

# Practical Paranoia™ macOS 10.13

## Security Essentials

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

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

**TPP**  
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

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

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

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

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

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

Cover design by Ed Brandt

ISBN-10: 1976513650

ISBN-13: 978-1976513657

# Dedication

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



# Contents At A Glance

Dedication.....	3
Contents At A Glance.....	5
Contents In Detail.....	7
1 Thank You for Studying Practical Paranoia!.....	19
2 Introduction.....	21
3 Data Loss.....	33
4 Passwords.....	63
5 System and Application Updates.....	105
6 User Accounts.....	119
7 Storage Device.....	151
8 Sleep and Screen Saver.....	163
9 Malware.....	169
10 Firewall.....	209
11 Firmware Password.....	221
12 Lost or Stolen Device.....	225
13 Local Network.....	251
14 Web Browsing.....	297
15 Email.....	387
16 Apple ID and iCloud.....	487
17 Documents.....	509
18 Voice, Video, and Instant Message Communications.....	561
19 Internet Activity.....	585
20 Social Media.....	635
21 When It Is Time to Say Goodbye.....	701
22 Miscellaneous.....	713
23 The Final Word.....	723
macOS 10.13 Security Checklist.....	725
Revision Log.....	731
Index.....	733



# 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
2.6.1 Newsletter.....	29
2.6.2 Blog.....	29
2.6.3 Facebook.....	29
2.6.4 Practical Paranoia Paperback Book Upgrades.....	29
2.6.5 Practical Paranoia Kindle Updates.....	30
2.6.6 Practical Paranoia Online Live Student Edition Updates.....	30
2.7 Notes for Instructors, Teachers, & Professors.....	31
2.8 Update Bounty.....	32
3 Data Loss.....	33
3.1 The Need for Backups.....	34
3.1.1 Assignment: Format the Backup Drive for Time Machine or Carbon Copy Cloner.....	39
3.1.2 Assignment: Configure Time Machine.....	42
3.1.3 Assignment: Integrity Test the Time Machine Backup.....	44
3.1.4 Assignment: Install and Configure Carbon Copy Cloner.....	46
3.1.5 Assignment: Test Run the First Clone Backup.....	53
3.1.6 Assignment: Encrypt the Clone Backup.....	56
3.1.7 Assignment: Integrity Test the Clone Backup.....	59
4 Passwords.....	63
4.1 The Great Awakening.....	64
4.2 Strong Passwords.....	65

## Contents In Detail

4.2.1	Assignment: Create a Strong User Account Password.....	68
4.3	Keychain.....	73
4.3.1	Assignment: View an Existing Keychain Record.....	77
4.4	Challenge Questions.....	80
4.4.1	Assignment: Store Challenge Q&A in the Keychain.....	80
4.4.2	Assignment: Access Secure Data from Keychain.....	83
4.5	Harden the Keychain.....	86
4.5.1	Assignment: Harden the Keychain With a Timed Lock.....	86
4.6	Synchronize Keychain Across macOS and iOS Devices.....	89
4.6.1	Assignment: Activate iCloud Keychain Synchronization.....	89
4.7	LastPass.....	94
4.7.1	Assignment: Install LastPass.....	94
4.7.2	Assignment: Use LastPass to Save Website Authentication Credentials.....	98
4.7.3	Assignment: Use LastPass to Auto Fill Website Authentication .....	100
4.8	Password Policies.....	101
4.8.1	Assignment: Password Policies with macOS Server.....	101
5	System and Application Updates.....	105
5.1	System Updates.....	106
5.1.1	Assignment: Configure Apple System and Application Update Schedule.....	107
5.2	Manage Application Updates With MacUpdate Desktop.....	110
5.2.1	Assignment: Install and Configure MacUpdate Desktop.....	110
5.2.2	Assignment: Application Updates with MacUpdate Desktop	115
5.3	Additional Reading.....	117
6	User Accounts.....	119
6.1	User Accounts.....	120
6.2	Never Log in As an Administrator.....	122
6.2.1	Assignment: Enable the Root User.....	122
6.2.2	Assignment: Login as the Root User.....	126
6.2.3	Assignment: Change the Root User Password.....	129
6.2.4	Assignment: Disable the Root User.....	130
6.2.5	Assignment: Create an Administrative User Account.....	130
6.2.6	Assignment: Change from Administrator to Standard User...	132
6.3	Application Whitelisting and More with Parental Controls.....	134

## Contents In Detail

6.3.1	Assignment: Configure a Parental Controls Account .....	135
6.3.2	Assignment: View Parental Controls Logs.....	146
6.4	Policy Banner.....	148
6.4.1	Assignment: Create a Policy Banner .....	148
7	Storage Device .....	151
7.1	Block Access to Storage Devices .....	152
7.1.1	Assignment: Disable USB, FireWire, and Thunderbolt Storage Device Access .....	152
7.1.2	Assignment: Enable USB, FireWire, and Thunderbolt Storage Device Access .....	153
7.2	FileVault 2 Full Disk Encryption.....	154
7.2.1	Assignment: Boot into Target Disk Mode.....	155
7.2.2	Assignment: Boot into Recovery HD Mode .....	155
7.2.3	Assignment: Boot into Single-User Mode.....	156
7.2.4	Assignment: Enable and Configure FileVault 2 .....	156
7.3	FileVault Resistance to Brute Force Attack.....	160
7.4	Remotely Access and Reboot a FileVault Drive .....	161
7.4.1	Assignment: Temporarily Disable FileVault.....	161
8	Sleep and Screen Saver .....	163
8.1	Require Password After Sleep or Screen Saver .....	164
8.1.1	Assignment: Require Password After Sleep or Screen Saver ...	164
9	Malware.....	169
9.1	Anti-Malware .....	170
9.1.1	Assignment: Install and Configure Bitdefender (Home Users Only) .....	174
9.1.2	Assignment: Install and Configure Bitdefender GravityZone Endpoint Security (Business Users).....	190
9.2	Additional Reading .....	207
10	Firewall.....	209
10.1	Firewall 210	
10.1.1	Assignment: Activate the Firewall .....	211
10.1.2	Assignment: Close Unnecessary Ports .....	214
11	Firmware Password .....	221
11.1	EFI Chip .....	222
11.1.1	Assignment: Enable the Firmware Password.....	222
11.1.2	Assignment: Test the Firmware Password .....	223

## Contents In Detail

11.1.3	Assignment: Remove the Firmware Password .....	223
12	Lost or Stolen Device.....	225
12.1	Find My Mac .....	226
12.1.1	Assignment: Activate and Configure Find My Mac.....	226
12.1.2	Assignment: Use Find My Mac From A Computer .....	233
12.1.3	Assignment: Use Find My Mac From An iPhone or iPad .....	237
12.2	Prey 240	
12.2.1	Assignment: Enable the Guest User Account.....	240
12.2.2	Assignment: Create a Prey Account .....	241
12.2.3	Assignment: Install Prey .....	244
12.2.4	Assignment: Configure Prey .....	246
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 .....	302
14.3	Private Browsing.....	304
14.3.1	Assignment: Safari Private Browsing .....	304
14.3.2	Assignment: Firefox Private Browsing.....	306

## Contents In Detail

14.3.3	Assignment: Google Chrome Incognito Mode .....	307
14.4	Secure Web Searches.....	309
14.4.1	Assignment: Make DuckDuckGo Your Safari Search Engine.	309
14.4.2	Assignment: Make DuckDuckGo Your Firefox Search Engine 310	
14.4.3	Assignment: Make DuckDuckGo Your Chrome Search Engine 311	
14.5	Clear History .....	313
14.5.1	Assignment: Clear the Safari History .....	313
14.5.2	Assignment: Clear the Firefox Browsing History .....	314
14.5.3	Assignment: Clear the Chrome History .....	315
14.6	Browser Plug-Ins .....	317
14.6.1	Assignment: Install TrafficLight Plug-In for Safari.....	317
14.6.2	Assignment: Install TrafficLight Plug-In for Google Chrome	320
14.6.3	Assignment: Install TrafficLight For Firefox.....	322
14.6.4	Assignment: Find and Remove Extensions from Safari .....	324
14.6.5	Assignment: Find and Remove Extensions from Chrome.....	325
14.6.6	Assignment: Find and Remove Add-Ons from Firefox .....	326
14.7	Fraudulent Websites .....	328
14.8	Do Not Track.....	332
14.8.1	Assignment: Secure Safari.....	333
14.8.2	Assignment: Secure Firefox.....	334
14.8.3	Assignment: Secure Chrome.....	336
14.8.4	Assignment: Install Ghostery for Safari.....	338
14.8.5	Assignment: Install Ghostery for Chrome .....	340
14.8.6	Assignment: Install Ghostery for Firefox .....	344
14.9	Adobe Flash and Java .....	352
14.9.1	Assignment: Configure Oracle Java for Automatic Updates...	352
14.10	Web Scams .....	356
14.10.1	Recovering From A Web Scam.....	356
14.11	Tor 359	
14.11.1	Assignment: Install Tor for Anonymous Internet Browsing...	361
5.1.1	Assignment: Configure Tor Preferences.....	371
14.12	Onion Sites and the Deep Web.....	382
14.13	Have I Been Pwned .....	383
14.13.1	Assignment: Has Your Email Been Hacked.....	383

## Contents In Detail

14.13.2	Assignment: What To Do Now That You Have Been Breached	386
15	Email.....	387
15.1	The Killer App.....	388
15.2	Phishing.....	389
15.3	Email Encryption Protocols .....	391
15.4	TLS and SSL With Mail App .....	392
15.4.1	Assignment: Determine if Sender and Recipient Use TLS.....	392
15.5	Require Google Mail to be TLS Secured .....	395
15.5.1	Assignment: Configure Google G-Suite Mail for Only TLS....	395
15.6	HTTPS with Web Mail.....	397
15.6.1	Assignment: Configure Web Mail to Use HTTPS.....	397
15.7	End-To-End Secure Email With ProtonMail .....	398
15.7.1	Assignment: Create a ProtonMail Account .....	399
15.7.2	Assignment: Create and Send an Encrypted ProtonMail Email	403
15.7.3	Assignment: Receive and Respond to a ProtonMail Secure Email	407
15.8	End-To-End Secure Email With GNU Privacy Guard .....	412
15.8.1	Assignment: Install GPG and Generate a Public Key .....	413
15.8.2	Assignment: Add Other Email Addresses to a Public Key .....	418
15.8.3	Assignment: Configure GPGMail Preferences.....	424
15.8.4	Assignment: Install a Friend's Public Key .....	426
15.8.5	Assignment: Send a GPG-Encrypted and Signed Email .....	427
15.8.6	Assignment: Receive a GPG-Encrypted and Signed Email.....	429
15.8.7	Assignment: Encrypt and Sign Files with GPGServices .....	431
15.9	End-To-End Secure Email With S/MIME.....	437
15.9.1	Assignment: Acquire a Free Class 1 S/MIME Certificate.....	438
15.9.2	Assignment: Acquire A Class 3 S/MIME Certificate for Business Use.....	445
15.9.3	Assignment: Purchase a Class 3 S/MIME Certificate for Business Use.....	454
15.9.4	Assignment: Install a Business S/MIME Certificate.....	465
15.9.5	Assignment: Exchange Public Keys with Others .....	469
15.9.6	Assignment: Send S/MIME Encrypted Email.....	472
15.10	Virtru Email Encryption .....	475

## Contents In Detail

15.10.1	Assignment: Create a Free Virtru for Gmail Account.....	476
15.10.2	Assignment: Send Encrypted Gmail With Virtru.....	482
15.10.3	Receive and Reply to a Virtru-Encrypted Email .....	484
16	Apple ID and iCloud.....	487
16.1	Apple ID and iCloud.....	488
16.1.1	Assignment: Create an Apple ID.....	489
16.1.2	Assignment: Enable 2-Factor Authentication .....	494
16.1.3	Sign in to Your iCloud Account.....	503
17	Documents.....	509
17.1	Document Security.....	510
17.2	Password Protect a Document Within Its Application .....	511
17.2.1	Assignment: Encrypt an MS Word Document .....	511
17.3	Encrypt a PDF Document.....	514
17.3.1	Assignment: Convert a Document to PDF for Password Protection.....	514
17.4	Encrypt a Folder for Only macOS Use.....	517
17.4.1	Assignment: Create an Encrypted Disk image .....	517
17.5	Encrypt A Folder for Cross Platform Use With Zip.....	521
17.5.1	Assignment: Encrypt A File or Folder Using Zip .....	521
17.5.2	Assignment: Open an Encrypted Zip Archive.....	527
17.6	Cross-Platform Disk Encryption.....	529
17.6.1	Assignment: Download and Install VeraCrypt .....	529
17.6.2	Assignment: Configure VeraCrypt.....	536
17.6.3	Assignment: Create a VeraCrypt Container .....	542
17.6.4	Assignment: Mount an Encrypted VeraCrypt Container .....	554
18	Voice, Video, and Instant Message Communications .....	561
18.1	Voice, Video, and Instant Messaging Communications .....	562
18.2	HIPAA Considerations .....	564
18.3	Wire 565	
18.3.1	Assignment: Install Wire .....	565
18.3.2	Assignment: Invite People to Wire .....	570
18.3.3	Assignment: Import Contacts into Wire .....	575
18.3.4	Assignment: Secure Instant Message a Wire Friend. ....	576
5.1.2	Assignment: Secure Voice Call with A Wire Friend .....	580
18.3.5	Assignment: Secure Video Conference with a Wire Friend ....	583
19	Internet Activity.....	585

