Digital Hygiene and Digital Literacy Resource Guide

This collection of resources and guides was compiled by members of Generations of Indian Valley as part of a multi-week learning and research project.

Deep dive into digital literacy and online safety and security

- “Guide to Internet Safety” PowerPoint slidedeck (RSVP; email only)

Shared Terminology

- **Media** – All the ways and means we communicate and consume information in the 21st century, including online, broadcast, and print media, as well as social media, news, games, and advertising. We may also think about the various media technologies and digital devices we use every day (smartphones, tablets, laptops, smart TVs, etc.).
- **Internet** – “The large system of connected computers around the world that allows people to share information and communicate with each other” (Cambridge Dictionary, https://dictionary.cambridge.org/us/dictionary/english/internet)
    - **Wi-Fi** – Wireless internet connection that can be shared with multiple devices in a home or business, either privately or publicly, using a wireless router.
        - *Resource*: Are Public Wi-Fi Networks Safe? What You Need to Know (https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know)
    - **Smart technologies** – Any electronic device, system, or appliance that can be connected to the internet.
        - *Resource*: Smart Technology for Later Life (https://www.independentage.org/get-advice/technology/smart-devices)
    - **Internet of Things** – “Refers to the network of physical devices that use sensors to gather data about their environment and share information with each other through the internet. There are billions of devices and machines making up the Internet of Things. These include smartphones, fitness trackers, driverless cars, and even sensor-equipped jet engines, among others.”

- *Resource*: The Pros and Cons of Smart Devices (https://www.completetechnology.com/2021/11/the-pros-and-cons-of-smart-devices/)

- **Hardware / Software / Firmware** – Hardware refers to the physical device and its components (computer, phone, tablet, etc.). Software refers to the non-physical features of your device that you interact with (apps, web browser, games, etc.). Firmware is a specific type of software for a specific device that you don't directly interact with.
    - *Resource*: Hardware vs. Software vs. Firmware: What's the Difference? (https://www.lifewire.com/hardware-vs-software-vs-firmware-whats-the-difference-2624567)
    - *Resource*: What are the most common symbols used by computers? (https://www.computerhope.com/issues/ch001801.htm)
- **Web Browser / Search Engine** – A web browser is the application you use to access and navigate the internet (Google Chrome, Microsoft Edge, Mozilla Firefox, etc.). A search engine is a website that organizes and helps you find other websites using keywords (Google, Bing, DuckDuckGo, etc.).
    - *Resource*: Web Browsers vs. Search Engines: What's the Difference? (https://nordvpn.com/blog/browser-vs-search-engine/)
- **Apps / Websites** – Apps are downloaded to your device and serve a specific function. A website allows you to access information through your web browser. For example, you can access your bank's website through your web browser (Google Chrome, Microsoft Edge, etc.) OR you can access your bank through an app that you download to your smartphone or tablet.
    - *Resource*: Is It Better to Use an App or a Website? (https://www.expressvpn.com/blog/is-it-better-to-use-app-or-website/)
- **URL (Uniform Resource Locator) / Hyperlink** – A URL is the unique address of a website or file online. A hyperlink allows you to quickly access a webpage or file online by clicking or tapping on your screen.
    - *Resource*: The Dangers of Randomly Clicking Links (https://www.foolproofme.org/articles/395-the-dangers-of-randomly-clicking-links)
- **HTTP vs HTTPS** – HTTP stands for HyperText Transfer Protocol, and it is what transfers data between a web server and web browser. Basically, it is what allows you to access information online. Every URL will be preceded by HTTP or HTTPS. The "S" means that the website is secured through encryption (protects data by scrambling it). Look for sites that are HTTPS – they are more secure than HTTP sites, and less likely to be hacked.

