Internet Safety

Phishing

A scam by which a target is duped into revealing personal or confidential information which the scammer can use illicitly. Being tricked into installing a piece of software that you did not mean to install can also be a form of phishing. You can research common scams and how to report them at https://www.usa.gov/stop-scams-frauds. You will also find more information about phishing and cybersecurity in general at our SOU IT Department website located at https://inside.sou.edu/it.

Email

- Companies should never ask you for your password or require that you log in to verify your credentials. Most companies will not even include links to their login pages in their emails.
- Examine the URLs of the links in the email by hovering your mouse pointer over them. Where are they trying to take you? If it seems suspicious, don't click it! You can always go the company's website on your own to log in if necessary. You never have to use an email link to get to the websites you visit already.
- Never trust an email just because it looks legitimate.

Phone

- Companies should never ask you for your sensitive information over the phone if they initiated the call, and they should never ask you for your passwords. If someone tries this, tell them that you are going to hang up and call them back at their company's publicly-listed phone number.
- Technology companies will never contact you about problems on your computer. They aren't monitoring your computer for signs of trouble, and do you really want them to be? If you get a call from someone claiming to be tech support from a company, hang up, and whatever you do, don't let them connect remotely to your computer.
- Be suspicious anytime someone tries to pressure you with the "ticking time bomb" threat. "Act now or else you're going to lose everything!" This is a common con-artist trick.

Software and Websites

- Be cautious when downloading software from websites that like to display manipulative advertisements. Either learn how to determine which download button to click or get your software from another source that respects your time.
- Never react to browser windows claiming that your computer is infected. Just close them. You should also familiar yourself with what your computer's legitimate security alerts look like. They will usually contain the name of your anti-virus software.
- Be cautious when installing freeware software that comes with bundled adware or spyware. You can always opt out of installing those annoying extras, but they'll often try to trick you into installing them anyway.
- https://www.ninite.com is a great website that enables you to bundle downloads for many common software products into one convenient package that is safe and free of junkware.

Updates

Updates are vital to protect you from exploits that cyber criminals discover in the various programs we use every day. Not updating your software is like leaving your doors and windows unlocked.

Operating System

- **Windows 10**: Go to your Start Menu, click on Settings, and then select Update & Security.
- **Windows 8, 7, and Vista**: Go to your Start Menu, click on Control Panel, and then find the Windows Update control panel applet.
- **Macintosh**: Click on the Apple icon in the top-left corner of your screen, select App Store, and then click on the Updates button in the App Store.

Web Browsers

- **Firefox**: https://support.mozilla.org/en-US/kb/update-firefox-latest-version
- **Chrome**: https://support.google.com/chrome/answer/95414
- **Internet Explorer / Edge:** Updates come included in your Windows updates.
- **Safari**: Updates come included in your Macintosh updates.

Browser Plugins

- **Java**: Oracle is ending support for Java for personal computers as of January 2019. You should uninstall Java and find alternatives to any apps that rely on it.
- **Flash**: https://get.adobe.com/flashplayer
- **Silverlight**: https://www.microsoft.com/getsilverlight

Microsoft Office and other Products

- **Microsoft Office**: http://tinyurl.com/jdn6h5w (redirects to the Office update page)
- **Adobe Acrobat Reader**: https://get.adobe.com/reader
- Other products: https://www.ninite.com

Router Firmware

- Updating your router's firmware carries inherent risks. If you decide to do it yourself, be sure to follow all instructions provided by your router's manufacturer.
- **Linksys**: http://www.linksys.com/us/support-article?articleNum=132961
- **Belkin**: http://www.belkin.com/us/support-article?articleNum=10797
- **ASUS**: http://www.asus.com/microsite/2014/networks/routerfirmware_update/
- **D-Link**: http://support.dlink.com/ and then look for your router model.
- **Netgear**: http://tinyurl.com/z9t5vql (redirects to the Netgear support page)
- **Charter**: https://www.spectrum.net/contact-us/
- **Centurylink**: http://internethelp.centurylink.com/internethelp/downloads-auto-firmware.html

Remediation

We try our best to prevent disaster, but sometimes we have to perform remediation. Here's how.