## Contents In Detail

19.1	Virtual Private Network.....	586
19.2	Gateway VPN.....	587
19.2.1	Assignment: Search for a VPN Host .....	591
19.3	NordVPN.....	593
19.3.1	Assignment: Create a NordVPN Account .....	593
19.3.2	Assignment: Configure IKEv2 VPN With NordVPN .....	598
19.4	Resolving Email Conflicts with VPN.....	604
19.5	Mesh VPN.....	605
19.6	LogMeIn Hamachi .....	606
19.6.1	Assignment: Create a LogMeIn Hamachi Account.....	606
5.1.3	Assignment: Add Users to a Hamachi VPN Network.....	619
19.6.2	Assignment: File Sharing Within a Hamachi VPN Network..	629
19.6.3	Assignment: Screen Share Within Hamachi VPN.....	631
19.6.4	Assignment: Exit the Hamachi VPN Network.....	633
20	Social Media.....	635
20.1	What, me worry?.....	636
20.2	Protecting Your Privacy On Social Media.....	637
20.3	Facebook.....	638
20.3.1	Assignment: Facebook Security and Login .....	638
20.3.2	Assignment: Facebook Privacy Settings.....	643
20.3.3	Assignment: Timeline and Tagging Settings .....	645
20.3.4	Assignment: Facebook Manage Blocking.....	646
20.3.5	Assignment: Facebook Public Posts .....	648
20.3.6	Assignment: Facebook Apps.....	650
20.3.7	Assignment: What Does Facebook Know About You.....	660
20.4	LinkedIn .....	666
20.4.1	Assignment: LinkedIn Account Security.....	666
20.4.2	Assignment: Find What LinkedIn Knows About You.....	673
20.5	Google 675	
20.5.1	Assignment: Manage Your Google Account Access and Security Settings.....	675
20.5.2	Assignment: Enable Google 2-Step Verification.....	692
20.5.3	Find What Google Knows About You .....	697
21	When It Is Time to Say Goodbye.....	701
21.1	Preparing a Computer for Sale or Disposal.....	702
21.1.1	Assignment: Prepare Your Mac For Sale Or Disposal.....	702

## Contents In Detail

21.1.2	Assignment: Secure Erase the Drive .....	706
21.1.3	Assignment: Install macOS 10.13.....	711
22	Miscellaneous.....	713
22.1	Date and Time Settings .....	714
22.2	Assignment: Configure Date & Time .....	715
22.3	Securing Hardware Components .....	717
22.4	National Institute of Standards and Technology (NIST) .....	719
22.4.1	NIST-Specific Security Settings .....	719
22.5	United States Computer Emergency Readiness Team (US-CERT) .....	721
23	The Final Word .....	723
23.1	Additional Reading .....	724
	macOS 10.13 Security Checklist .....	725
	Revision Log.....	731
	Index.....	733

## 4 Passwords

*For a people who are free, and who mean to remain so, a well-organized and armed militia is their best security.*

–Thomas Jefferson<sup>1</sup>

*Knowledge, and the willingness to act upon it, is our greatest defense.*

–Marc L. Mintz<sup>2</sup>

### What You Will Learn In This Chapter

- Create a strong password
- Use the Keychain
- View an existing Keychain record
- Challenge questions
- Store challenge Q&A in Keychain
- Access secure data from Keychain
- Harden the Keychain
- Synchronize Keychain across macOS and iOS devices
- Use LastPass to save website credentials
- Create Password Policies

---

<sup>1</sup> [https://en.wikipedia.org/wiki/Thomas\\_Jefferson](https://en.wikipedia.org/wiki/Thomas_Jefferson)

<sup>2</sup> <https://mintzit.com/>

## 4.1 The Great Awakening

In June 2013, documents of NSA origin were leaked to The Guardian newspaper<sup>3</sup>. The documents provided evidence that the NSA was both legally and illegally spying on United States citizens' cell phone, email, and web usage. These documents, while causing gasps of outrage and shock by the public, revealed little that those of us in the IT field already did not know/suspect for decades: every aspect of our digital lives is subject to eavesdropping.

The more cynical amongst us go even further, stating that *everything* we do on our computers *is* recorded and subject to government scrutiny.

But few of us have anything real to fear from our government. Where the real problems with digital data theft come from are local kids hijacking networks, professional cyber-criminals who have fully automated the process of scanning networks for valuable information, competitors/enemies and malware that finds its way into our systems from criminals, foreign governments, and our own government.

The first step to securing our data is to secure our computers and mobile devices. Remember, we are not in Kansas anymore.

---

<sup>3</sup> [https://en.wikipedia.org/wiki/NSA\\_warrantless\\_surveillance\\_controversy](https://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)

## 4.2 Strong Passwords

We all know we need passwords. Right? But do you know that *every* password can be broken? Start by trying *a*. If that does not work, try *b*, and then *c*. Eventually, the correct string of characters will get you into the system. It is only a matter of time.

Way back in your great-great-great grandfather's day, the only way to break into a personal computer was by manually attempting to guess the password. Given that manual attempts could proceed at approximately 1 attempt per second, an 8-character password became the standard. With a typical character set of 24 (a-z) this created a possibility of  $24^8$  or over 100 billion possible combinations. The thought that anyone could ever break such a password was ridiculous, so your ancestors became complacent.

This is funny when you consider that research has shown that most passwords can be guessed. These passwords include: name of spouse, name of children, name of pets, home address, phone number, Social Security number, and main character names from Star Trek and Star Wars (would I kid you?). Most computer users are unaware that what they thought was an obscure and impossible-to-break password could be cracked in minutes.

It gets worse. A while back the first hacker wrote password-breaking software. Assuming it may have taken 8 CPU cycles to process a single attack event, on an old computer with a blazing 16 KHz CPU that would equate to 2,000 attempts per second. This meant that a password could be broken in less than 2 years. Yikes.

IT directors took notice.

So down came the edict from the IT Director that we *must* create *obscure* passwords: strings that include upper and lower case, numeric, and symbol characters. But in many cases, this was a step backward. Since a computer user could not remember that their password was 8@dC%Z#2, the user often would manually record the password. That urban legend of leaving a password on a sticky note under the keyboard? I have seen it myself more than a hundred times.

Come forward to the present day. A current quad-core Intel i7 with freely available password-cracking software can make over 10 billion password attempts

## 4 Passwords

per second. Create an army of infected computers called a botnet to do your dirty work<sup>4</sup> and you can likely achieve over a hundred trillion attempts per second, unless your system locks out the user after x number of failed log on attempts.

What does this mean for you? The typical password using upper and lower case, number, and symbol now can be cracked with the right tools in under than 2 minutes. If using just a single computer to do the break in, make that a week. Don't believe it? Look at the *haystack*<sup>5</sup> search space calculator.

If we use longer passwords, we can make it too time consuming to break into our system, so the bad guys will move on to someone else.

But you say it is tough enough to remember 8 characters, impossible to remember more?

This is true, but only if we keep doing things as we have always done before. Since virtually all such attacks are now done by automated software, it is only an issue of length of password, not complexity. So, use a passphrase that is easy to remember, such as, "Rocky has brown eyes" (which at 100 trillion attempts per second could take over 1,000,000,000,000,000 centuries to break – provided Rocky is not the name of your beloved pet and thus more guessable).

How long should you make your password, or rather, passphrase? As of this writing, Apple<sup>6</sup>, Google<sup>7</sup> and Microsoft<sup>8</sup> recommends a minimum of 8 characters. US-CERT<sup>9 10</sup> currently recommends at least 15 for administrative accounts, at least 8 for non-administrators. Cisco recommends<sup>11</sup> at least 8. My recommendation to clients is a minimum of 15, in an easy-to-remember, easy-to-enter phrase.

---

<sup>4</sup> <http://en.wikipedia.org/wiki/Botnet>

<sup>5</sup> <https://www.grc.com/haystack.htm>

<sup>6</sup> <https://support.apple.com/en-us/HT201303>

<sup>7</sup> <https://support.google.com/a/answer/33386?hl=en>

<sup>8</sup> [https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft\\_Password\\_Guidance-1.pdf](https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf)

<sup>9</sup> <https://security.web.cern.ch/security/recommendations/en/passwords.shtml>

<sup>10</sup> <https://www.us-cert.gov/ncas/alerts/TA11-200A>

<sup>11</sup> [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_aaa/configuration/15-sy/sec\\_usr\\_aaa-15-sy-book/sec-aaa-comm-criteria-pwd.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-sy/sec_usr_aaa-15-sy-book/sec-aaa-comm-criteria-pwd.html)

## 4 Passwords

In addition to password length, it is critical to use a variety of passwords. In this way, should a bad entity gain access to your Facebook password, that password cannot be used to access your bank account.

Yes, soon you will have a drawer full of passwords for all your different accounts, email, social networks, financial institutions, etc. How to keep all of them organized and easily accessed amongst all your various computers and devices? More on that later in the *LastPass* section of this *Password* topic.

### **Apple Password Recommendations**

- Maintain an 8-character minimum length
- At least one number
- Include both upper and lowercase letters
- For a stronger password, add additional characters and punctuation marks

### **Microsoft Password Recommendations**

- Maintain an 8-character minimum length
- Eliminate character-composition requirements
- Eliminate mandatory periodic password resets for user accounts
- Ban common passwords, to keep the most vulnerable passwords out of your system
- Educate your users not to re-use their password for non-work-related purposes
- Use multi-factor (2-factor) authentication

### **US-CERT Password Recommendations**

- Private and known only by one person
- Not stored in clear text in any file or program, or on paper
- Easily remembered
- At least 15 characters long for administrators, at least 8 characters long for non-administrators

## 4 Passwords

- A mixture of at least 3 of the following: upper case, lower case, digits, and symbols
- Not listed in a dictionary of any major language
- Not guessable by any program in a reasonable time frame

### 4.2.1 Assignment: Create a Strong User Account Password

As password cracking is now done through automated software, complexity isn't nearly as important as it was when humans were attempting the crack. This is to say that a password of 1111111111111111 is about as secure as f^w1&%Ge0\*\$W18. I recommend using a passphrase—easy to remember, easy to enter, at least 15 characters. For example, *I love brown eyes* is an excellent password.

In this assignment, you create a strong password for your computer account.

1. Think up a password for yourself that is consists of at least 15 easy-to-remember and easy-to-enter characters, and meets the strength/complexity required by your organization.

## 4 Passwords

2. Test how difficult it is to break your password by visiting haystack at <https://www.grc.com/haystack.htm>.

**GRC's Interactive Brute Force Password "Search Space" Calculator**  
(NOTHING you do here ever leaves your browser. What happens here, stays here.)

No Uppercase     16 Lowercase     No Digits     3 Symbols   

**this is my password**

Enter and edit your test passwords in the field above while viewing the analysis below.

**Brute Force Search Space Analysis:**

Search Space Depth (Alphabet):	26+33 = <b>59</b>
Search Space Length (Characters):	19 characters
Exact Search Space Size (Count): <small>(count of all possible passwords with this alphabet size and up to this password's length)</small>	4,504,143,715,596,357, 284,195,985,482,676,599
Search Space Size (as a power of 10):	$4.50 \times 10^{33}$

**Time Required to Exhaustively Search this Password's Space:**

Online Attack Scenario: <small>(Assuming one thousand guesses per second)</small>	1.43 billion trillion centuries
Offline Fast Attack Scenario: <small>(Assuming one hundred billion guesses per second)</small>	14.32 trillion centuries
Massive Cracking Array Scenario: <small>(Assuming one hundred trillion guesses per second)</small>	14.32 billion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

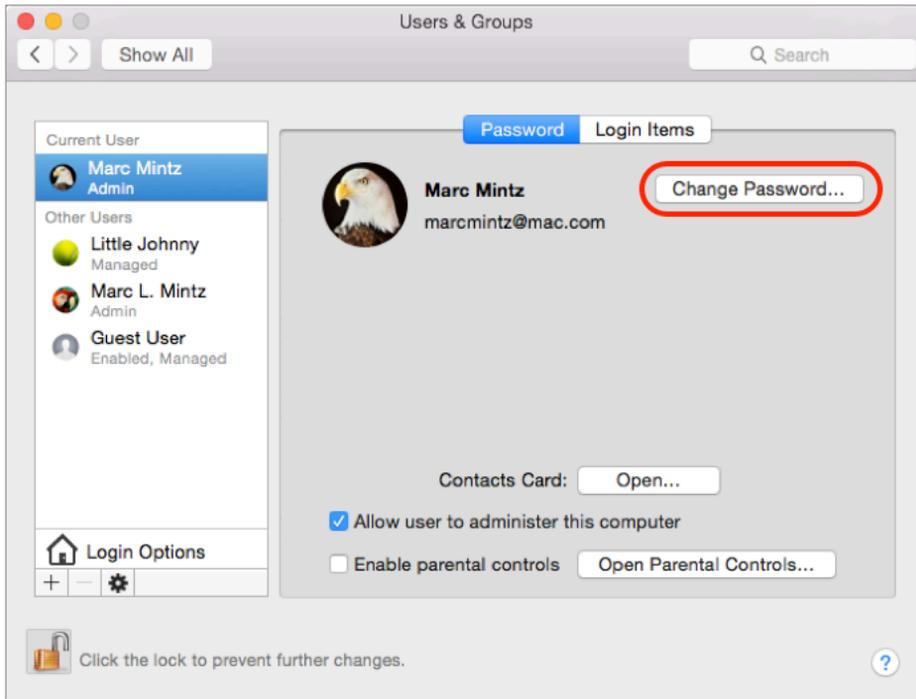
3. Record your new password in a way that is secure, and you can find when you need it. I recommend using LastPass (more on that later in this chapter), or Apple Contacts.
4. Exit the browser.