    - *Resource*: Difference Between HTTP:// and HTTPS:// (https://www.geeksforgeeks.org/difference-between-http-and-https/)
- **Spam / Phishing / Smishing** – Spam is a term used to refer to all unwanted electronic messages that you receive via email or text messages. Phishing refers to malicious spam that is disguised as legitimate in order to trick you into sharing personal information or downloading malicious software on your device. Smishing refers to phishing attacks through your text messages with the same aim as email-based phishing.
    - *Resource*: What Spam Email Is and How to Stop It? (https://www.usnews.com/360-reviews/privacy/what-spam-email-is)
- **VPN (Virtual Private Network)** – A VPN is a subscription service that protexts your internet connection and privacy online by encrypting your data, hiding your location, and will allow you to use public Wi-Fi safely.
    - *Resource*: Best VPN Service 2024 - VPNs Tested by Our Experts (https://www.cnet.com/tech/services-and-software/best-vpn/)
- **Multi-Factor or Two Step Authentication** – A security method for email, banking, or other online services that requires you to verify your identity by providing two or more credentials (e.g., a password and a verification code).
    - *Resource*: More Than a Password - Protect Yourself from Malicious Hackers with Multifactor Authentication (https://www.cisa.gov/MFA)
- **Cookies** – "Cookies are small text files containing unique data to identify your computer to the network…The main purpose of web cookies is to make the internet experience easier for users…Cookies do contain data, and that typically includes a unique identifier and a site name. A cookie could also include personally identifiable information such as your name, address, email, or phone number if you've provided that information to a website."
    - *Resource*: What Are Internet Cookies and How Are They Used? (https://allaboutcookies.org/what-is-a-cookie)
    - *Resource*: How To Clear Cookies in Chrome, Safari, Edge, and Firefox (https://www.hellotech.com/guide/for/how-to-clear-cookies-chrome-safari-mozilla-firefox-edge)
- **Cloud** – "The cloud refers to software and services that run on the Internet, instead of locally on your computer. Most cloud services can be accessed through a Web browser like Firefox or Google Chrome, and some companies offer dedicated mobile apps. Some examples of cloud services include Google Drive, Apple iCloud, Netflix, Yahoo Mail, Dropbox and Microsoft OneDrive."
    - *Resource*: Too Embarrassed to Ask: What Is 'The Cloud' and How Does It Work?

(https://www.vox.com/2015/4/30/11562024/too-embarrassed-to-ask-what-is-the-cloud-and-how-does-it-work)

How to secure and manage your email

- How to make your email more secure:
    - Use a unique password that's easy for you to remember OR set up a password manager
        - *Resource*: The Best Password Managers to Secure Your Digital Life (https://www.wired.com/story/best-password-managers/)
    - Setup Multi-factor (2-step) authentication
    - Consider a VPN and/or Aunthenticator
        - *Resource*: The Best Authenticator Apps for 2024 (https://www.pcmag.com/picks/the-best-authenticator-apps)
    - Check your Data & Privacy settings
- Clean up and manage your email:
    - Delete or Mark as Read everything that's more than 3-6 months old
    - Setup Labels to organize your important emails
    - Empty your Trash and Spam regularly
    - Block unwanted junk and/or Unsubscribe from unwanted newsletters and advertisements
    - Report Spam / Phishing on suspicious emails
    - Star the emails you need to Reply to

Organizing your device and minimizing distractions

- How to Declutter Your Phone (https://www.nytimes.com/wirecutter/blog/declutter-speed-up-phone/)
- How to Organize Your Digital Files (https://www.nytimes.com/wirecutter/guides/how-to-organize-your-digital-files/)
- 11 Ideas for How to Organize Digital Files (https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/11-ideas-for-how-to-organize-digital-files)
- Utilize Digital Wellbeing tools on your smartphone to minimize distractions (Go to Settings → Digital Wellbeing)
    - Check your daily usage
    - Dashboard: Set timers for different apps