- **System Restore** for Windows: http://www.wintuts.com/System-Restore
- **Time Machine** for Macintosh: https://support.apple.com/en-us/HT201250
- **Malwarebytes** for both Macintosh and Windows: https://www.malwarebytes.com

Total System Reset

This is a method of last resort designed to reset your operating system to its original state when you first booted up the computer. **ALWAYS BACK UP YOUR DATA AND ENSURE YOU HAVE THE MEANS TO REINSTALL ALL PROGRAMS YOU'VE DOWNLOADED OR PURCHASED PRIOR TO ATTEMPTING A SYSTEM RESET**. The process will undo everything. Professional assistance is recommended.

- **Macintosh**: https://support.apple.com/en-us/HT201314
- **Windows 8 and 10**: http://www.tenforums.com/tutorials/4130-reset-windows-10-a.html
- **Windows 7 and Vista:** Get a professional to help you.

Encryption

Keeps your digital life private.

HTTPS

- Encrypts your connection to individual websites. Especially important for online banking and shopping.
- Look for the padlock icon next to the URL of the website you're visiting. The URL will also begin with http**S**:// as opposed to http://.

VPN

- Encrypts your connection to the Internet by directing all of your traffic through a trusted proxy via an encrypted tunnel. Adds an extra layer of protection on top of HTTPS and also provides anonymity. Can be used on a variety of devices, including laptops, tablets, and cell phones. It is highly recommended to use a VPN service while traveling and connecting to open Wi-Fi networks that do not require a password to connect.
- **Paid VPN Services**: https://www.privacytools.io/#vpn (focuses on anonymity and government jurisdiction) and https://vpn-services.bestreviews.net/vpn-comparison (focuses on features)

Local Encryption

Keeps your files private using strong, non-reversible encryption. Cannot view them without the password. **Be careful when using this kind of encryption because if you lose the password, you will NOT be able to recover your data.** That's the whole point.

- **Veracrypt** (cross-platform, capable of whole-disk encryption or file/folder encryption): https://www.veracrypt.fr/en/Home.html

- **File Vault** (Macintosh): https://support.apple.com/en-us/HT204837
- **Bitlocker** (Windows): http://tinyurl.com/jdc6xkd (redirects to a tutorial on setting up Bitlocker)

Password Management

Passwords secure much of our lives: our personal information, our data, and our money. **It is not enough to keep reusing the same, weak passwords on the Internet.** Passwords should be lengthy (12 characters or more—the longer the better), complex (a mixture of uppercase and lowercase letters, numbers, and symbols), unique (use different passwords for everything), and ideally randomized (meaningless gibberish is good). **Password managers** can help by remembering, and even generating, passwords for you in a secure fashion. They work by encrypting your passwords with a **master password**, which you must not lose or forget, but the risk of losing your master password pales in comparison to the risk of having your passwords compromised.

- **KeePass**: http://keepass.info
    - KeePass is open source, free, and very secure because you retain exclusive control of the encrypted password database.
    - Open source means that security experts worldwide can audit the program's code every time it changes. Transparency ensures its security.
    - You can upload the encrypted password database to cloud providers such as Dropbox and Google Drive if you want to sync it between devices. This is still secure because without *your* master password, the file can't be opened by the cloud provider.
- **LastPass**: http://lastpass.com
    - LastPass is a freemium, cloud-based password management service. The free features are enough for most people, and you can upgrade to their premium version at any time.
    - LastPass is extremely convenient since it ties into your web browser and syncs your passwords across all of your devices for you. It also makes it easy to audit your passwords and it can even alert you if your credentials for a website have appeared in a known data breach.
    - Although LastPass is closed-source and retains a copy of your password database, they have a good reputation for transparency and proper security and supposedly they never receive your master password—decryption happens locally on your computer—so they can't decrypt your password database. That could change, however.
- **Apple Key Chain**: http://tinyurl.com/a9brnch (redirects to a tutorial on Key Chain Access)
    - Built into the Macintosh operating system and integrates into all of their products and services.
    - Can be synced through iCloud. See https://support.apple.com/en-us/HT204085
    - Implements great security, but it is closed source and controlled by Apple, so just like with LastPass, you are trusting the company to respect your privacy now and in the future.
- Other options: https://www.privacytools.io/#pw

Two-Factor Authentication

Authentication factors include something you know (e.g. a password), something you have (e.g. a key), and something you are (e.g. your fingerprint). The more factors you use, the more secure your authentication method is. Many online banking websites, stock trading websites, and email providers now support two-factor authentication, usually in the form of one-time codes that they generate and send to you via your cell phone in addition to asking for a password. This means that if a criminal wants to impersonate you, they now need not only your password, but also the code sent to your cell phone. This protects you from password leaks, but not necessarily from phishing.

