving away from it in favor of SMB, the long-time Windows standard. SMB[10] is the preferred protocol for macOS. You will likely have faster network throughput using SMB.



3. When the *Authentication* window appears, select *Registered User,* and then enter your authorized *Name* and *Password,* and then select the *Connect* button.

[9] *https://en.wikipedia.org/wiki/Apple_Filing_Protocol*
[10] *https://en.wikipedia.org/wiki/Server_Message_Block*

4. The available volumes (sharepoints) will appear. Select the desired volume, and then select the *OK* button.



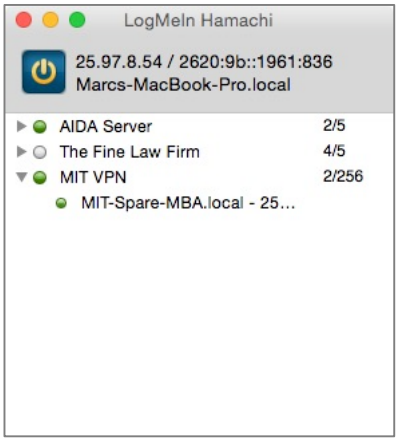
5. The volume will mount to your desktop. Double-click to open and navigate it just as if it were located on your physical network.
6. To file share, all you need do is drag and drop between your computer drives and the mounted volume.
7. When you are ready to disconnect from the remote computer, drag the mounted volume into the *Eject* Dock icon.

19.5.4 Assignment: Screen Share Within Hamachi VPN

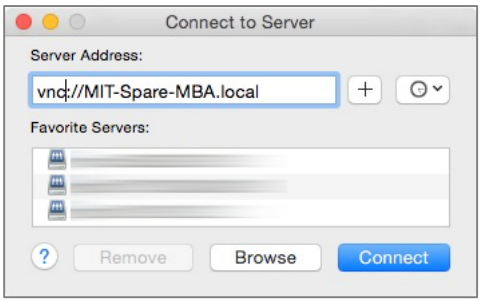
In this assignment, you screen share within the Hamachi VPN environment. If you have followed the previous assignment, then screen sharing is almost identical to file sharing.

Before we begin, please make sure the other computer has *System Preferences* > *Sharing* > *Screen Sharing* enabled, and that you know a username/password allowed to screen share.

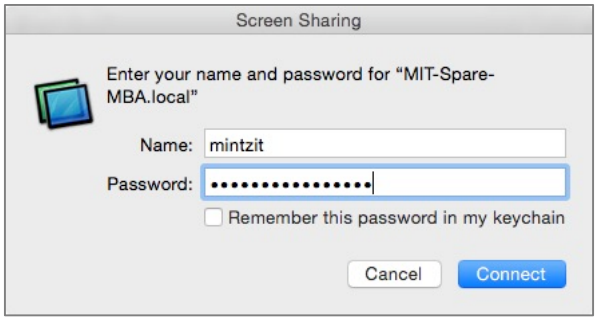
1. Launch *Hamachi*, and verify the target computer is showing as *Online*. In this example, the other computer is named *MIT-Spare-MBA.local.*



2. On your macOS/OS X computer, in the *Finder,* select the *Go* menu > *Connect to Server.* Enter *vnc://<name of computer>* (to create a *Virtual Network Control* connection), and then select the *Connect* button.



3. At the authentication prompt, enter the authorized *Name* and *Password*, and then select the *Connect* button.

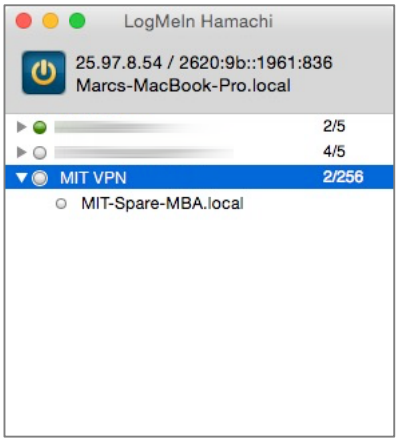


4. The screen of the remote computer will appear. You will be able to control it with your mouse and keyboard.
5. To exit out of screen sharing, close the *screen sharing* window.

19.5.5 Assignment: Exit the Hamachi VPN Network

In this assignment, you stop VPN so that you are no longer connected to the VPN network.

1. On your computer, in the Hamachi window, right-click on the connected network name, and then select *Go Offline* menu. The network button will turn from green to white, indicating you are no longer connected.



2. You may now *Quit* LogMeIn Hamachi.

Great work! You can now create a military-grade, encrypted network, on the fly, so that your friends or business associates can share files, screen share, etc. without fear of data or activities being spied upon.

19.6 Resolving Email Conflicts with VPN

Some email servers will send up a red flag and then block user access to email when the user switches to a VPN connection. This is a good thing as it indicates the email provider is highly sensitive to any possible security breach. In all cases there is a resolution available, although the steps to take will vary with each provider.

As an example, I have outlined below what occurs when using VPN with a Gmail account, and how to gain access to your email after the blockage.

1. The user starts a VPN program to encrypt all data between the user's computer and the Internet.
2. The user attempts to receive Gmail.
3. Google sees attempted access from an unknown machine (the Proxy Server), and blocks access to the account.
4. Both an email and a text from Google are sent notifying the user of suspicious activity. Select the link in either message.
5. The first support file opens. Select the link.
6. In the authentication window, enter your email and password, and then select the *Sign In* button.
7. Another support window opens, explaining the next steps to take. Select the Continue button.
8. The final support window opens. Following the instructions, return to your email application and access your Gmail within 10 minutes. This will provide Google with the authentication to release your account.

20 Social Media

A lot of people say that social media is making us all dumber, but I not think that.
–Unknown author

What You Will Learn In This Chapter

- Create strong passwords for social media sites
- Enable Login Approvals/Two-Factor Authentication
- Configure Facebook, LinkedIn, and Google privacy settings

20.1 What, me worry?[1]

There is no denying that social media[2] has provided us with new levels of connectivity and communication. Victims of natural and man-made catastrophes can instantly assure family and friends of their location and health. Job searches have been reduced to a couple mouse clicks, and those who once would have had no voice, may now have a voice that is heard around the world.

It's this last feature that is a true double-edged sword.

Virtually all social media is free to the user. Few users ever question how a service such as Facebook, that may have operating expenses of 12 *billion* dollars[3], not only can afford such expense, but then go on to have a profit of 10 *billion* dollars. The business model for social media is based somewhat on advertising, but far more so on selling information about *you* to the advertisers.

Social media knows more about you than your mother. Their systems know what you are doing on their site–as well as all ancillary sites such as games, messengers, etc. that are in any way associated with the social media main site–how long you stay on each page, where you came from to land on that page, where you jump off to, what you have purchased, your interests, issues that prompt strong emotion, and more. The data and metadata held by social media sites has been shown to be an extremely accurate predictor of behavior. It is *this* information that is so very valuable to advertisers–and to potential employers, and the government.

It has become the norm for HR departments to scan all social media of a potential employee. The belief is that what a person expresses in social media is a more accurate and honest representation than the employment form or initial interview.

It should be needless to mention that government agencies closely track social media to predict and stop the next terrorist attack, as well as other lesser crimes.

---

[1] Alfred E. Neuman, *https://en.wikipedia.org/wiki/Alfred_E._Neuman*
[2] *https://en.wikipedia.org/wiki/Social_media*
[3] *https://finance.yahoo.com/quote/FB/financials?ltr=1*

20.2 Protecting Your Privacy on Social Media

Privacy on social media starts with understanding that social media watches *everything* you do, when you do it, how long you do it, and who you do it with. It also becomes your *brand*, intentional or not. It colors how others–friends, family, employers, and government–will see you. To this effect, you must manage your brand. This is done by being fully mindful of *everything* about your social media pages. Does it represent you in the best light? If taken out of context, how would it be interpreted?

The next step is to take whatever measures the social media site provides to ensure only those you want in, get in.

20.3 Facebook

Facebook is the reigning king of social media. Whether due to lax security concerns, or the wild popularity of the site, account breaches and hacks are common. Fortunately, Facebook has taken user-centric security controls out of the shadows, and made them easily accessible.

20.3.1 Assignment: Facebook Security and Login

Where You're Logged In

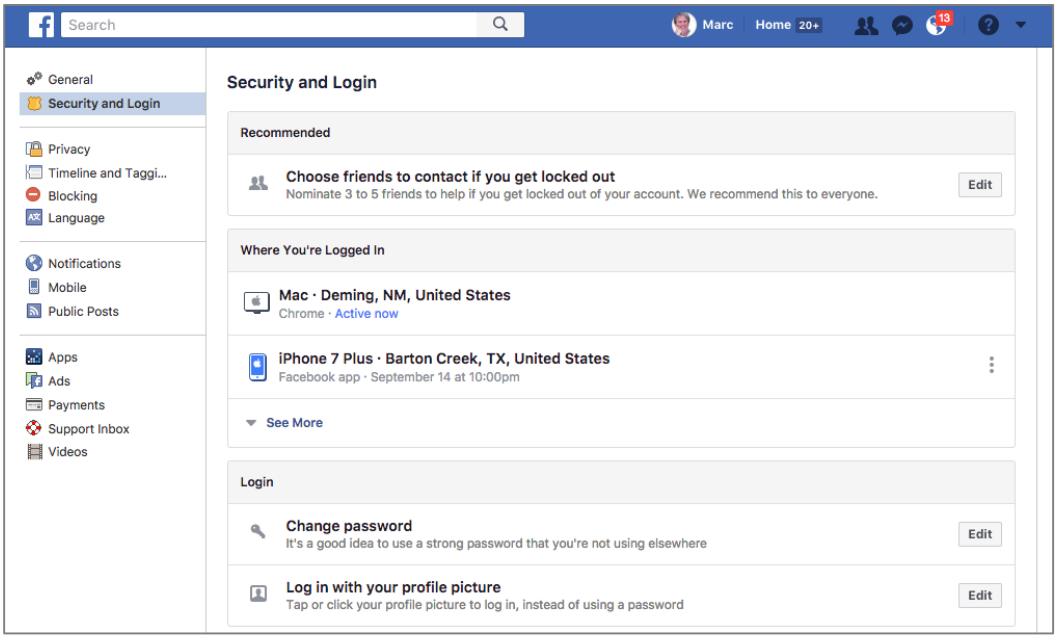
Facebook allows you to see what devices have logged in with your account credentials. Should you not recognize one of these devices, you can immediately log it out of Facebook.

Password

The need for a strong Facebook password is no different than that for your computer. In this assignment, you change your current Facebook password to a strong password.

1. Open a browser to *https://facebook.com/*, and then log into your account.
2. Click the downward triangle at the top right corner of the Facebook window, and then select *Settings*.
3. From the sidebar, select *Security and Login*.

4. Under the *Security and Login* main heading > *Where You're Logged In*, review all of the devices logged in with your credentials.



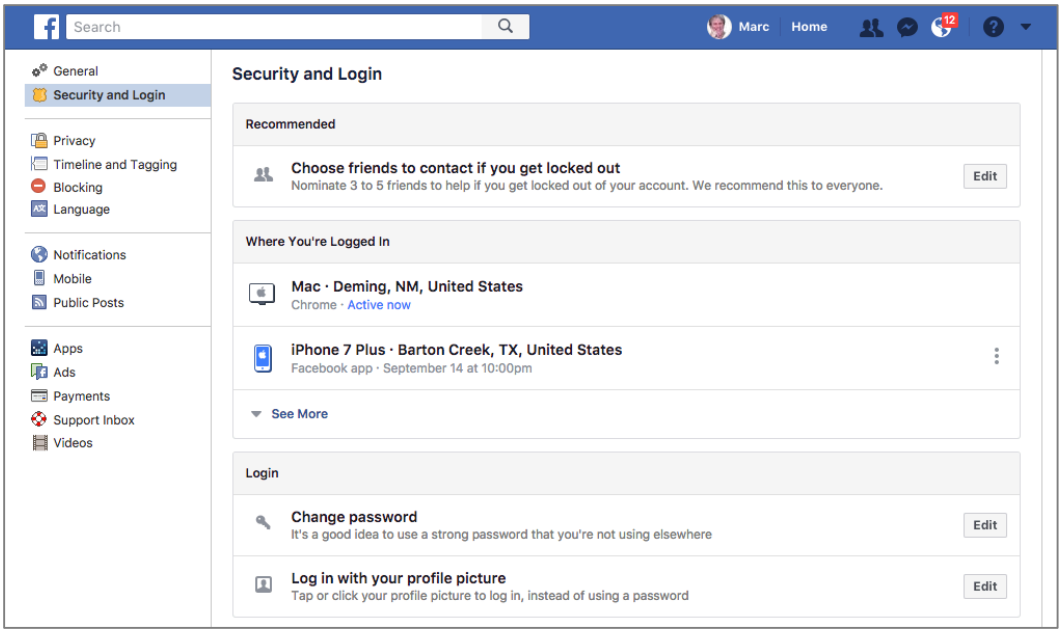
5. If a device is not recognized as yours, select the 3 dots to the right of the device > *Not You?*

6. Repeat for each device you don't recognize.

Create a new strong password

A strong password is just as vital for your social media sites as it is for your banking sites.

7. In the *Facebook Settings* > *Security and Login,* next to *Login* > *Change password,* select *Edit.*

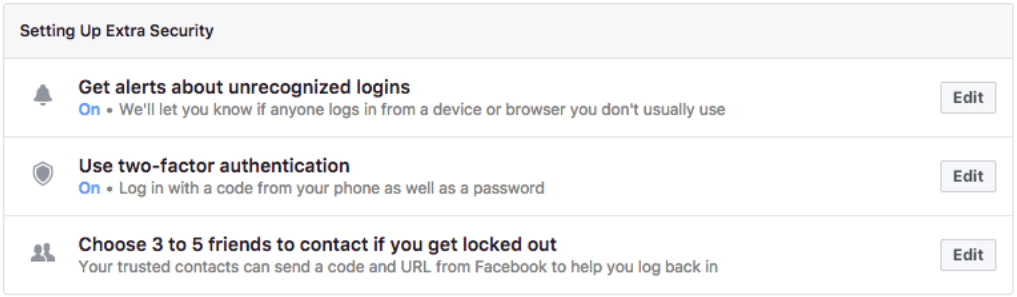


8. Enter your *Current* password, enter your *New*, strong password in the *New* and *Re-type new* fields, and then click *Save* Changes.

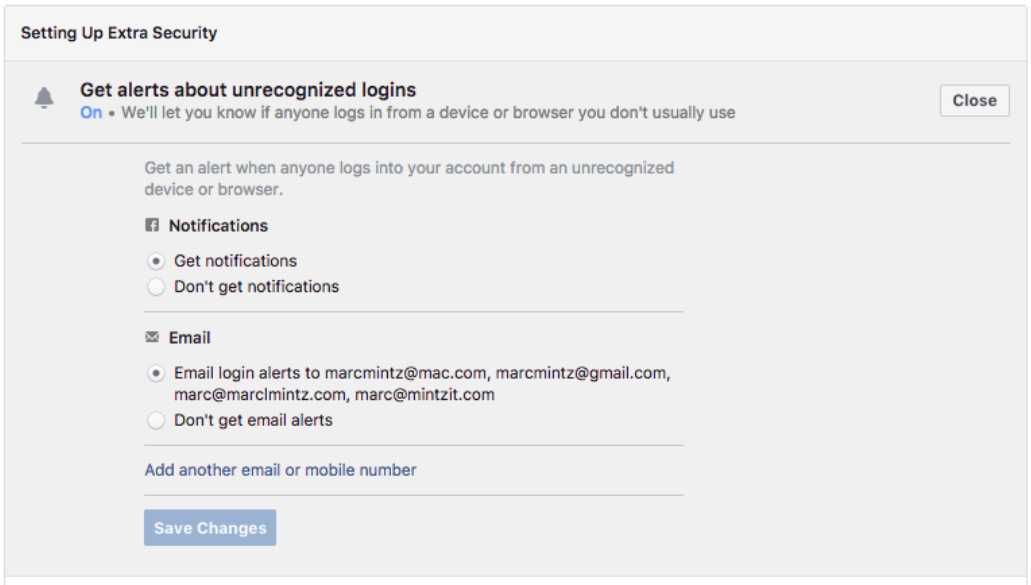
Get alerts about unrecognized logins

If someone does get around your security precautions and logs into your Facebook account, have Facebook alert you, so that you can log them off (step 1 in this assignment).

9. In the *Facebook Settings > Security and Login*, under the *Setting Up Extra Security* section, select *Get alerts about unrecognized logins*.



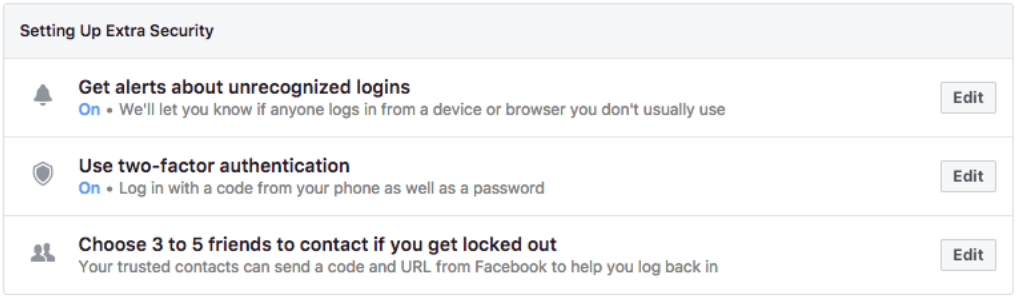
10. Enable *Get Notifications,* and then add the email address(es) to which notifications are to be sent. When done, click *Save Changes.*



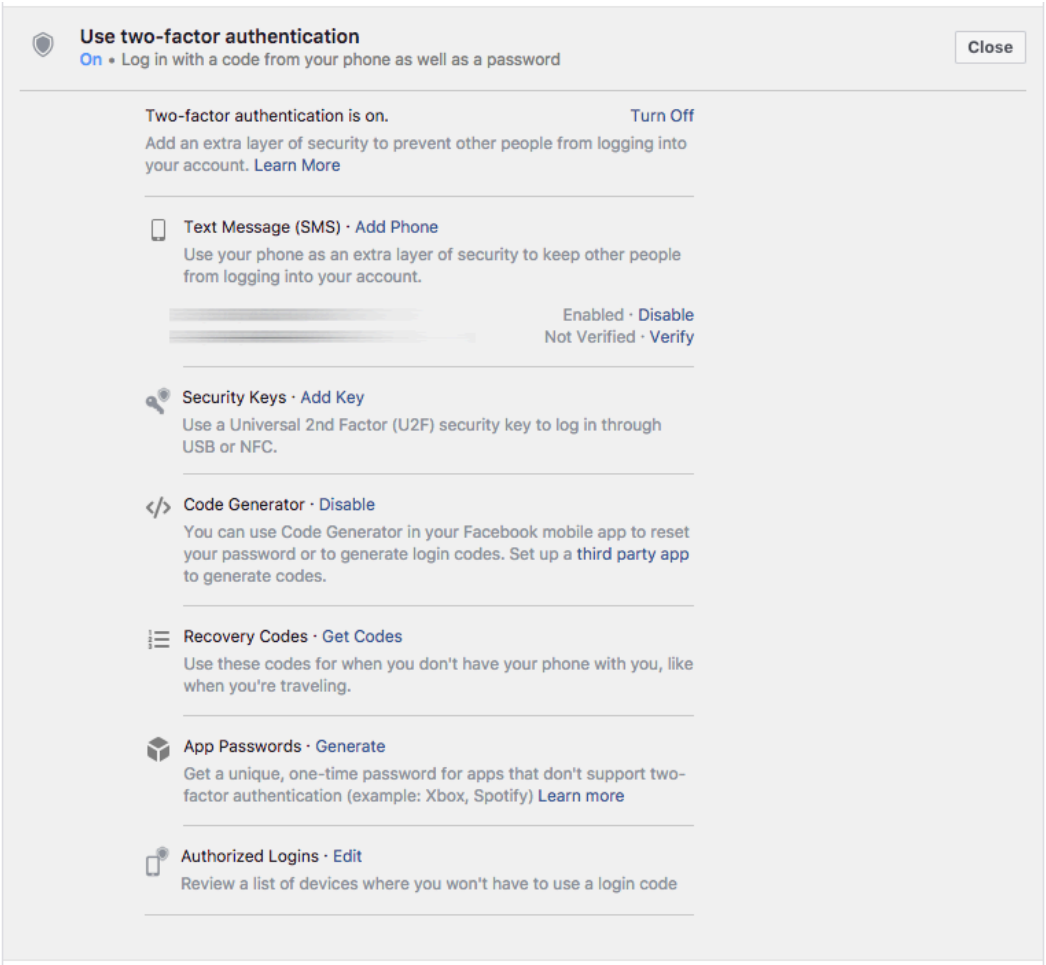
Facebook two-factor authentication

Every password can be broken. It is only a matter of resources (time and cpu cycles). Two-factor authentication can prevent a criminal from using your Facebook credentials.

11. In the *Facebook Settings* > *Security and Login*, under the *Setting Up Extra Security* section, select *Use two-factor authentication*.



12. The *Use two-factor authentication* area opens. In this screenshot, it has been partially configured.



13. *Turn On* two-factor authentication, adding your mobile phone number.
14. Select *Recovery Codes – Get Codes.*
15. At the prompt, enter your Facebook password.
16. The *Your Recovery Codes* window appears with a list of 10, 1-time use codes. These may be used to authenticate with Facebook if you don't have access to your mobile phone.

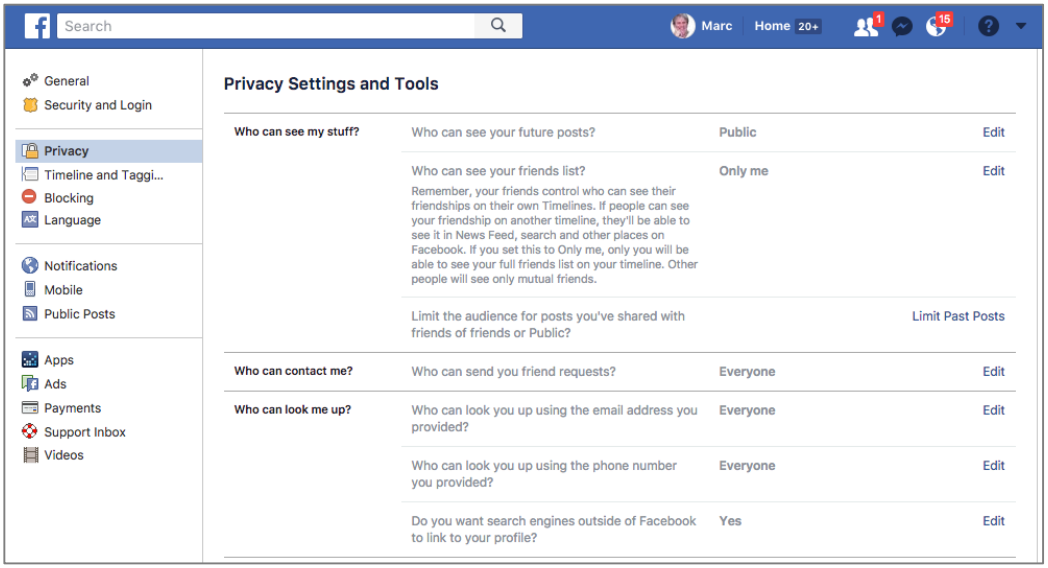
17. Securely record these numbers (you can copy/paste).
18. Close the *Your Recovery Codes* window.