    - Bedtime mode: Set Bedtime mode by turning on Grayscale and/or Do Not Disturb for a certain time period
    - Focus mode: You can pause distracting apps and set schedules
    - Manage Notifications: Turn off unnecessary notifications
- Organize apps
    - Touch and Hold the App → Click App Info
        - You can Uninstall, Disable an/or Force Stop (Delete/Disable apps you don't use)
        - Check Notifications and Permissions
        - Clear Storage or Cache
    - Hold the App and Move It
        - You can Remove from Screen (Remove any app you don't use)
        - You can Group it with similar Apps to free up space and organize
- Manage Storage (Go to Settings → Storage)
    - You can turn on Storage Manager (deltes backups of photos and videos)
    - Check what's using up the most storage (photos, videos, games, apps)
    - Delete unnecessary storage

Phishing Scams

- Google Jigsaw Phishing Quiz (https://phishingquiz.withgoogle.com/)
- Federal Trade Commission Consumer Advice (https://consumer.ftc.gov/)
    - Scams (https://consumer.ftc.gov/scams)
    - How to avoid a scam (https://consumer.ftc.gov/articles/how-avoid-scam)
    - What to do if you were scammed (https://consumer.ftc.gov/articles/what-do-if-you-were-scammed)
    - How to recognize a fake Geek Squad renewal scam (https://consumer.ftc.gov/consumer-alerts/2022/10/how-recognize-fake-geek-squad-renewal-scam)
- 20 phishing email examples for 2024 (https://www.aura.com/learn/phishing-email-examples)
- Berks couple loses $18,000 to 'Geek Squad' refund scam (https://www.readingeagle.com/2024/04/09/berks-couple-lose-18000-to-geek-squad-refund-scam/)

Evaluating news and information online

- AdFontes Media Bias Chart (https://adfontesmedia.com/)
  - This chart measures both the left-right political bias of information sources as well as news value and reliability. It's important to check the methodology (https://adfontesmedia.com/how-ad-fontes-ranks-news-sources/) of these kinds of rating systems. This is a "living" chart so the left-central-right spectrum is always shifting.
- All Sides Media Bias Chart (https://www.allsides.com/media-bias)
  - This organization rates the left-right bias (https://www.allsides.com/media-bias/media-bias-chart) of online, political news sites, and they also create a factcheck bias chart (https://www.allsides.com/media-bias/fact-check-bias-chart), rating the left-right bias of leading factchecking organizations. They claim to be "more comprehensive in its methodology" than other resources, and that the ratings "reflect the average judgment of all Americans, not just a panel of insiders" (https://www.allsides.com/media-bias/media-bias-rating-methods).
- Media Bias/Fact Check (https://mediabiasfactcheck.com/)
  - They claim to be "the most comprehensive media bias resource on the internet." You can peruse their large database of news sites and organizations by a variety of bias categories, and they have a news feed with more recent factchecks and retracted or corrected news stories. Be sure to check their methodology (https://mediabiasfactcheck.com/methodology/). This site has a lot of ads, however.
- The Trust Project's Trust Indicators (https://thetrustproject.org/trust-indicators/)
  - This is a very good collection of indicators and questions for evaluating the credibility and trustworthiness of news and information.
- RAND's "Tools that Fight Disinformation Online" (https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html)
  - A comprehensive collection of tools, games, and other resources aimed at helping folks mitigate the spread and influence of disinformation.
- NewsGuard (https://www.newsguardtech.com/how-it-works/)
  - This is a browser plugin that will show you a reliability score of news stories or sites that you encounter online -- they call themselves "The Internet Trust Tool." This is a subscription service, but it looks like it's free

through Microsoft Edge. You can check out their rating process and criteria (https://www.newsguardtech.com/ratings/rating-process-criteria/).

