PRACTICAL AND ETHICAL ISSUES IN INFORMATION SECURITY FOR NEUROPSYCHOLOGISTS

DARCY COX, PSY.D., R.PSYCH., ABPP
ROBERT N. DAVIS, PH.D., ABPP

LEARNING OBJECTIVES

1. Describe how to encrypt, lock, and install a remote “wipe” function on your iOS or Android device.

2. Demonstrate how to encrypt your drives: lock and encrypt your laptop and your flash drives, select and use encrypted cloud storage providers.

3. Describe how to create good passwords and how to effectively manage multiple passwords.

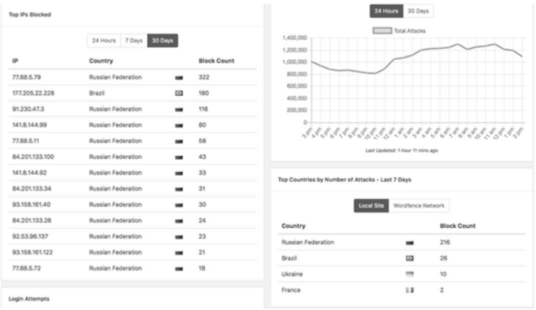
DISCLOSURES & CONFLICTS

Zero, zilch, nada for both of us!

THREATS WE CAN VS. CANNOT CONTROL

- If the FBI, NSA, CSIS, or Anonymous want into your systems, they will probably find a way.
- Insurance companies, banks, and merchants make big juicy targets and may do a poor job with their security. Equifax, anyone?
- By controlling your own passwords, phone, and drives, you can at least lessen the risks you can’t fully control.

EXAMPLE OF WEB PAGE LOG



Top IPs Blocked

IP	Country		Block Count
77.88.5.79	Russian Federation	▬	322
177.205.22.228	Brazil	▭	180
91.230.47.3	Russian Federation	▬	116
141.8.144.99	Russian Federation	▬	80
77.88.5.11	Russian Federation	▬	58
84.201.133.100	Russian Federation	▬	43
141.8.144.92	Russian Federation	▬	33
84.201.133.34	Russian Federation	▬	31
93.158.161.40	Russian Federation	▬	30
84.201.133.28	Russian Federation	▬	24
92.53.96.137	Russian Federation	▬	23
93.158.161.122	Russian Federation	▬	21
77.88.5.72	Russian Federation	▬	18

Login Attempts

Last Updated: 1 hour 11 mins ago

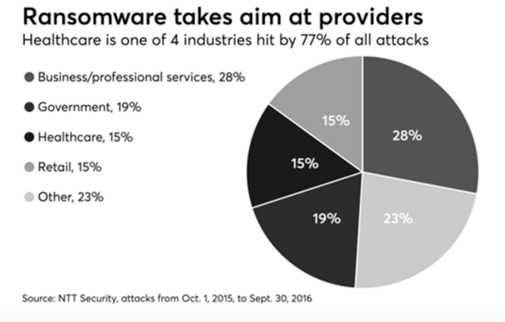
Top Countries by Number of Attacks - Last 7 Days

Country		Block Count
Russian Federation	▬	216
Brazil	▭	26
Ukraine	▭	10
France	▭	2

WHO’S BEEN HACKED RECENTLY?

- Equifax, 143 million people compromised
- Anthem Blue Cross, 80 million users
- Augusta University Medical Center (6,109 patients affected); phishing email
- In 2016, a California hospital became the first to pay a $17,000 ransom to cyber criminals who held its medical records and crucial computer systems ‘hostage’ for over 10 days.
- Types of data stolen: Names, DOB, SSN, addresses, emails, income data, credit card info, health information

HACKERS LOVE HEALTHCARE DATA


Ransomware takes aim at providers

Healthcare is one of 4 industries hit by 77% of all attacks

Source: NTT Security, attacks from Oct. 1, 2015, to Sept. 30, 2016

INFORMATION SECURITY: A CASE STUDY AND SPECIAL GUEST

- Please welcome our special guest, Dr. Barbara Baer.