20.3.2 Assignment: Facebook Privacy Settings

Facebook Privacy Settings allow you to filter who can see your posts, contact you, and look you up.

In this assignment, you configure your Facebook Privacy Settings.

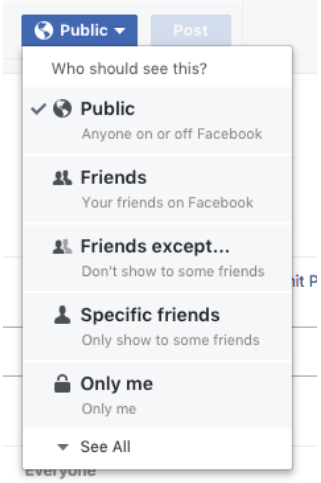
1. From Facebook 3-line menu, select *Settings,* and the sidebar select *Privacy*.



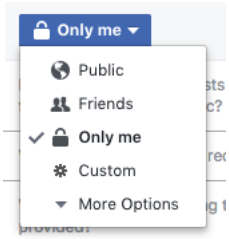
Who can see my stuff?

2. To the far right of *Who can see my stuff?* > *Who can see your future posts?* click *Edit*. Configure to your taste.

- Note: Although mine is set to *Public,* I don't recommend this setting for most others. My site is strictly for business, and not a personal Facebook page.

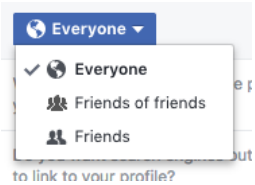


3. To the far right of *Who can see your friends list?* click *Edit*. It is generally considered a breach of etiquette to share the identity of your friends. Select *Only me.*

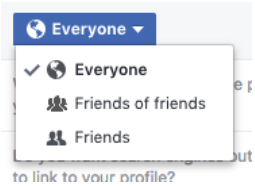


4. To the far right of *Who can contact me? > Who can send you friend requests,* select *Edit*. Configure to your taste.

5. To the far right of *Who can look me up? > Who can look you up using the email address you provided?* select *Edit*. Configure to your taste. However, for your privacy, it is recommended that only *Friends* be selected.



6. To the far right of *Who can look me up? > Who can look you up using the phone number you provided?* select *Edit.* Configure to your taste. However, for your privacy, it is recommended that only *Friends* be selected.

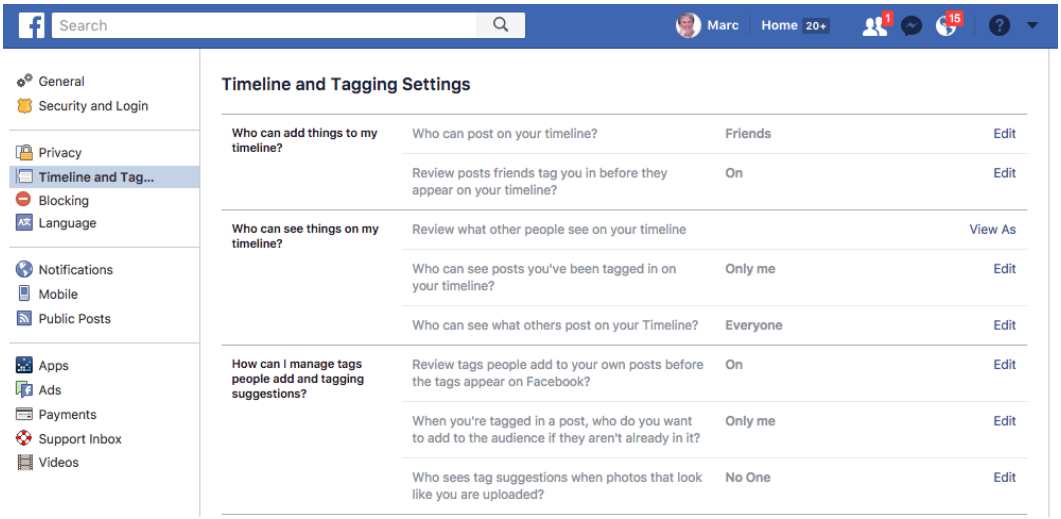


7. To the far right of *Who can look me up? > do you want search engines outside of Facebook to link to your profile?* select Edit. If you are interested in personal privacy, select *No.*

20.3.3 Timeline and Tagging Settings

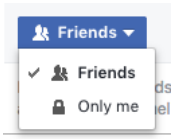
In this section, you configure who is able to post to your timeline, who can see your timeline, and how to deal with others who tag you.

1. In *Facebook Settings*, select *Timeline and Tagging Settings* from the sidebar.

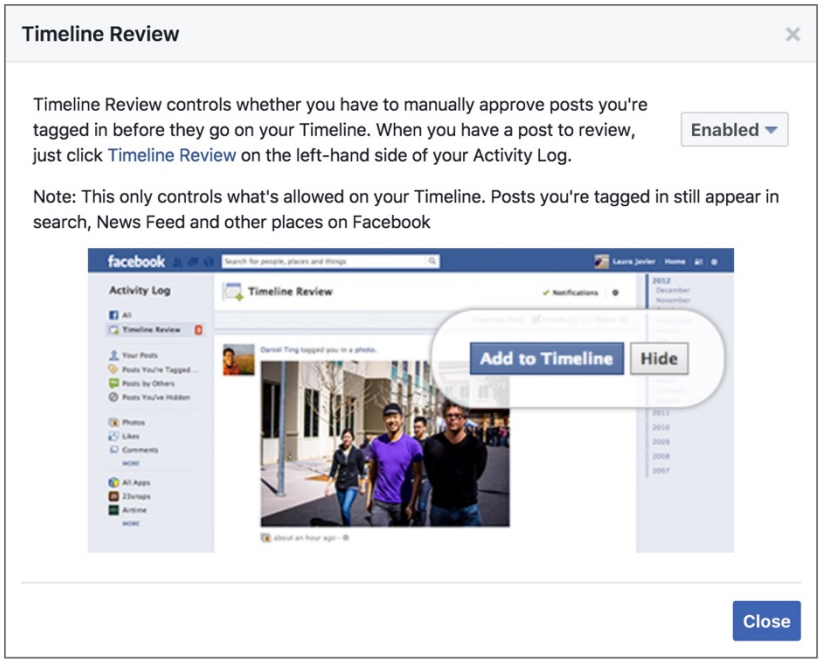


Who can add things to my timeline?

2. To the far right of *Who can add things to my timeline? > Who can post on your timeline?* select Edit. Configure to your taste.



- Note: This controls what is allowed on your Timeline. Posts you are tagged in will still appears in the Facebook search, News Feed, and other places on Facebook.

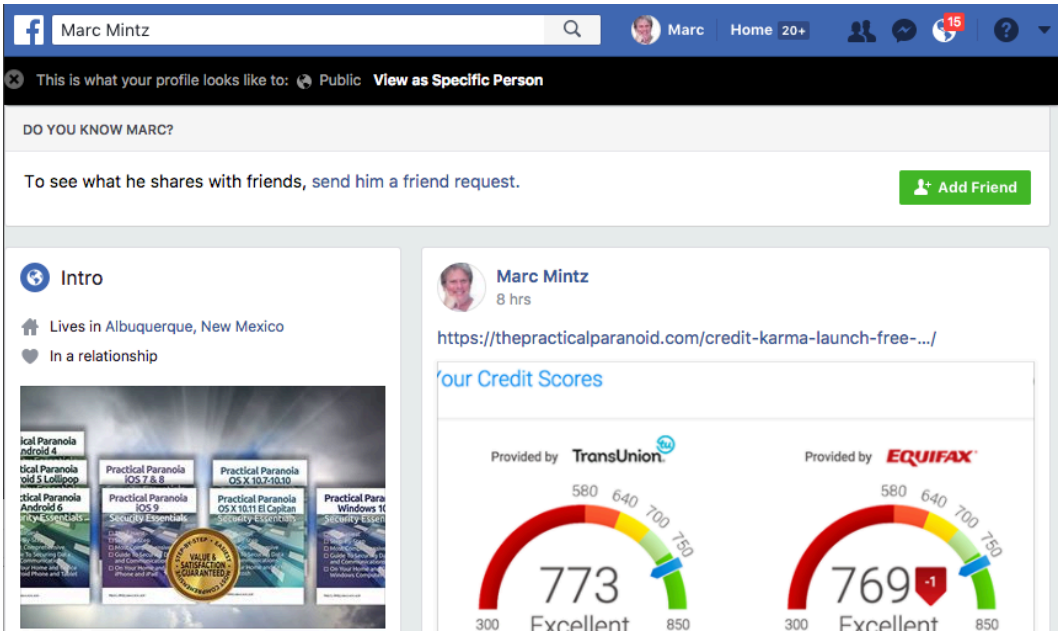


3. To the right of *Who can add things to my timeline? > Review posts friends tag you in before they appear on your timeline?* select Edit. Set this to *On,* or be prepared for your site to turn into a Wild West show.

Who can see things on my timeline?

4. To the right of *Who can see things on my timeline? > Review what other people see on your timeline* select *View As*. Your Facebook page opens, allowing you

to view the page as others do. From the top of the page you can change *This is what your profile looks like to:*____



5. If horror has just run up your spine, it may be a good time to edit your Facebook account.
6. Click the *Back* button to return to *Settings.*
7. To the right of *Who can see things on my timeline? > Who can see posts you've been tagged in on your timeline?* select *Edit*, and then configure to your taste. I recommend setting to *Only me.*
8. To the right of *Who can see things on my timeline? > Who can see what others post on your timeline?* select *Edit,* and then configure to your taste.

How can I manage tags people add and tagging suggestions?

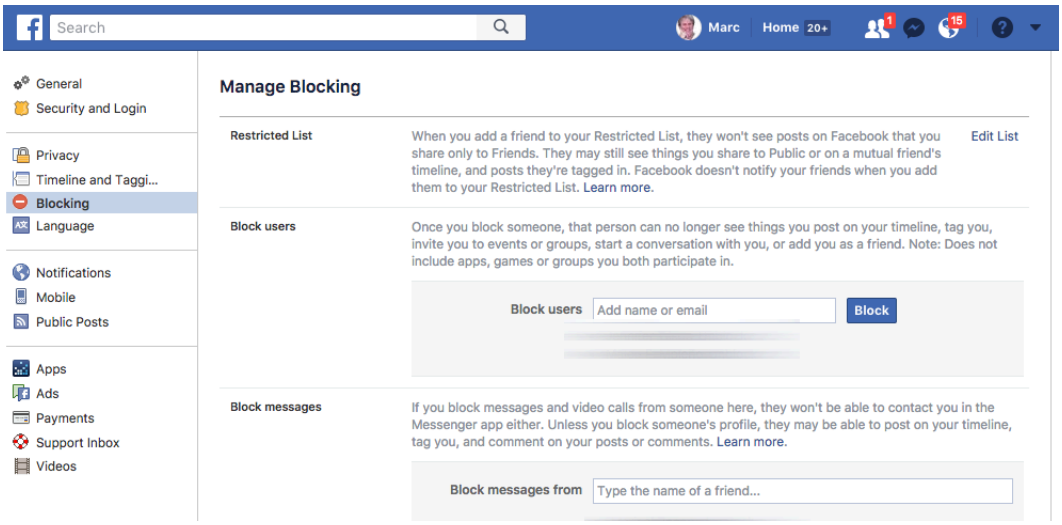
9. To the right of *How can I manage tags… > Review tags people add to your own posts before the tags appears on Facebook* select *Edit,* and then set to *On.*

10. To the right of *How can I manage tags… > When you're tagged in a post, who do you want to add to the audience if they aren't already in it?* select *Edit*, and then configure to taste. I recommend setting to *Only me.*
11. To the right of *How can I manage tags… > Who sees tag suggestions when photos that look like you are uploaded?* select *Edit,* and then set to *No One.*

20.3.4 Assignment: Facebook Manage Blocking

Although Facebook has a financial stake in sucking you into everything that happens on the site, they do allow some freedom to block users, messages, apps, invites, and pages.

1. Open *Facebook Settings > Blocking.*



Restricted List

When a friend is added to the *Restricted List*, they won't see posts on Facebook that are shared only to Friends.

2. To the right of *Restricted List* select *Edit List.*
3. If you have Facebook Friends that you don't want to see posts restricted to your Friends, add their name to this list, and then click *Finish.*

Block Users

If you block a Facebook user, they can't see your timeline posts, tag you, invite you, converse with you, or add you as a friend.

4. Should you have a troll bothering you that should be blocked, in the *Block users* field add their name.

Block app invites

Once you block app invites from a Facebook user, all future app requests from them are ignored.

5. If you are bombarded with app invites from a Facebook user, in the *Block invites from* field, add their name.

Block event invites

Once you block event invites from a Facebook user, all future event invitations from them are ignored.

6. If you are bothered with event invites from a Facebook user, in the *Block invites from* field, enter their name.

Block apps

When blocking an app, it can no longer contact you or access no-public information about you through Facebook.

7. To block an app, in the *Block apps* field, enter the name of the app.

Block Pages

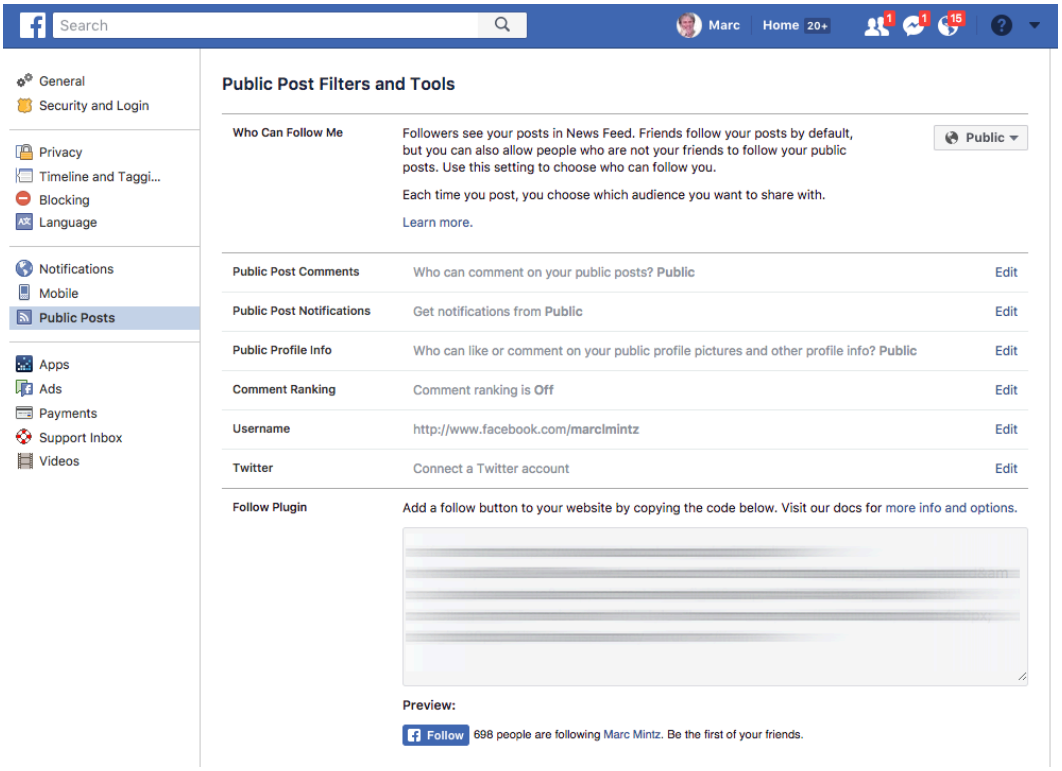
When blocking a Page, there can be no more interaction between you and the Page.

8. To block a page, in the *Block Pages* field, enter the name of the Page.

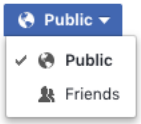
20.3.5 Assignment: Facebook Public Posts

Think deep about who you wish to see your posts. Remember that colleges, recruiters, human resource departments, and more may be watching for you.

1. Open *Facebook Settings > Public Posts.*



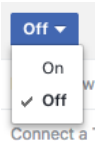
2. To the right of *Who Can Follow Me,* select who can follow your posts by default.



3. To the right of *Public Post Comments,* select who can comment on your public posts.

4. To the right of *Public Post Notifications,* select if you wish to be notified when people who aren't your friends follow you, like or comment on your public posts.

5. To the right of *Comment Ranking,* select if you wish to see the most relevant comments on your public posts first.



6. You may change your Facebook username from the *Username* field.

20.3.6 Assignment: Facebook Apps

Developers that have their apps and games on Facebook are monetizing through *your* information. When signing up for these items, you give the developer authorization to see your profile, and know almost everything that Facebook knows about you. They may then take your information and use it for their own marketing projects, or sell the information to others.

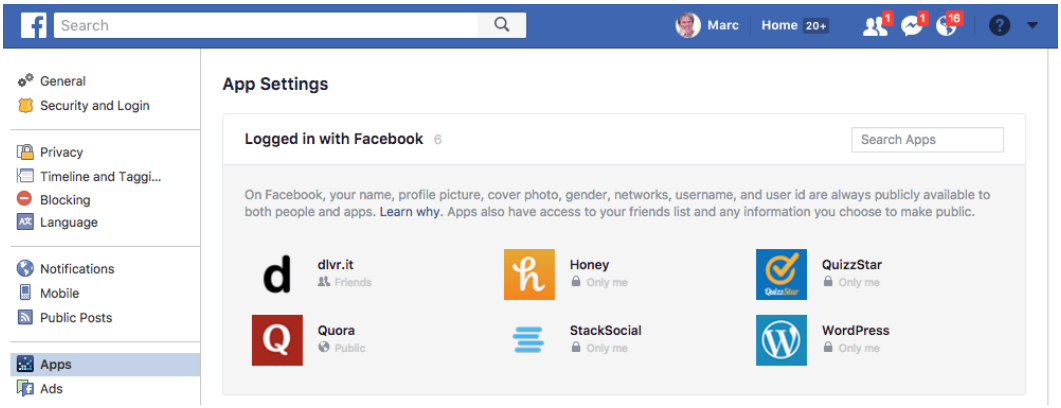
In other words, if you indulge in Facebook apps or games, you've come close to giving up on privacy.

However, you can still use these apps and games. All you need do is to create another Facebook account *just* for this purpose, and provide minimal personal information in your Facebook profile.

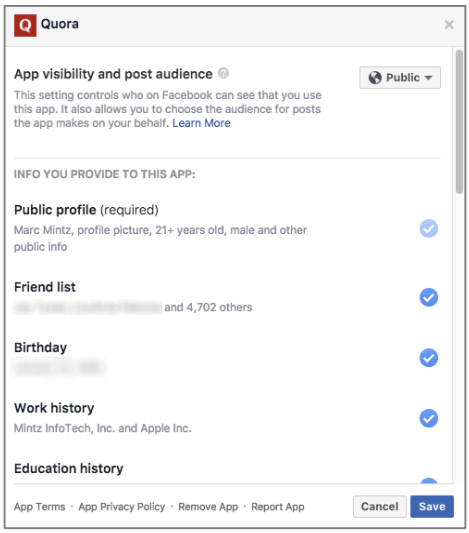
It must be noted that some of your apps were intentionally selected by the Facebook user, but most are unintentionally selected. This can happen when you respond to a Friend's request to play a Facebook game, or take a quiz on Facebook. Because it can happen with just a single click, and appear completely innocent, it's a good idea to schedule a weekly review of your Facebook apps.

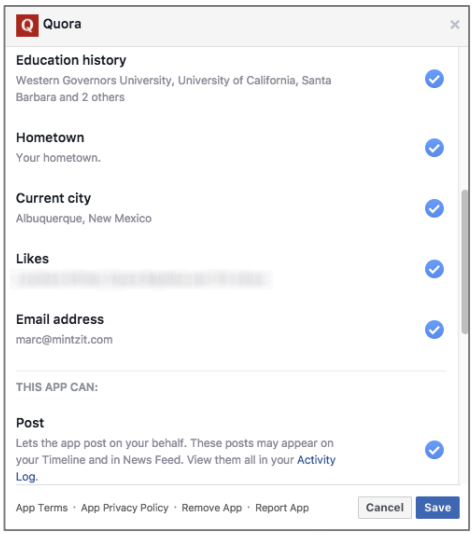
Logged in with Facebook

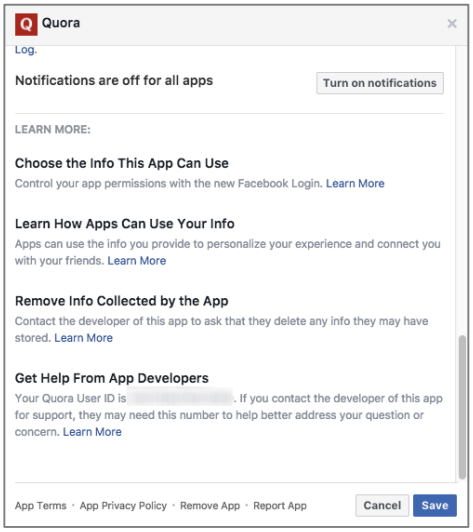
1. Open *Facebook Settings* > *Apps*. The *Logged in with Facebook* field displays the apps for which you are logged in with your Facebook account display.



2. Click on either the name, icon, or pencil (edit) icon for the app. For my example, I'm selecting *Quora*. This opens the *App Information Window*. Give deep thought as to what info you wish the developer to have. You may disable some of these options. However, if you have been using the app for longer than a second, the developer already has all this data. Although there is the option to *Remove Info Collected by the App,* if you believe that has an effect in the real world, I have a bridge to sell you.