Strategies/resources for managing information overload

- Name It to Tame It: Emotional Regulation Strategy (IREX; email only)
- SIFT method of factchecking/verifying information (https://hapgood.us/2019/06/19/sift-the-four-moves/)
- Critical Ignoring method for mitigating information overload (https://www.psychologytoday.com/us/blog/talking-apes/202211/do-you-really-want-click)
- Snopes.com factchecking site (https://www.snopes.com/)
- Factcheck.org factchecking site (https://www.factcheck.org/)
- Poynter's MediaWise for Seniors free online course (https://www.poynter.org/mediawise/programs/seniors/)
- University of Maine's News Literacy Challenge (https://libguides.library.umaine.edu/newslit/)

Alternative and Budget Phone Plans

- Tello (https://tello.com/buy/custom_plans)
- Mint Mobile (https://www.mintmobile.com/cell-phone-plan-for-seniors/)
    - *Resource*: Mint Mobile vs. Tello Mobile: Which budget carrier is right for you? (https://www.businessinsider.com/guides/tech/mint-mobile-vs-tello-mobile)
- Consumer Cellular (https://www.consumercellular.com/shopping/choose/plan)
- Boost Mobile (https://www.boostmobile.com/)

Strategies for Passwords

By Jerri Thompson

My first passwords were Jerri7 and readingmom8. I used them for everything. Not a good idea. My first bank passwords used my anniversary and my husband's name. Not a good idea. My daughter tried to get me to use a password manager, but I couldn't seem to get the hang of it.

I had to develop my own system. I have two. All my passwords are unique. I sometimes use a phrase like a movie title—some old rather obscure title that I liked or some combination of my children's initials that I then modify by making certain letters into either numbers or special symbols. The letter "l" or "L" might become a 1. The letter "A" might become an *. I do not change just one thing. That might be easy for someone to guess, so I change several different things.

Some things to remember when creating strong passwords: Longer is better; eight characters is a minimum. Do not be predictable like using a line of letters from the keyboard, or the word password, or a series of numbers in order. Do not use personal information, yours or anyone else's like your children's names or birthdates. Do not use the same password for all your accounts.

Strategies for creating passwords:

1. Use four random words somehow related in your mind. For example, "ActsColossiansTimothySamuel" are four random books of the Bible not in order. Then I would add numbers and special symbols in different spots.
2. Use the first letters of the words in a sentence. Do not use a familiar phrase like "To be or not to be, that is the question." Use something like "My son was born at Shadyside Hospital in 1987" to make "Mswb@SHi1987". By the way, that sentence is not even true about me.
3. Misspell words deliberately. Use *Krying* for Crying or *Dubble* for Double. Use numbers for some letters. However, be careful not to use common ones. "L3tM31n" for "LetMeIn" is too common.
4. Use arithmetic like "Dog+Chicken=6Legs"
5. Use punctuation marks and special characters, especially the less common ones like the brackets and arrows within phrases.
6. Don't use "MickeyMouse" or even "M1ck3yM0us3". Maybe use "M1ck3yDuck*?!"

Other things to add to secure your account logins:

1. Two-factor authentication: After entering your password, the bank or other institution sends you a code by text, email, or phone call that must be entered to complete the login to your account.
2. Security questions: Use fake questions and/or fake answers or at least obscure answers that no one could find online or in normal conversation with you. For example: Who was your childhood best friend? Maybe you could use the real name if she is no longer in your life, but maybe you could use your worst enemy instead.
3. On accounts you want to be very secure, change your password frequently (every three months).

As important as it is to keep other people out of your accounts, it is also important that you are able to remember the passwords and the answers to the security questions (especially if some of them are make-believe). A password book may help but keep it in a secure place. An encrypted password file on your computer that requires a password to get into may help, but don’t lose the computer.

Protection from Bad Actors and Threats

By Carl Thompson

Simply by being alive we are subject to bad actors (any person or entity that has malicious or unlawful intent) and other threats. Some of them can come to us directly, such as someone that impersonates a utility worker to gain access into our house. Others can come to us through the media, particularly those with two-way communications such as the telephone or the internet. The emphasis of this section will be with the internet. The only way we can be free from online threats is to not be connected to the internet. This is a very difficult position to maintain, so what can we do to protect ourselves online? Bad actors may use many schemes, but what they are usually ultimately seeking, especially when targeting individuals, is money. This section more specifically deals with some of the high level things that can be done to protect ourselves while using the internet.