THE CIA MODEL

- C = Confidentiality (control/restrict access to only authorized individuals; "need-to-know")
- I = Integrity (information is accurate and not altered by unauthorized person)
- A = Availability (information is accessible when needed)

SOME QUESTIONS TO ASK YOURSELF

1. What are your most critical data?
2. Where are they stored and in what format?
3. Who has access to those data?
4. How is access to the data monitored and/or recorded?
5. What are some possible disaster scenarios that may disrupt the confidentiality, integrity, or availability of your critical data?

INFORMATION SECURITY: RELEVANT ETHICAL ISSUES

- **3.04 Avoiding Harm**
  (a) Psychologists take reasonable steps to avoid harming their clients/patients, students, supervisees, research participants, organizational clients, and others with whom they work, and to minimize harm where it is foreseeable and unavoidable.
- **4.01 Maintaining Confidentiality**
  Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be regulated by law or established by institutional rules or professional or scientific relationship.

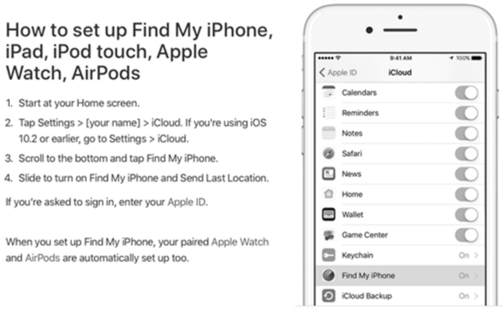
OTHER RELEVANT ETHICAL STANDARDS

- **6.01 Documentation of Professional and Scientific Work and Maintenance of Records**
  Psychologists create, and to the extent the records are under their control, maintain, disseminate, store, retain, and dispose of records and data relating to their professional and scientific work in order to (1) facilitate provision of services later by them or by other professionals, (2) allow for replication of research design and analyses, (3) meet institutional requirements, (4) ensure accuracy of billing and payments, and (5) ensure compliance with law.
- **6.02 Maintenance, Dissemination, and Disposal of Confidential Records of Professional and Scientific Work**
  (a) Psychologists maintain confidentiality in creating, storing, accessing, transferring, and disposing of records under their control, whether these are written, automated, or in any other medium.

SECURE YOUR IOS DEVICES

- iOS = Apple’s mobile operating system
- First step: have a passcode that is at least six digits long!
- Require passcode immediately (Settings -> Touch ID & Passcode -> Require Passcode -> Immediately).
- Enable erasure after 10 failed passcode attempts (Settings -> Touch ID & Passcode -> Erase Data -> On).
- Next, enable Find My iPhone.

SET UP FIND MY IPHONE



How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods

1. Start at your Home screen.
2. Tap Settings > [your name] > iCloud. If you're using iOS 10.2 or earlier, go to Settings > iCloud.
3. Scroll to the bottom and tap Find My iPhone.
4. Slide to turn on Find My iPhone and Send Last Location.

If you’re asked to sign in, enter your Apple ID.

When you set up Find My iPhone, your paired Apple Watch and AirPods are automatically set up too.

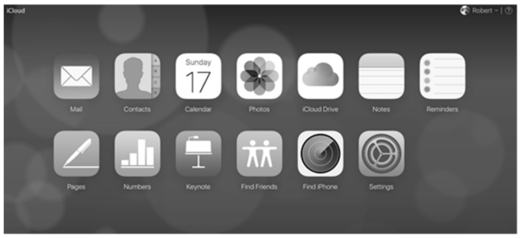
FIND MY MAC

- macOS = Apple’s computer operating system
- Set up Find My Mac:
- Apple icon -> System Preferences -> iCloud.
- Select Find My Mac.
- Note: Location services must be enabled.

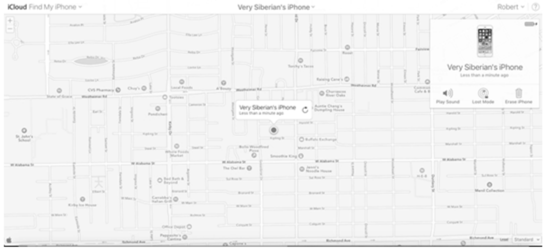
LOCATE, LOCK, PLAY A SOUND, OR ERASE YOUR DEVICE

- Go to icloud.com on any browser and sign in to see available options.
- Or, use the Find My iPhone app on a different device.