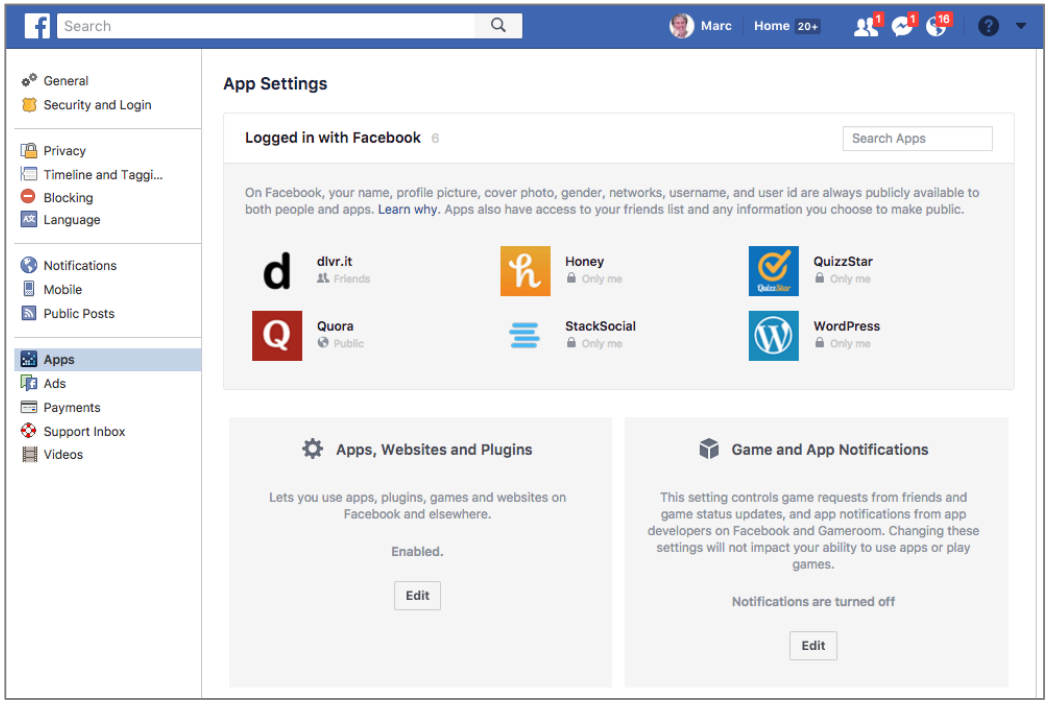




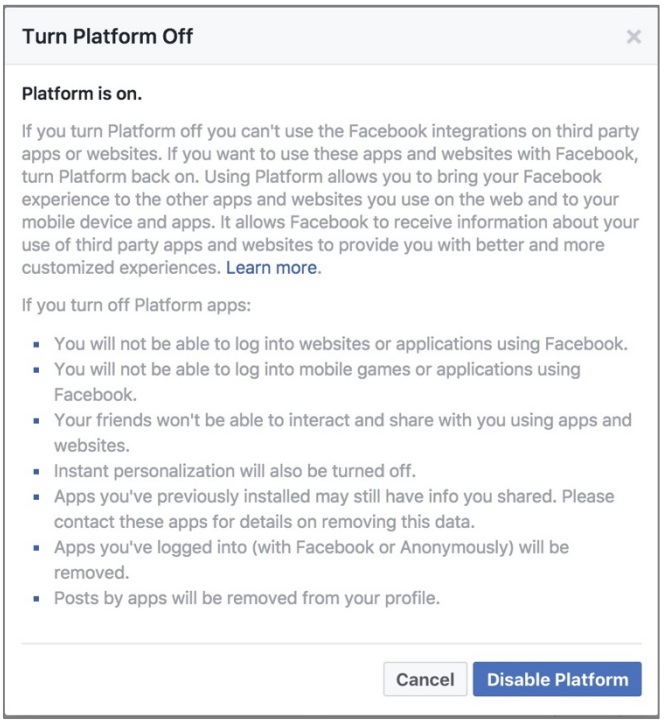
3. If there are data points you want to block this app from accessing, you can click the target check mark. Understand, this is shutting the barn door after the cows are out.
4. If you wish to remove this app, so that it no longer has access to your Facebook information, select the *Remove App* at the bottom of the window.
5. When you have completed configuring your app settings, click *Save* or *Cancel.*
6. The app will no longer appear in the *Logged in with Facebook* field.

Apps, Websites, and Plugins

7. Select *Facebook Settings* > *Apps* > *Apps, Websites, and Plugins,* and then click *Edit*.



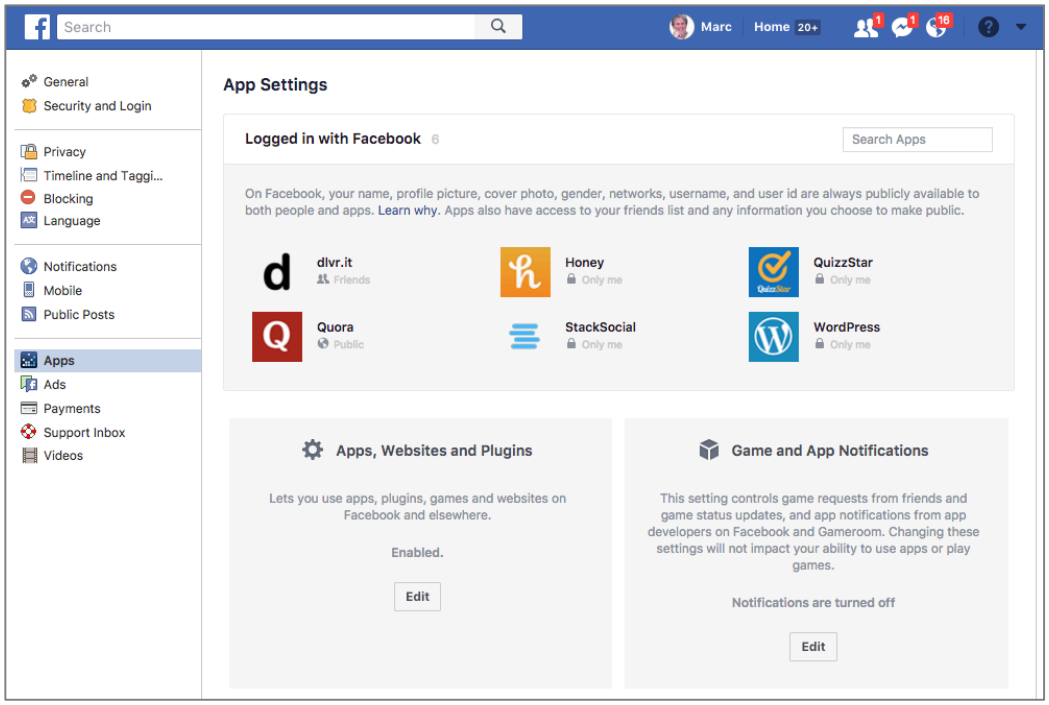
8. By default, *Apps, Websites and Plugins* is *Enabled*. If you wish to disable it, click the *Edit* button. The *Turn Platform Off* window appears. Read the warning well. You may not be able to function well on Facebook with these features disabled.



9. Once you have reviewed the warning, select either *Cancel* or *Disable Platform*.

Game and App Notifications

10. Select *Facebook Settings* > *Apps* > *Game and App Notifications*, and then select *Edit*.

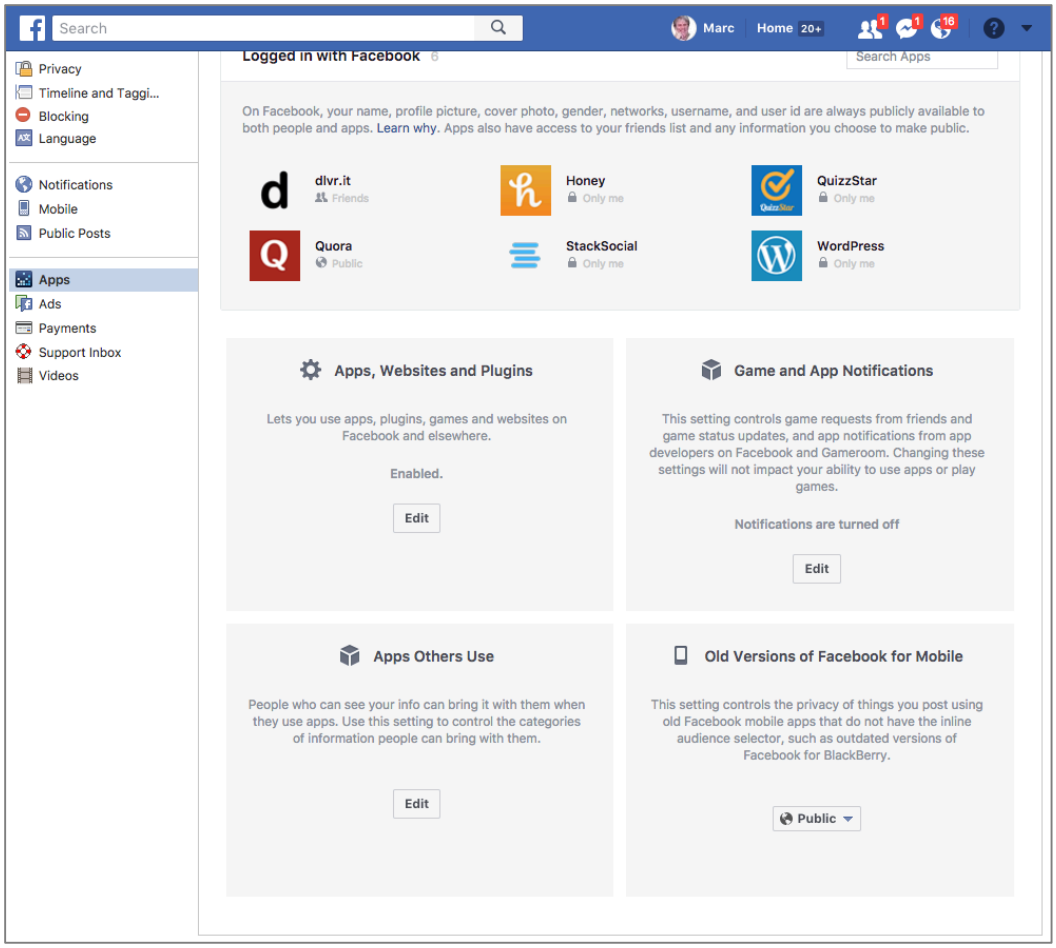


11. This setting has no impact on privacy or security. However, if you would prefer that Facebook games and apps not send notifications to you, click the *Edit* button, and then click the *Turn off* button.

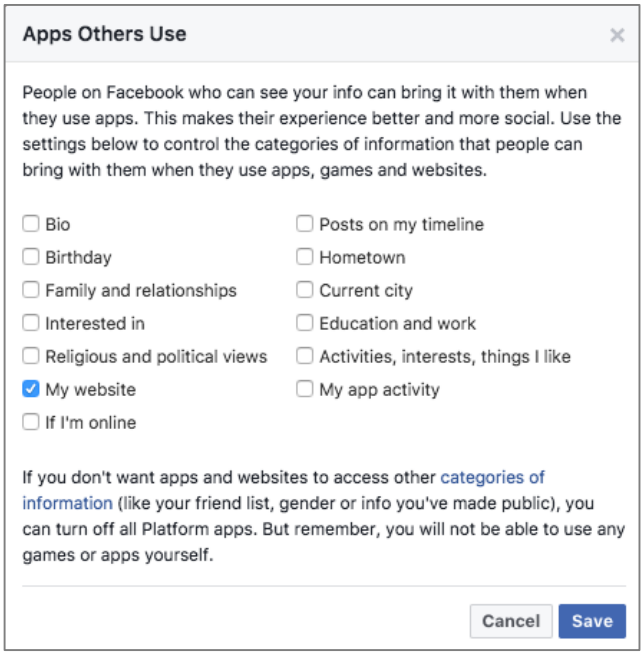
Apps Others Can Use

When someone on Facebook who can see your information then uses an app, by default that app has access to a great deal of your Facebook data. This setting allows you to manage what information apps that others are using has access to.

12. Select *Facebook Settings* > *Apps* > *Apps Others Use*, and then select *Edit*.



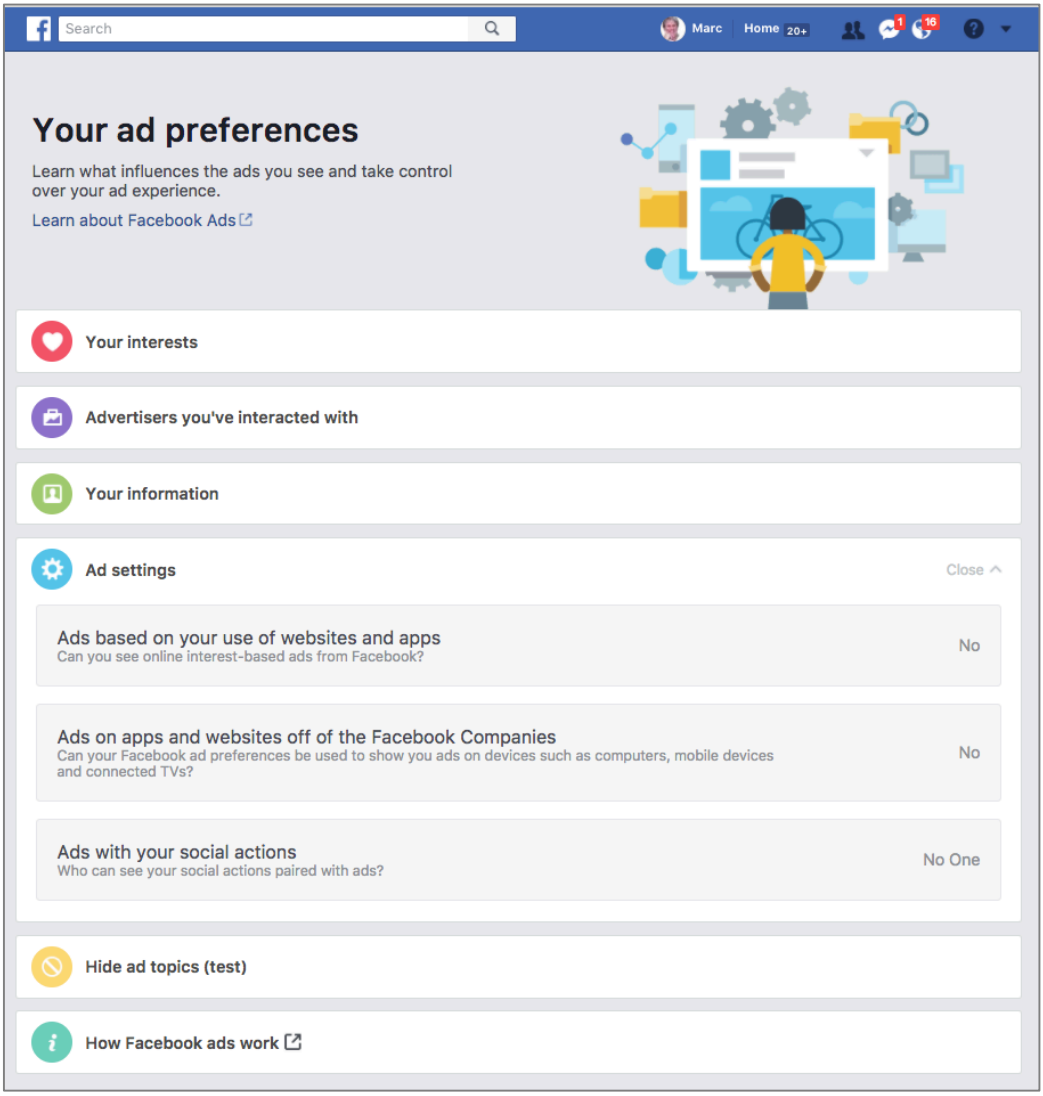
13. In the *Apps Others Use* window, you can manage what information the apps other people are using have access to. When complete, click the *Save* button.



Ads

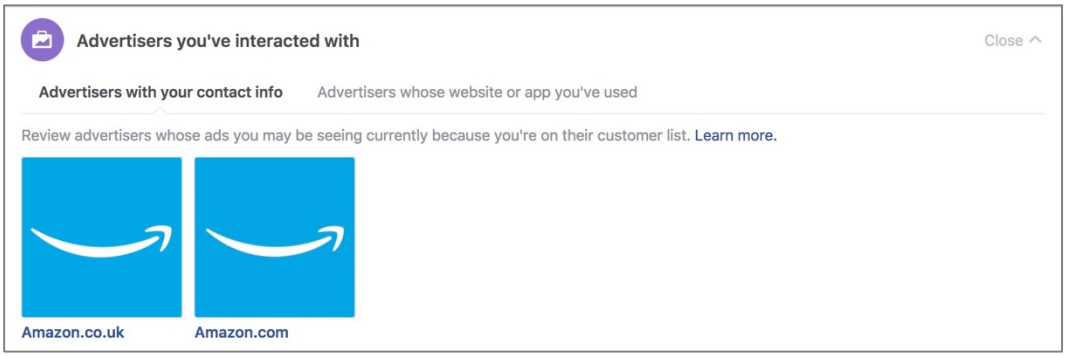
Not only does Facebook and all the games and apps associated with it make money from your information, they also are in the (gasp) advertising business. Although you can't get away from being inundated with ads while on Facebook, you can request that they have less access to your personal information during the process.

14. Select *Facebook Settings* > *Ads*. This will open the *Your ad preferences* page.

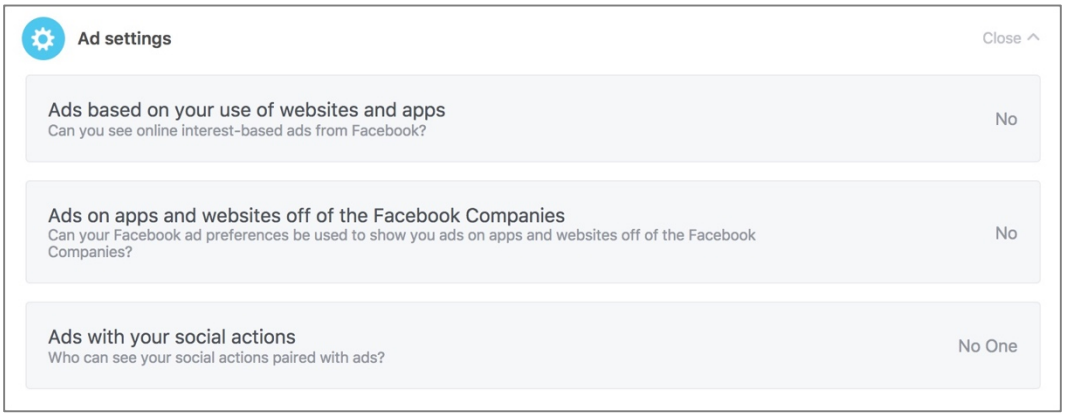


15. If you would like to see ads based on your stated interests, click *Your interests*, and then select your target areas of interest. Or better yet, remove your interests so that the advertisers know less about you.

16. To see which advertisers have you on their mailing list due to interacting with them on Facebook, click *Advertisers you've interacted with.* When done, click *Close.*



17. Click *Ad settings.*



18. To prevent ads based on websites and apps associated with Facebook that you have visited or used, set *Ads based on your use of websites and apps* to *No.*
19. To prevent ads based on websites and apps not associated with Facebook that you have visited, set *Ads on apps and websites off of the Facebook Companies* to *No.*
20. To prevent your friends from seeing ads stating *<Your Name> Likes This,* set *Ads with your social actions* to *No One.*
21. Click *Close.*

22. If you have difficulty falling to sleep at night, click *How Facebook ads work*.

20.4 LinkedIn

While Facebook is the current reigning king of non-business social media, LinkedIn holds the crown for business. Whether it be to market one's services, look for a new job, or simply network with other business people, LinkedIn is the place to be.

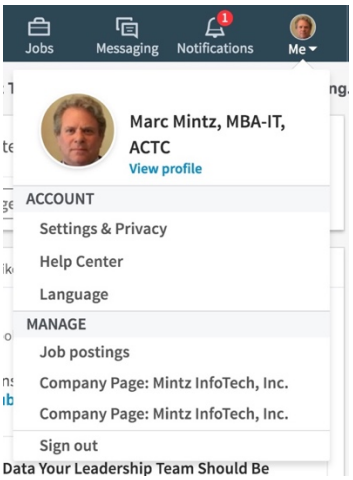
But just as with all other social media sites, it is vital to be mindful of privacy and security on LinkedIn. It could be business suicide to have anything but the very best be associated with your account.

20.4.1 Assignment: LinkedIn Account Security

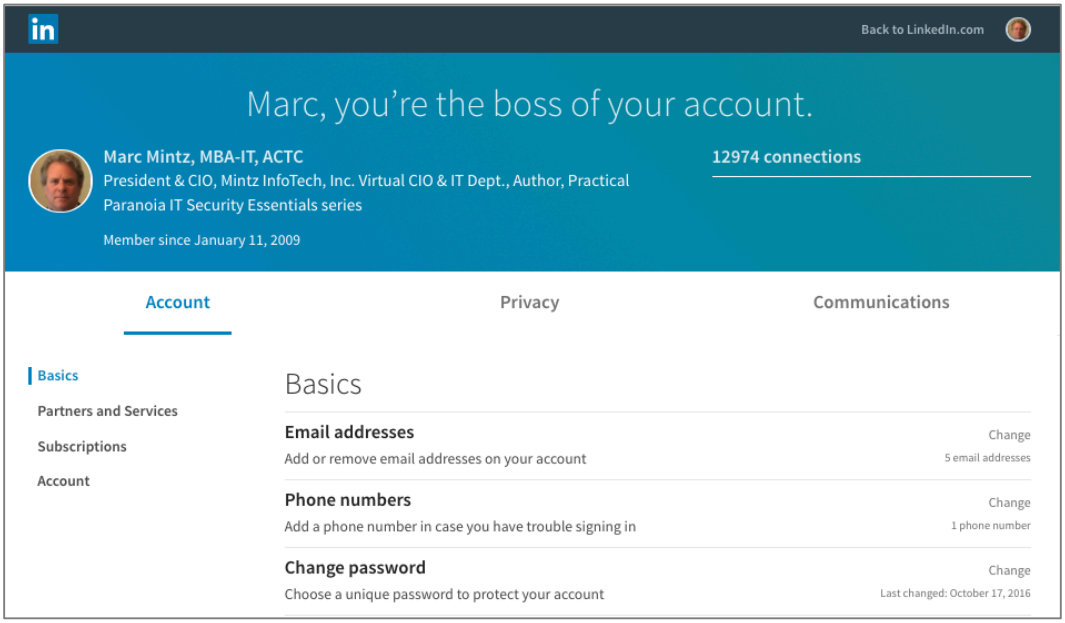
The need for a strong LinkedIn password is no different than that for your computer.

In this assignment, you change your current LinkedIn password to a strong password.

