**STEP 1 - IDENTIFY WHERE YOU HAVE IMPORTANT STUFF**

* What’s important? That’s different for each of us.
  1. Online investment sites: Fidelity, Charles Schwab, Ameritrade
  2. Bank websites: SunTrust, Chase, Wells Fargo
  3. Cloud storage: Dropbox, iCloud, OneDrive
  4. Social Media: Facebook, Twitter, Instagram
  5. Home Security: Brinks, SimpliSafe, ADT
  6. Backup Devices: USB drives, Backup drives, Cloud backups
  7. Digital Devices: Computers, Laptops, Mobile devices
* Make a list of all your important digital resources and prioritize them.
* Use what you learn in this talk to properly secure these important resources.
* Establish a Digital Executor: Someone you trust who could access your digital resources if needed. (They will need to have your list of important digital resources and access to your password manager (your IDs and Passwords)

**STEP 2 - USE A PASSWORD MANAGER**

* Password Managers are encrypted digital vault applications.
* One password can be used to open the password vault, but 2FA (Two factor Authentication) is recommended. If you are only going to use a password to access your password manager – IT MUST BE A COMPLEX PASSWORD!
* Some password managers can manage IDs and passwords while syncing across Windows, MacOS, Android and Apple mobile devices.
* Most can auto-generate complex passwords. You will not need to “remember” passwords! You only need to use your password manager to provide the password.
* Many password managers are Integrated with browsers and can automatically populate the ID and password for you.
* Chrome, Safari, Firefox, iCloud Keychain and other options exist, but generally, a specialized password manager is best.

Some examples:

* + LastPass
  + 1Password
  + BitWarden (Free)
  + Dashlane
  + Keeper
  + KeePass (free)
  + Password Safe (free)

Password Managers vary in functionality and cost.

Use search engine to learn about them and find one that works best for you.

This will take some time, a few hours, taking notes, comparing, until you decide.

You will find published comparisons online which will help too.

**STEP 3 - USE ANTIVIRUS SOFTWARE**

Antivirus software is a huge help, but it is not guaranteed protection. These products can include many features. Do some comparison shopping or ask advice from family or computer services providers with appropriate technically knowledge.

* [Avast](http://www.avast.com/), [AVG](http://www.avg.com/), [Avira](http://www.avira.com/), [Kaspersky](http://support.kaspersky.com/), [Norton](https://security.symantec.com/), [McAfee](https://www.mcafee.com/en-us/index.html), [ClamAV](https://www.clamav.net/), [Microsoft Windows Defender](https://www.microsoft.com/en-us/windows/comprehensive-security),  [Sophos](http://www.sophos.com/), [MalwareBytes](https://www.malwarebytes.com/)

**STEP 4 - KEEP YOUR MOBILE DEVICES, COMPUTERS, HOME WIRELESS ACCESS POINTS PATCHED. ETC.**

Install software updates and important patches the ensure that identified weaknesses that could be exploited by malware (malicious software e.g. viruses, trojans, spyware, etc.) or hackers.

**STEP 5 - ALWAYS – ALWAYS – ALWAYS MAKE BACKUPS OF ANY IMPORTANT DATA**

* + Cloud
  + USB device (e.g. Thumb drive, USB drive)
  + NAS (Network Attached Storage)
  + Paper

**OTHER IMPORTANT THINGS TO REMEMBER:**

**CONSIDER USING TWO COMPUTERS**

1. One computer only for important things like holding important data and accessing financial, banking, or other important sites. **Never use this computer for anything else.**
2. A second computer for social media, playing games, web searching, casual Internet usage. This computer has a far higher chance of infection, compromise, so do not have important data on it. Definitely use 2FA on any password safe that is on a computer which has a higher risk of infection.

**IMPROVE YOUR AUTHENTICATION SECURITY**

Wherever possible, especially for very important websites, financial, etc. use Two Factor Authentication (2FA) also called Multi factor Authentication (MFA).

Only using a password as a single method of authentication is no longer considered very secure as a general practice. Using a long complex password is very good, but in today’s world, more than one authentication mechanism is far better. Transition yourself to start using more than one method of authentication. This usually involves using a password plus something else. The “something else” can be a code sent to you in a test message (very common, but not the most secure), a code provided by an application such as google authenticator or Authy, something you physically have, such as a Yubikey (most secure). Most websites will have information about what they support for 2FA. You can call their technical support for assistance in setting it up.