ICLOUD IN BROWSER



ICLOUD IN BROWSER



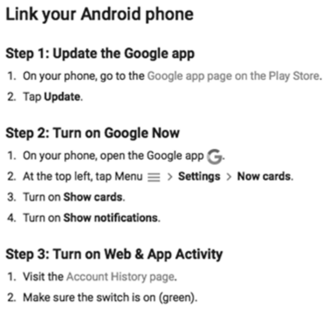
IOS COMPLEX PASSWORD

- You can set a complex passcode for your iPhone/iPad/iOS device
- New passcode can include numbers, letters, and special characters
- Settings > General > Passcode Lock > Turn off “Simple Passcode”
- IOS 7- passcode can be up to 90 characters
- Probably not necessary for the average user

FIND MY DEVICE (ANDROID)

- Android = Google’s operating system for mobile devices.
- Find My Device is on by default if the device is associated with a Google account. Hence, please take that step! ☺
- If you don’t use Gmail, set up a Google account for the email account you use.
- https://accounts.google.com/signupwithoutgmail

FIND MY DEVICE (ANDROID)



Link your Android phone

Step 1: Update the Google app

1. On your phone, go to the Google app page on the Play Store.
2. Tap **Update**.

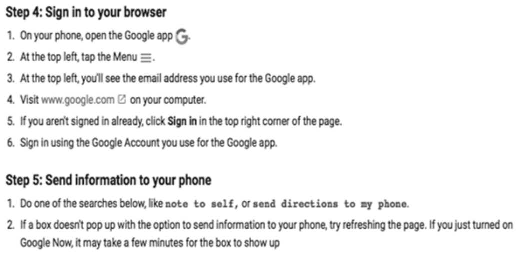
Step 2: Turn on Google Now

1. On your phone, open the Google app.
2. At the top left, tap Menu ≡ > **Settings** > **Now cards**.
3. Turn on **Show cards**.
4. Turn on **Show notifications**.

Step 3: Turn on Web & App Activity

1. Visit the Account History page.
2. Make sure the switch is on (green).

FIND MY DEVICE (ANDROID)



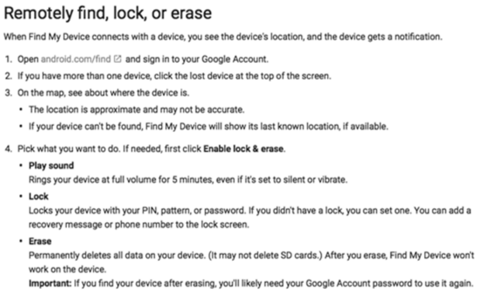
Step 4: Sign in to your browser

1. On your phone, open the Google app.
2. At the top left, tap the Menu ≡.
3. At the top left, you'll see the email address you use for the Google app.
4. Visit www.google.com on your computer.
5. If you aren't signed in already, click **Sign in** in the top right corner of the page.
6. Sign in using the Google Account you use for the Google app.

Step 5: Send information to your phone

1. Do one of the searches below, like `note to self`, or `send directions to my phone`.
2. If a box doesn't pop up with the option to send information to your phone, try refreshing the page. If you just turned on Google Now, it may take a few minutes for the box to show up

FIND MY DEVICE (ANDROID)



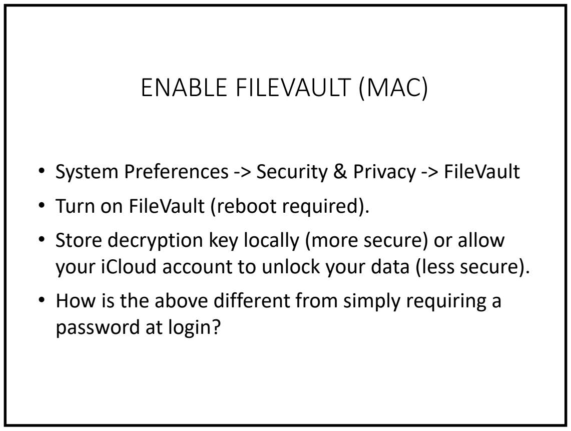
Remotely find, lock, or erase

When Find My Device connects with a device, you see the device's location, and the device gets a notification.