1. Open a browser to *https://linkedin.com/*.
2. From the tool bar, select the *Me* icon > *Settings & Privacy*.



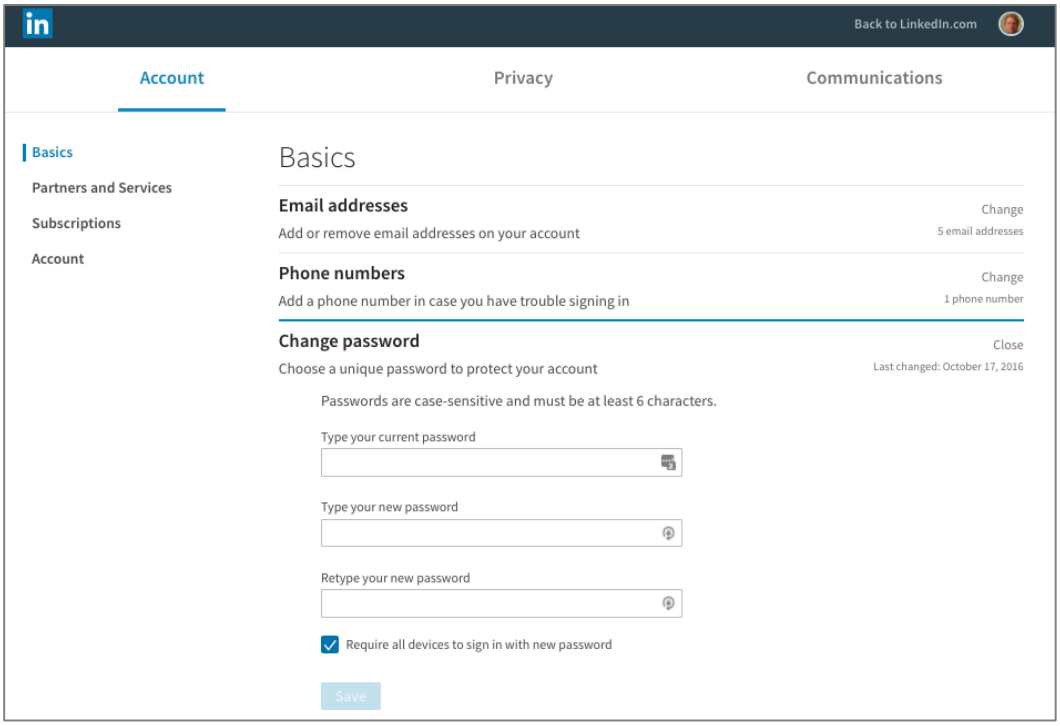
3. The *Settings & Privacy* page opens.



Set a strong password

4. Select the *Account* tab, *Basics* from the sidebar, and then to the right of *Change Password,* click *Change.*

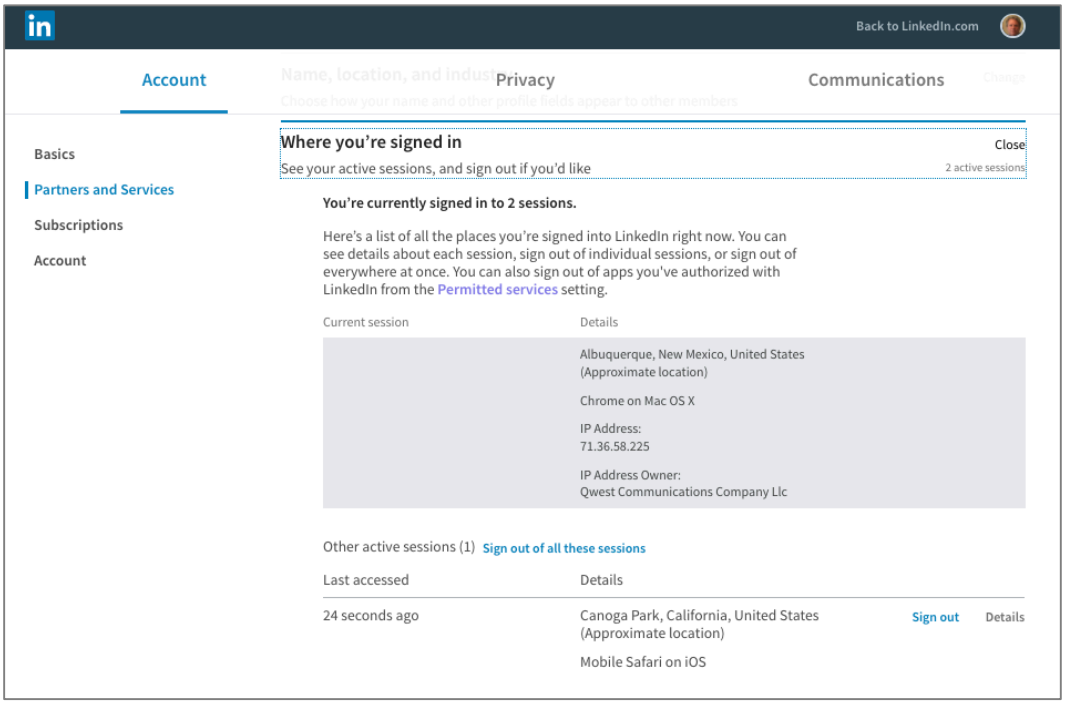
5. In the *Change password* area enter your current password, your new password, retype your new password, and then select *Save*.



Verify where you're signed in

If someone has penetrated your LinkedIn account, you will be able to see unknown devices signed in. If so, you can kick them off.

6. In *LinkedIn Settings & Privacy* page, *Account* tab, *Basics* sidebar > *Where you're signed in* area, select *Change.* View where you are currently logged in to LinkedIn.

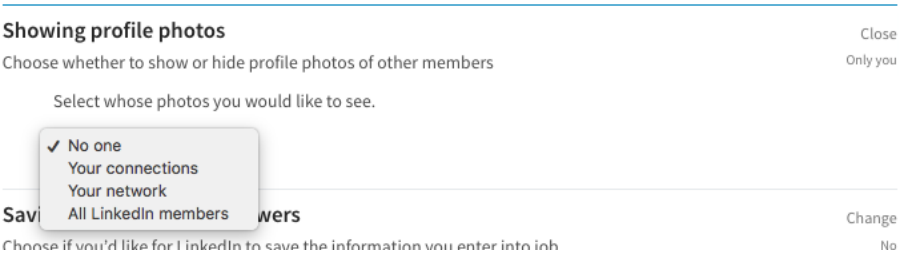


7. If you don't recognize any of these devices, you may kick them off individually by selecting *Sign out,* or kick everyone off by selecting *Sign out of all these sessions.*

Showing profile photos

You may have reason not to want your face to be seen or recognized by the LinkedIn community. You can choose who gets to see your profile photos.

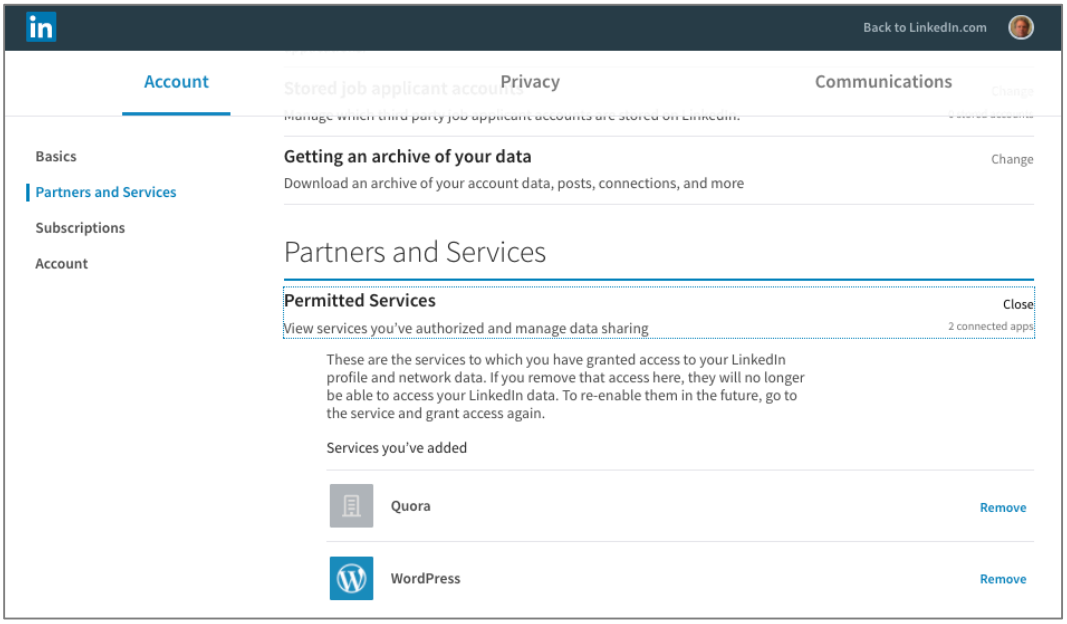
8. In *LinkedIn Settings & Privacy* page, *Account* tab, *Basics* sidebar > *Showing profile photos* area, select *Change*. Configure to your taste.



Partners and Services

Most LinkedIn members don't realize they have authorized many organizations to access their data. LinkedIn allows you to see who has been authorized, and if desired, cut them off.

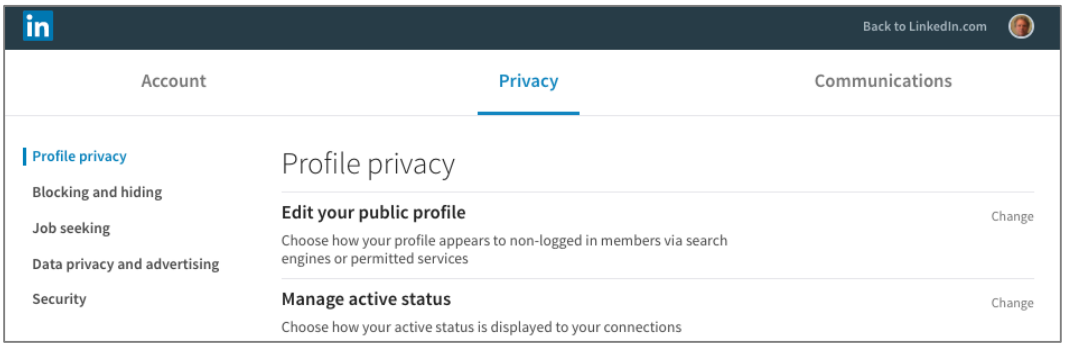
9. In *LinkedIn Settings & Privacy* page, *Account* tab, *Partners and Services* sidebar > *Permitted Services* area, select *Change*. Configure to your taste.

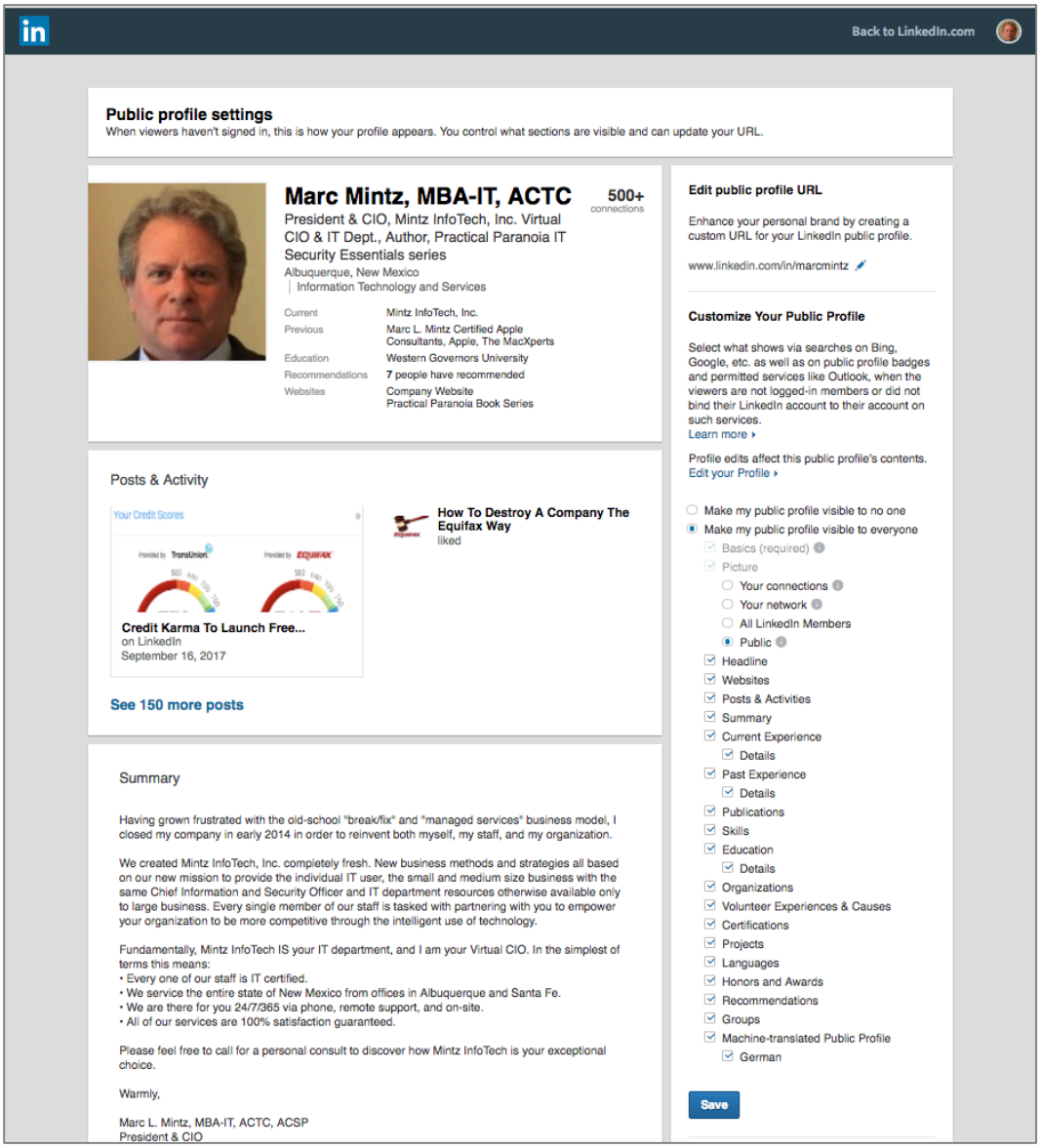


20.4.2 Assignment: LinkedIn Privacy Settings

In this assignment, you configure LinkedIn privacy settings.

1. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Edit your public profile* area, select *Change*. Configure to your taste. When complete, select *Save*.

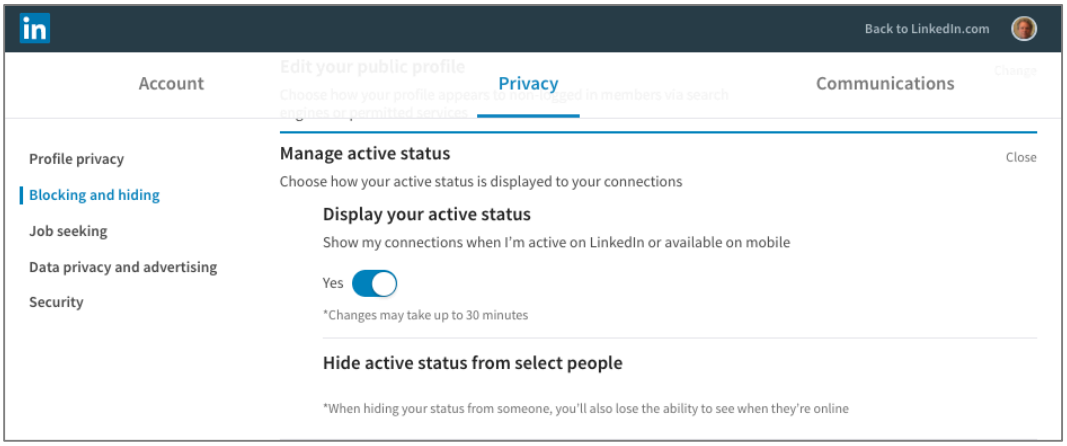




Manage active status

You are able to choose who can see when you are online.

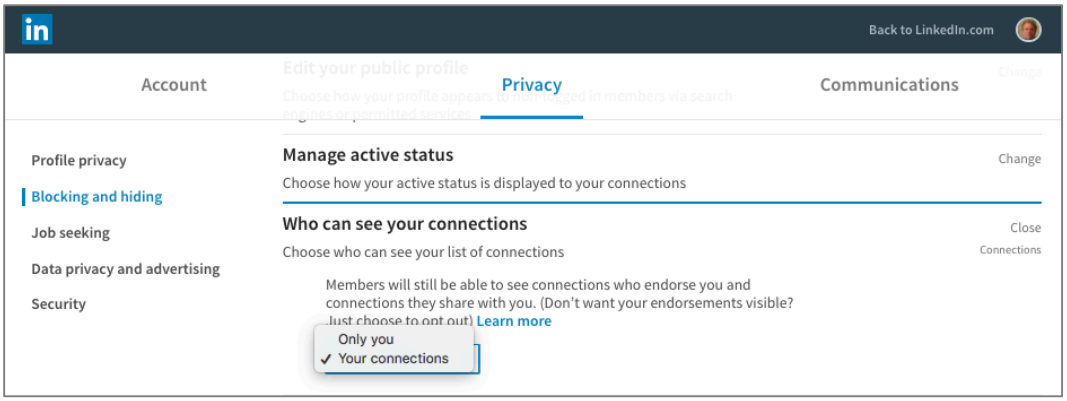
2. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Manage active status* area, select *Change*. Configure to taste.



Who can see your connections

LinkedIn is in large part about networking. You may choose to let others see your connections.

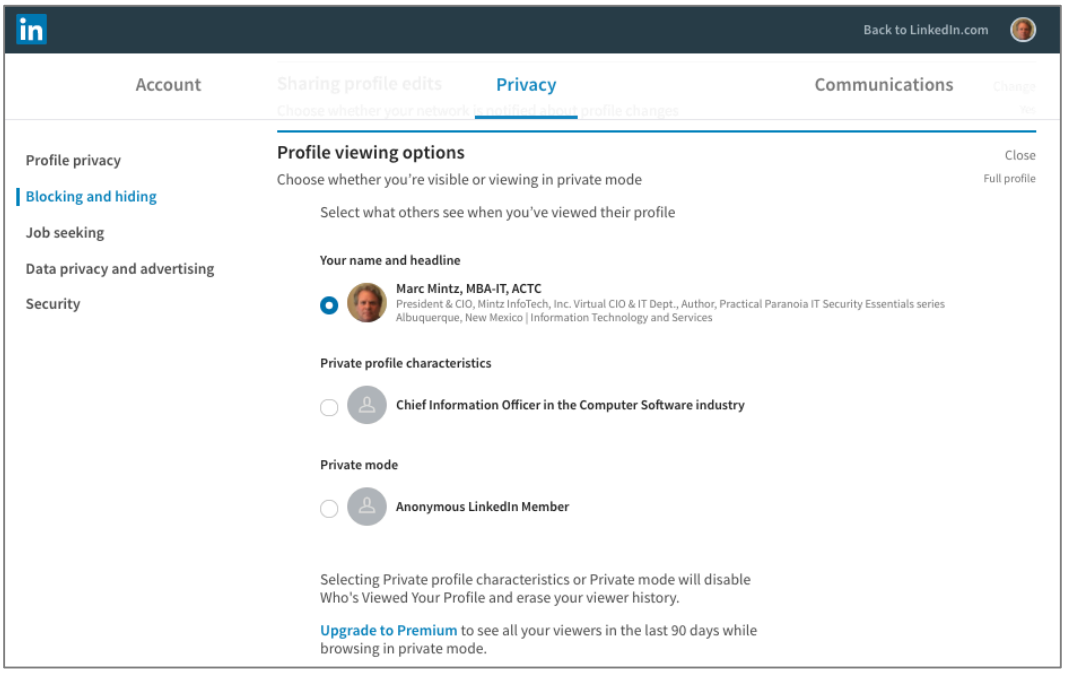
3. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Wo can see your connections* area, select *Change*. Configure to taste.



Profile viewing options

You may configure how transparent your identity is on LinkedIn.

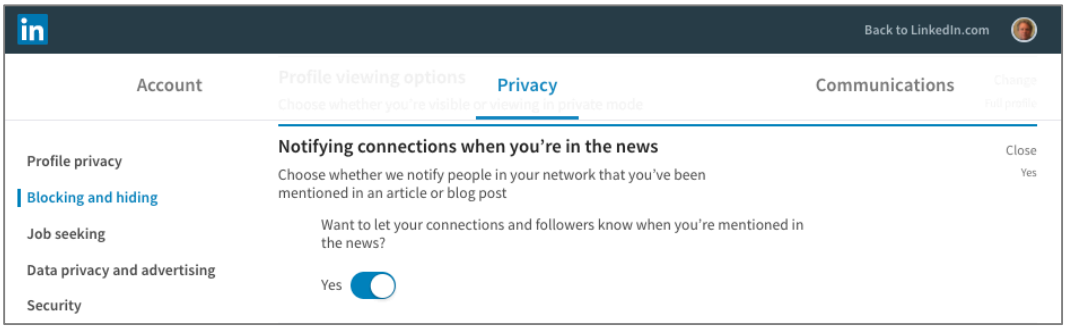
4. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Profile viewing options* area, select *Change*. Configure to your taste.



Notifying connections when you're in the news

This could be good or bad news. A national merit award, or a best-forgotten night on the town. Choose wisely.

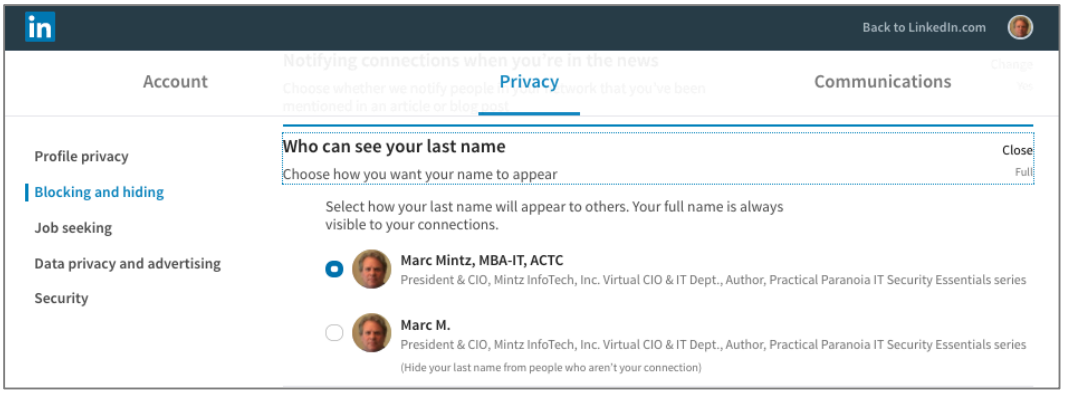
5. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Notifying connections when you're in the news* area, select *Change*. Configure to your taste.



Who can see your last name

This ties in with your level of transparency.