### Change Your Old Password to the Strong Password

5. Log in to your computer using your user account.
6. Click on *Apple* menu > *System Preferences* > *Users and Groups*.

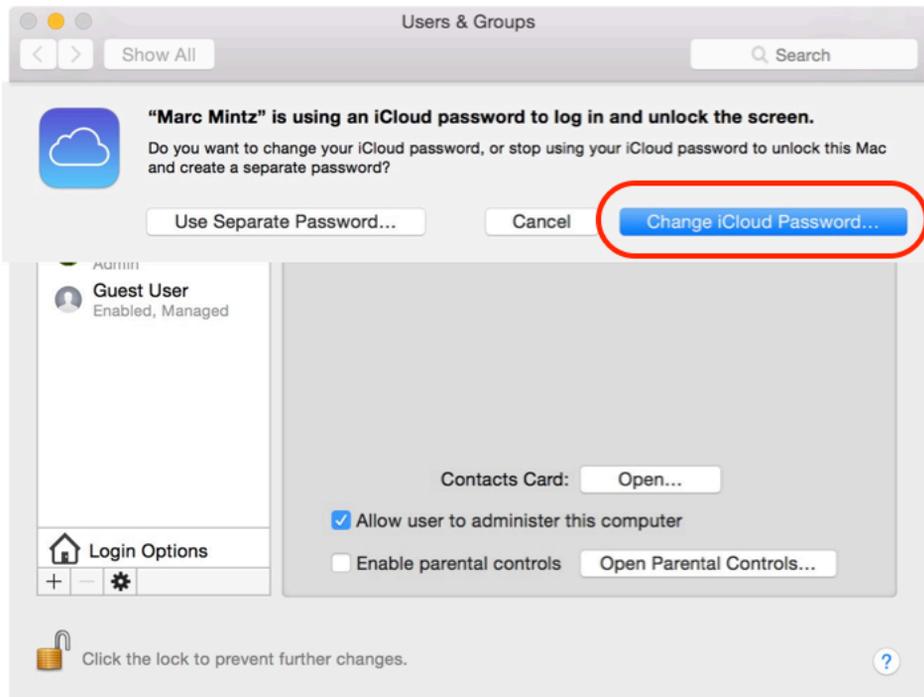
## 4 Passwords

7. Select the *Change Password* button:



- Note: When changing a user/login password, if possible, the change should be made while logged in with that user account. Doing so will simultaneously change the *Keychain* password to match. The *Keychain* stores usernames and passwords. When changing the user/login password in any other way, the *Keychain* password remains unchanged. If the user doesn't then know the password to the *Keychain*, it is impossible to ever open again, and all stored passwords will be lost. More on *Keychain* later in this chapter.
8. By default, your login password is set the same as your iCloud password. You will be asked if you want to *Use Separate Password...*, or to *Change iCloud Password...*
    - a. Synchronizing the iCloud and login password makes remembering both easier, and accessing your iCloud data from a new computer easier, but it also presents a roadblock to login should the Apple authentication servers be offline (as has happened at least once).

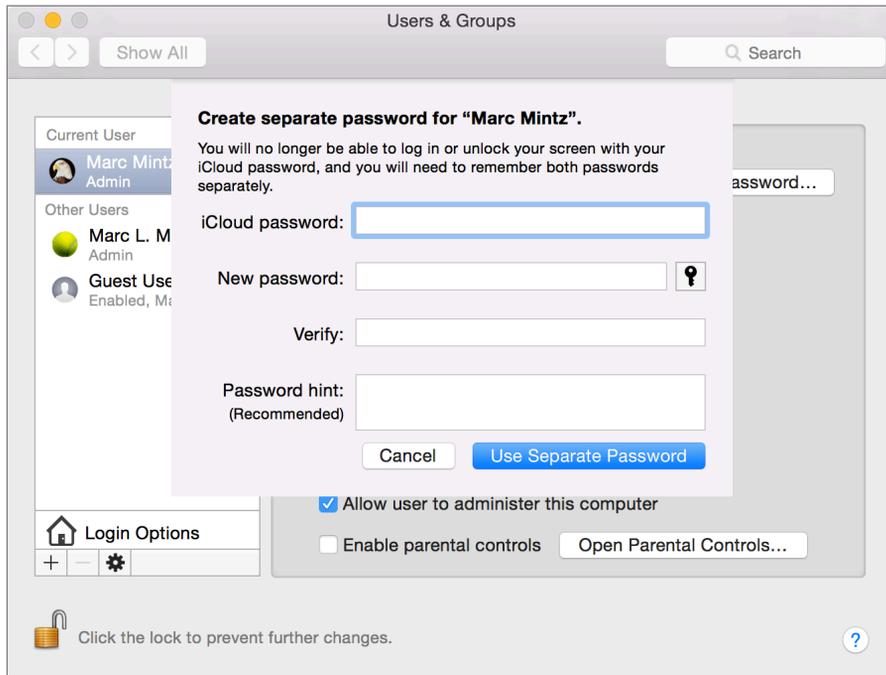
## 4 Passwords



- b. If you select Change iCloud Password, a browser opens to the My Apple ID page at Apple so that you may manage your ID.

## 4 Passwords

- c. If you select *Use Separate Password*, the *Create separate password for “<user name>”* window appears so that you may create a password. At the prompt, enter your *iCloud password*, *New password*, *Verify* your new password, and then select the *Use Separate Password* button:



## 9. Quit System Preferences.

Your new, strong password now is in effect.

## 4.3 Keychain

In our grandparent's day, life was so much simpler. I'm not talking about politics or sociology, but, well... to give an example: My grandfather had four keys in his pocket at all times: one for home, one for the car, and the other two he could never remember what for.

In today's world, the realm of keys has expanded into the digital world. You now have keys or passwords for logging on to your computer, your phone, your tablet, your email, many of the websites you visit, Wi-Fi access points, servers, your frequent flyer account, etc. In my case, I have 857 passwords in use. I know because they are all neatly stored in a database so that I don't have to remember them.

Unfortunately for most of us, our "keys" are not very well organized, so when we need to access our mail from another computer, or order a book on Amazon, we are stuck.

By default, your Mac stores most usernames and passwords used to access Wi-Fi networks, servers, other computers, and websites. The exceptions are usually websites that are programmed specifically so they do not have credentials saved. These are typically financial institutions.

The built-in tools that store this information automatically can also be used to manually store any text-based data. This includes credit card information, software serial numbers, challenge Q&A, offshore banking information, etc.

Your Mac has two locations to store keys:

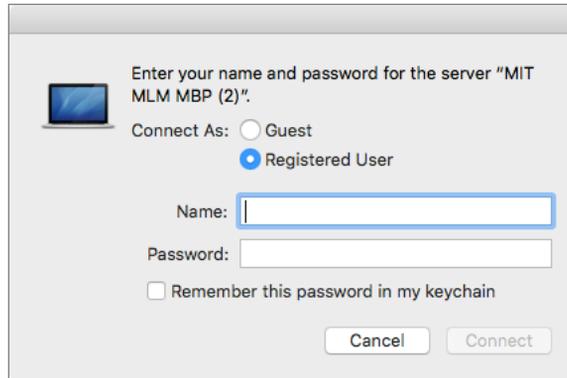
- Safari, which stores only credentials for websites visited with Safari.
- Keychain database, which stores username, password, and URL for websites which request authentication, Wi-Fi networks, servers, other computers you access, email accounts, and encrypted drives.
  - Located at *~/Library/Keychain*
  - Opened with the *Keychain Access* utility

Keychain is what interests us here.

## 4 Passwords

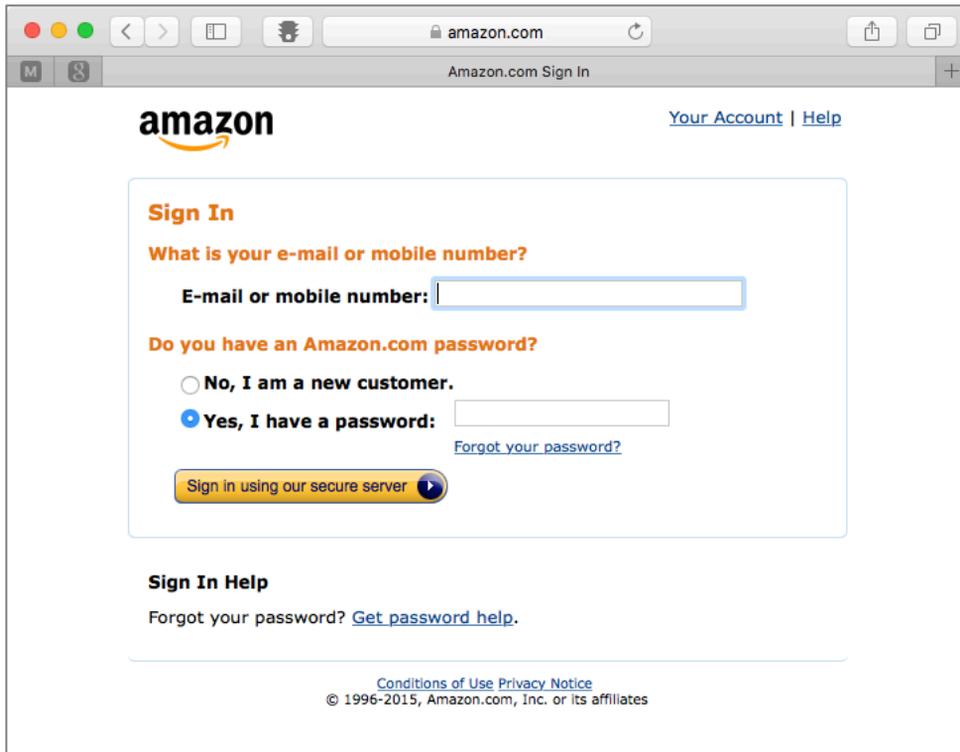
Let's take the case of visiting a website that requires a username and password, connecting to another computer or server, or performing some other action that triggers an authentication request. The following are the steps as they typically occur:

1. A prompt appears requesting a username and password.
  - Typical default authentication window for a server:



## 4 Passwords

- Typical authentication window for a website:



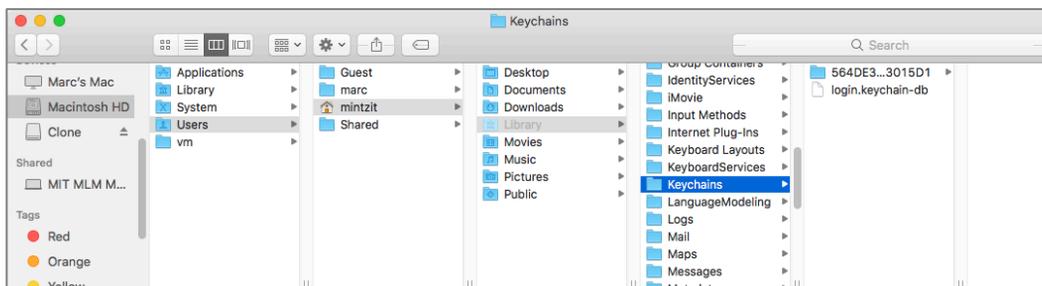
The image shows a screenshot of a web browser displaying the Amazon.com Sign In page. The browser's address bar shows "amazon.com" and the page title is "Amazon.com Sign In". The Amazon logo is at the top left, and links for "Your Account" and "Help" are at the top right. The main content area is titled "Sign In" and asks "What is your e-mail or mobile number?". Below this is a text input field. The next question is "Do you have an Amazon.com password?". There are two radio button options: "No, I am a new customer." (unselected) and "Yes, I have a password." (selected). To the right of the "Yes" option is another text input field. Below the password field is a link that says "Forgot your password?". At the bottom of the form is a yellow button with a play icon that says "Sign in using our secure server". Below the form is a "Sign In Help" section with a link "Forgot your password? Get password help.". At the very bottom, there are links for "Conditions of Use" and "Privacy Notice", and a copyright notice: "© 1996-2015, Amazon.com, Inc. or its affiliates".

2. Enter your username and password. In most cases, there is a checkbox to *Remember this password in my Keychain*. Enable that checkbox, and then click Enter or Continue.
3. The website takes you to the appropriate secured page or the other computer mounts a drive on your Mac.

Behind the curtain, your Mac has copied your username and password into the Keychain database, named *Login.Keychain*.

## 4 Passwords

This database is in your Home *Library/Keychains* folder. The database is military grade AES 256 encrypted, safe from prying eyes.



The next time you visit this same website or server, the steps change somewhat:

1. You surf to the website or select a server to access.
2. A prompt appears requesting a username and password.
3. Behind the scenes your web browser or Finder asks: "Has the Keychain stored the credentials for this site or server?"
4. A query is made of the Keychain database based on the URL of the site or the name of the server.
5. If Keychain has stored the username and password associated with the URL or server (it has), the credentials are automatically copied/pasted into the *username* and *password* fields.
6. Select *Enter*.
7. The website takes you to the appropriate secured page or the server share point mounts.

Note that you did not need to know your credentials—Keychain did it all for you.