1. Open android.com/find and sign in to your Google Account.
2. If you have more than one device, click the lost device at the top of the screen.
3. On the map, see about where the device is.
   - The location is approximate and may not be accurate.
   - If your device can't be found, Find My Device will show its last known location, if available.
4. Pick what you want to do. If needed, first click **Enable lock & erase**.
   - **Play sound**
     Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate.
   - **Lock**
     Locks your device with your PIN, pattern, or password. If you didn't have a lock, you can set one. You can add a recovery message or phone number to the lock screen.
   - **Erase**
     Permanently deletes all data on your device. (It may not delete SD cards.) After you erase, Find My Device won't work on the device.
     Important: If you find your device after erasing, you'll likely need your Google Account password to use it again.

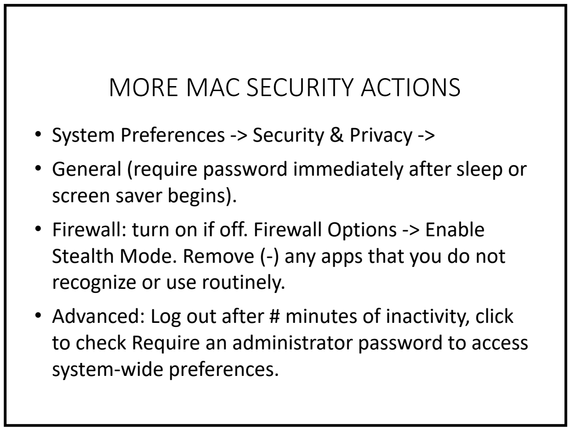
ENCRYPT YOUR DRIVES

- All drives housing patient data should be encrypted.
- Password protect your computer at login and when your screen saver engages.
- If you use Windows, turn on BitLocker.
- If you use Mac, turn on FileVault.
- Password protection does not necessarily imply encryption. If you’re not sure, check documentation.



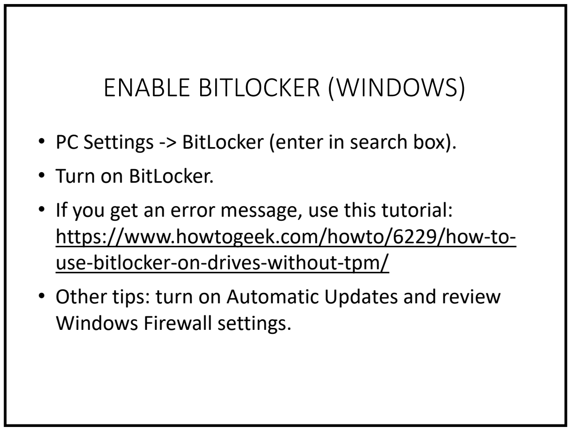
ENABLE FILEVAULT (MAC)

- System Preferences -> Security & Privacy -> FileVault
- Turn on FileVault (reboot required).
- Store decryption key locally (more secure) or allow your iCloud account to unlock your data (less secure).
- How is the above different from simply requiring a password at login?



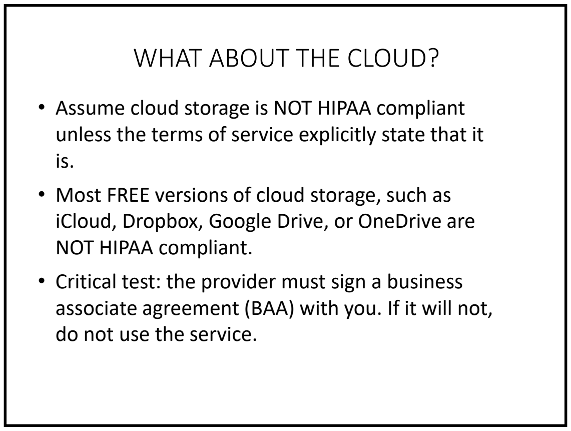
MORE MAC SECURITY ACTIONS

- System Preferences -> Security & Privacy ->
- General (require password immediately after sleep or screen saver begins).
- Firewall: turn on if off. Firewall Options -> Enable Stealth Mode. Remove (-) any apps that you do not recognize or use routinely.
- Advanced: Log out after # minutes of inactivity, click to check Require an administrator password to access system-wide preferences.