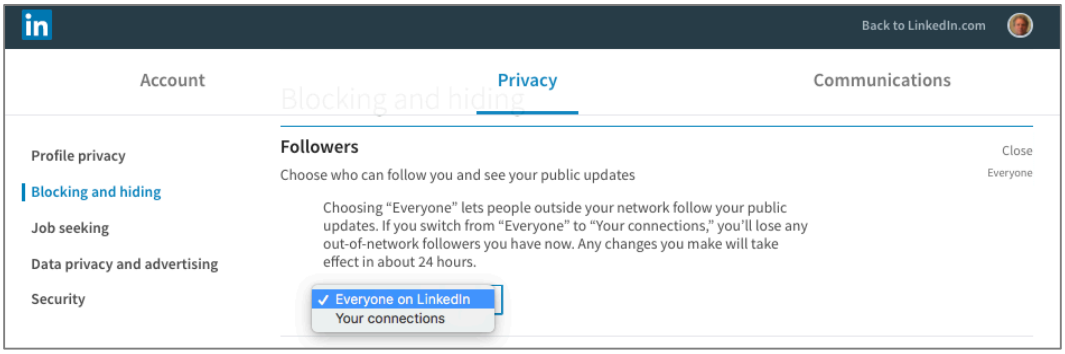
6. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Profile privacy* sidebar > *Who can see your last name* area, select *Change*. Configure to your taste.



Followers

Choose who can follow you and see your public updates.

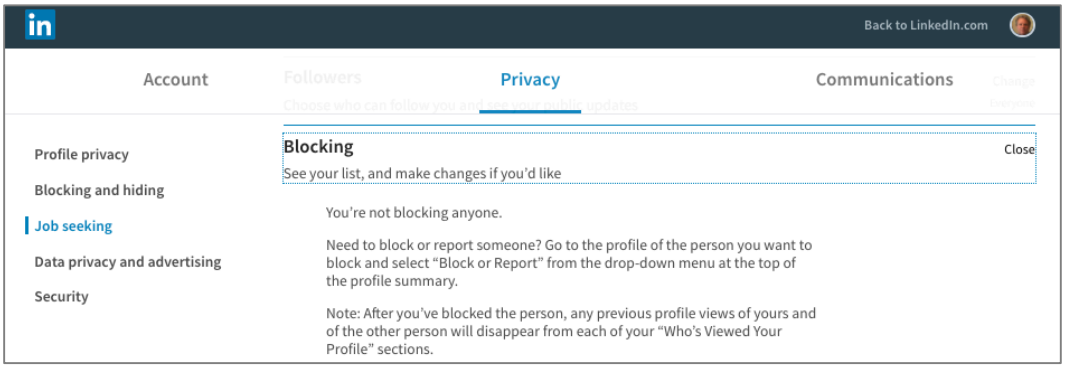
7. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Blocking and hiding* sidebar > *Followers* area, select *Change*. Configure to your taste.



Blocking

This area displays who you are currently blocking. If you need to block a LinkedIn user, Go to their profile, and then select *Block or Report*.

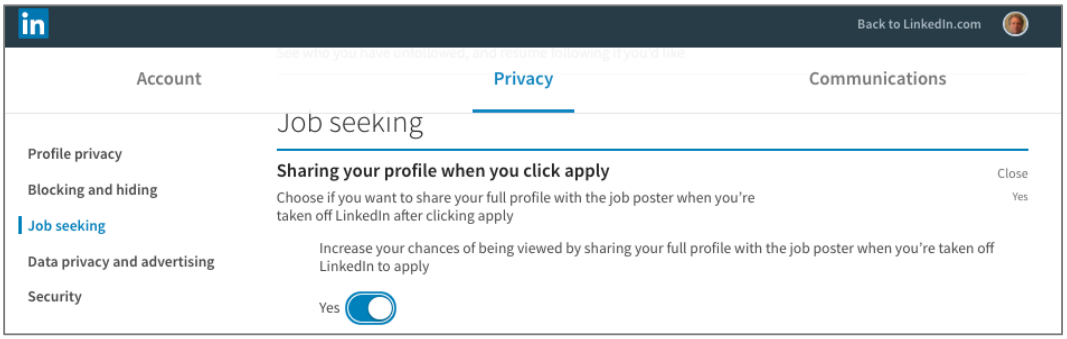
8. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Blocking and hiding* sidebar > *Blocking* area, select *Change*.



Job seeking–Sharing your profile when you click apply

If you want to share your full profile with a job poster after clicking *apply*.

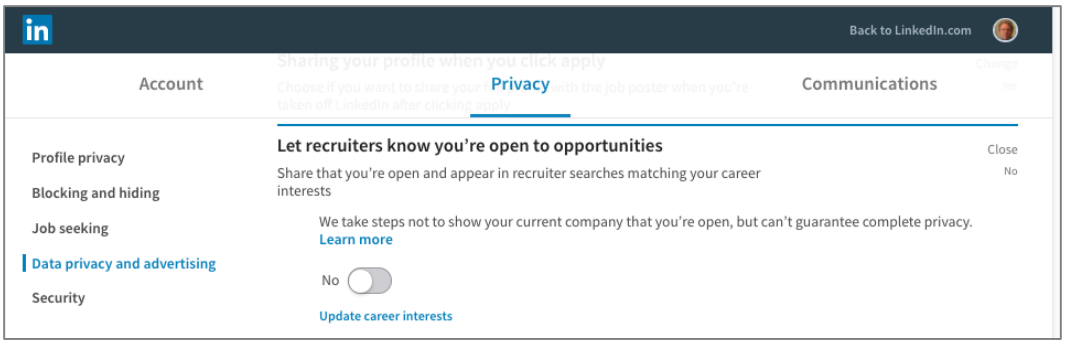
9. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Job seeking* sidebar > *Sharing your profile when you click apply* area, select *Change,* and then configure to your taste.



Let recruiters know you're open to opportunities

Setting this option to *Yes* will let job recruiters know that you are interested in changing jobs. However, your own company may see this as well.

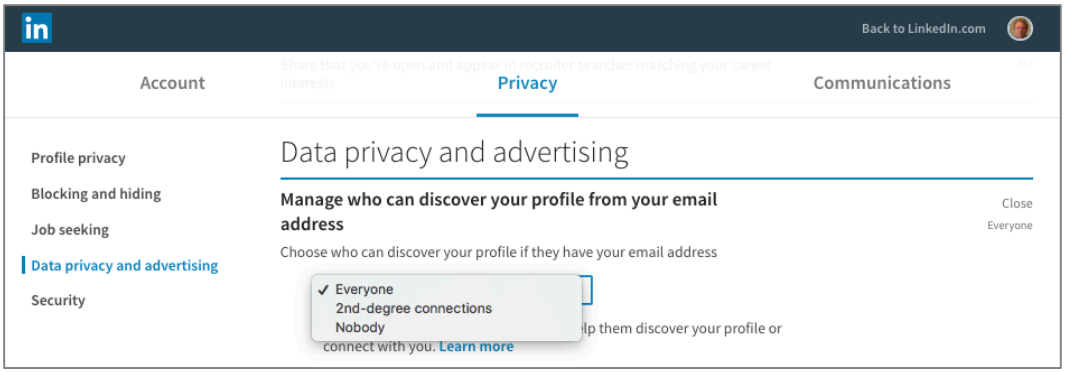
10. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Job seeking* sidebar > *Let recruiters know you're open to opportunities* area, select *Change,* and then configure to your taste.



Data privacy and advertising–Manage who can discover your profile from your email address

This setting allows you to choose if just by having your email address your profile can be found.

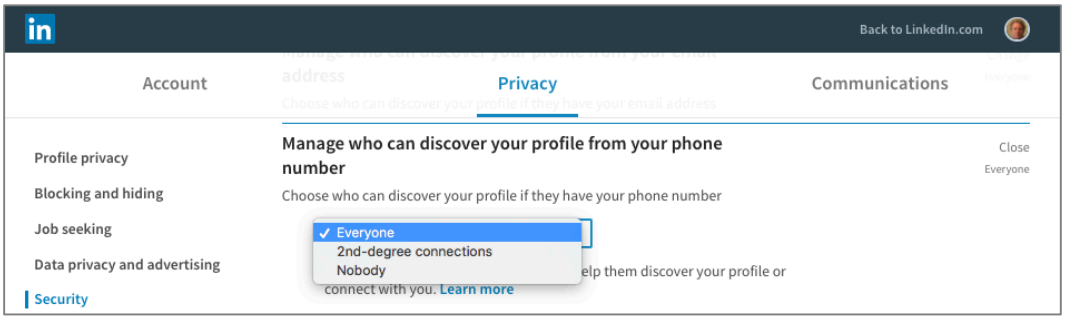
11. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Data privacy and advertising* sidebar > *Manage who can discover your profile from your email address* area, select *Change,* and then configure to your taste.



Manage who can discover your profile from your phone number

Save as above, but using your phone number to locate your profile.

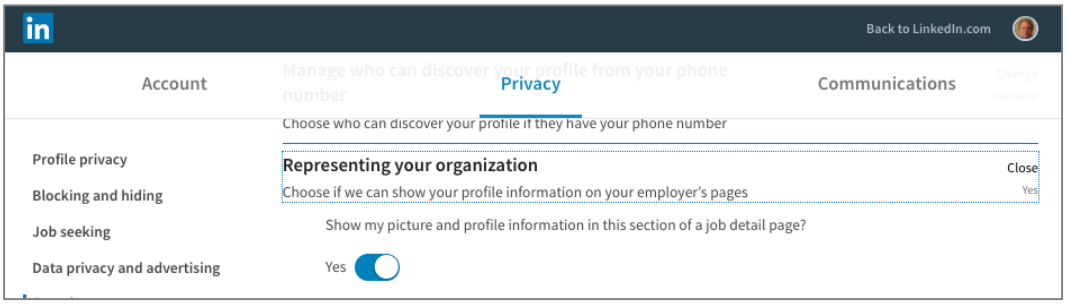
12. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Data privacy and advertising* sidebar > *Manage who can discover your profile from your phone number* area, select *Change,* and then configure to your taste.



Representing your organization

Choose if LinkedIn can show your profile on your employer's LinkedIn pages.

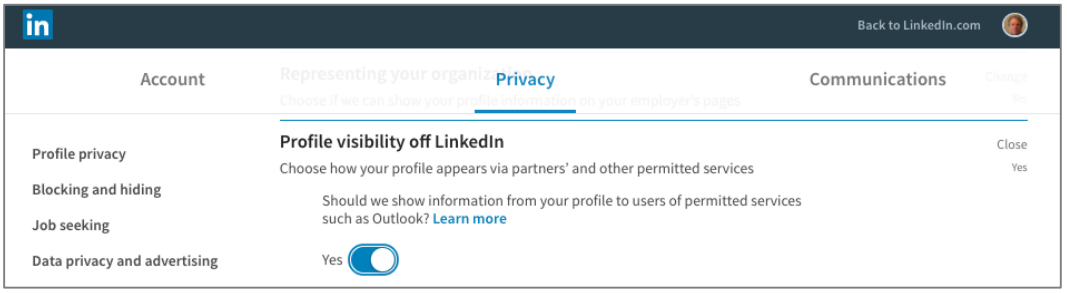
13. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Data privacy and advertising* sidebar > *Representing your organization* area, select *Change,* and then configure to your taste.



Profile visibility off LinkedIn

Choose how your profile appears via partners' and other permitted services**.**

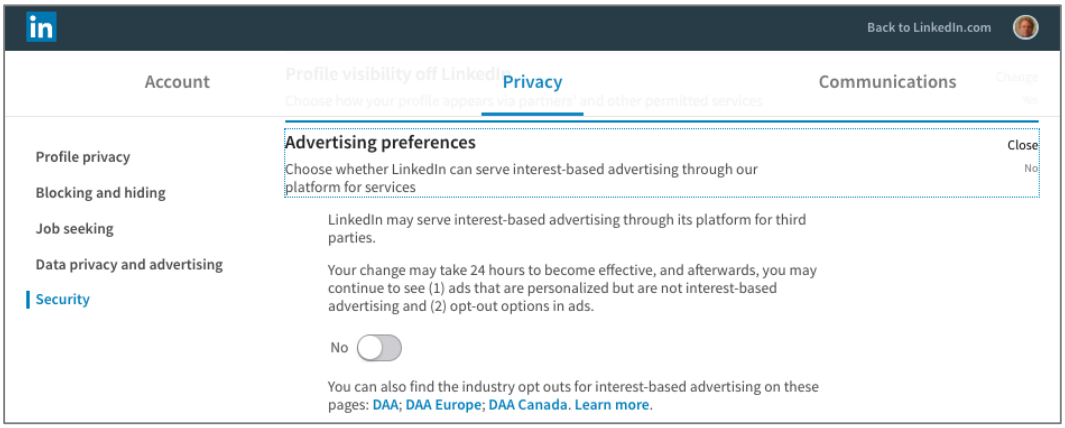
14. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Data privacy and advertising* sidebar > *Profile visibility off LinkedIn* area, select *Change,* and then configure to your taste.



Advertising preferences

LinkedIn exists for only one reason–to monetize the information they have harvested regarding you and all other members. Choose whether Linked can serve interest-based advertising (as opposed to random advertising).

15. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Data privacy and advertising* sidebar > *Advertising preferences* area, select *Change,* and then configure to your taste.

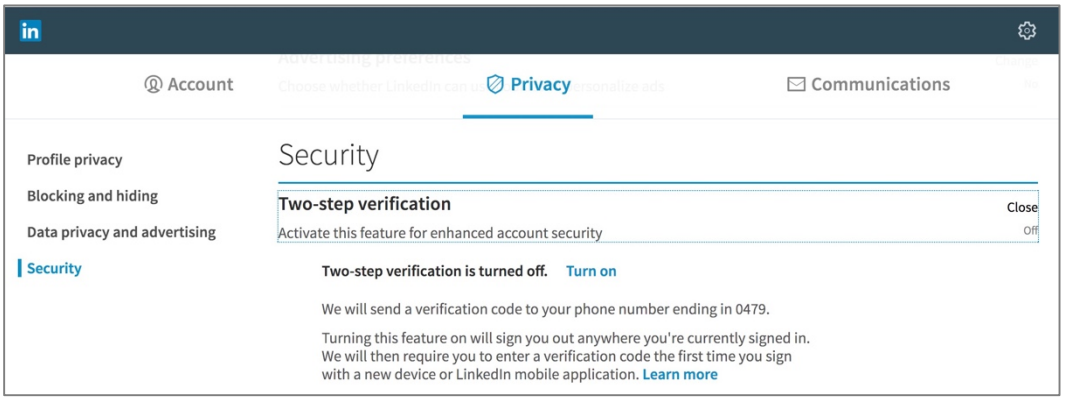


Security–Two-step verification

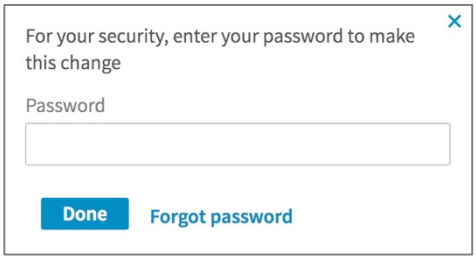
Every password can be broken. The current best solution to blocking criminals from accessing your password-protected accounts is with Two-step verification, also known as 2-factor authentication.

16. In *LinkedIn Settings & Privacy* page, *Privacy* tab, *Security* sidebar > *Two-step verification* area, select *Change.*

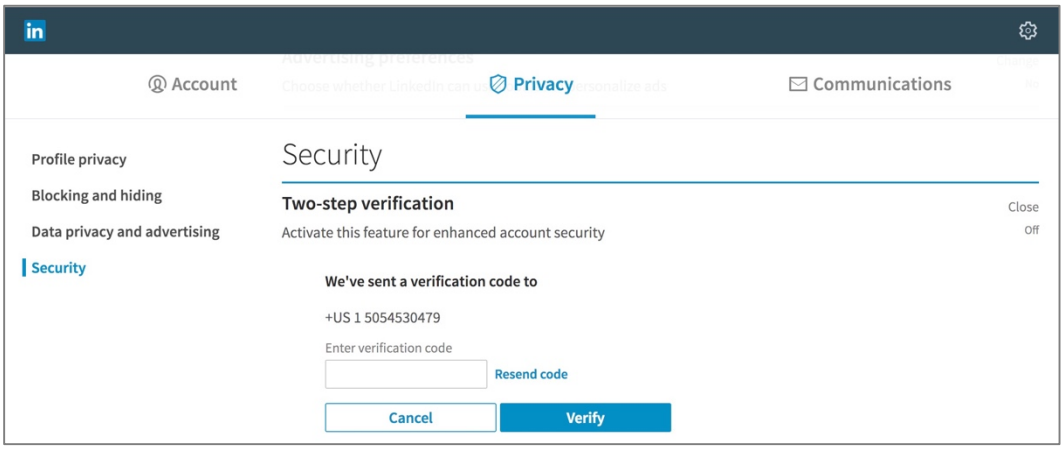
17. If Two-step verification is turned off, click Turn *On.*



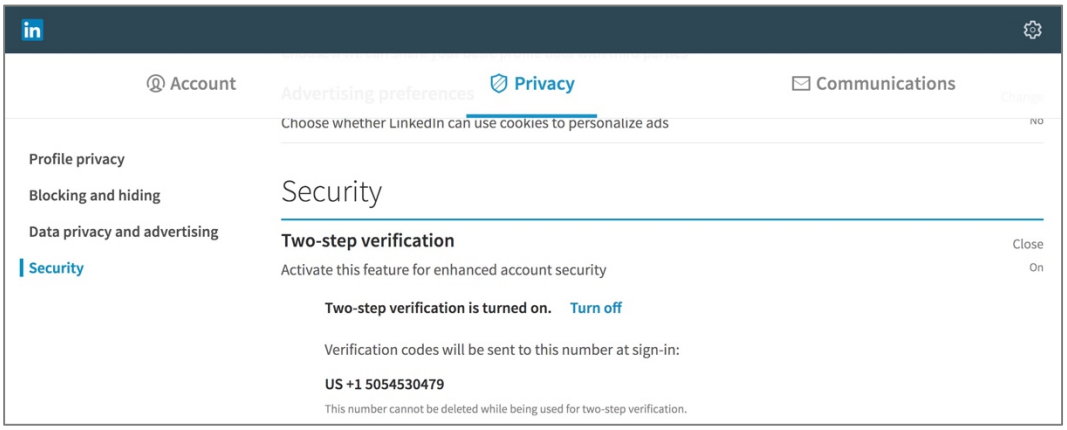
18. In the authentication window, enter your LinkedIn *Password*, and then click the *Done* button.



19. Your mobile device will be sent a verification code. In the Two-step verification window, enter it, and then click the *Verify* button.



20. Once verified, click *Close*.



The next time that you log in to LinkedIn, you will receive a verification code via SMS which must be entered to access LinkedIn.

20.5 Google–More Than a Search Engine

Although most people think of Google as a search engine, it has become far more than that. Over one billion people use their mail, maps, YouTube, and Google Play services[4]. Chances are that you use Google every day. The result is a tremendous warehouse of data points about your searches, site visits, hangout partners, purchases, and so much more.

And yet, at the same time Google provides the tools to help guard your privacy. NOW is a good time to put this to use.

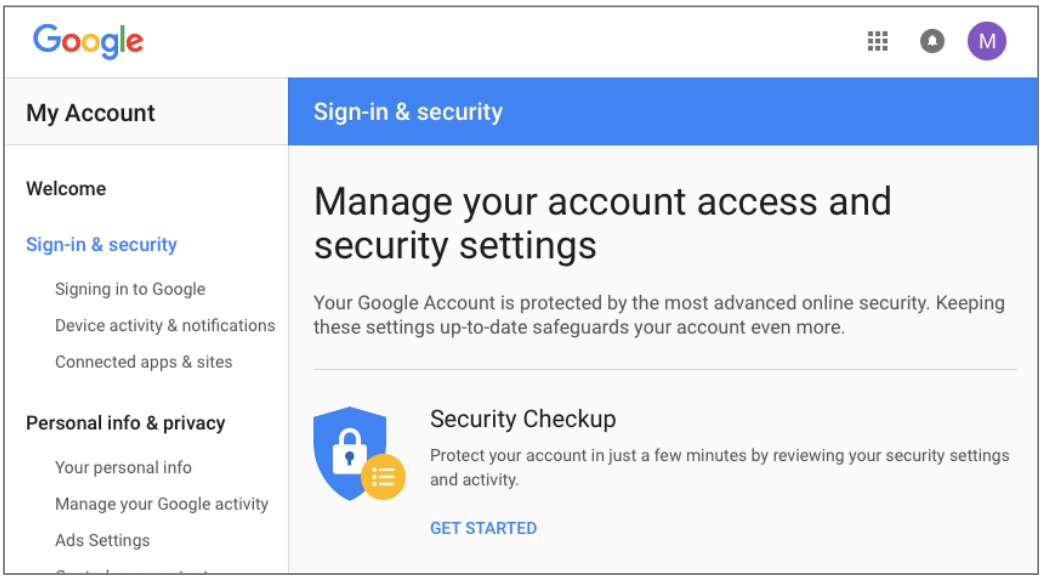
20.5.1 Assignment: Manage Your Google Account Access and Security Settings

In this assignment, you begin the process of securing a Google account.

- Prerequisite: Access to an existing Google account.

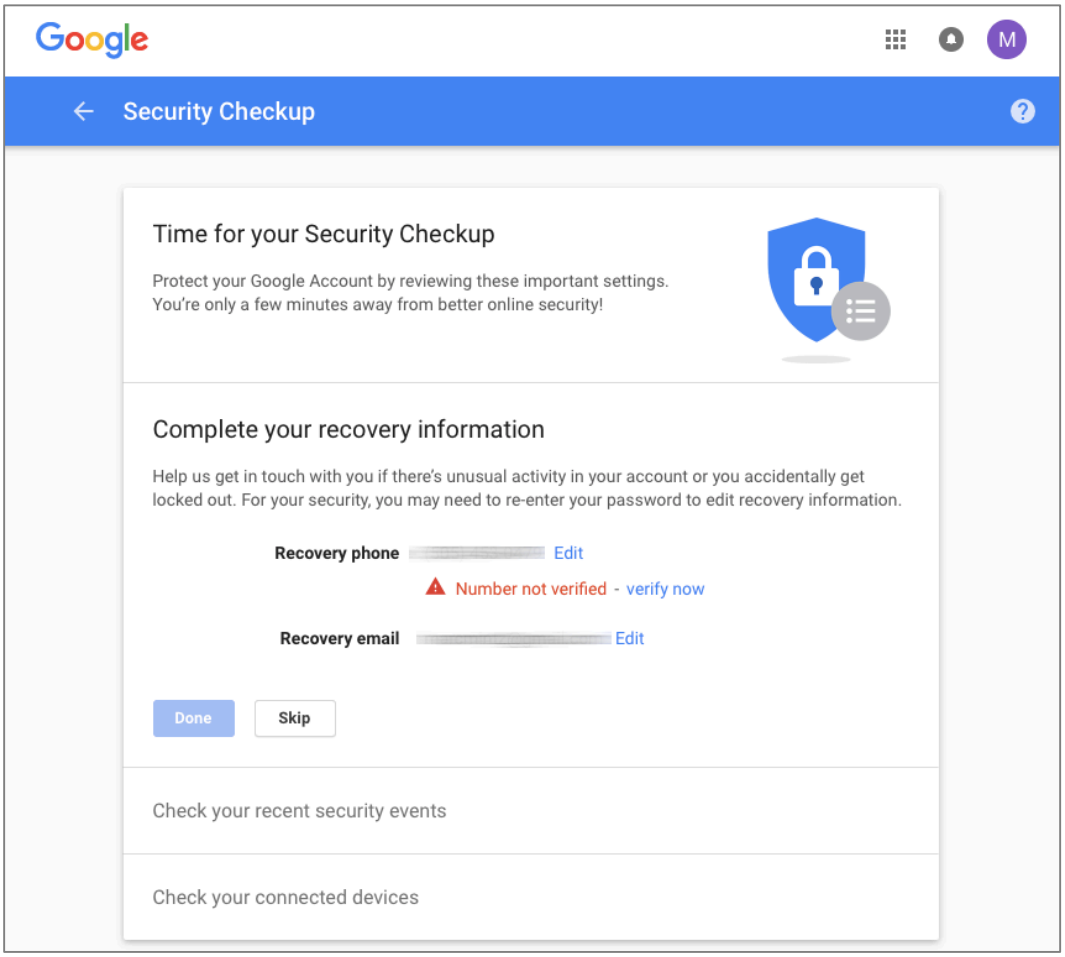
[4] *http://www.digitaltrends.com/web/gmail-joins-the-billion-users-club/*

1. Open a web browser to the Google Security page *https://myaccount.google.com/intro/security*, sign in, and then click *Sign-in & security* from the side bar.