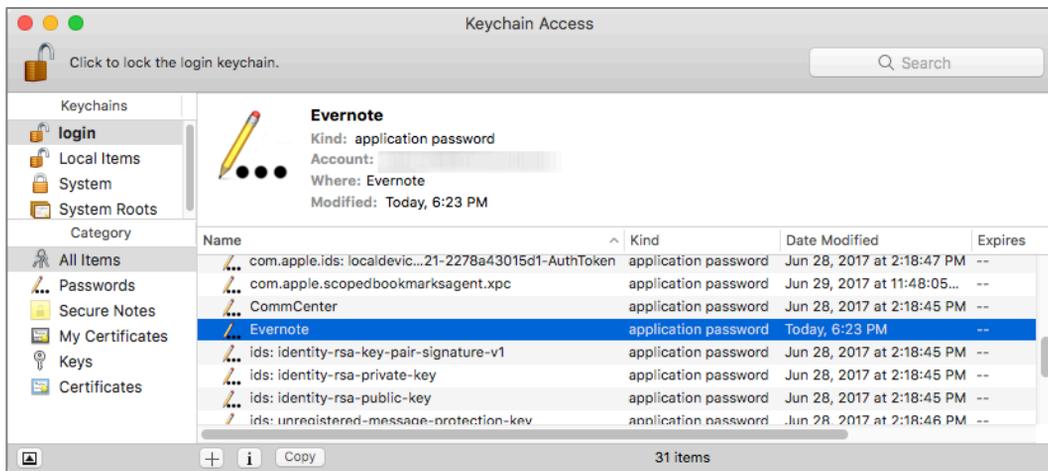
macOS ships with a tool allowing the user full access to the database, named *Keychain Access*, located in the `/Applications/Utilities` folder.

### 4.3.1 Assignment: View an Existing Keychain Record

Perhaps a trusted visitor needs access to your Wi-Fi network, and you have forgotten the password to that network. The Keychain database has it stored, you just need to look for it.

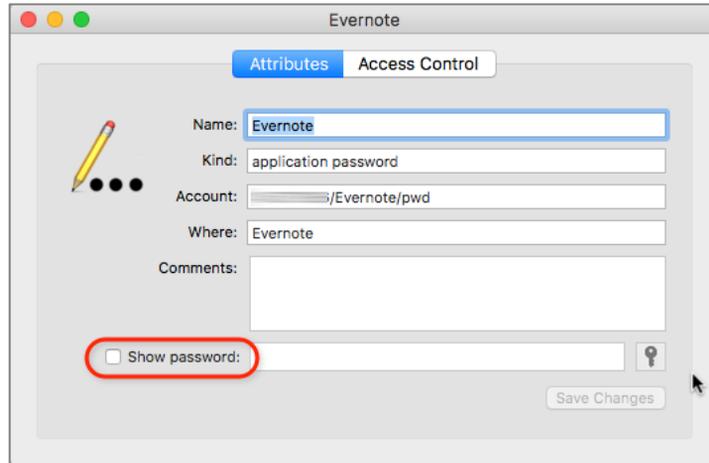
In this assignment, you examine a record in the Keychain.

1. Launch *Keychain Access* (located in */Applications/Utilities/*).
2. From the sidebar, in the *Keychains* field, select *login*. This is the database that holds your secure information.
3. From the sidebar, in the *Category* field, select *All Items*.
4. In the center, main area of the window, double-click on the *target record*, in this example, *Evernote*.

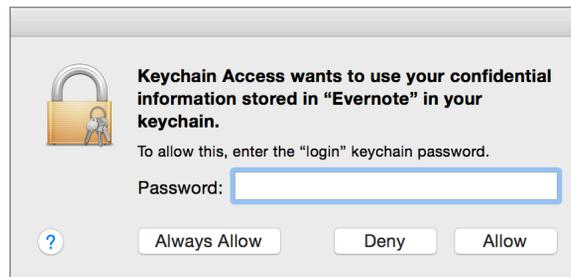


## 4 Passwords

5. The records *Attributes* window will open. At the bottom of the *Attributes* window you will see *Show Password*. Enable the checkbox. This will open the authentication window.

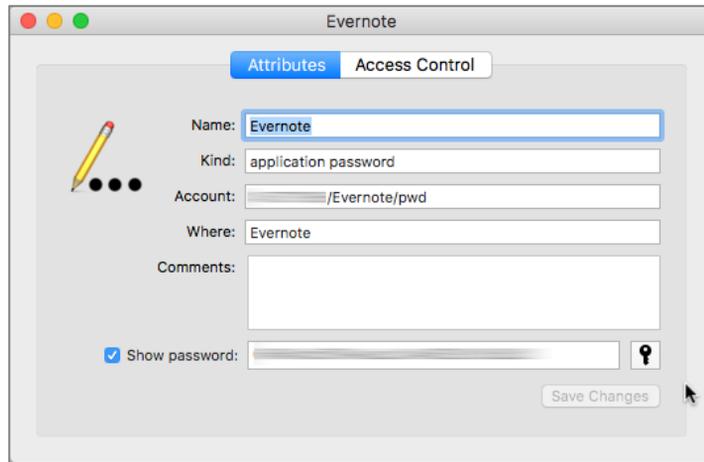


6. At the prompt, enter your Keychain password. By default, this is the same as your user account password. This will authorize Keychain to show you the password. Then click the *Allow* button.



## 4 Passwords

7. The *Show Password* field will now display the needed password.



8. Quit Keychain Access.

## 4.4 Challenge Questions

A Challenge Question is a way for websites to authenticate who you claim to be when you contact support because of a lost or compromised password.

For example, when registering at a website you may see: *Question – Where did your mother and father meet?*

The problem with this strategy is that most answers easily are discovered with an Internet search of your personal information, or a bit of social engineering.

The solution is to give bogus answers. For example, my answer to the question; *Where did your mother and father meet?* may be; *1954 Plymouth back seat*. It would not be possible for a hacker to discover this answer, as it is completely bogus. My mother tells me it was a 1952 Dodge.

Unless you are some type of savant, there is no way you will remember the answers to your challenge questions. But, there is no need to remember. We already have a built-in utility that is highly secure and designed to hold secrets such as passwords–Keychain Access!

Although Keychain can automatically record and auto fill usernames and passwords, it will require manually entering other data such as challenge Q&A.

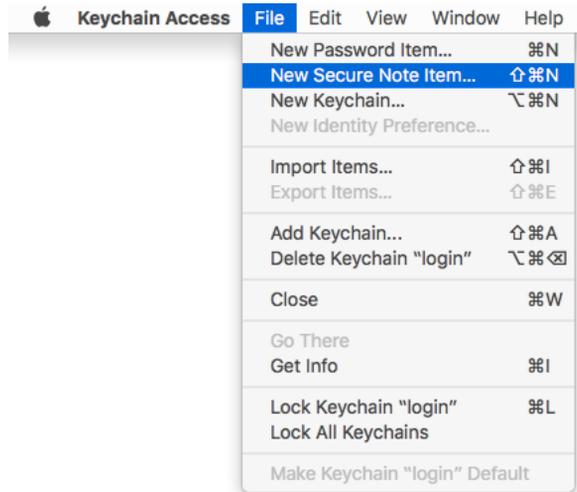
### 4.4.1 Assignment: Store Challenge Q&A in the Keychain

In this assignment, you manually store the challenge Q&A for a pretend website, myteddybear.com.

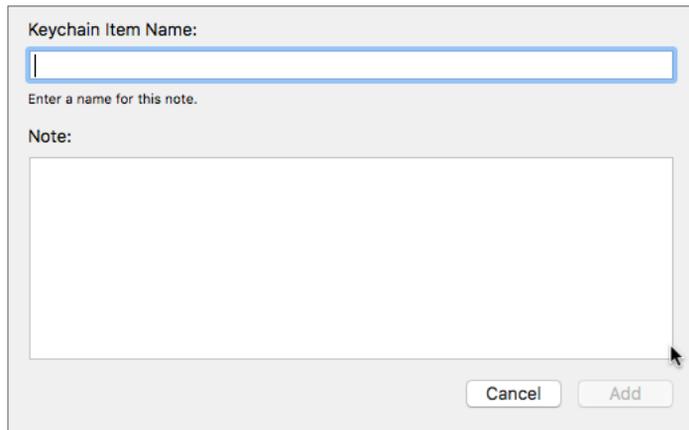
1. Open *Keychain Access.app*, located in */Applications/Utilities*.

## 4 Passwords

2. Select the Keychain Access *File* menu > *New Secure Note item...*



3. The Keychain *Item Name* window appears.

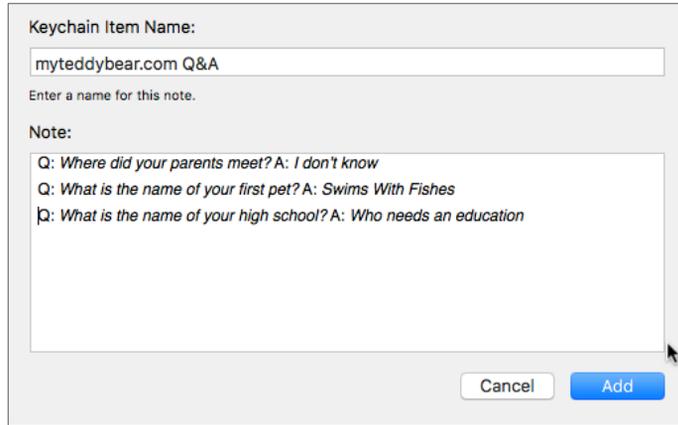


4. In the *Keychain Item Name* field, enter: *myteddybear.com* Q&A.
5. In the *Note* field, enter:  
Q: *Where did your parents meet?* A: *I don't know*

## 4 Passwords

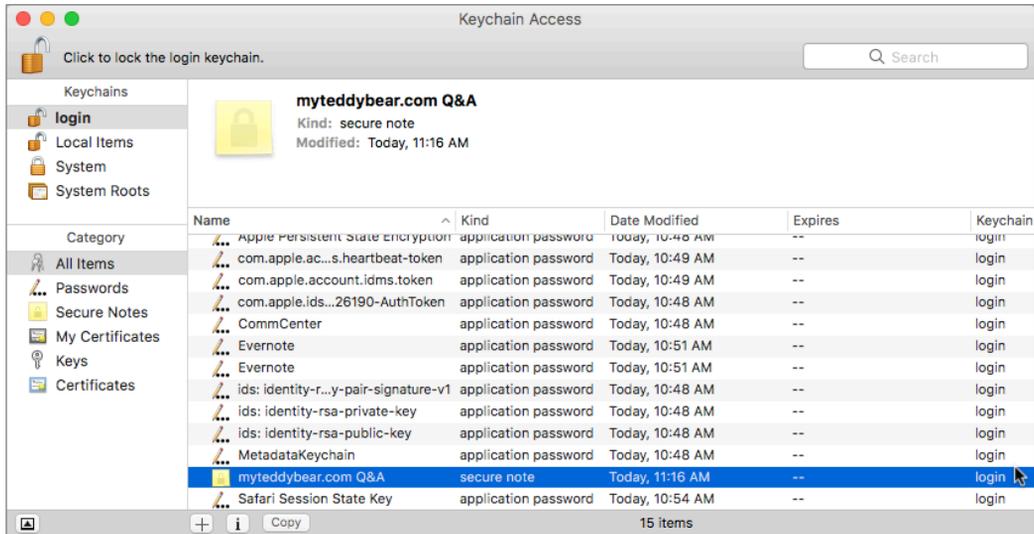
Q: *What is the name of your first pet?* A: *Swims With Fishes*

Q: *What is the name of your high school?* A: *Who needs an education*



6. Select the *Add* button.

7. You will find your new Secure Note within all your other Keychain items.



8. Quit Keychain Access.

Your challenge questions and answers are now securely stored.

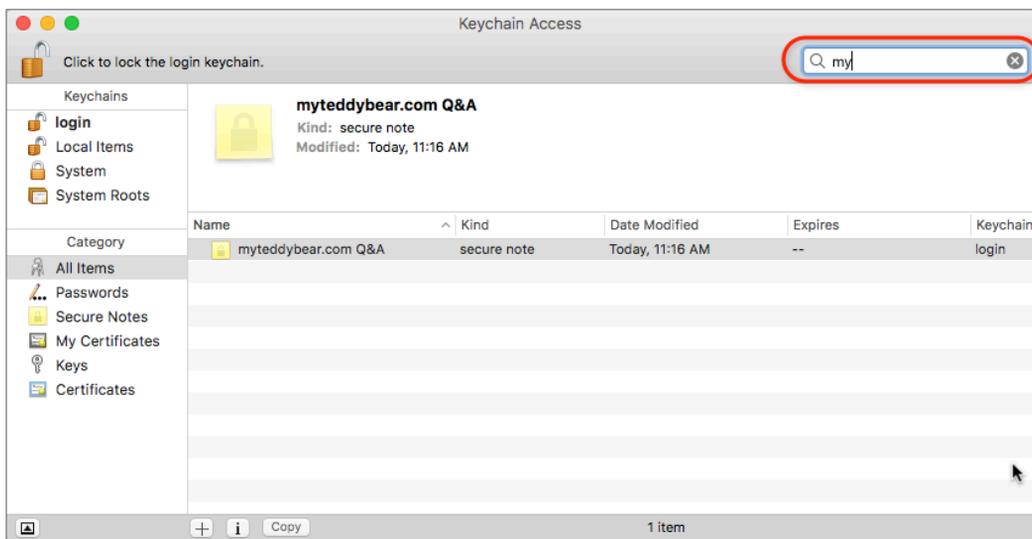
### 4.4.2 Assignment: Access Secure Data from Keychain

There may come a time that you forget your password to myteddybear.com. A call to technical support with a request to either retrieve or reset your password is met with a challenge question. If you are like me, your synapses holding that memory have long died out.

