# 10 tips to defend your online data

**Image:** Included in toolkit.

**Suggested Alt Text:** Cybersecurity badge with checkmark, several people, and icons representing phishing, credit card theft, and computer, mobile device, and internet cyberattacks.

The [global cost of cybercrime](https://www.usaid.gov/digital-development/cybersecurity/economic-growth-briefer#:~:text=According%20to%20one%20estimate%2C%20the,the%20People's%20Republic%20of%20China.) topped $8 trillion in 2023 — translating to over $250,000 a second worldwide — and is expected to rise to over $23.84 trillion by 2027. North America remains the most targeted for ransomware attacks, [up 50% from 2022](https://www.securityinfowatch.com/cybersecurity/press-release/53081204/ransomware-attacks-in-november-rise-67-from-2022). Since 2020, the [health sector alone has experienced a 45 percent increase](https://www.hipaajournal.com/healthcare-industry-cyberattacks-increase-by-45/#:~:text=A%20new%20report%20from%20Check%20Point%20shows%20attacks,all%20industry%20sectors%20worldwide%20over%20the%20same%20period.) in cyber-attacks.

Hackers are targeting health and data partners and Veterans with phishing to ransomware every day to steal data and wreak havoc on U.S. health care and other services. Veterans are often targeted by criminals attempting to fraudulently receive benefits or access valuable data.

**Defending the galaxy of Veteran data**

The defenders of Veteran online data include VA, Veterans, caregivers, and family members. As the largest health care provider in the nation, VA:

* Uses automated tools and cybersecurity expertise to detect and thwart malicious cyber activity every day.
* Adheres to “Zero Trust” principles in that we assume our perimeter and network are always subject to assault and vulnerable. Based on this assumption, we have multiple layers and tools in use to limit access and rapidly detect, remediate, and protect against any attack.
* Intercepted in 2023 over one trillion potential security events and blocked nearly a billion malicious emails.
* Confirms 96 percent of VA staff use multi-factor authentication (MFA) to verify their identity before they can log in to VA systems — and restricts access to Veteran data to only VA staff with a need to know for delivering services to the Veteran.

**What you need to know to guard Veteran data**

As Veterans, caregivers, and family members, protect your personal data online by:

1. [Securing your information](https://digital.va.gov/cyber-spot/tips-and-tricks-to-secure-your-clicks/) with [multi-factor authentication](https://digital.va.gov/cyber-spot/from-vulnerable-to-verified-mfa-saves-the-day/) — it’s easy to do!
2. Being alert to and report [phishing and smishing attempts](https://digital.va.gov/cyber-spot/phishing-without-rods/).
3. Encrypting your data using a VPN.
4. **Not** saving your passwords to your browser.
5. [Regularly updating the software on your devices and computers](https://digital.va.gov/cyber-spot/defending-digital-threats-one-update-at-a-time/);

many updates include security protections against the latest threats.

1. Avoiding using public Wi-Fi.
2. **Not** clicking on unknown or unfamiliar attachments and links.
3. Shopping only on legitimate, secure, and trusted websites.

## [Protecting your benefits against Payment Redirection Fraud](https://news.va.gov/124837/protect-your-benefits-combatting-payment-redirection-fraud/).

1. Deleting rarely used or unused applications and using a browser instead.

When it comes to protecting Veteran data online, it takes multiple defenders working side by side to guard the galaxy of Veteran information. Check out [VA’s Cybersecurity Spot](https://digital.va.gov/cyber/) for the resources you need.