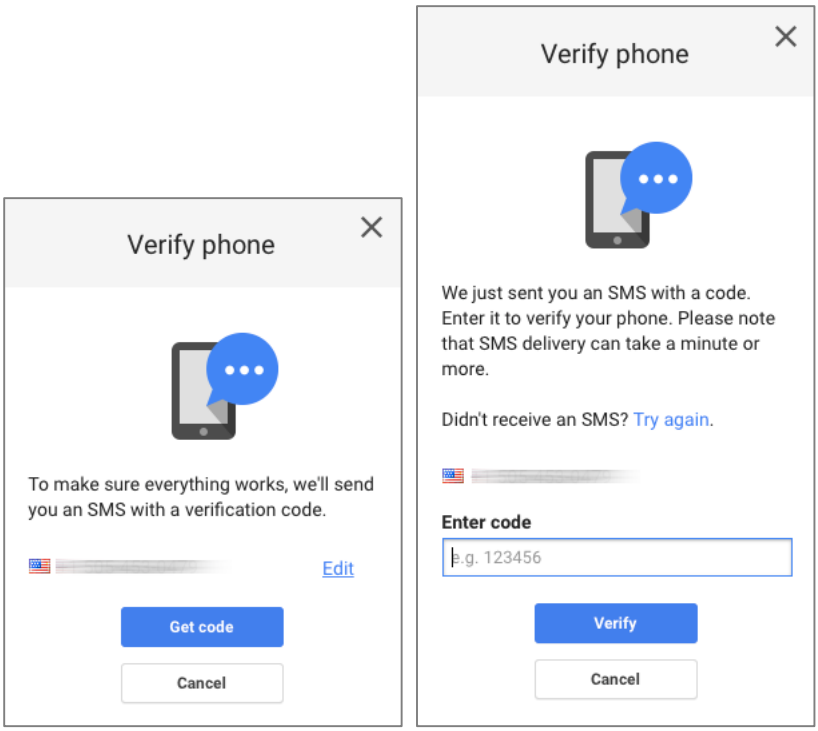


2. Under *Security Checkup*, click *GET STARTED*.

3. In the event Google detects unusual activity on this account, or if you get locked out, you will need to have a recovery phone and recovery email on record with Google. These are used to authenticate your identity.



- *Recovery Phone:* If the listed number is not correct, click *Edit,* and then enter the correct phone number.
- *Number not verified:* If the recovery phone number is not verified, click *verify now.* The phone number can't be used for authentication until it is verified. After clicking *Get code,* a code will be sent to the phone number. Enter the received code, and then click *Verify*.

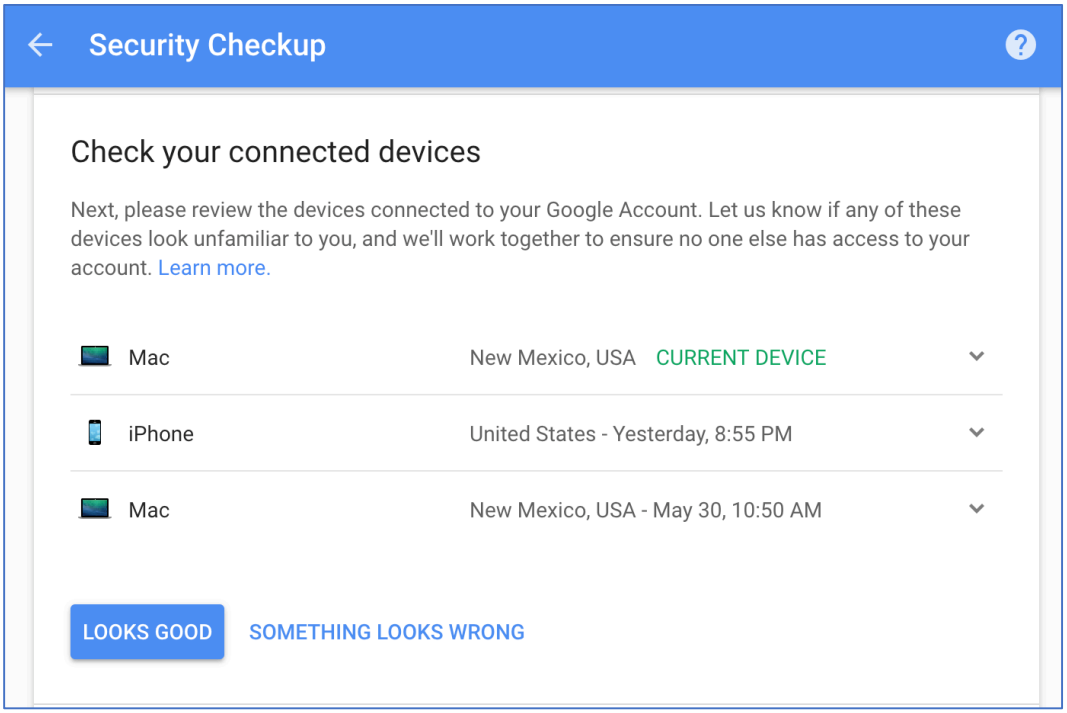


- *Recovery email:* If the listed address is not correct, click *Edit,* and then enter the correct address.

4. When complete, click *Done.*

Check Your Connected Devices

5. The *Check your connected devices* section appears.



- If anything looks suspicious, click the *Something looks wrong* button, and then follow the on-screen instructions.
- If everything looks ok, click the *Looks good* button.

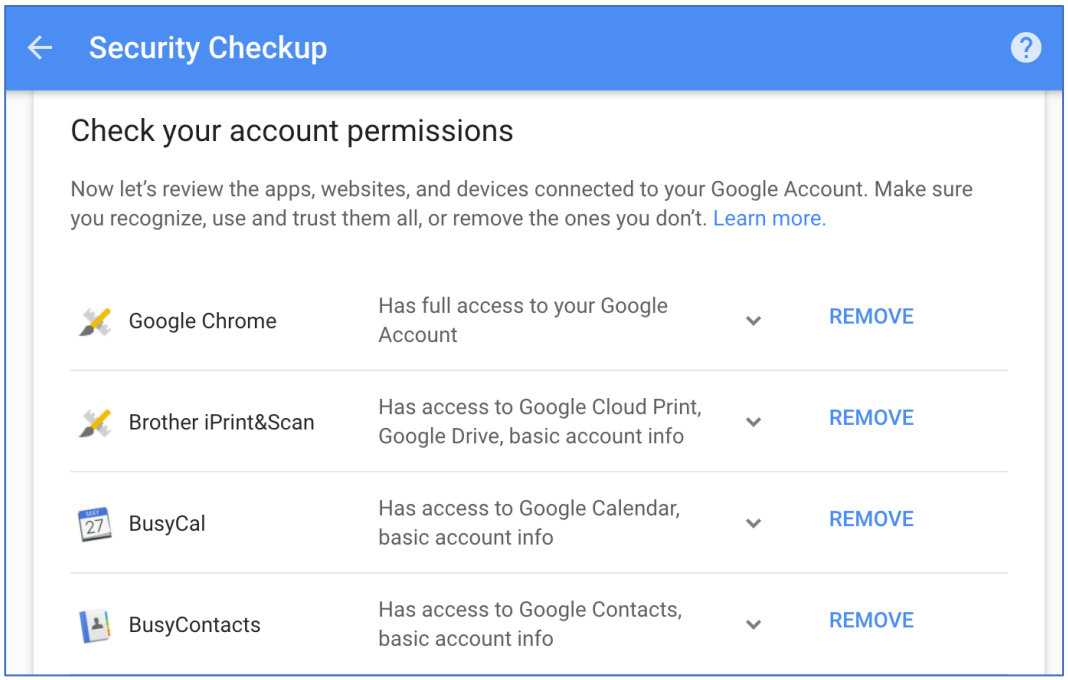
Check Your Account Permissions

Many websites and apps offer to connect to your Google account. In my example below, Google Chrome, Brother iPrint&Scan, BusyCal, and BusyContacts are all applications that connect to Google for data feeds. Websites may do the same, or

you may have an app or website that you can log into using your Google credentials.

Be mindful that all of these apps and websites may have access to some or all of the information that Google holds about you.

6. The *Check your account permissions* section appears.
7. If you see any item that should not have access to your Google account, click the *REMOVE* link.

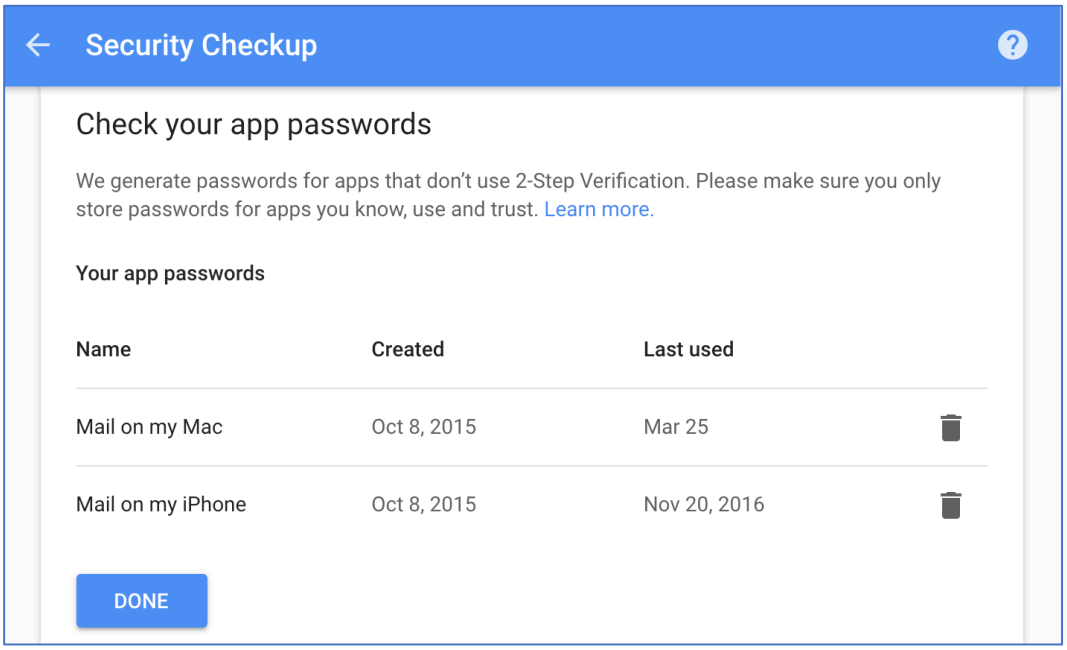


8. When complete, click the *DONE button.*

Check Your App Passwords

Some apps and applications that connect with your Google account do not support 2-Step Verification. To ensure the security of the data managed by these apps if you do have 2-Step Verification active (and you should), they must have a separate *app password.*

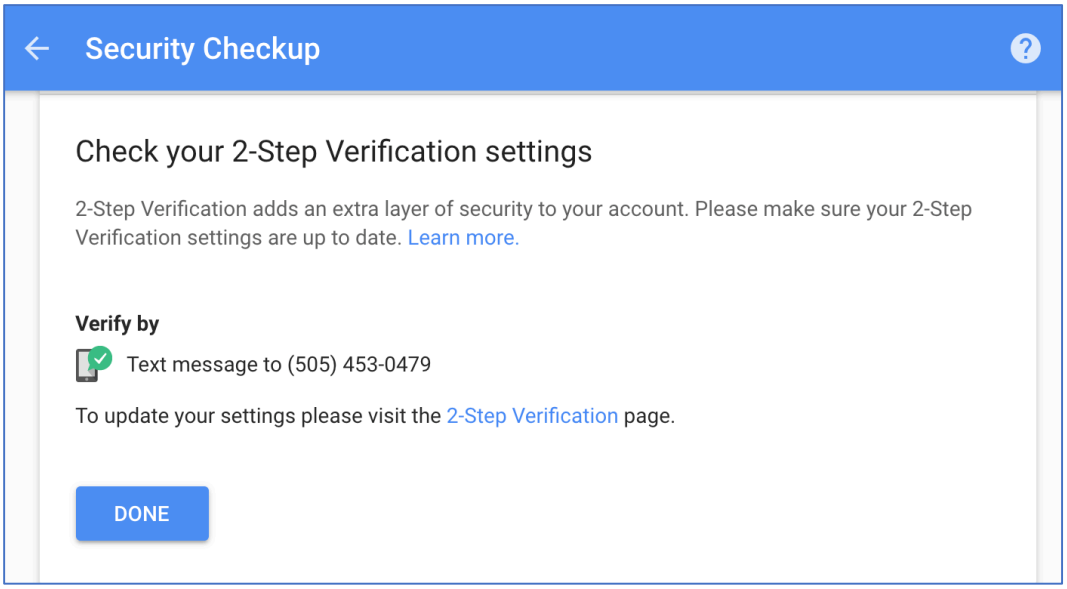
9. The *Check your app passwords* section appears.
10. If you see any apps that you don't use, click the trash icon to the right of the app to remove its app password. This way, nobody else will be able to use the app with your Google account.



11. When complete, click the *DONE* button.

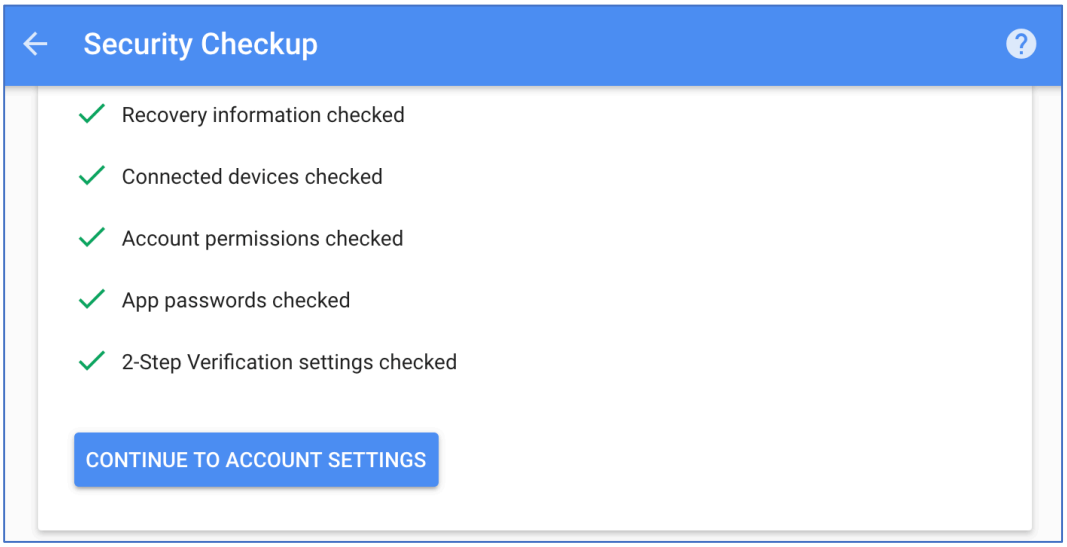
Check Your 2-Step Verification Settings

12. If you already have Google 2-Step Verification active, the next section to appear is Check your 2-Step Verification settings.
    - If you do not currently have 2-Step Verification enabled, skip to ***Account Settings.*** In the next assignment, you will enable Google 2-Step Verification.



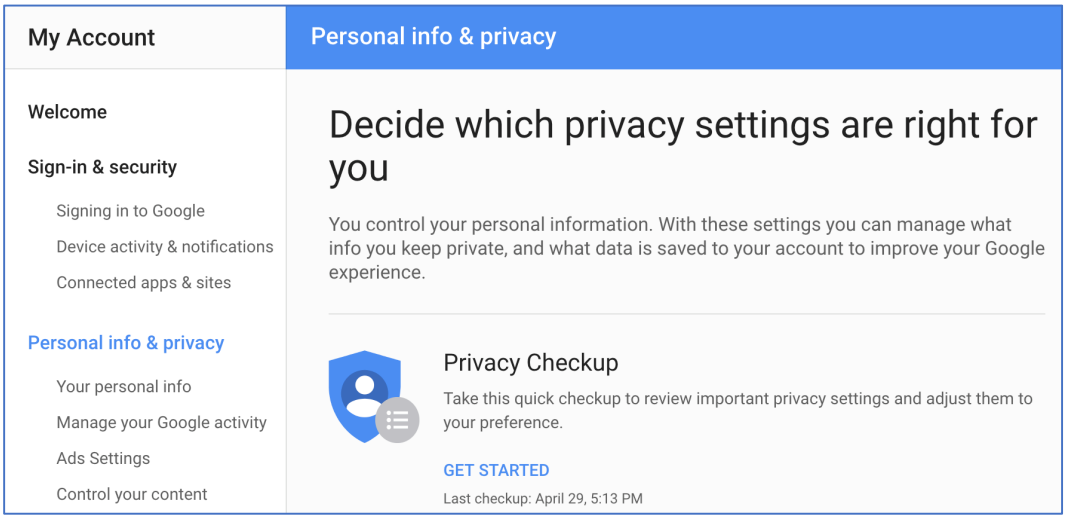
13. If you need to make changes, click the *2-Step Verification* page link
14. When complete, click *DONE.*

15. Click *CONTINUE TO ACCOUNT SETTINGS*.

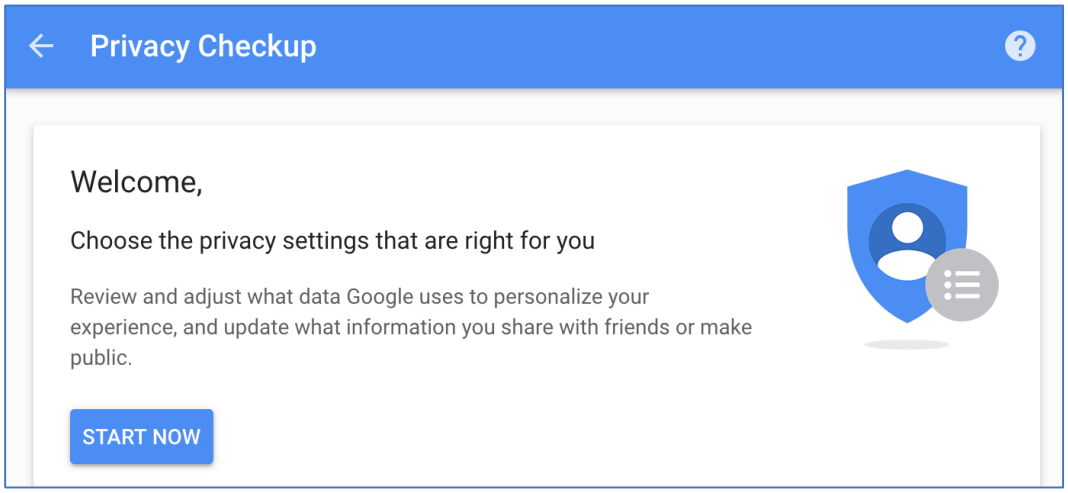


Account Settings

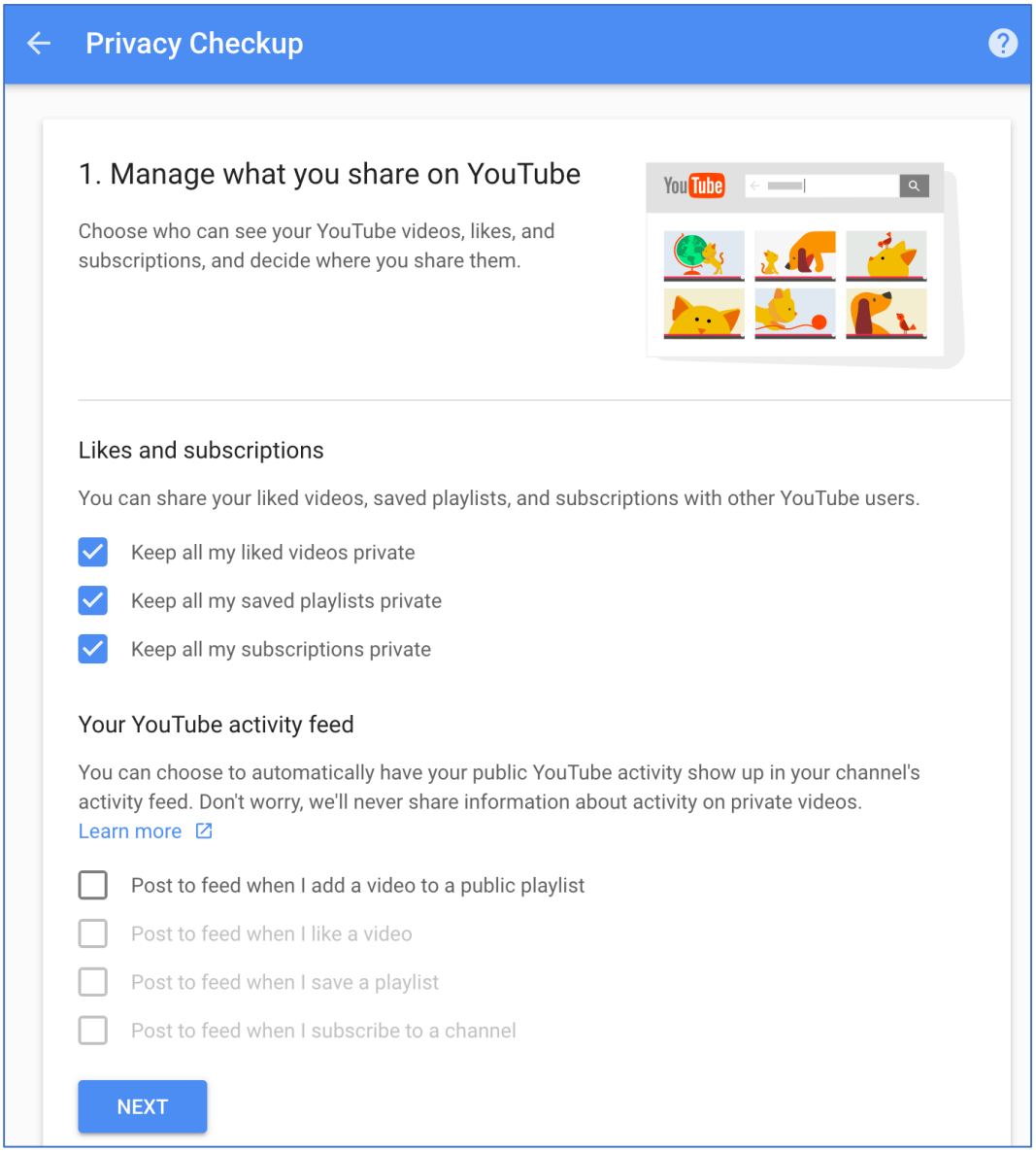
16. You are returned to the *My Account* page.
17. From the sidebar, select *Personal info & privacy*, and then click the *GET STARTED* link.