But, no worries! You do remember that you have the habit of storing all your important data securely in your Keychain.

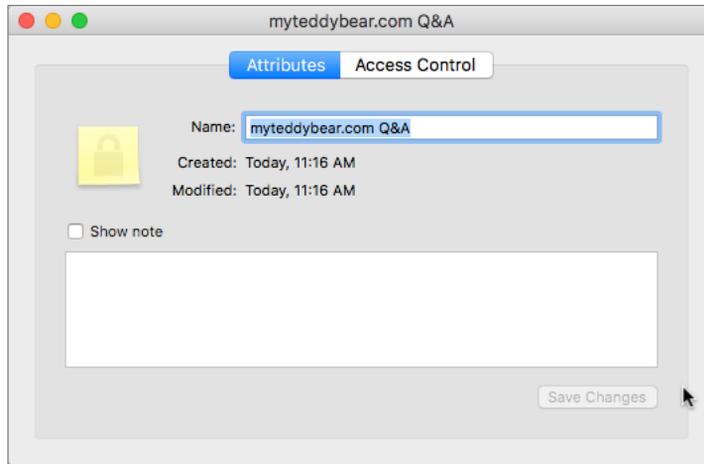
In this assignment, you retrieve your challenge Q&A for myteddybear.com.

1. Open Keychain Access.app, located in */Applications/Utilities*.
2. Click in the *search* field at the top right corner of the *Keychain Access* window.
3. Enter: *myteddybear*. As you type, only those records matching your search string appear, until only the proper record shows.

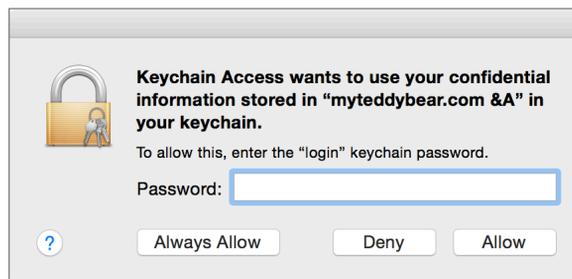


## 4 Passwords

4. Double-click on the myteddybear.com record to open it. Your password is not initially displayed. This is intentional, doubly protecting your data.

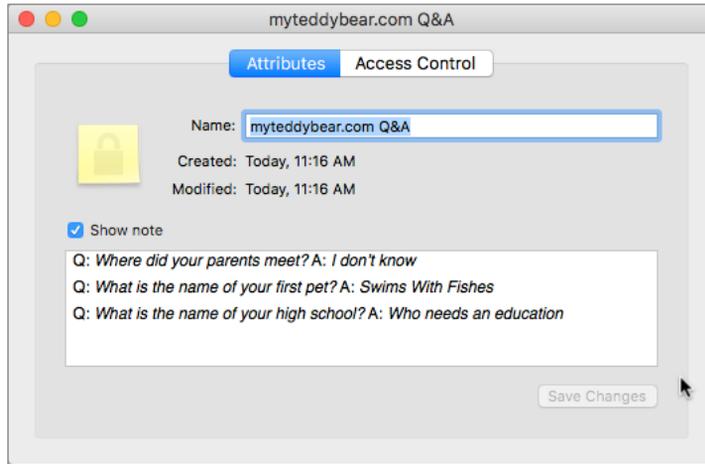


5. Enable the *Show note* checkbox.
6. You are prompted to enter your Keychain password. By default, this is the same as your log in password. Enter your Keychain password, and then click either the *Always Allow*, or *Allow*, button. By selecting *Always Allow*, you will not be asked to verify your Keychain password for this record in the future. If you select *Allow*, you have access to your data, but you will be prompted for your Keychain password in the future.



## 4 Passwords

7. After selecting either *Always Allow* or *Allow*, you see your challenge Q&A.



8. Close the window and Quit *Keychain Access*.

## 4.5 Harden the Keychain

The work we have done so far in Keychain Access is all that is necessary for almost every environment. Some situations call for even greater levels of security—think military bases, the computer used by the CEO, and my aunt Rose who needs to protect her secret recipe for kosher raisin noodle Koogles.

There is an option to further protect the Keychain—have your Keychain automatically log off after X minutes of inactivity.

By default, the Keychain remains unlocked if the user remains logged in. There is the option to set the Keychain to automatically lock after a specified amount of inactivity time.

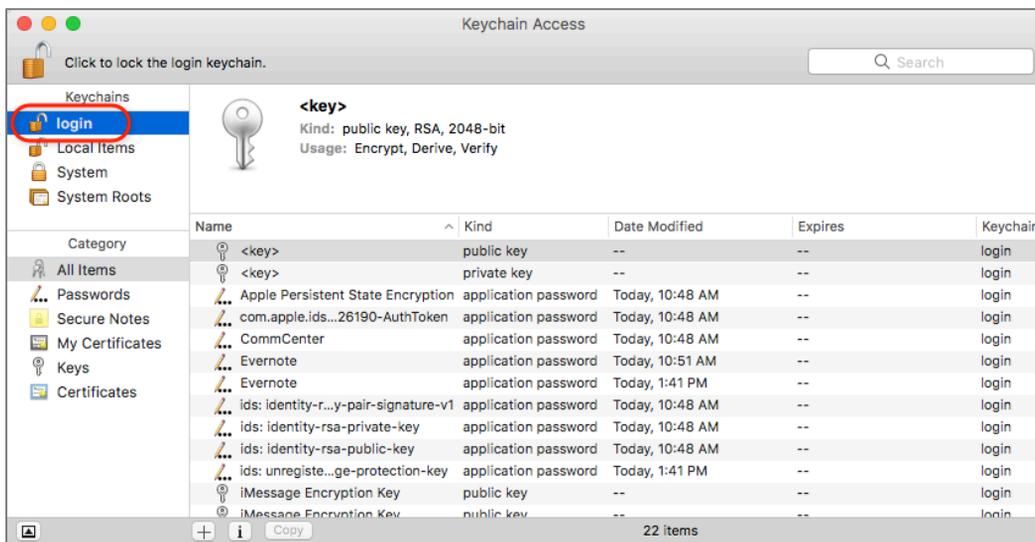
Let's say Keychain Access to automatically lock the Keychain after 5 minutes of inactivity. Upon log in, if the Keychain password is the same as the log in password, the Keychain will unlock and remain unlocked for 5 minutes. If you need an auto fill from data held in Keychain after that 5 minutes, you are prompted for the Keychain password. If within 5 minutes another auto fill is needed, the data is pulled from Keychain automatically. But when 5 minutes or more has passed, the Keychain will lock automatically.

### 4.5.1 Assignment: Harden the Keychain With a Timed Lock

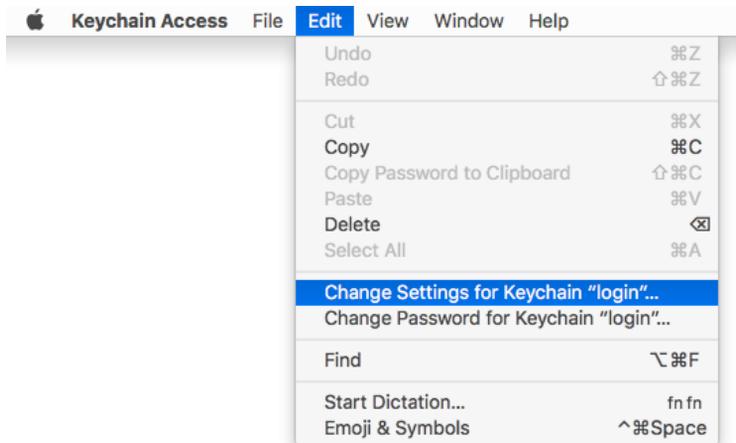
In this assignment, you give your Keychain a timeout to automatically lock after it has not been used for 1 minute.

## 4 Passwords

1. Open Keychain Access, located in */Applications/Utilities*. From the top of the sidebar, select the *login* keychain.

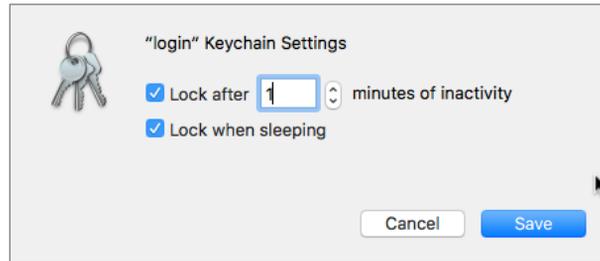


2. Select the Keychain Access *Edit* menu > *Change Settings for Keychain "login"...*



## 4 Passwords

3. The *Login Keychain Settings* window will open. Configure as follows:



- Enable the *Lock after* \_\_\_ *minutes of inactivity* checkbox, and then set this to 1 minute.
  - Enable the *Lock when sleeping* checkbox.
4. Select the *Save* button.
  5. Quit Keychain Access.
  6. Sit on your thumbs for 60 seconds—time enough for the Keychain to lock.
  7. Open a browser and visit a website or connect to another computer on your network that you frequent with a password that otherwise auto fills. You find you now are prompted to enter the password for the Keychain it to open.
  8. If you do not need a hardened Keychain, repeat steps 1–3, and then when the *Login Keychain Settings* window appears, disable the checkboxes. Then select the *Save* button.
  9. Quit Keychain Access.

Your Keychain will now automatically lock, preventing anyone from accessing all your passwords should you step away from your desk with your system awake and no screen saver in place.

## 4.6 Synchronize Keychain Across macOS and iOS Devices

Perhaps like me, you have a need to access most of these passwords and challenge answers anywhere, anytime. When I have my computer with me, no worries. But what if I don't? It would be a rare event indeed for me to be without my computer or my iPhone, so I keep my Keychain on my iPhone as well.

If you have upgraded to macOS 10.12 or higher, OS X 10.9 or higher, and iOS 7 or higher, Apple has you handled. With the most recent incarnations of both operating systems, Apple has added *Keychain* to the iCloud synchronization scheme. This allows your Keychain database to be synchronized between all your computers, iPhones, and iPads.

### 4.6.1 Assignment: Activate iCloud Keychain Synchronization

Synchronizing your Keychain with iCloud allows all your macOS 10.12 and higher, OS X 10.9 and higher, and iOS 7 and higher devices share your keychain.

In this assignment, you enable iCloud Keychain synchronization.

## 4 Passwords

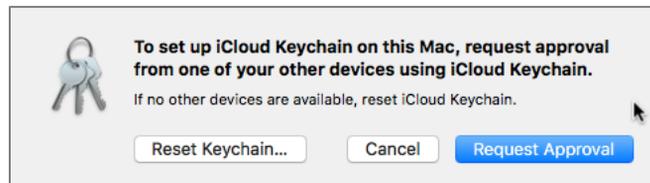
1. Open the *Apple* menu > *System Preferences* > *iCloud*.



2. Select the *Keychain* checkbox. The *Enter your Apple ID password to setup iCloud Keychain* dialog box appears.
3. Enter your Apple ID password, and then select the *OK* button.

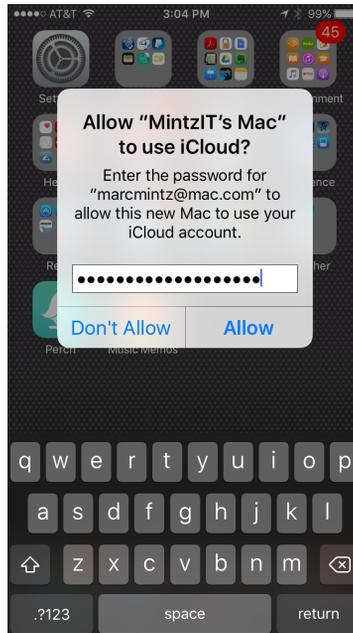


4. If you have previously created a 2-step verification for your Apple ID, the *Keychain Setup* dialog box opens. Select the *Request Approval* button.



## 4 Passwords

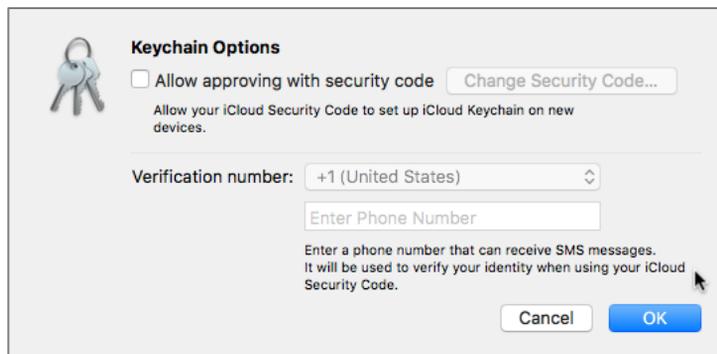
5. A request will be sent to the other devices currently approved on your account to approve this device. Enter your Apple ID password, and then click *Allow*.



6. Go back to *System Preferences*, and notice that the *Keychain* is now enabled.

### **Further secure your keychain:**

7. In the *iCloud Preferences*, select the *Keychain Options* button.
8. The *Keychain Options* window opens:



9. Enable the *Allow approving with security code* checkbox.

## 4 Passwords

10. The *Create an iCloud Security Code* window opens. Enter a 6-character code that can be used to enable your other Apple devices to share and synchronize Keychains, and then select the *Next* button.
  - Notes: If you would like a more complex code, you can select the *Advanced...* button instead.

