**Phishing–without rods**

**Image:** Included in toolkit.

**Alt Text:** A Veteran interacting with a mobile device.

It happens all the time. You get an email from a trusted source. It could be a friend or family member, a retailer you frequent often, or even a subscription renewal. You open it, everything looks normal, and then you see a hyperlink. Without thinking twice, you click it, unaware of the scam on the other side. According to Microsoft's [The New Future of Work](https://www.microsoft.com/en-us/research/uploads/prod/2021/01/NewFutureOfWorkReport.pdf)report, 62 percent of security professionals say phishing scams have increased more than any other threat since the pandemic. These scams are expected to persist.

The hook

Phishing is a widespread cybercrime in which attackers use social engineering to deceive individuals into revealing sensitive information by posing as a trustworthy source. Attackers frequently adapt their strategies to exploit current events, so it's essential to remain vigilant to avoid these types of attacks.

Don’t become the bait

Signed into law recently, the PACT Act expands VA's health care and benefits for Veterans and survivors exposed to burn pits and other toxic substances. These benefits have become a direct target for scammers. Veterans eligible for or receiving these and other VA benefits should exercise extreme caution when opening messages or clicking on links from unknown or untrusted sources. Consider the following suggestions to avoid being lured to the bait:

* Ensure the sender is legitimate and matches the organization it claims to be.
* Check for slight variations, misspellings, or extra characters in the email address.
* Hover your cursor over any links in the email before clicking on them to verify they are from sources you trust and recognize.
* Be cautious of urgent, threatening, or overly enticing language that prompts immediate action.
* Avoid downloading attachments unless you're expecting them and trust the sender.
* Beware of requests for personal information. Legitimate organizations typically won't ask you to provide sensitive information via email.
* If you receive a suspicious email, contact the sender through an official and verified channel to confirm its authenticity.
* Use the "report phishing" button, if available, to notify the service provider about the malicious email.

Now let’s reel it in

Phishing is a widespread threat that targets anyone with an email address. And [smishing](https://digital.va.gov/cyber-spot/smish-smish-dont-get-phished/) targets you via text message. Staying vigilant and practicing good cyber hygiene is essential to protecting your personal and sensitive information. It's important to know that phishing tactics can evolve, so staying informed and being proactive is vital to safeguard yourself against these threats. Always prioritize security and verify the authenticity of emails, especially when they involve sensitive information or urgent actions. And be sure to keep yourself updated on the latest [cybersecurity best practices](http://www.digital.va.gov/cyber).