The first line of defense against bad actors is to not let them into your house or in this case into your computer or other device. This is accomplished by a firewall. The firewall is a combination of software and hardware that isolates your computer from the internet and acts as the go-between. It monitors the data stream that is attempting to enter your computer and will not allow unauthorized data to enter the computer. The firewall is kind of like the bouncer at the door to a bar: only letting invited and authorized guests in. Typically, any computer operating system such as Windows comes with a default firewall. Other firewalls can be installed, including those that are free or are bundled with other protection packages.

The next line of defense is the AntiVirus (AV) software. Even if the data is authorized to pass through the firewall, other threats can be hidden deeper within the data stream. The AV software is used to scan (compare) the data within the computer with data from known threats. AV bad actors will include viruses, malware, and ransomware. The AV software can typically be set up to scan data as it is coming in from the internet and isolate or remove any malicious data. The AV software can generate a report of threats identified and actions taken. It is also important to periodically update the AV software and to scan the data on the computer hard drives. This needs to be done since bad actors are constantly developing new and different forms of malicious data to evade the AV software. Although some computers come with free or trial versions already installed on the computer, and free AV software can be installed, as with most things that are free they are usually very limited in what they can do and will likely require an upgrade to a paid version to be convenient, versatile, or more useful.

The firewall and AV software are absolute essentials for any computer connected to the internet. They are developed to keep the bad actors out of your computer. Another way bad actors operate is to intercept, decode, and eavesdrop on your data as it is being transmitted from your computer. This is where the Virtual Private Network (VPN) comes in. A VPN is established when communication between your computer and the VPN computer is established. The most important aspect of the VPN is that the information that is transmitted on it is encoded in such a manner to make it very difficult to understand even if eavesdropping. Each device connected to the internet has a unique IP address to identify it. The VPN establishes a temporary IP address for the device. This hides the actual device making it more difficult to locate. As a bonus, a choice of countries for the temporary IP address is usually available. This will make it appear that the computer is located in a different country, which can be useful under some circumstances. Like AV software, there are free versions available, but they are usually limited in their use of resources and an upgrade to a paid version is quite often needed. Quite often AV software and VPN software can be purchased as a bundled package from various sellers.

So far, we have talked about proactive means to protect ourselves from bad actors and threats. What is our recourse if these fail and we find ourselves the victim of identity theft, which is perhaps the worst outcome from these bad actors? Fighting to restore our proper identity can be an overwhelming and time consuming proposition. Identity theft insurance such as LifeLock (https://lifelock.norton.com/) is available for this situation. With this insurance, if you become the victim of identity theft, typically an agent familiar with the process of restoring someone’s identity is assigned to help guide you through the process. They will help ensure that all steps in the process are completed to minimize the damage and restore those parts of the identity that were stolen. However, unlike the AV and VPN software, identity theft insurance does not need to be installed. Rather, information to be monitored such as bank accounts, phone numbers, email addresses, etc., are entered into a database. Should any unusual activity be found with any of these, a notification is sent to you, usually by text or email, notifying you of the activity – the necessary action can then be taken. Periodic summaries of any activity or the lack thereof are quite often provided, as well. Part of the protection also includes reimbursement for expenses incurred in re-establishing proper identity. Identity theft insurance can be purchased from insurance companies, but quite often it is bundled with AV and VPN software.

Norton/LifeLock is one of the more well known AV/VPN/Identity Theft Insurance providers and will be used as a price comparison. The cost for AV software for one device (computer, tablet, phone, etc.) is about $60 per year. To bundle the VPN with the AV software, the annual cost is about $95 for three devices (about $32 per device). To bundle AV, VPN and LifeLock identity protection, the annual cost is about $180 for ten devices (about $18 per device). One should note that other benefits besides those described here are also included with the various options and bundles. Likewise, other Identity Theft options are separately available.