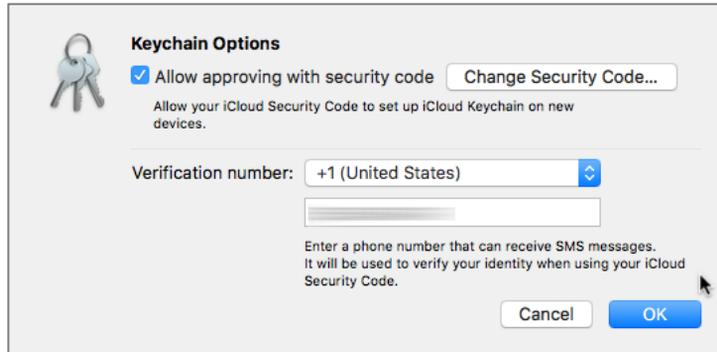


11. The same security window appears again to verify your security code. Reenter the code, and then select the *Next* button.
12. The *Enter a phone number that can receive SMS messages* window opens. This will be used by Apple to verify your identity when using the security code. Enter your phone number, and then select the *Done* button.



## 4 Passwords

13. You are returned to the *Keychain Options* window. Select the *Done* button.



14. At the *Enter your Apple ID password to update your account settings* window, enter your Apple ID password, and then select the *OK* button.



15. *Quit* System Preferences.

Your Keychain on this computer will now synchronize automatically with your iCloud account, and therefore with all other OS X, macOS, and iOS devices synchronizing on the same account.

## 4.7 LastPass

A great solution to the problem of password management is *LastPass*<sup>12</sup>.

There are three important advantages of LastPass:

- You no longer must concern yourself with Internet passwords—the correct response becomes automatic. LastPass will keep your Internet passwords available in each of your browsers.
- Stores and share your passwords with all your devices—even across operating systems. It also securely stores manually entered data such as challenge questions.
- The for-fee version allows sharing of selected passwords with others in the group.

LastPass provides the following solutions:

- Provides free (ad supported) and premium (no ads) options
- Automatically remembers your Internet passwords, fully encrypted
- Auto fills web-based forms and authentication fields
- Stores notes and challenge questions and answers (Q&A), fully encrypted
- Synchronizes across multiple browsers
- Synchronizes across multiple computers
- Synchronizes across Android, BlackBerry, iOS, Linux, macOS, Windows
- Automatically generates very strong passwords, which since you do not need to remember them, provide even greater online security.

### 4.7.1 Assignment: Install LastPass

The free version of LastPass works indefinitely across devices.

---

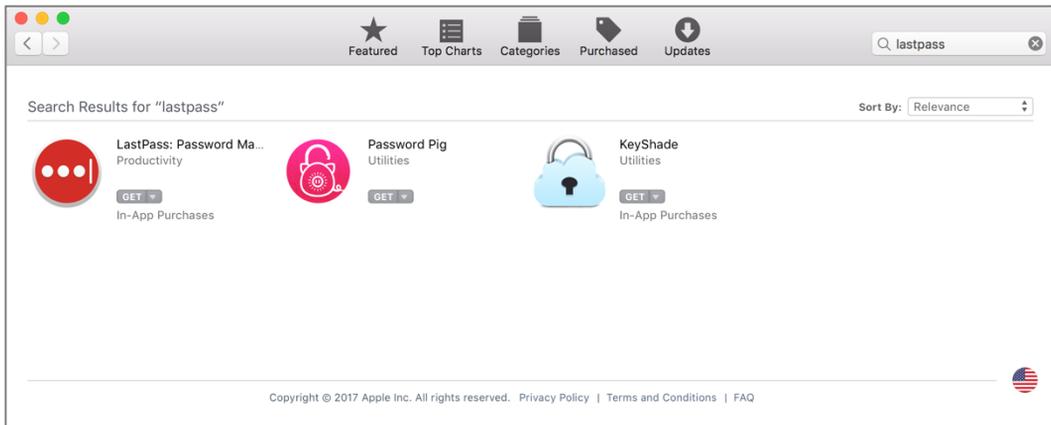
<sup>12</sup> <http://www.LastPass.com>

## 4 Passwords

In this assignment, you download and install LastPass on your macOS computer.

### Download the LastPass Installer

1. Open the *App Store*.
2. In the *Search Field*, enter *LastPass*, and then tap the *Return/Enter* key.
3. In the *LastPass* area, select *Get*. LastPass will download.



### Install LastPass

4. Once LastPass has downloaded, double-click to launch it.

## 4 Passwords

5. Select *Create an Account*, and then enter your *Email* address, a password in the *Master Password* field, a *Password Reminder*, and then click *Create Account*.

▼ Create an Account

Email:

Master Password:

Password Reminder:

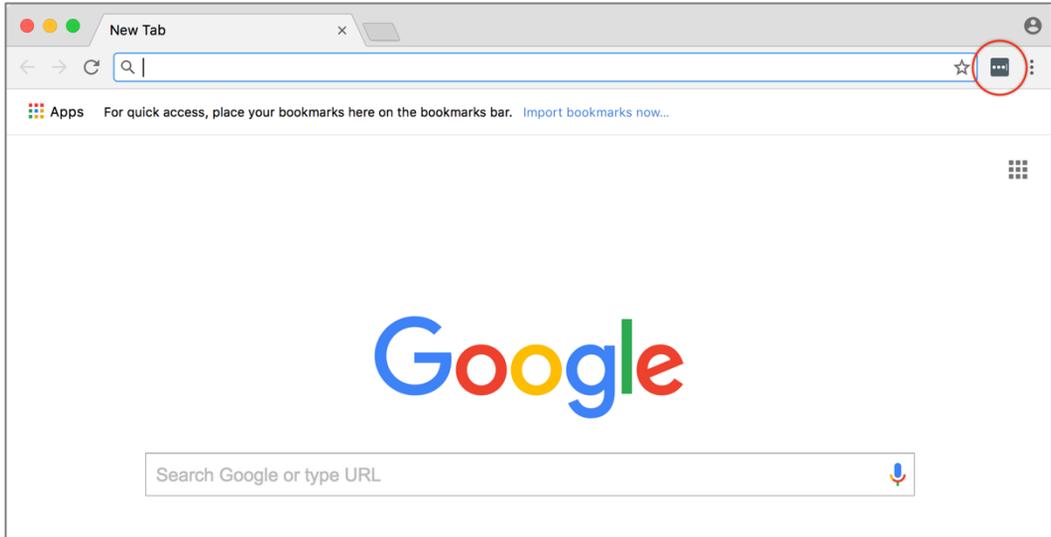
I have read and agree to the [Terms](#) and [Privacy Policy](#).

[Create Account](#)

► Log In

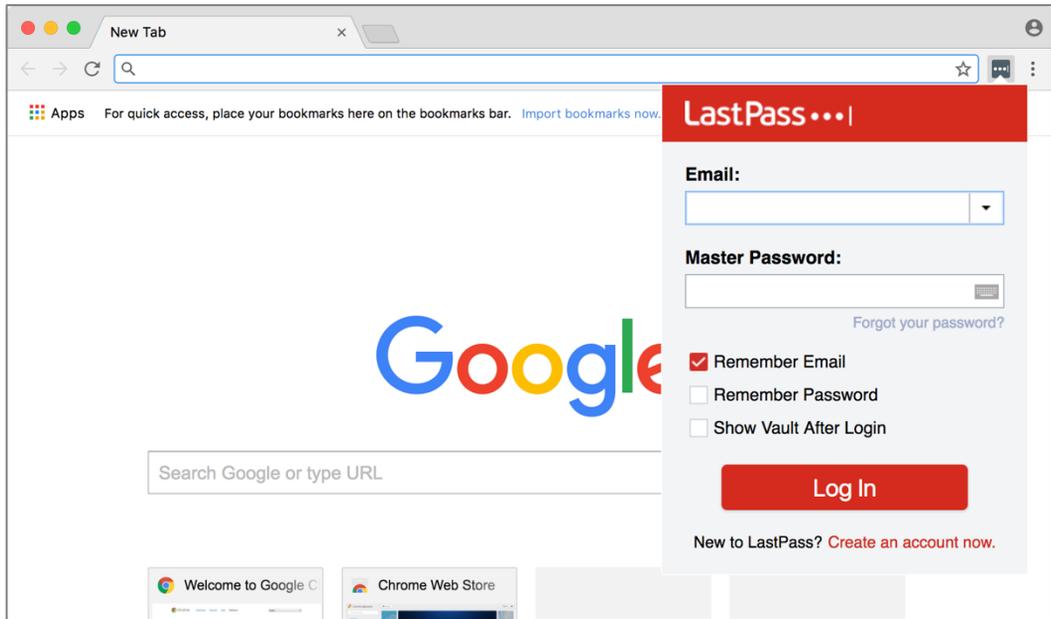
## 4 Passwords

6. LastPass automatically installs its extension into Chrome, Edge, Internet Explorer, Firefox, Opera, and Safari. Open a browser. In this example, it is Chrome. The LastPass extension displays as three dots ...



## 4 Passwords

7. In your browser, click the LastPass extension icon. The LastPass window opens.



8. Enter the *email* address to be linked to LastPass, and then the *Master Password* you created in an earlier step, and then click *Log In*.
9. The LastPass window goes away, and LastPass is now active within your browser.
10. If you use multiple browsers, repeat steps 6-9 with each.

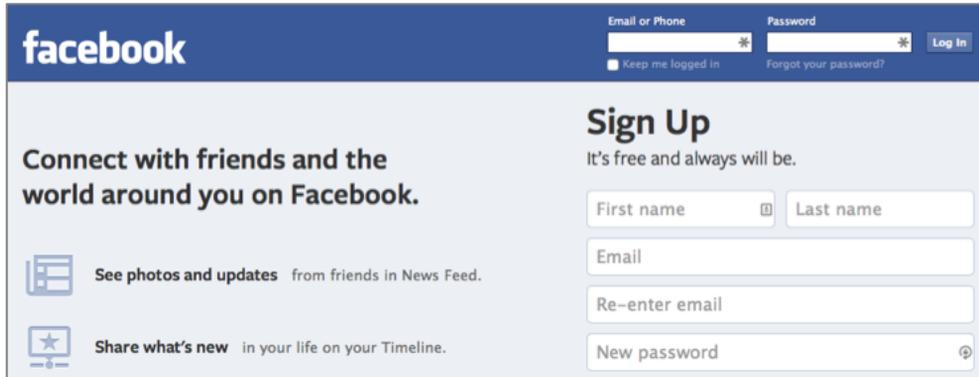
### 4.7.2 Assignment: Use LastPass to Save Website Authentication Credentials

Once you have LastPass installed, it's time to put it to use.

In this assignment, you use LastPass to store the user name and password for Facebook.

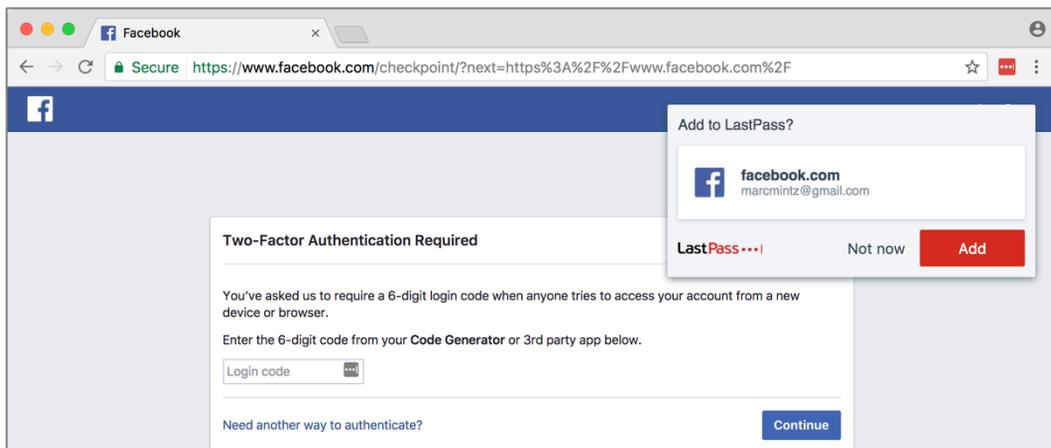
## 4 Passwords

1. Use your browser to visit Facebook <https://facebook.com>.



The screenshot shows the Facebook sign-up page. At the top, there is a navigation bar with the Facebook logo on the left and login fields on the right. The login fields include "Email or Phone" and "Password", both with asterisks indicating they are required. There are also checkboxes for "Keep me logged in" and "Forgot your password?", and a "Log in" button. Below the navigation bar, the main content area is split into two columns. The left column contains the text "Connect with friends and the world around you on Facebook." and two icons: one for "See photos and updates from friends in News Feed." and another for "Share what's new in your life on your Timeline." The right column is titled "Sign Up" and includes the text "It's free and always will be." Below this, there are four input fields: "First name" and "Last name" (with a plus icon), "Email", "Re-enter email", and "New password" (with a password strength indicator icon).

2. As this is the first time you have visited Facebook since installing LastPass, your log in credentials have not yet been stored in LastPass. Enter your Email or Phone and Password information, and then select the *Log in* button.
3. LastPass will detect that there is a form on this page, and present an option to remember your credentials. This will appear just under the navigation bar. Select the *Add* button.