**WHEN YOU ONLY USE PASSWORDS**

1. 14 character or longer passwords
2. Use upper case, lower case, numeric, punctuation characters
3. Use different password for each website
4. Avoid using names of family, pets, terms related to hobbies, birthdays, etc. Social media information can help hackers figure out passwords.
5. Avoid writing passwords down on sticky notes, etc.
6. Pass Phrases are good: Let’s drive my T3sla. I’ll sail the 7 Seas%
7. Combine languages: beautiful cielo aujourd’hui
8. Use different email addresses: for financial, gaming, shopping...

**BE CAUTIOUS ABOUT YOUR EMAILS & TEXT MESSAGES**

We all get emails and text messages from friends and family.

Just because we know the person who sent the message, it **does not mean** the message is safe.

* If anything looks off; the time the message was sent, the wording in the message, the attachment or Website link (URL), **think twice before opening the document or clicking on the link.**
  + Contact the person to verify they personally sent the message
  + Hover mouse over (don’t click) link to see if it looks legitimate. [PuppiesForFree.com](http://corriandertest.hmswgroup.com/) really is <http://corriandertest.hmswgroup.com>
    - Think! This maybe looks legit? But nothing related to animals!
    - It just looks a bit off! BEST NOT TO CLICK ON IT
  + Emails / texts that evoke a sense of Urgency, too good to be true statements, Order/Delivery (we are always receiving packages – so we tend to think it would be legit), Legal or Financial concerns – USE CAUTION
  + Save file and scan with antivirus software before opening
  + 12 people become victim of cybercrime every single second.

**SECURELY REMOVE ALL DATA FROM ANY COMPUTER, MOBILE DEVICE, USB DRIVE**

Before you throw away or give away any digital device make sure your data is securely removed. Remember that just deleting a file is not deleting the actual data. You may want to research how to do this or get technical help.

* Giving someone an old computer, mobile device, USB device?
* Selling an old computer, mobile device, USB device?
* Lending someone an old computer, mobile device, USB device?
* Long term storage of an old computer, mobile device, USB device?
* Are you deleting files and formatting hard disks to get rid of old data?
* How to securely wipe data? If technically minded, Google it, Otherwise have a professional do it.
* CLOUD STORAGE – Some providers wipe data, Some providers encrypt data
  + Some do not securely remove the data
    - Dropbox just hides the file – You can select permanent delete.
    - Google Drive used Trash – again select permanent delete.
    - Microsoft OneDrive uses Recycle Bin – delete files in the recycle bin.
* IN ALL CASES – You should probably consider securely “wiping” the data.

**WEB BROWSERS**

Browser extensions – are often part of tools like Password Managers, but some extensions could be malicious

* + Steal credentials
  + Install and run crypto mining software (software that uses your computer resources to create crypto currency e.g. bitcoin)
  + Even extensions from legit web stores such as Google Web Store have been malicious.  
     [Browser extensions](https://chrome.google.com/webstore/category/extensions?hl=en) can be incredibly handy and useful, but compromised extensions — depending on the level of “permissions” or access originally granted to them — *also can give attackers access to all data on your computer and the Web sites you visit*. <https://krebsonsecurity.com/2018/09/browser-extensions-are-they-worth-the-risk/>

If your browser does a popup saying something like “This site is not secure”, “Your connection is not private” and/or something about “Attackers may be trying to steal your information , **do not continue onto the website.**

**VPN**

Use a VPN if you:

1. Frequently use Hotel, Airport, Coffee shop or City Wifi networks
2. Are concerned about Internet privacy

What to look for when shopping for a VPN:

* 1. Provider says they do not collect any logs
  2. Provider has lots of VPN servers in the countries/area you are interested in
  3. Provider supports high speed connections
  4. Provider provides client software for your devices, Computer, Mobile devices, etc.

How to find a VPN?

1. Just search VPN Internet search engines.
2. Sometimes it is available with services you already have, Lifelock, Antivirus, etc.

**FIREWALL**

Firewalls are standard features in Windows and MACs. They are typically already running in a basic configuration that is generally sufficient. If you have particular concerns, please get help from someone who understands firewalls.

-10-9-2019 Tips from Greg Leibolt, Cyber Security Professional