# How to Protect Yourself from Cyber-Attacks and Scams

**Image:** Attached in email.

**Suggested Alt Text:** Laptop computer with a big lock on the screen and user’s hands on keyboard.

As technology advances, scammers are becoming smarter in their attacks. VA is committed to protecting Veterans’ benefits against fraudulent activity and raising awareness of the various cyber scams impacting Veterans and their beneficiaries.

Staying informed of evolving fraud tactics is important to protect yourself and your benefits. One of the newest ways fraudsters engage in cyber-attacks is by using Artificial Intelligence (AI) tools, collectively referred to as [generative AI](https://www.harvardonline.harvard.edu/blog/benefits-limitations-generative-ai) and Large Language Models (LLM). These are systems that can create synthetic text (A type of data that is created using machine learning algorithms to generate new content that is similar in structure to existing data), images, source code, and other forms of media at an incredible speed. Depending on the prompts given by the user, the outputs can range from realistic to stylized (Realistic outputs refer to lifelike and accurate models, while stylized outputs emphasize exaggerated features and depart from real-world accuracy). LLMs are an essential part of deep learning, which is the foundation of ChatGPT and other Natural Language Processing technologies currently receiving widespread attention. Veterans should be aware of this technology and its potential for accessing their personally identifiable information and potentially compromise their benefit payments.

**Examples of generative AI scams include:**

* Creating fake identities or impersonating real people to access secure information and claims for benefits.
* Developing convincing voice or video messages to be used in engineering attacks, such as making fraudulent changes to direct deposit information.
* Automating phishing attacks by creating mass fake emails or text messages to trick Veterans into giving away sensitive information.

Veterans should be aware of cyber scams targeting their benefits, including phishing, identity theft, spoofing, email scams, ransomware, forgery and wire and mail fraud.

**VA recommends following these** [**tips**](https://digital.va.gov/cyber-spot/tips-and-tricks-to-secure-your-clicks/) **to practice safe online behavior and prevent fraud:**

* **Screen emails carefully**, and only open emails from senders you know and trust. Delete and block emails from unknown or suspicious senders.
* **Be cautious of** **popups and links** on websites, emails and texts that can be used to infect your device with harmful malware.
* **Limit the Personally Identifiable Information (PII) you post online**, such as your address, date of birth, workplace, or kinship details.
* **Delete old social media accounts** and limit your online presence and available biographical information.
* **Maximize privacy settings** on all active social media accounts to protect information from unknown users.
* **Do not accept friend or connection requests from individuals with only an online presence.** Only add friends or connections you know and trust in real life, not those who you have only met online.
* **Download strong antivirus software** to protect yourself from malware attacks.
* **Be aware of signs of a malware infection**. If your computer runs unusually slowly or frequently crashes without explanation, it may be an indication it is infected with malware.
* **Never send bank information or payment to “online friends” or others.** Scammers may threaten to destroy your files or data if you do not send payment or banking information. If you are a victim of ransomware, do not respond to any threat and [report the incident](https://www.ic3.gov/Home/ComplaintChoice/default.aspx) immediately.

VA is working to combat cyber threats and better safeguard Veterans benefits. These actions include enhancing security around direct deposit changes, collaborating with Federal partner agencies, and developing communications to increase awareness around cyber fraud.

VA provides essential [tools and resources](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdigital.va.gov%2Fcyber%2F&data=05%7C01%7C%7C197d7a7bc52e4a7a823008dbc502051f%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638320384701731035%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=6EQtjJvEKyl6GqmEdgkbt22KE3I43y%2FipgmhIbzDQFA%3D&reserved=0) to help you protect your data. To boost your cybersecurity awareness and safeguard your data, watch VA’s [Protecting Veteran Information video](https://youtu.be/EltGZDku0co).

If you miss a VA benefits payment, identify a discrepancy in payments, or find suspicious activity with your direct deposit account, contact VA immediately at 1-800-827-1000. You can also file a complaint with the [Federal Trade Commission (FTC)](https://reportfraud.ftc.gov/#/).

To learn more about protecting Veterans from fraud, visit [www.va.gov/VSAFE](https://www.va.gov/initiatives/protecting-veterans-from-fraud/).