The screenshot shows a browser window with the Facebook login page. The address bar shows the URL <https://www.facebook.com/checkpoint/?next=https%3A%2F%2Fwww.facebook.com%2F>. The page content includes a "Two-Factor Authentication Required" section with a message: "You've asked us to require a 6-digit login code when anyone tries to access your account from a new device or browser. Enter the 6-digit code from your Code Generator or 3rd party app below." There is a "Login code" input field and a "Continue" button. A "Need another way to authenticate?" link is also present. A LastPass popup is overlaid on the right side of the page, titled "Add to LastPass?". It shows the Facebook logo, the domain "facebook.com", and the email "marcmintz@gmail.com". Below this, there are three buttons: "LastPass" (with a red dot), "Not now", and "Add" (in a red box).

4. Quit your web browser.

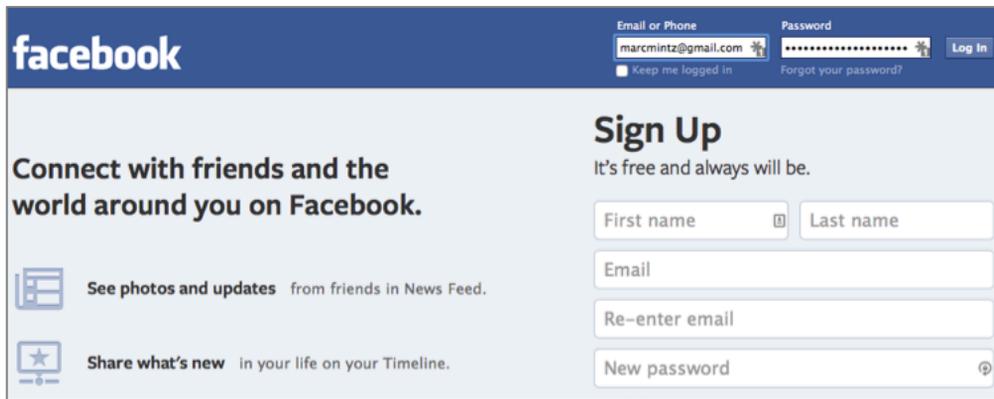
Your Facebook account credentials are now stored in LastPass, so you do not need to remember them.

### 4.7.3 Assignment: Use LastPass to Auto Fill Website Authentication

When LastPass has saved user name and password information for a site, you will never need to manually enter that information again.

In this assignment, you revisit Facebook and allow LastPass to enter your credentials.

1. Launch your browser and then go to *Facebook* at <https://facebook.com>. Take note that your authentication credentials have been automatically entered for you by LastPass.



2. Quit your browser.

You have just successfully proved that LastPass is saving your credentials.

## 4.8 Password Policies

Within the government, military, financial, and healthcare environments, setting *password policies* is often a regulatory mandate. Although not a mandate for the home and general business computer, doing so makes a lot of sense.

A password policy is a set of rules to help users create and use passwords. You have likely seen password policies in use when creating a password for your online banking or shopping, and were alerted that your password needed to be longer, or have a special character.

In an IT environment which is controlled by either a Microsoft Active Directory or macOS Server, password policies can be enforced from the server. Within environments without a server, you can enforce password policies using either the Terminal for command line control, or the macOS Server app for graphical control. In the following exercise, even though your computer is not in an environment controlled by a server, you will install and configure macOS server to manage password policies on a computer.

### 4.8.1 Assignment: Password Policies with macOS Server

The primary difference between the Mac computer you are using, and a Mac server is the installation of the Apple Server app. The server app is available from the App Store for \$19.95. Compared to the time and energy required to properly configure password policies through the command line, this is a bargain.

Should you be feeling particularly nerdy, open the *Terminal.app*, enter *man pwpolicy*, and then tap the *Return/Enter* key. *pwpolicy* is the command-line method of setting password policy in macOS. Although *pwpolicy* still works under macOS 10.13, it is mostly deprecated. The modern method of controlling password policies is with *profile keys*<sup>13</sup>.

---

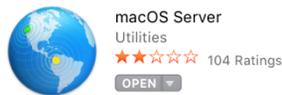
<sup>13</sup> <https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>

## 4 Passwords

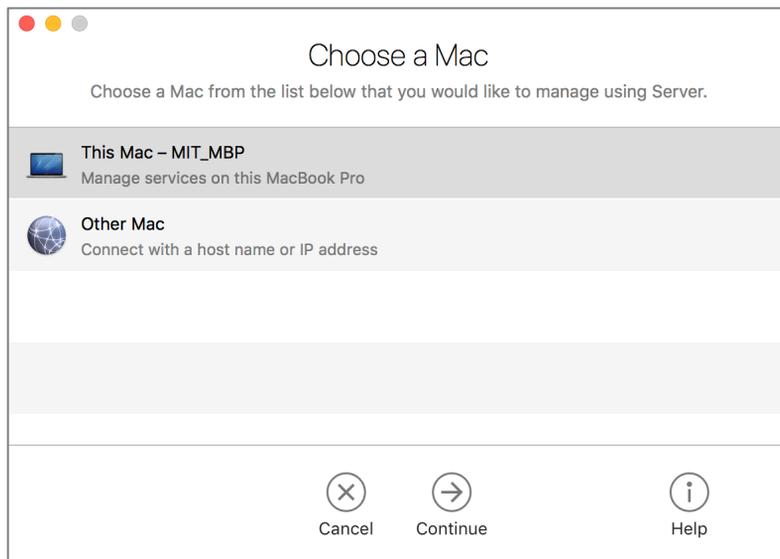
In this assignment, you will install and configure macOS Server app to manage password policies on your computer, for all users of your computer.

### Install macOS Server app

1. Open *Apple* menu > *App Store*.
2. In the *search* field, enter *Server*, and then tap the *Enter* or *Return* key.
3. Click the *macOS Server* icon.

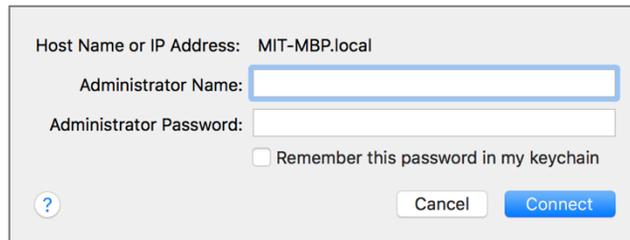


4. Purchase macOS Server app.
5. Once macOS Server app has downloaded to your computer, double-click to open it (located in the */Applications* folder).
6. At the *Choose a Mac* window, select *This Mac*, and then click the *Continue* button at the bottom center of the window.



## 4 Passwords

- At the authentication window, enter an administrator's name and password, and then click the *Connect* button.
  - NOTE: Do not enable *Remember this password in my keychain*. This will help prevent unauthorized users from accessing the server app.



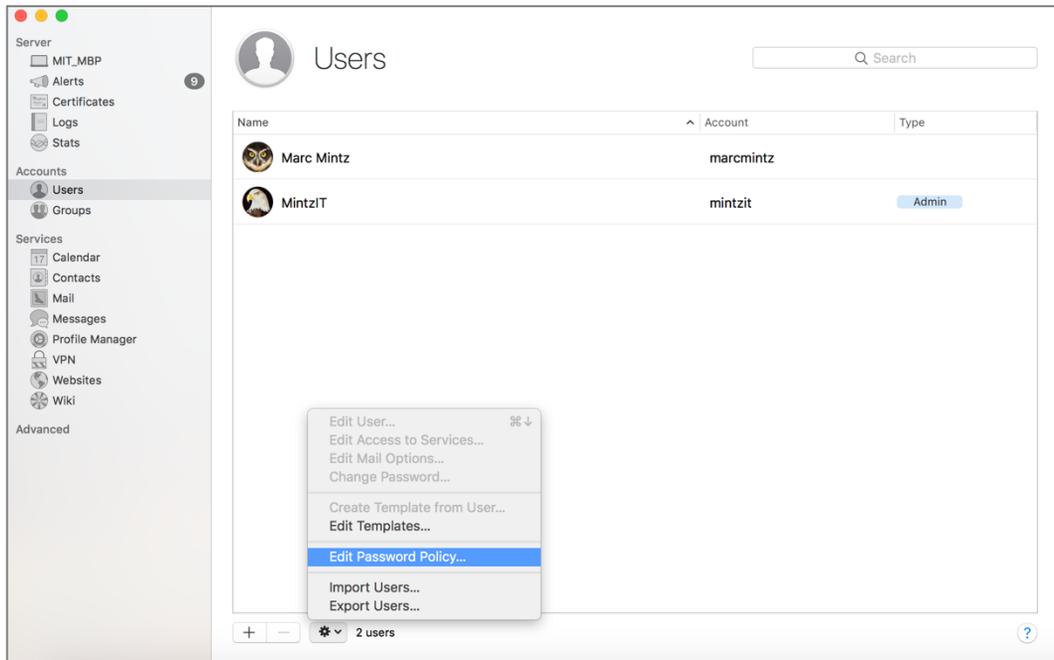
Host Name or IP Address: MIT-MBP.local

Administrator Name:

Administrator Password:

Remember this password in my keychain

- Select *Users* in the sidebar, click the *gear* icon > *Edit Password Policy...*

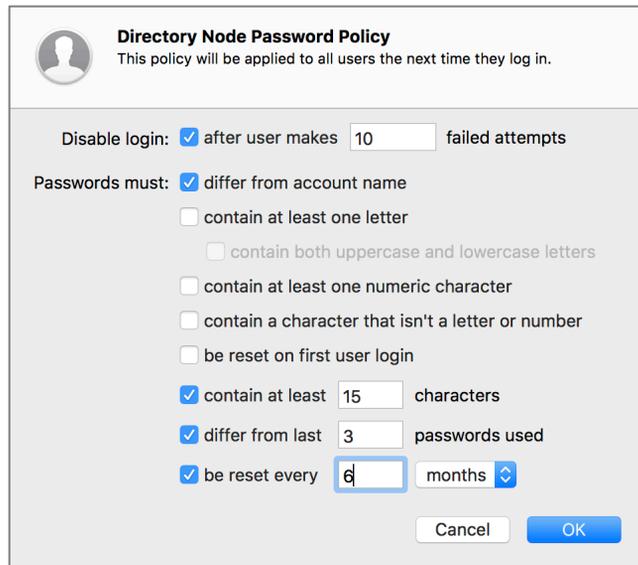


The screenshot shows the 'Users' management interface. The sidebar on the left is expanded to 'Users'. A context menu is open over the user list, with 'Edit Password Policy...' selected. The user list contains two entries:

Name	Account	Type
Marc Mintz	marcmintz	
MintzIT	mintzit	Admin

- In the *Directory Node Password Policy* window, configure to your taste.
  - NOTE: Based on the definition of *Strong Password* used in this book, and the loosening requirement for frequent password changes, you may want to configure your policies as below:

## 4 Passwords



**Directory Node Password Policy**  
This policy will be applied to all users the next time they log in.

Disable login:  after user makes  failed attempts

Passwords must:  differ from account name

contain at least one letter

contain both uppercase and lowercase letters

contain at least one numeric character

contain a character that isn't a letter or number

be reset on first user login

contain at least  characters

differ from last  passwords used

be reset every  months

Cancel OK

10. Click *Ok* button, and then *Quit* Server app.
11. Restart the computer to implement the change.

### Test the Password Policy

12. Once logged back into your computer, open *Apple* menu > *System Preferences* > *Users & Groups*.
13. Try to change your own password, using one that does not you're your new password policy. Notice how you are alerted and that you must follow policy.
14. Cancel the password change.
15. Authenticate as an administrator.
16. Create a new user account, and attempt to assign it a password that does not meet your new password policy. Notice how you are alerted and that you must follow policy.
17. Cancel creating a new user.
18. Exit System Preferences.



# Revision Log

20180420, v2.0

- The majority of chapters have been edited for updated information.
- *Chapter 2.6* renumbered for readability.
- *Chapter 4.5.1 Assignment: Harden the Keychain with a Different Password* removed. As of macOS 10.13.4 the login keychain password cannot be changed from the user account login password.
- *Chapter 19.3 NordVPN* revised to create a free trial account.
- *Chapter 20.3 Facebook* heavily edited to reflect the revised privacy and timeline settings.
- *Chapter 20.4 LinkedIn* heavily edited to reflect the revised privacy settings.
- *Chapter 20.5 Google* heavily edited to reflect the revised privacy and Takeout options.

20180325, v 1.3

- *Chapter 4.8 Password Policies* added.
- *Chapter 12.1 Find My Mac* has been slightly edited.
- *Chapter 14.8 Do Not Track* has been edited to reflect changes in Ghostery, and the Chrome extension installation process.
- *Chapter 15.7 End-To-End Secure Email With GNU Privacy Guard* rewritten to reflect the major update of GPGTools.
- *Chapter 19.3 NordVPN* is rewritten from scratch from our previous recommended VPN host.

20171022, v1.2

- *Chapter 14 Web Browsing* is rewritten.

## Revision Log

- *Chapter 15 Email*, added *hacked-emails.com* for checking if your email account was included in site breaches.
- *Chapter 16 Apple ID and iCloud*, added that Two-Factor Authentication can use either text messaging or voice call.
- *Chapter 19 Internet Activity*, changed the recommended VPN provider to *Perfect-Privacy.com*.

20171001, v1.1

- Updated chapter *Documents > Encrypt A Folder for Cross Platform Use With Zip* to use Keka, instead of the depreciated macOS built-in tools.

