**Talk Data to Me**

**Image:** Included in toolkit.

**Alt Text:** A group of people in a huddle all using their cell phones.

You would be surprised what can be shared about you from your online behavior: website history, online shopping, social media, and more comprise your digital footprint. This includes personal data traces left behind, which can be used by cybercriminals to steal your identity or access your personal accounts.

Posting personal information online like your current location or hometown, or even referring to your favorite movie could give cybercriminals answers to commonly used security questions. This is why data privacy should be a priority concern for each of us.

Data privacy is the right to choose what information you share. Although it’s nearly impossible to keep all your data private from everyone, you still have options. The first step is knowing your privacy rights on any given website or device (pro tip: always check Privacy Policies) and sharing only the data you deem appropriate.

You can proactively take these steps to manage and protect your data:

* **Limit the information you share.** The first line of your personal data defense is you. If you share your personal information online, you risk having it leaked. You can significantly improve your data security if you keep it private. If you want to share it online, read the site’s Privacy Policy to ensure it doesn’t store and share your data with third parties.
* **Save passwords to your browser or Operating Systems (OS) password keeper.** Using a browser or OS password keeper is the best way to ensure that you’re using complex, unique passwords across all websites and services. These password keepers can notify you if one of these passwords is compromised. Even if your device is stolen, your password keeper is still protected and will typically use multi-factor authentication or biometrics (such as your fingerprint) before allowing you to access saved login information. [Learn more about password protection.](https://consumer.ftc.gov/articles/password-checklist)
* **Don’t click on unfamiliar attachments and links.** Cybercriminals often use email to access your data through phishing. Phishing is unsolicited emailing or calls that aim to deceive the receivers into providing money, personally identifiable information (PII), or other sensitive information such as credit card numbers, passwords, or W2s. Once you click a suspect link, your device will get infected with malware. The safest practice is to avoid clicking on unfamiliar attachments and links. [Learn more about how to up your phishing game.](https://digital.va.gov/security-excellence/hook-line-and-sinker/)
* **Update all your tools, applications and Operating Systems (OS).** Every app and tool you use, including the underlying operating system, is a piece of software that requires regular updates. These updates don’t just include the new and improved features but also vulnerability patches and security updates. It’s paramount to update your operating system, apps and tools to prevent vulnerability exploits and keep your data safe.

Data breaches and cyberattacks continue to rise. It is critically important to minimize your visibility to cybercriminals by understanding and monitoring your online activity. Given the risks, adopting strong cybersecurity and privacy practices is a powerful way to protect your data. [Start with this cybersecurity checklist](https://digital.va.gov/cyber/spring-into-action/)!