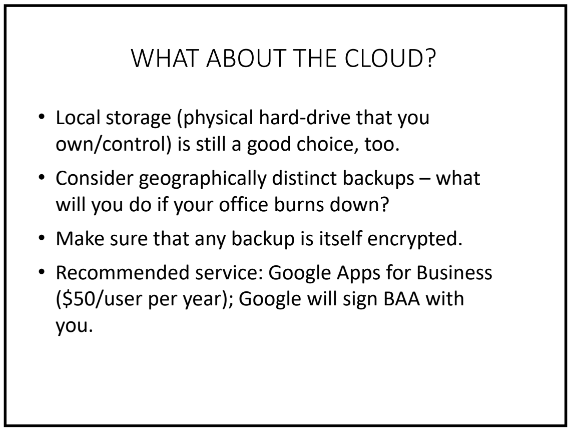
ENABLE BITLOCKER (WINDOWS)

- PC Settings -> BitLocker (enter in search box).
- Turn on BitLocker.
- If you get an error message, use this tutorial: https://www.howtogeek.com/howto/6229/how-to-use-bitlocker-on-drives-without-tpm/
- Other tips: turn on Automatic Updates and review Windows Firewall settings.



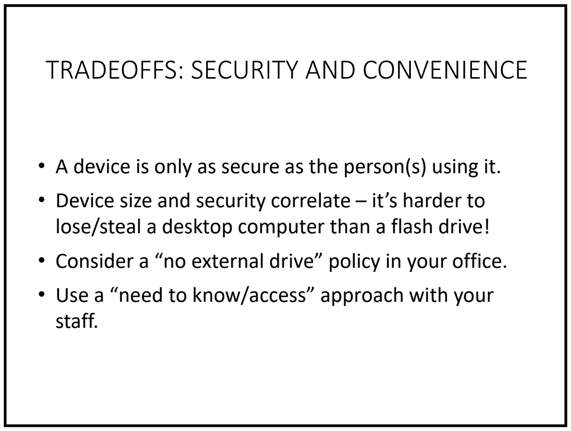
WHAT ABOUT THE CLOUD?

- Assume cloud storage is NOT HIPAA compliant unless the terms of service explicitly state that it is.
- Most FREE versions of cloud storage, such as iCloud, Dropbox, Google Drive, or OneDrive are NOT HIPAA compliant.
- Critical test: the provider must sign a business associate agreement (BAA) with you. If it will not, do not use the service.



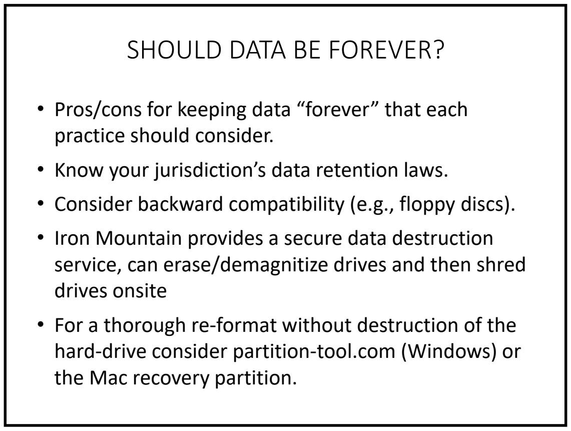
WHAT ABOUT THE CLOUD?

- Local storage (physical hard-drive that you own/control) is still a good choice, too.
- Consider geographically distinct backups – what will you do if your office burns down?
- Make sure that any backup is itself encrypted.
- Recommended service: Google Apps for Business ($50/user per year); Google will sign BAA with you.



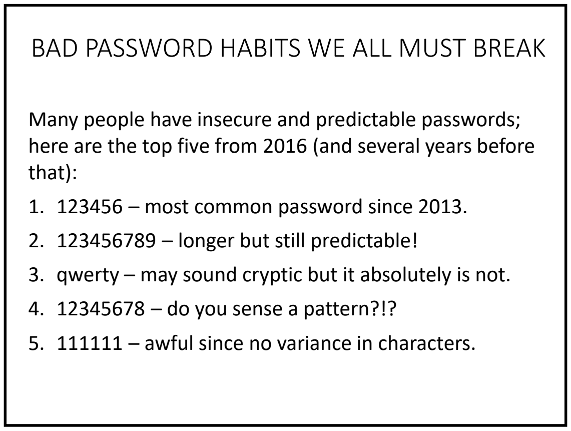
TRADEOFFS: SECURITY AND CONVENIENCE

- A device is only as secure as the person(s) using it.
- Device size and security correlate – it's harder to lose/steal a desktop computer than a flash drive!
- Consider a "no external drive" policy in your office.
- Use a "need to know/access" approach with your staff.