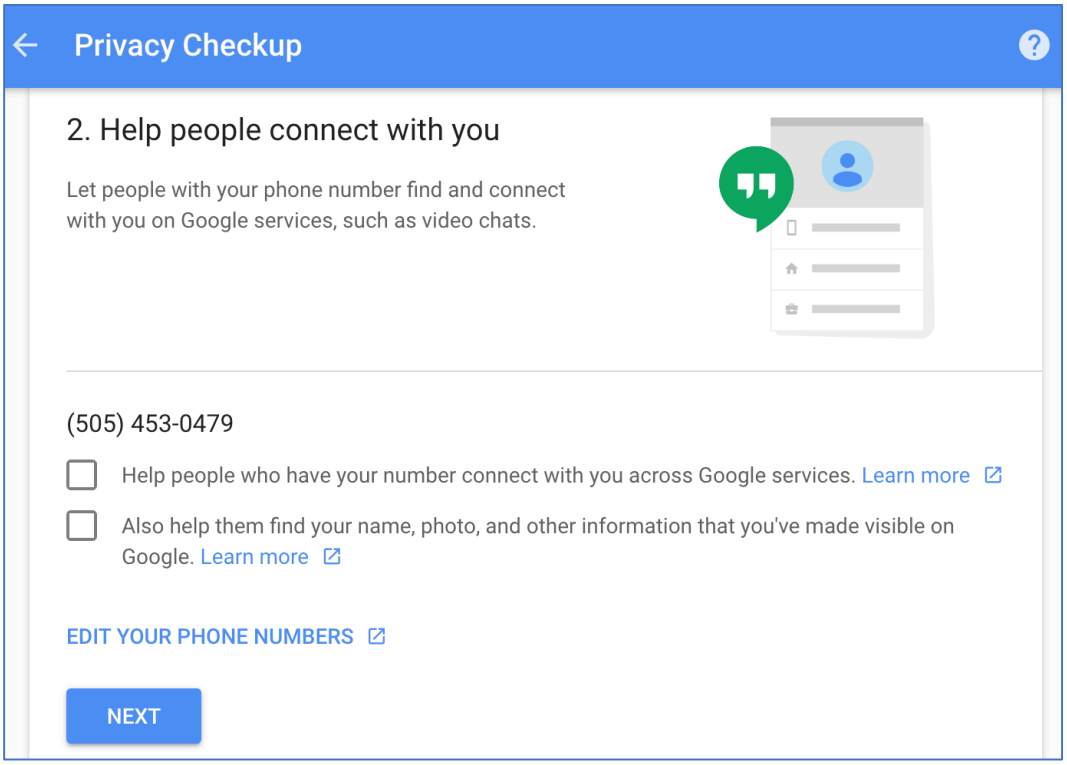
18. In the *Welcome* page, click *START NOW*.



19. In the *Manage what you share on YouTube* page, configure to your taste. Shown below is my recommendation for highest privacy.

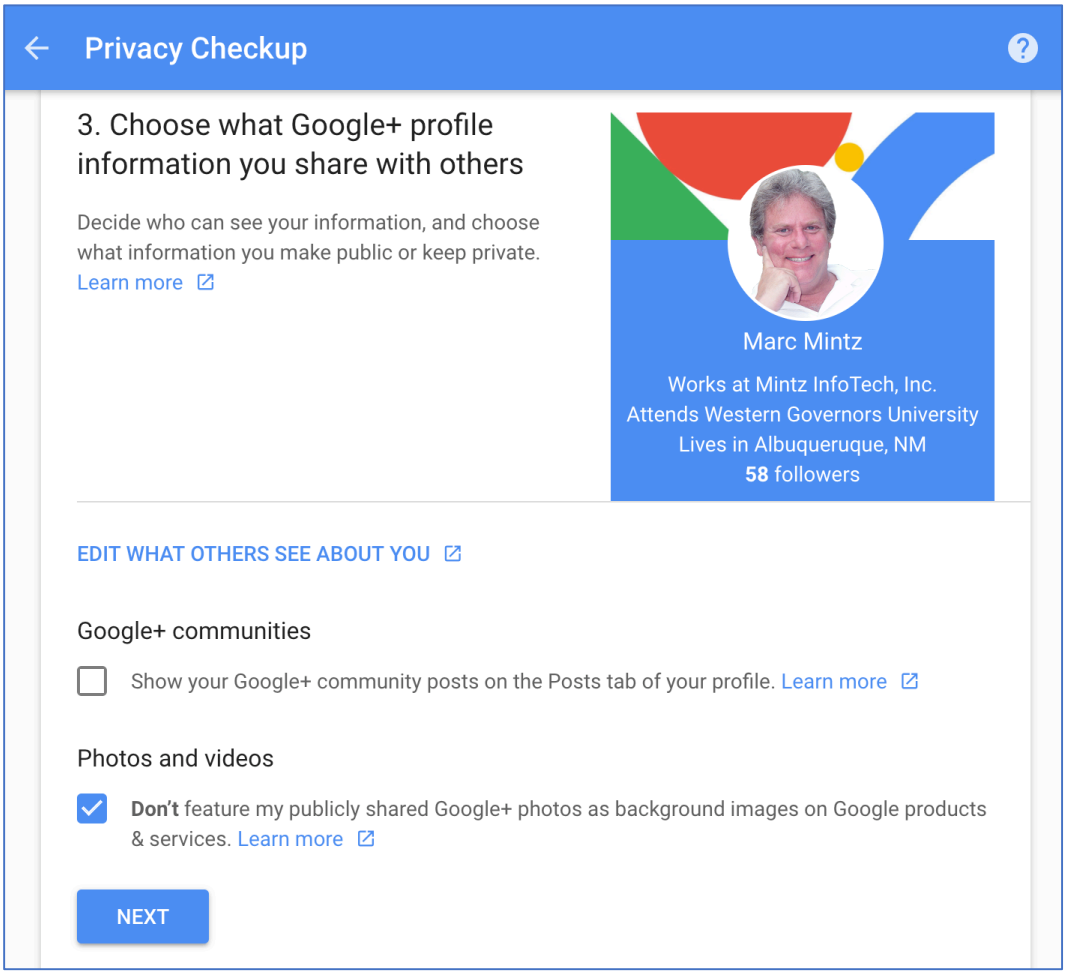


20. In the *Help people connect with you* page, configure to your taste. My recommendation for highest privacy is shown below.



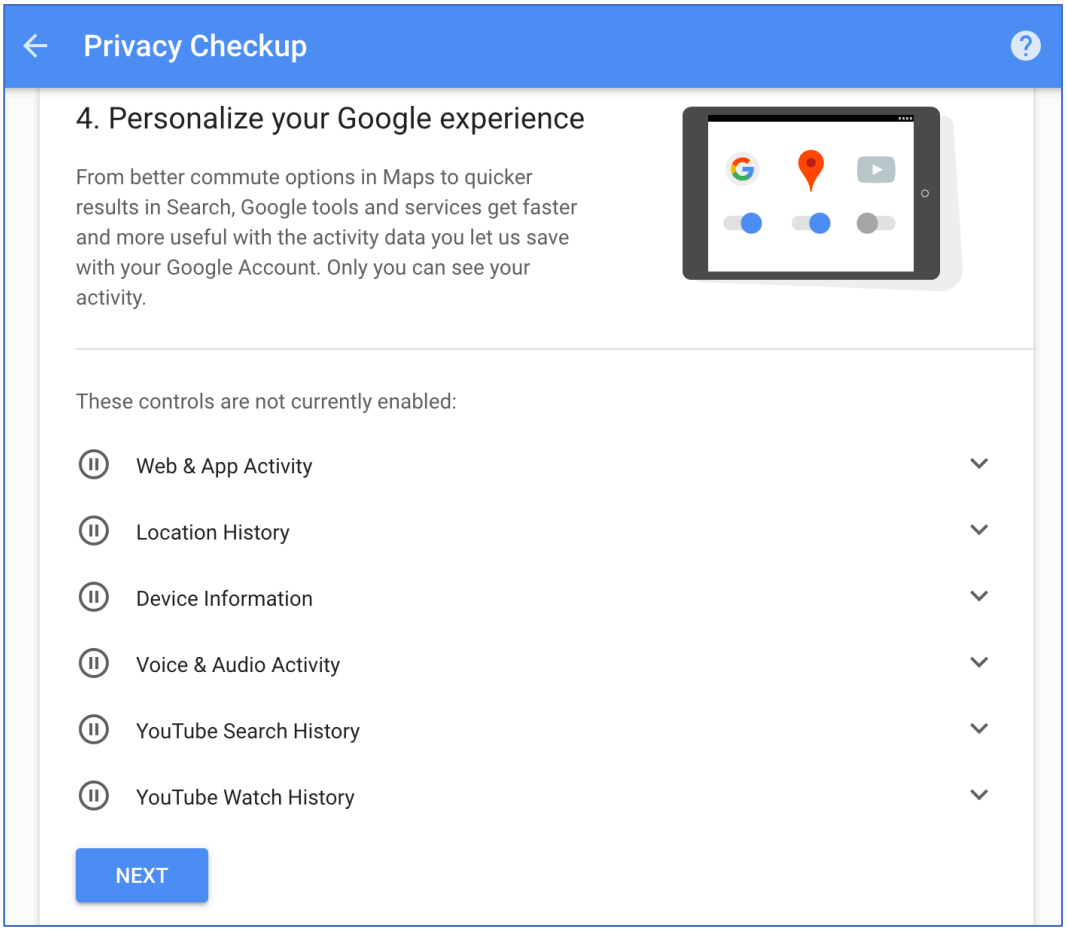
21. When complete, click *NEXT*.

22. In the *Choose what Google+ profile information you share with others,* configure to your taste. My recommendation for highest security is shown below.



23. When complete, click *NEXT*.

24. In the *Personalize your Google experience* page, configure to your taste. My recommendation for highest security are shown below.

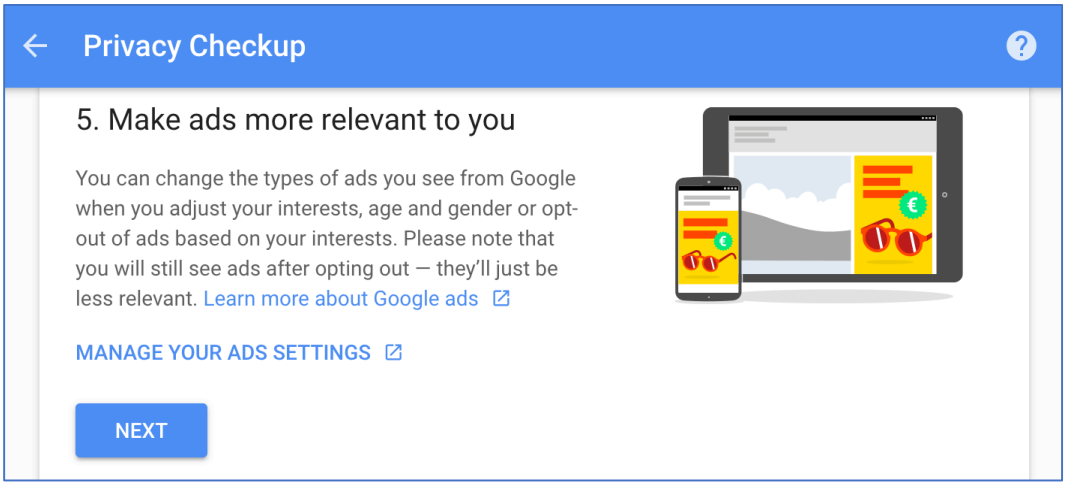


25. When complete, click *NEXT*.

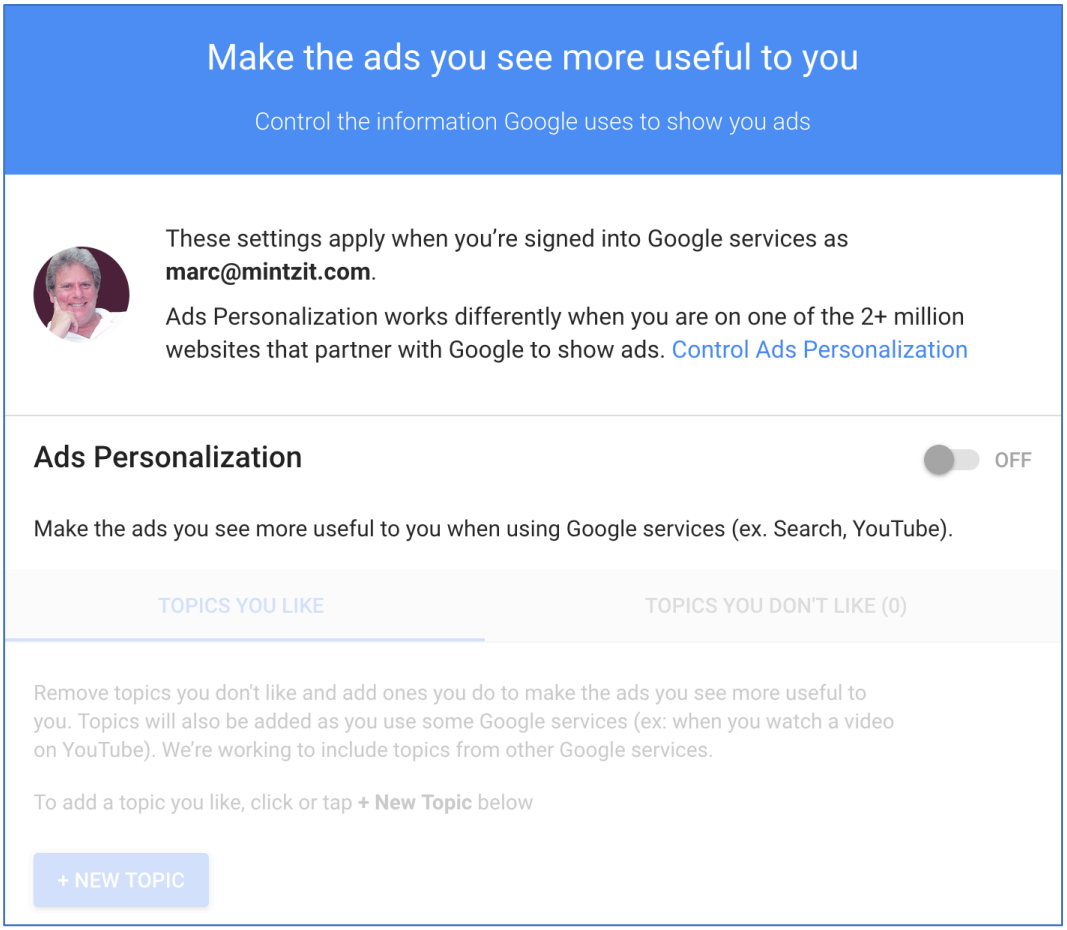
Ads Personalization

All the information Google has on you may be shared with advertisers. This is done to provide targeted ads. If you prefer not to have your information shared with advertisers, you will still see ads, but they won't be targeted to you.

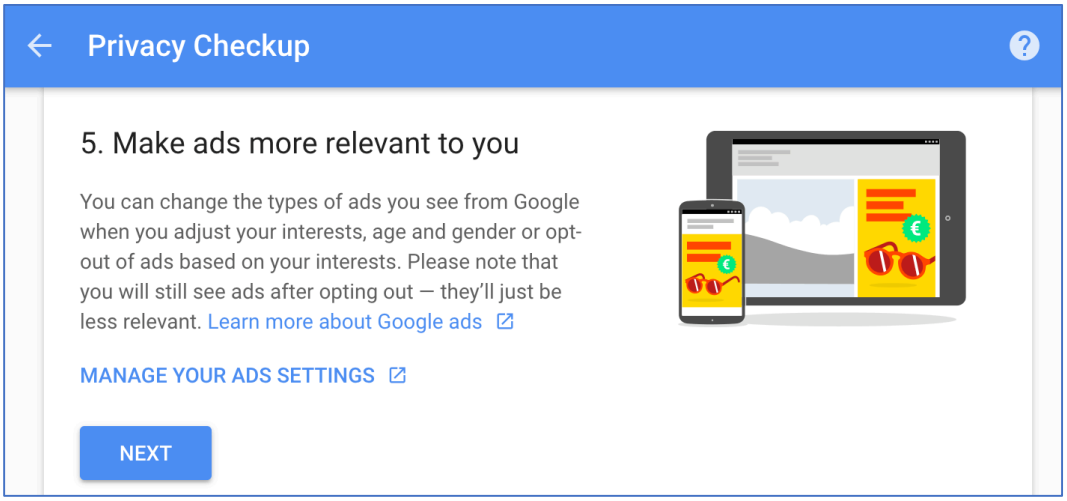
26. In the *Make ads more relevant to you* page, click *MANAGE YOUR ADS SETTINGS*.



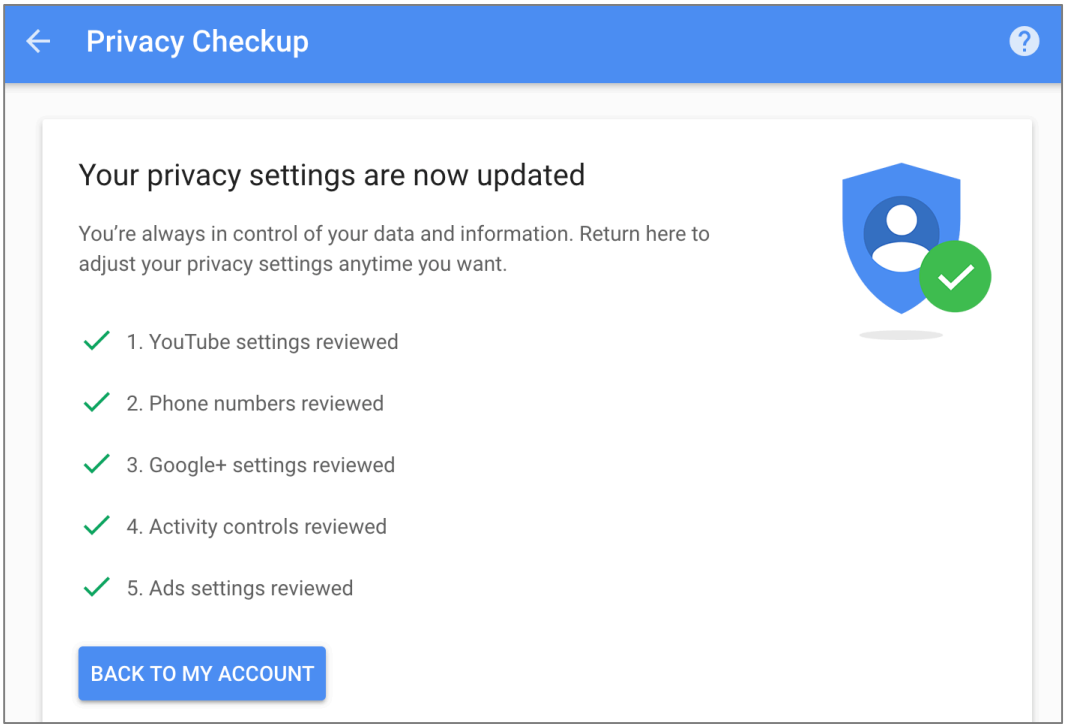
27. To stop Google sharing your information with advertisers, turn *Ads Personalization* to *OFF*.



28. Return to the *Privacy Checkup* section, *Make ads more relevant to you* page, and then click *NEXT*.



29. In the *Your privacy settings are now updated* page, click *BACK TO MY ACCOUNT*.



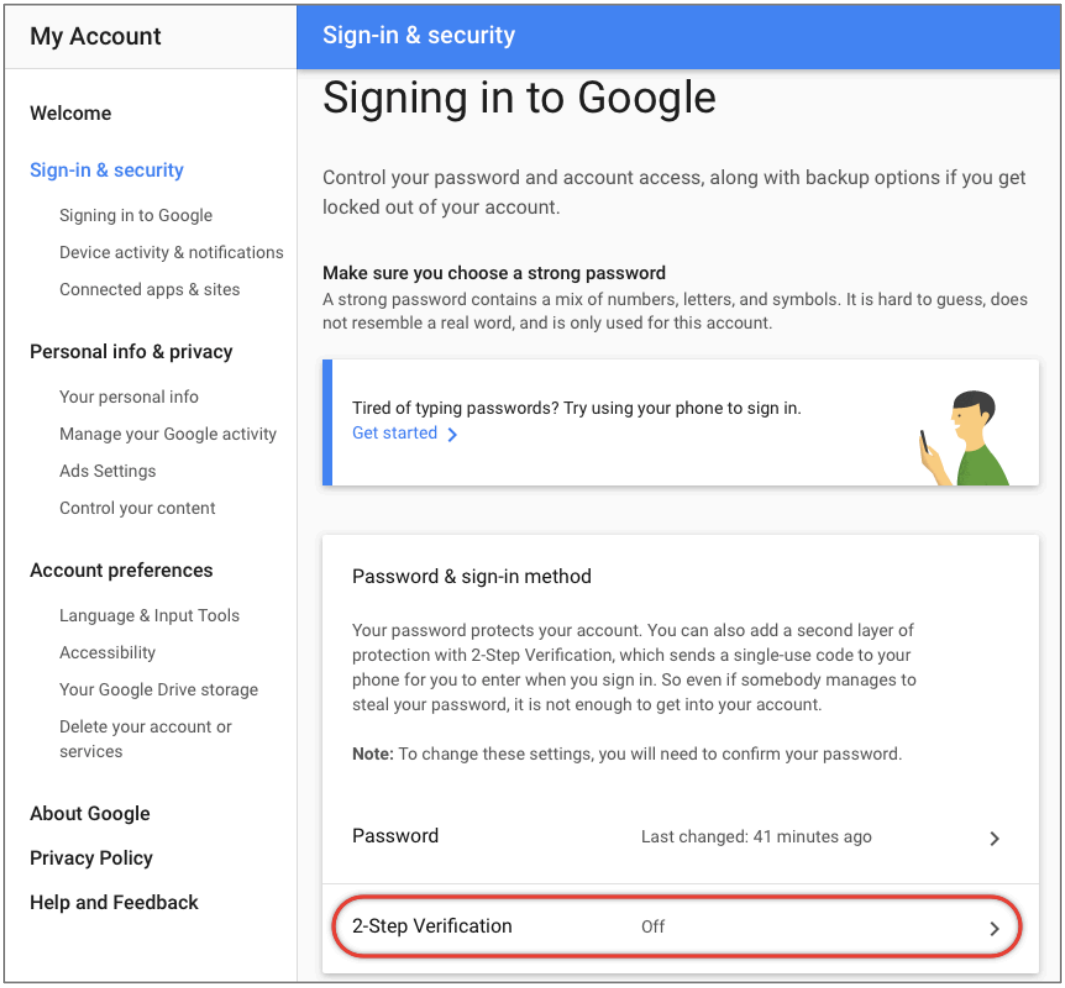
30. From the *My Account* page, you may further configure your personal preferences from the sidebar, or exit. If you haven't yet configured your Google 2-Step Verification, stay right where you are for the next assignment.

