Digital Privacy & Security

Definitions/Terms

Privacy:
"The state or condition of being free from being observed or disturbed by other people."*

Security:
"The state of being free from danger or threat."*

Malware:
Malicious software

Virus:
A specific class of malware that replicates itself.

Spyware:
A specific class of malware that collects user data including browsing habits, financial information, account information, and passwords.

Ransomware:
A new form of malware that hijacks computers and files by encrypting them, not releasing them until a ransom is paid.

Phishing:
A malicious attempt to trick users into sharing personal or account information.

Threat Modeling: Identify the risks and mitigations

A process that identifies and assesses risks and actions to mitigate those risks.

- What assets do you want to protect?
- Who are your adversaries?
- What are the consequences if you fail? What are the threats?
- What is the risk? How likely is the threat to occur?

Tools, Systems, and Equipment

- Anti-Malware, Antivirus and AntiSpyWare Software
  - These are your front line defense against malware and attacks. There are free packages; Internet Service Providers often include this a part of their service. Install this and keep it up-to-date.
- Automatic or Regular updates and patches
  - Updates are integral in maintaining security. As soon as an update launches, your device is at greater risk until you install the update. Exploits in this instance are called Zero-day Attacks; once the vulnerability is known, it can be more easily exploited.
- Firewalls
  - A network security device that monitors traffic and blocks traffic according to security rules.

Tools, Systems, and Equipment (Continued)

- Encryption and Encrypted Email
  - This security feature protects data from others gaining access without the key. It turns plain text into scrambled encoded data that is then unlocked by authorized access with a key. Unencrypted email can be intercepted and read by others, including the email provider.
    - ProtonMail, Tutanota, etc.
- VPNs
  - Virtual Private Networks (VPNs): Consider adding this tool, especially if you travel or ever use public Wi-Fi. It provides an encrypted connection between a device and a network.
- Secure your Router
  - Change the default SSID/wireless name.
  - Change the default password.
  - Hide the signal so that you have to enter it manually to connect.
  - Update the firmware on your router.
- Secure Browsing
  - Make sure websites have a lock symbol or use https, especially if you are entering account information, making transactions, or inputting personal information. Without this, your information can be visible to others. Try browser extensions or add-ons that ensure a secure connection.
- Private Browsing
  - Incognito Mode, InPrivate Browsing, Privacy Mode
    - https://us.norton.com/internetsecurity-privacy-how-does-incognito-mode-work.html
  - DuckDuckGo Search Engine
  - TOR Browser (this can access the dark web, so beware)
- Password Managers
  - Subscription based service to both securely store encrypted passwords and help generate random and secure passwords. Look at Consumer Reports for reviews. There are some open source ones like KeePass.
- Social Media, Online Account Settings, and Device Settings
  - Most default settings are fully open and not secure.
  - Make sure you configure settings to protect yourself the way that suits your risk tolerance.
  - Look at Location Services on devices and account settings.
  - Know who you are sharing data with on Social Media account settings.
  - Privacy Settings How-To's https://teachingprivacy.org/prevention/

- ❖ Check Credit History & Monitor Data Breaches
  - https://www.consumer.ftc.gov/articles/0155-free-credit-reports
  - https://www.identitytheft.gov/info-lost-or-stolen

Behaviors

- ❖ Strong Passwords (Single Factor Authentication)
  - Use long, random, complex and unique passwords. Consider passphrases.
  - Consider Password Managers to help manage and generate passwords.
  - Do not reuse passwords for multiple accounts.
  - Do not use common passwords.
  - Do not use personal information in your password.
  - Do not use keyboard patterns in your password.
- ❖ Two-Step Verification/Two-Factor Authentication (2FA or MFA)
  - Requires two types of information to gain access to an account: a password, a code/pin, or a biometric like a fingerprint.
- ❖ Evaluate and Avoid risky links, emails, and websites – Phishing and Scams
  - Pay attention to search results before clicking links. Do you trust the link? Does it look suspicious? Is it an ad link instead of the direct website?
  - Your bank and other businesses should never contact you to verify account information.
  - Hover over a link to see the full address displayed at the bottom left of your screen.
  - When in doubt, never click a link or open an attachment. Call the bank or business or go directly to their website.
- ❖ Be aware of what you share
  - Sharing things like your birthday, your alma mater, your pet, answering quizzes that ask for your favorite food, color, first boyfriend/girlfriend all reveal private information online that can be answers to security questions. Beware!
- ❖ Update regularly (software, firmware, etc.)

Implement

Take action on at least one of these tools or behaviors that you are not already using. Every step and precaution you take means you have more control in protecting your privacy and security.

*Source: https://www.lexico.com

Additional Resources and Extra Reading

- Consumer Reports Ratings or Information (available with your ORPL library card)
  - Anti-Malware Software, Password Managers
  - Wireless Routers
    - https://www.consumerreports.org/digital-security/ways-to-boost-router-security/
  - General
    - https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now/
  - VPNs
    - https://www.consumerreports.org/vpn-services/choosing-a-vpn-for-added-internet-security/
    - https://www.consumerreports.org/privacy/how-to-choose-a-vpn-for-digital-privacy-and-security/
- Norton - Securing a Wireless Router
  - https://us.norton.com/internetsecurity-how-to-how-to-securely-set-up-your-home-wi-fi-router.html
- Microsoft Top Tips for Online Safety and Myth vs. Fact
  - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1ImTu
  - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE1ImTt
- FTC information on Malware
  - https://www.consumer.ftc.gov/articles/0011-malware
- FTC information on Identity Theft, Spyware and Phishing
  - https://www.ftc.gov/news-events/media-resources/identity-theft
- Norton Cyber Hygiene
  - https://us.norton.com/internetsecurity-how-to-good-cyber-hygiene.html
- Cybersecurity and Infrastructure Security Agency (CISA) Good Security Habits
  - https://www.us-cert.gov/ncas/tips/ST04-003
- San José Public Library Privacy Lab – Privacy Tools
  - https://www.sjpl.org/privacy/get-started-today
- RiseUp - Better Web Browsing
  - https://riseup.net/en/better-web-browsing
- PC Magazine – Password Managers
  - https://www.pcmag.com/picks/the-best-password-managers
- Lifewire – Secure Email 2020
  - https://www.lifewire.com/best-secure-email-services-4136763
- Stay Safe Online, National Cyber Security Alliance – Online Shopping
  - https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/
- Cybersecurity, Ready.gov
  - https://www.ready.gov/cybersecurity