SHOULD DATA BE FOREVER?

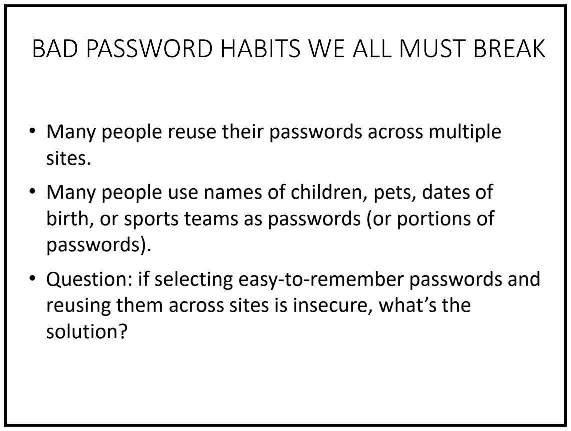
- Pros/cons for keeping data "forever" that each practice should consider.
- Know your jurisdiction's data retention laws.
- Consider backward compatibility (e.g., floppy discs).
- Iron Mountain provides a secure data destruction service, can erase/demagnitize drives and then shred drives onsite
- For a thorough re-format without destruction of the hard-drive consider partition-tool.com (Windows) or the Mac recovery partition.



BAD PASSWORD HABITS WE ALL MUST BREAK

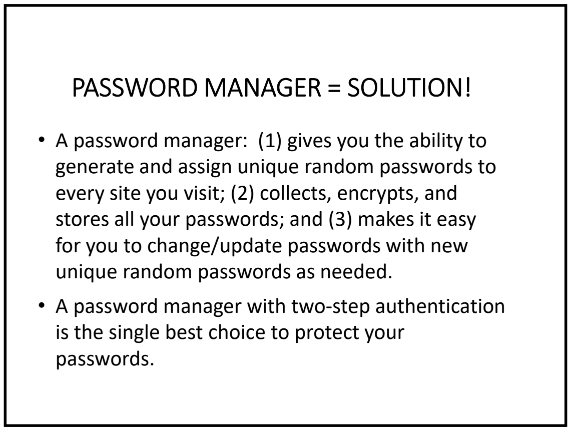
Many people have insecure and predictable passwords; here are the top five from 2016 (and several years before that):

1. 123456 – most common password since 2013.
2. 123456789 – longer but still predictable!
3. qwerty – may sound cryptic but it absolutely is not.
4. 12345678 – do you sense a pattern?!?
5. 111111 – awful since no variance in characters.



BAD PASSWORD HABITS WE ALL MUST BREAK

- Many people reuse their passwords across multiple sites.
- Many people use names of children, pets, dates of birth, or sports teams as passwords (or portions of passwords).
- Question: if selecting easy-to-remember passwords and reusing them across sites is insecure, what's the solution?



PASSWORD MANAGER = SOLUTION!

- A password manager: (1) gives you the ability to generate and assign unique random passwords to every site you visit; (2) collects, encrypts, and stores all your passwords; and (3) makes it easy for you to change/update passwords with new unique random passwords as needed.
- A password manager with two-step authentication is the single best choice to protect your passwords.

PASSWORD MANAGER = SOLUTION!

- Most web browsers have built-in password managers. We do NOT recommend these.
- iCloud keychain is an option for Mac and iOS devices.
- Examples of stand-alone password managers: LastPass, 1Password, Dashlane, or True Key.

PASSWORD MANAGER = SOLUTION!

- Hackers do not sit and try to guess your password- they have automated programs to try passwords and these programs are pretty sophisticated.
- Your password manager password should be long, 20-30 characters or more.
- Your password manager password should be as random and individual as you can make it.
- https://identitysafe.norton.com/password-generator

OVERVIEW OF LASTPASS

1. Create an account at lastpass.com.
2. Create a master password.
3. Set up two-step authentication.
4. Create your vault.
5. Use LastPass for all new passwords.
6. Be prepared for an emergency.