20170923, v1.01

- Updated chapter *When It Is Time To Say Goodbye*

20170918, v1.0

Initial release

# Index

- 2-Factor Authentication 488, 489, 728
- 2-step verification ..... 90, 692, 697
- 802.1x ..... 253, 255
- access point ..... 257
- administrative 122, 130, 132, 133, 212
- administrator 58, 122, 131, 133, 227, 230, 260
- Administrator ..... 120, 122, 132, 134
- AES ..... 76, 255, 541, 547
- Airport ..... 35, 36, 259, 260, 262, 267, 272, 274
- Al Gore ..... 561
- Andrew S. Tanenbaum ..... 713
- Android ..... 529, 589
- Anonymous Internet Browsing .. 361
- antenna ..... 252
- anti-malware ..... 108, 134, 170, 171
- Antivirus 170, 174, 175, 177, 182, 185, 201
- App Store ..... 108, 109, 237, 488
- Apple ID .. 71, 90, 108, 233, 237, 487, 488, 489, 508
- Application Updates ..... 110, 115
- Assignment 39, 42, 44, 46, 53, 56, 59, 68, 77, 80, 83, 86, 89, 94, 98, 100, 101, 107, 110, 115, 122, 126, 129, 130, 132, 135, 146, 148, 152, 153, 155, 156, 161, 164, 174, 190, 211, 214, 222, 223, 226, 233, 237, 240, 241, 244, 246, 257, 259, 263, 267, 275, 285, 291, 300, 304, 306, 307, 309, 310, 311, 313, 314, 315, 317, 320, 322, 324, 325, 326, 333, 334, 336, 338, 340, 344, 352, 361, 371, 383, 386, 392, 395, 397, 399, 403, 407, 413, 418, 424, 426, 427, 429, 431, 438, 445, 454, 465, 469, 472, 476, 482, 489, 494, 511, 514, 517, 521, 527, 529, 536, 542, 554, 565, 570, 575, 576, 580, 583, 591, 593, 598, 606, 619, 629, 631, 633, 638, 643, 645, 646, 648, 650, 660, 666, 673, 675, 692, 702, 706, 711, 715
- Aung San Suu Kyi ..... 387
- AV Comparatives ..... 170
- Avira ..... 172
- Backblaze ..... 38
- backup .34, 35, 36, 37, 44, 59, 60, 237
- Ban Ki-moon ..... 151
- Benjamin Franklin ..... 119, 297
- Bitdefender .. 171, 174, 177, 185, 190, 201
- Blog ..... 29
- Boot Camp ..... 170, 171
- broadcasting ..... 226, 252
- Broadcasting ..... 252
- Carbon Copy Cloner .. 36, 39, 46, 47, 48, 53, 54, 57
- Carbonite ..... 38
- Certificate Authorities ..... 437

## Index

- Challenge Question ..... 80
- Cisco ..... 66
- CISPA ..... 25
- Clear History ..... 313
- clone ..... 36, 37, 58, 59, 60, 61
- Clone ..... 51, 52, 53, 54, 56, 57, 58, 59
- Comodo 438, 442, 445, 452, 454, 455, 465, 467
- Computer theft ..... 34
- Cookies ..... 309
- crack ..... 65
- Criminal activities ..... 34
- Deep Web ..... 382
- Disk Decipher ..... 529
- Disk Utility ..... 39, 517
- DMZ ..... 284
- Do Not Track ..... 332
- DoD ..... 706, 707, 711
- DoE ..... 706, 711
- Dr. Seuss ..... 701
- DuckDuckGo ..... 309, 310, 311
- Ed Snowden ..... 382
- EDS ..... 529
- EFI Chip ..... 222
- Elayne Boosler ..... 221
- Elbert Hubbard ..... 163
- email ..... 403
- Email 99, 387, 391, 398, 407, 412, 416, 418, 420, 427, 429, 437, 438, 439, 440, 442, 446, 447, 463, 464, 465, 467, 468, 604, 731
- Encrypt... 58, 299, 431, 434, 435, 511, 514, 517, 521
- Encrypted Data Store ..... 529
- encrypted email... 391, 412, 413, 469, 470, 471, 472
- encryption 58, 59, 154, 159, 252, 254, 298, 391, 397, 398, 510, 511, 514
- Encryption... 154, 254, 257, 391, 436, 519
- Entropy ..... 34
- Erase ..... 237
- Ethernet ..... 233, 252, 253
- Facebook 29, 67, 98, 99, 100, 121, 134, 562, 636, 638, 643, 644, 645, 650, 666
- Facetime ..... 562
- FAT ..... 551
- FBI ..... 25
- FileVault ..... 56, 58, 59, 154, 156, 157, 159, 226, 510, 707, 726
- FileVault 2 . 56, 58, 59, 154, 156, 226, 510
- Find My iPhone... 234, 235, 237, 238, 239
- Find My Mac 226, 227, 233, 235, 237, 241
- Find My Mac? ..... 226
- Fire ..... 34
- firewall ..... 210, 211, 212, 256
- Firewall. 211, 212, 213, 215, 216, 217
- FireWire ..... 35, 39, 152, 153
- Firmware 221, 222, 223, 226, 285, 726
- firmware password ..... 223
- Firmware Password .... 159, 222, 223, 224, 726
- Flash ..... 25
- Gateway VPN ..... 587
- General Douglas MacArthur ..... 251
- George Carlin ..... 33
- Ghostery 333, 338, 340, 341, 344, 345, 346, 348

## Index

- GNU Privacy Guard.....398, 412, 731
- Google Hangouts ..... 562, 563
- GPA .....413
- GPG .....412, 413, 414, 418, 419, 426, 427, 428, 429, 431, 437, 469, 472
- GPG Keychain Access.418, 419, 426, 431
- GPG Public Key.....413
- Gpg4win.....413
- GPGMail.....424
- GPGTools..... 413, 426
- Gravity Zone .....171
- GravityZone . 190, 192, 193, 197, 200
- G-Suite ..... 38
- Guest.....121, 135, 226, 229, 231, 233, 726
- Hamachi606, 607, 619, 620, 621, 622, 625, 628, 629, 631, 632, 633, 634
- HaveIBeenPwned.....383
- haystack..... 66, 69
- HIPAA ..... 38
- Honore de Balzac .....169
- Hot Corners .....167
- https ..... 66, 69, 298, 299, 392, 397
- HTTPS ..... 299, 300, 391, 397, 727
- HTTPS Everywhere .....299, 300, 362
- Hypertext Transport Layer  
Secure.....391
- iCloud70, 71, 72, 89, 90, 93, 157, 158, 226, 233, 234, 487, 488, 489, 504, 505, 507, 728
- Incognito Mode.....304
- infected..... 66
- Insertion.....252, 253, 264, 276
- Integrity Test..... 44
- Integrity Testing.....59
- iOS..... 89, 412, 437, 529
- ipconfig .....270, 271, 279, 280
- iTunes.....489
- Java.....25
- Joseph Heller .....21
- Keka ..... 521, 522, 524, 525, 527
- keychain .....89
- Keychain70, 73, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 93, 258, 416, 419, 426, 427, 443, 444, 468, 725
- LAN .....256, 257
- LastPass .....67, 94, 95, 98, 100
- LinkedIn.....666
- Linux..... 359, 360, 412, 413, 529, 551
- Local Area Network.....256
- LogMeIn606, 610, 611, 613, 614, 615, 619, 621, 624, 625, 627, 628, 634
- MAC Address .....267, 274
- Mac OS Extended.....519, 551
- MacKeeper.....331
- MacUpdate ..... 110, 114, 115, 116
- MacUpdate Desktop..... 110, 115
- maintenance ..... 36, 122
- malware..... 122, 170
- Malware..... 34, 170
- Managed with Parental Controls121, 134, 135
- Marc L. Mintz ..... 21, 27, 28, 63
- Mintz's extrapolation of Sturgeon's Revelation.....24
- modem .....256
- Newsletter .....29
- NIST.....23, 547, 719, 721
- NordVPN.....593, 598

## Index

- NSA.. 23, 64, 222, 223, 547, 588, 605,  
706, 723
- NTP.....714, 715, 716
- Onion sites .....382
- Onion Sites .....382
- Parallels..... 171, 363
- Parental Controls 121, 134, 135, 136,  
146, 147
- passphrase ..... 66
- password .. 25, 58, 65, 66, 68, 69, 122,  
131, 133, 154, 158, 222, 223, 226,  
237, 253, 254, 260, 262, 392, 397,  
399, 488, 511, 517, 518, 519
- Password.....65, 68, 222, 262, 511
- Password Policies..... 101, 719
- permissions .....122
- PGP ..... 412, 437
- phishing ..... 25, 170
- Phishing .....389
- port..... 210, 284
- Port forwarding.....284
- Ports.....214
- Power surges ..... 34
- Practical Paranoia Book Upgrades29
- Practical Paranoia Updates ..... 29
- Pretty Good Privacy .....412
- Prey ..... 240, 241
- private browsing.....304
- ProtonMail... 398, 399, 403, 405, 407
- public key.....418
- Public Key.... 412, 413, 418, 423, 426,  
427, 429, 469, 470, 471, 472
- RADIUS.....253
- RAM-Resident Malware.....284
- Recovery HD.....53, 56, 222, 223, 708
- Recovery Key ..... 58
- Root..... 120, 122, 126, 129, 130
- router .....256, 257, 284, 285
- Router ..... 263, 284, 291
- S/MIME437, 438, 445, 454, 456, 461,  
464, 465, 469, 470, 472
- Sabotage ..... 34
- Screen Saver ..... 164, 167
- screensaver .....168
- SEC.....38
- Secure Socket Layer .....298
- Seneca .....105
- Server..... 35, 36, 252, 253
- SHA.....547
- Sharing Only .....121
- Single User Mode .....222
- Skype..... 562, 563
- sleep . 54, 59, 165, 166, 168, 267, 304,  
586
- Sleep ..... 159, 164, 167
- software 35, 38, 65, 66, 122, 170, 252,  
399
- SSL.....298, 392
- Standard..... 121, 133, 135, 415, 544
- Static electricity.....34
- stealth.....214
- switch.....256
- Symantec..... 25, 412
- System Updates .....105
- Tails359, 360, 361, 363, 381, 728, 729
- Takeout .....697, 731
- Target Disk Mode .....222
- Terrorist activities ..... 34
- theft ..... 25, 34, 35
- Theodore Roosevelt .....209
- Theodore Sturgeon .....24
- thepracticalparanoid.....470

## Index

- Thomas Jefferson ..... 63  
Thomas Sowell .....225  
Thunderbolt..... 35  
Time Machine..35, 36, 37, 39, 42, 43,  
44, 45, 46, 725  
TKIP .....255  
TLS..... 391, 392  
Tor359, 360, 361, 362, 363, 364, 365,  
366, 367, 369, 370, 371, 381, 382,  
727, 728  
TorBrowser ..... 363, 364, 369, 371  
Trafficlight.....320  
TrafficLight . 185, 186, 187, 201, 202,  
203  
Trojan horses ..... 25, 170  
TrueCrypt..... 529, 538  
Two-Step Verification.....508  
USB ..... 35, 39, 152, 153  
US-CERT .....106  
User Accounts .....119  
VeraCrypt.... 529, 536, 537, 541, 542,  
543, 544, 554, 555, 557, 558  
Virtru....475, 476, 477, 478, 480, 482,  
483, 484, 485  
virtual machine.....170  
Virtual Machine ..... 171, 363  
Virtual Private Network254, 299, 586  
viruses.....25  
VMware Fusion.....171  
VPN .....254, 259, 299, 586, 587, 588,  
589, 590, 593, 604, 605, 606, 617,  
619, 625, 628, 629, 631, 633, 728  
war driving .....25  
Water damage.....34  
Web Mail .....397  
WEP .....254, 257  
Whitelisting.....134  
Wi-Fi25, 226, 233, 252, 253, 254, 257,  
258, 259  
William Blum.....509  
William Hazlitt .....487  
Windows..... 152, 170, 171, 172, 270,  
279, 359, 412, 413, 529, 551, 589,  
630  
Wire .....565, 576, 578, 580  
worms.....25, 170  
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.**

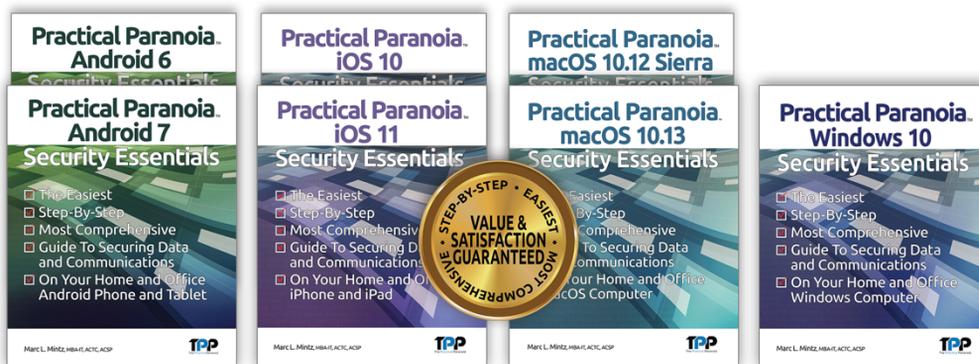
Mintz InfoTech, Inc. is uniquely positioned to be your Virtual CIO and provide you and your organization comprehensive technology support. With the only MBA-IT consultant and 100% certified staff in New Mexico, our mission is to provide small and medium businesses with the same Chief Information and 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](mailto:info@thepracticalparanoid.com)  
<https://thepracticalparanoid.com>