20.5.2 Assignment: Enable Google 2-Step Verification

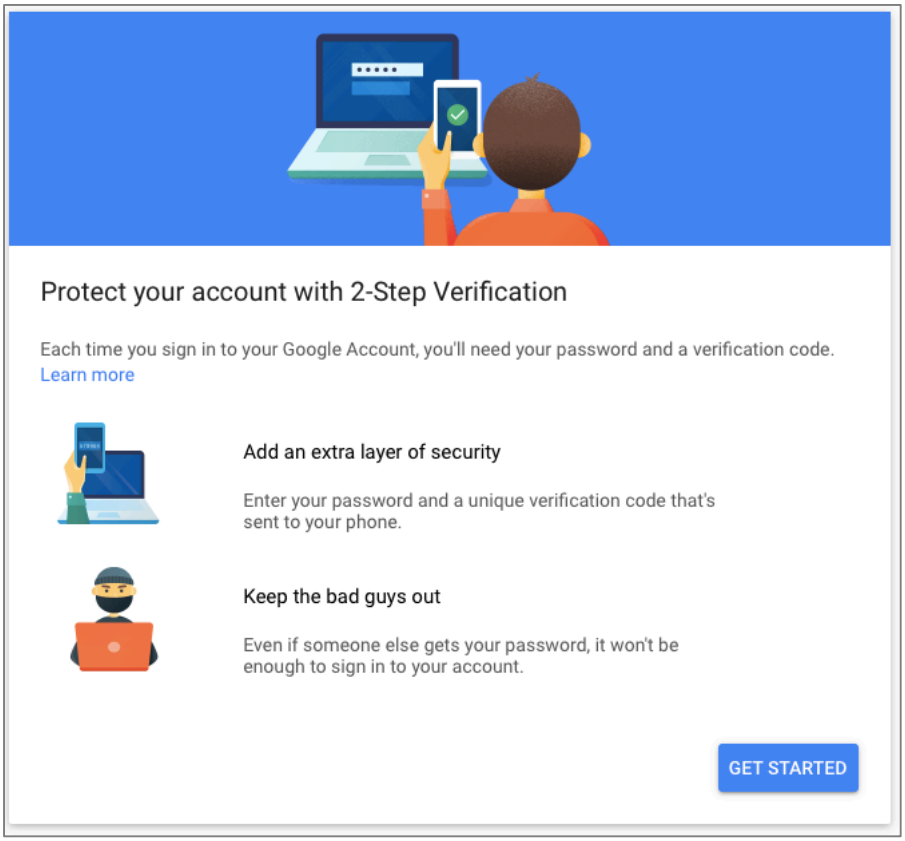
As we have discussed before, passwords may be cracked or discovered with a bit of social engineering. Two-factor authentication, or as Google calls it, 2-step verification make it significantly more difficult for someone else to access your account.

In this assignment, you enable Google 2-step verification.

1. If you have just completed the previous assignment, continue to step 2. If not, open a web browser to the Google Security page *https://myaccount.google.com/intro/security,* and then click *Signing in to Google* from the side bar.
2. Scroll down to *2-Step Verification.* If it reports *On*, your account is already protected. If it reports *Off,* click the > icon to continue.

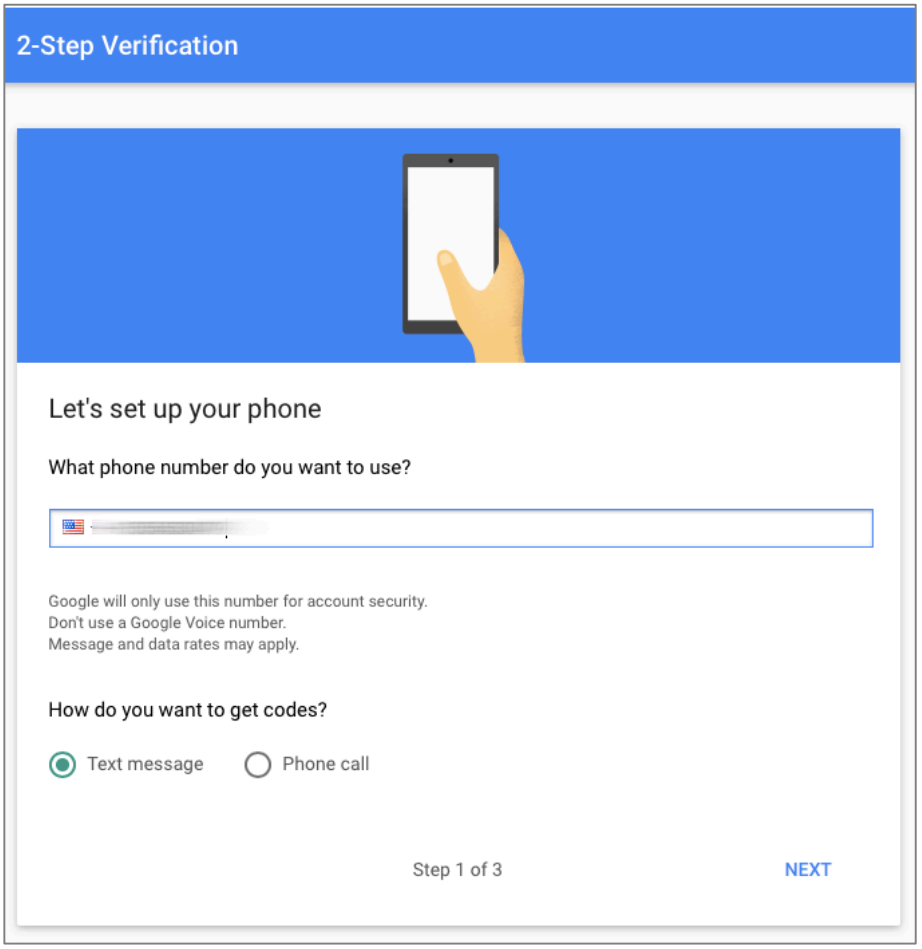


3. At the *Protect your account with 2-Step Verification* page, click the *Get Started* button. The Google login window appears.

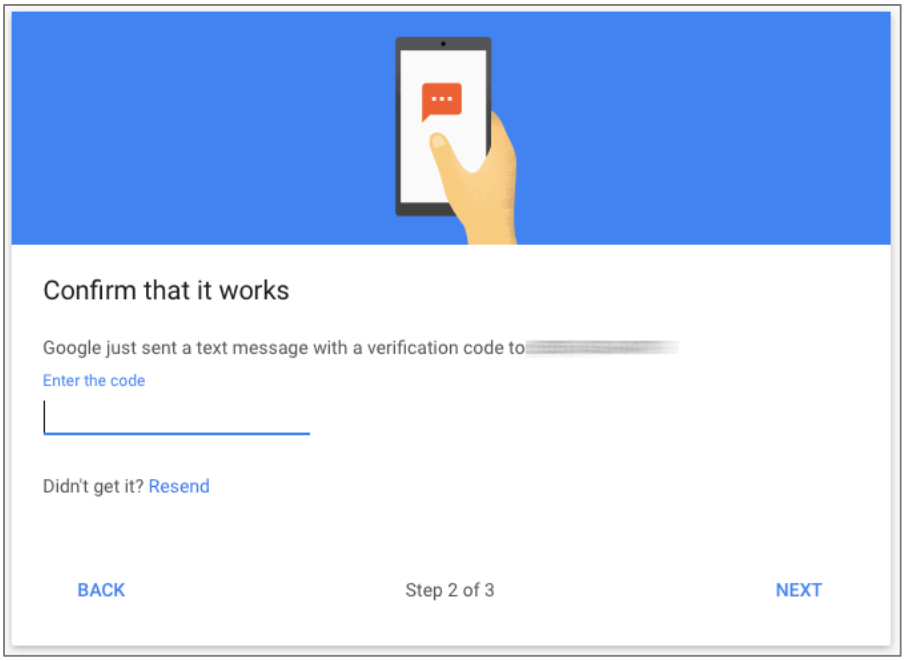


4. At the login window, enter your password, and then click the *Sign-In* button.

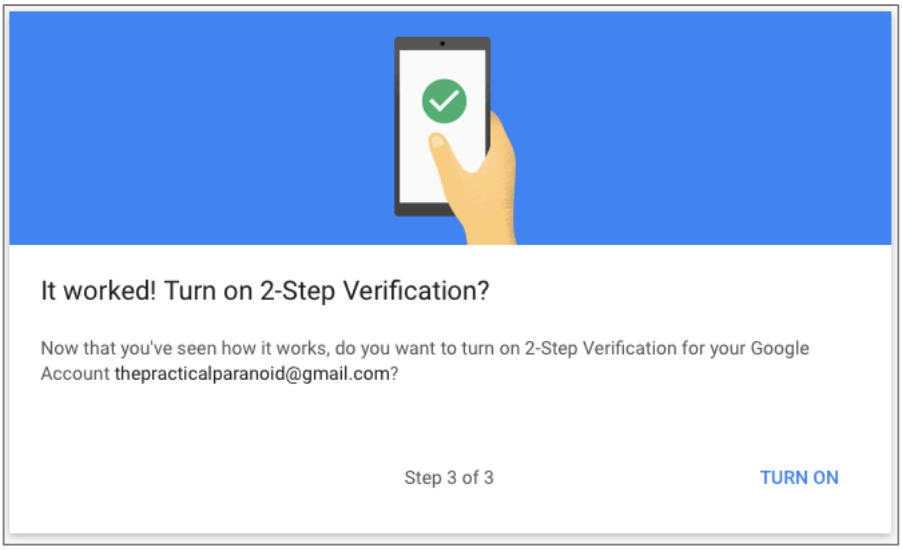
5. In the *What phone number do you want to use?* field, enter the number you will use, select to get your codes via *Text message* or *Phone call*, and then select *Next*.
    - Note: US-CERT has recently recommended to *not* receive authentication codes via text as this is easier to intercept.



6. In the *Confirm that it works* page, enter the code you received, and then select *Next*.



7. In the *It worked! Turn on 2-Step Verification* page, select *TURN ON*.



Your Google account is now hardened with 2-step verification.

Index

2-Factor Authentication..... 484, 485, 724
2-step verification.....95, 694, 699
802.1x.....253, 255
access point 257
administrative..... 124, 132, 134, 135, 214
administrator 59, 122, 124, 133, 134, 135, 136, 229, 231, 260
AES.....78, 255, 531, 537
Airport ...37, 259, 260, 262, 267, 272, 274
Al Gore 551
Andrew S. Tanenbaum..... 709
Android 520, 579
Anonymous Internet Browsing.. 354
antenna 252
anti-malware..... 110, 136, 172, 173
Antivirus..... 172, 176, 177, 179, 184, 187, 203
App Store..... 110, 111, 238, 484
Apple ID .. 73, 95, 110, 234, 238, 483, 484, 485, 504
Application Updates.....112, 117
Assignment 40, 43, 45, 47, 54, 57, 60, 61, 70, 79, 82, 85, 89, 91, 94, 99, 100, 103, 105, 109, 112, 117, 124, 128, 131, 132, 134, 137, 148, 150, 154, 155, 157, 158, 163, 166, 176, 192, 213, 216, 224, 225, 228, 234, 238, 241, 242, 245, 247, 257, 259, 260, 263, 267, 275, 285, 291, 300, 305, 307, 308, 310, 311, 312, 314, 315, 316, 318, 321, 323, 325, 326, 327, 334, 335, 338, 340, 345, 349, 354, 364, 376, 378, 384, 389, 392, 396, 400, 406, 412, 413, 418, 420, 422, 426, 427, 428, 432, 439, 448, 459, 463, 466, 471, 477, 479, 480, 481, 485, 490, 507, 510, 513, 517, 518, 520, 526, 532, 536, 539, 541, 544, 555, 560, 565, 566, 570, 573, 581, 583, 591, 596, 601, 612, 614, 616, 623, 624, 626, 628, 634, 640, 650, 660, 677, 694, 703, 711
Aung San Suu Kyi 379
AV Comparatives..... 172
Avira..... 174
Backblaze..... 40
backup. 36, 37, 38, 39, 45, 60, 61, 238
Ban Ki-moon 153
Benjamin Franklin 121, 297
Bitdefender.. 173, 176, 179, 187, 192, 203
Blog..... 29
Boot Camp 172, 173
broadcasting.....228, 252
Carbon Copy Cloner...38, 40, 47, 48, 49, 54, 55, 58
Carbonite..... 40
Certificate Authorities..... 431
Challenge Question..... 82

Cisco 68
CISPA 25
Clear History 314
clone 38, 52, 53, 54, 55, 57, 58, 59, 60, 61, 62
Comodo 432, 436, 439, 446, 448, 449, 460, 461
Computer theft 36
Cookies 310
crack 67
Criminal activities 36
Deep Web 375
Disk Decipher 520
Disk Utility 41, 513
DMZ 284
Do Not Track 333
DoD 702, 703, 707
DoE 702, 707
Dr. Seuss 701
DuckDuckGo 310, 311, 312
Ed Snowden 375
EDS 520
EFI Chip 224
Elayne Boosler 223
Elbert Hubbard 165
Email 104, 379, 383, 390, 396, 400, 405, 411, 412, 414, 426, 428, 431, 432, 433, 434, 436, 440, 441, 457, 458, 460, 461, 462, 630
Encrypt 59, 299, 422, 424, 425, 507, 510, 513, 517
Encrypted Data Store 520
encrypted email 383, 388, 405, 406, 463, 464, 465, 466
encryption 59, 60, 156, 161, 252, 254, 257, 298, 383, 389, 390, 426, 506, 507, 510, 515
Entropy 36
Erase 238, 703
Ethernet 234, 252, 253
Facebook 29, 69, 103, 104, 105, 123, 136, 552, 632, 634, 640, 641, 644, 650, 660
Facetime 552
FAT 541
FBI 25
FileVault 57, 59, 60, 156, 158, 159, 161, 228, 506, 703, 722
FileVault 2 ..... 57, 59, 60, 156, 158, 228, 506
Find My iPhone 235, 236, 238, 239, 240
Find My Mac 228, 229, 234, 236, 238, 242
Find My Mac? 228
Fire 36
firewall 212, 213, 214, 215, 217, 218, 219, 256
FireWire 37, 41, 154, 155
Firmware 223, 224, 225, 228, 285, 722
Firmware Password 161, 224, 225, 226, 722
Flash 25
Gateway VPN 577
General Douglas MacArthur 251
George Carlin 35
Ghostery 334, 340, 341, 342, 343, 344
GNU Privacy Guard 390, 405
Google Hangouts 552, 553

GPA 406
GPG.....405, 406, 408, 412, 413, 418, 419, 420, 426, 427, 428, 430, 431, 463, 466
GPG Keychain Access 412, 413, 418, 419, 430
GPG Public Key..... 406
Gpg4win 406
GPGMail..... 420
GPGTools.....406, 407, 418
Gravity Zone 173
GravityZone . 192, 194, 195, 199, 202
G-Suite 40
Guest 123, 137, 228, 229, 230, 232, 234, 722
Hamachi 601, 602, 614, 615, 616, 617, 620, 623, 624, 626, 627, 628, 629
HaveIBeenPwned 376
haystack 68, 71
HIPAA 40
Honore de Balzac 171
Hot Corners 169
https..68, 71, 298, 299, 300, 302, 303, 383, 384, 389, 390, 723
HTTPS Everywhere 299, 300, 355
Hypertext Transport Layer Secure..... 383
iCloud 72, 73, 74, 94, 95, 98, 159, 160, 228, 234, 235, 483, 484, 485, 500, 501, 503, 724
Incognito Mode..... 305
infected 68
Insertion 252, 253, 264, 276
Integrity Test..... 45
Integrity Testing..... 60
iOS 94, 405, 431, 520
ipconfig..... 270, 271, 279, 280
iTunes 485
Java 25
Joseph Heller..... 21
Keychain 72, 75, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 98, 258, 410, 413, 418, 420, 437, 438, 462, 721
LAN.....256, 257
LastPass..... 69, 99, 100, 103, 105
LinkedIn 660, 675
Linux 352, 353, 405, 406, 520, 541
Local Area Network..... 256
LogMeIn 601, 605, 606, 608, 609, 610, 614, 616, 619, 620, 622, 623, 629
MAC Address 267, 274
Mac OS Extended.....515, 541
MacKeeper 332
MacUpdate..... 112, 116, 117, 118
MacUpdate Desktop 112, 117
maintenance.....37, 124
Malware 36, 124, 172
Managed with Parental Controls.....123, 136, 137
MARC L. MINTZ.....17, 21, 27, 28, 65
Mintz's extrapolation of Sturgeon's Revelation..... 24
modem..... 256
Newsletter..... 29
NIST 23, 537, 715, 717
NSA ..23, 66, 224, 225, 537, 578, 600, 702, 719
NTP 710, 711, 712
Onion Sites..... 375

Parallels 173, 356
Parental Controls 123, 136, 137, 138, 148, 149
passphrase 68
password .. 25, 59, 67, 68, 70, 71, 124, 133, 135, 156, 160, 224, 225, 228, 238, 253, 254, 260, 262, 384, 389, 391, 484, 507, 513, 514, 515
Perfect-Privacy 583, 590, 591, 594, 596, 597, 724
permissions 124
PGP 405, 431
phishing 25, 172, 381
port 212, 284
Port forwarding 284
Ports 216
Power surges 36
Practical Paranoia Book Upgrades 30
Practical Paranoia Updates 29
Pretty Good Privacy 405
Prey 241, 242
private browsing 305
ProtonMail .. 390, 391, 392, 396, 398, 400
Public Key 405, 406, 411, 412, 418, 420, 426, 428, 463, 464, 465, 466
RADIUS 253
RAM-Resident Malware 284
Recovery HD 54, 57, 224, 225, 705
Recovery Key 59
Root 122, 124, 128, 131, 132
router 256, 257, 263, 284, 285, 291
S/MIME 431, 432, 439, 448, 450, 455, 458, 459, 463, 464, 466
Sabotage 36
Screen Saver 166, 169
screensaver 170
SEC 40
Secure Socket Layer 298
Seneca 107
Server 37, 252, 253
SHA 537
Sharing Only 123
Single User Mode 224
Skype 552, 553
sleep .. 55, 60, 161, 166, 167, 168, 169, 170, 267, 305, 576
software 37, 40, 67, 68, 124, 172, 252, 391
SSL 298, 384, 387, 390
Standard 123, 135, 137, 409, 534
Static electricity 36
stealth 216
switch 256
Symantec 25, 405
System Updates 107
Tails 352, 353, 354, 356, 374, 724
Target Disk Mode 224
Terrorist activities 36
theft 25, 36, 37
Theodore Roosevelt 211
Theodore Sturgeon 24
thepracticalparanoid 464
Thomas Jefferson 65
Thomas Sowell 227
Thunderbolt 37
Time Machine . 37, 38, 39, 40, 43, 44, 45, 46, 47, 721
TKIP 255
TLS 383, 384, 387

Tor 352, 353, 354, 355, 356, 357, 358, 359, 360, 362, 363, 364, 374, 375, 723, 724
TorBrowser 356, 357, 362, 364
TrafficLight . 187, 188, 189, 203, 204, 205, 321
Trojan horses 25, 172
TrueCrypt..... 520, 528
Two-Step Verification .504, 674, 675
USB.....37, 41, 154, 155
US-CERT..... 108
User Accounts..... 121
VeraCrypt.... 520, 526, 527, 531, 532, 533, 534, 544, 545, 547, 548
Virtru ...469, 471, 472, 473, 475, 477, 478, 479, 480
virtual machine.....172, 173, 356
Virtual Private Network..... 254, 299, 576
viruses 25
VMware Fusion 173
VPN.....254, 259, 299, 576, 577, 578, 579, 580, 583, 600, 601, 612, 614, 620, 623, 624, 626, 628, 630, 724
VPNArea 583
war driving 25
Water damage..... 36
Web Mail..... 389
WEP 254, 257
Whitelisting..... 136
Wi-Fi 25, 228, 234, 252, 253, 254, 257, 258, 259
William Blum..... 505
William Hazlitt 483
Windows 154, 172, 173, 174, 270, 279, 352, 405, 406, 520, 541, 579, 625
Wire..... 555, 566, 568, 570
worms 25, 172
WPA.....254, 255, 257
WPA2..... 254, 255, 257, 259, 262
zero-day exploits 26

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.

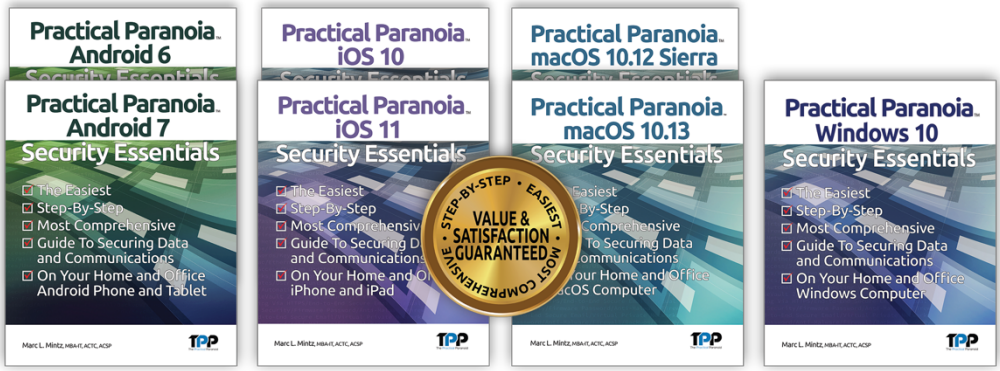
Let us contribute to your success.

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