- **DUO for your SOU Account**: https://support.sou.edu/kb/articles/691
- **Google Account** Two-Factor Authentication: https://www.google.com/landing/2step
- **Amazon** Two-Factor Authentication: https://www.amazon.com/gp/help/customer/display.html?nodeId=201962420
- **E*Trade** Two-Factor Authentication: www.etrade.com/onlinesecurity
- Check with your banks to see if they offer two-factor authentication for their online services.

Wi-Fi Security

Use WPA2 encryption when setting up your wireless network at home, be sure to choose a good password for it, and update the password periodically. When traveling or using public Wi-Fi, consider using a VPN service (see page 3), especially if the public Wi-Fi network is open (meaning that it doesn't require a password). Be careful that you don't accidentally connect to a fake Wi-Fi network with a similar name to the legitimate one you're trying to connect to (e.g. don't connect to the malicious "Coffeeshop wi-fi" when you meant to connect to the legitimate "Coffee Shop Wireless Network").

- Set up WPA2 on **Belkin** routers: http://www.belkin.com/us/support-article?articleNum=10805
- Set up WPA2 on **Linksys** routers: http://www.linksys.com/us/support-article?articleNum=139152
- Set up WPA2 on **Netgear** routers: https://kb.netgear.com/000028991/Securing-your-wireless-network-using-WPA2
- Set up WPA2 on **Asus** routers (enter product model name): http://www.asus.com/support
- Set up WPA2 on **D-Link** routers: http://tinyurl.com/gmnl24j (redirects to support article)
- Manage Wi-Fi on **Charter** Routers: http://www.charter.net/support/internet/spectrum-home-wifi
- Manage W-Fi on **Centurylink** Routers: http://internethelp.centurylink.com/internethelp/wireless.html

Information Leaks

Sometimes your personal information and even your passwords will be leaked by the companies you've done business with—or even by the government. This is seemingly unavoidable in modern life, so you had best have a plan.

- **Password leak:** The company will notify you, or else you'll probably hear about it in the news. Hopefully your password was encrypted by the company (if it wasn't, you should never do business with them again), which buys you some time because encrypted passwords have to be cracked before they can be used. If your password was strong because you followed my advice in this class, you should have ample time to change it before the criminals can crack it. (Weak passwords can be cracked in minutes whereas strong passwords can take years to crack.) If you were only using that password on the website that got breached, then you're done. If not, you'll have to update that password everywhere else you've used it.
- **Personal Information leak:** The company will notify you, or else you'll probably hear about it in the news. Your information may have been encrypted, but even if it was, it won't be difficult for crackers to break it because it will follow well-defined patterns. Assume that your name, address, date of birth, social security number, and any other information that may have been leaked is now somewhere on the Internet for criminals to bid on. Identity theft is what you need to be on the lookout for. Monitoring services can help with that, but they won't prevent the problem. Credit freezes are a better option.
    - **Credit freezes**: http://tinyurl.com/nzdwbwt (redirects to an excellent blog article by a security researcher on how to deal with credit freezes)
    - **Identifytheft.gov** (report and recover from identity theft): https://identitytheft.gov
- **Your SOU email and your data stored on SOU devices can be subpoenaed if you are ever the subject of a legal investigation pertaining to your position at SOU.** Do not conduct personal business on your SOU accounts or devices.

Card and Password Skimming

Whether your credit card or debit card uses a magnetic strip or a RFID/NFC (radio) chip, it can be skimmed. Skimming refers to when a criminal copies the information on your card or passport without your knowledge or permission. This information can be used to charge purchases to your accounts or to steal your identity.

- You can protect yourself from magnetic strip skimming by inspecting ATM and other card reading terminals prior to using them. See how your terminal compares to other terminals nearby. Trust your instinct if something looks off about it.
- If you do not trust someone to handle your credit card where you cannot see them, consider paying with cash instead.
- You can protect yourself from RFID/NFC skimming by placing your RFID/NFC equipped credit cards, debit cards, and passports in a specially designed wallet, purse, case, or sleeve. A homemade sleeve can be constructed out of aluminum foil.
- Be especially cautious of skimming when traveling. Tourists make tempting targets.
- Keep an eye on your account statements.