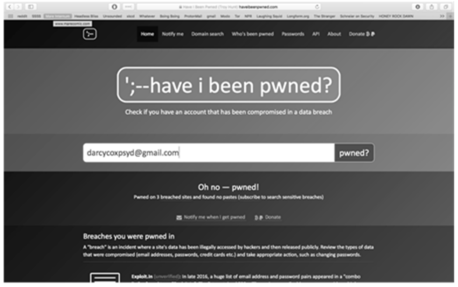
WHEN DO I CHANGE MY PASSWORDS?

1. Any instance of employee turnover.
2. Any time you have a personal break-up or divorce, or issue with a co-worker.
3. When new equipment is purchased.
4. Anytime you hear about a data breach on the news and think “Hey, I worked/shopped/paid my taxes there!”

WHEN DO I CHANGE MY PASSWORDS?

5. Otherwise, every 3 to 6 months.
6. NEVER, under ANY CIRCUMSTANCES, should you EVER respond to an UNSOLICITED email prompting you to click on a link in an email to change your password (or do anything, really).
7. Use the free VirusTotal service to scan anything suspicious (virustotal.com).

WHY DO I HAVE TO CHANGE MY PASSWORD SO OFTEN?



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

darcycoxpsyd@gmail.com

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

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

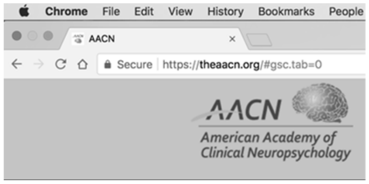
Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo

2-STEP AUTHENTICATION

- Uses (1) a strong, unique password and (2) some other datum (often a text message) to log into an account.
- May need for each login attempt or in special circumstances.
- Create a “back door” for yourself – a back-up printout with codes to use if you cannot get a text.
- Available for many types of services.

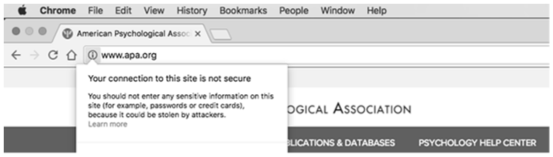
BONUS MATERIAL! BROWSER SECURITY

- Be sure that any critical website uses the https prefix and has a solid lock icon like this:


Chrome
File
Edit
View
History
Bookmarks
People
AACN
Secure
https://theaacn.org/#gsc.tab=0
AACN
American Academy of Clinical Neuropsychology

BONUS MATERIAL!
BROWSER SECURITY

- Not like this:



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Learn more

BONUS SECTION!
BROWSER SECURITY

- Chrome, Safari, Opera, and Firefox all use the Google safe browsing service.
- IE or Microsoft Edge are the worst possible choice of browser from a security standpoint.
- Browser plugins (e.g., Adobe Flash) are one of the most common sources of vulnerability.

BONUS SECTION!
EMAIL SECURITY

- Never send PHI by email unless it is encrypted.
- Recommended encrypted email: Proton Mail.
- What is the critical test for a service that will be involved in the storage/transfer of PHI?

VIRTUAL PRIVATE NETWORK (VPN)
PROTECT YOURSELF FROM DODGY WI-FI

- Your ISP may track you (e.g., websites you're visiting and data you're sharing with those sites if not secure).
- When using public Wi-Fi, the provider may be collecting and analyzing the data for marketing purposes or "sniffing" your traffic.
- Compromised Wi-Fi can also send malware to your browser.

VIRTUAL PRIVATE NETWORK (VPN)
PROTECT YOURSELF FROM DODGY WI-FI

- NEVER accept/download any "pop-up" updates when using hotel Wi-Fi or other public Wi-Fi, even if it appears to be from a company you know and use (e.g., Adobe).
- When you use a VPN, your online activities are encrypted and the ISP cannot eavesdrop or insert content.
- Favorites: Opera VPN (iOS/Android); privateinternetaccess.com for computers.

SOME FINAL THOUGHTS

- Home and office routers must be updated regularly, default passwords changed.
- Use a separate guest network for outsiders when possible.
- Beware the so-called Internet of Things (IoT).