# Hook, Line, and Sinker – How to Up Your Phishing Game

**Image:** Included in toolkit.

**Suggested Alt Text:** Malicious actor creating a fake webpage, sending a link to a Veteran, the Veteran opening the fake webpage and submitting information, which the attacker steals and uses, leading to identity theft.

About 156 million phishing emails are sent around the world every day, so it’s important that you stay vigilant both at work and in your personal lives. As VA’s first line of defense, it’s every employee’s responsibility to be savvy about recognizing phishing attempts and other scams!

## Lifecycle of a Phish

Cybercriminals start by choosing someone or a group of people that they want to target and choosing the type of information they want to gain access to. Their goal may be to get Veteran financial or health information, or to release ransomware into a system and demand ransom money from the users.

Attackers often compromise their host with a phishing email. The victim clicks on a malicious link or reveals the information that the attacker is seeking, believing the email is real. Once they bite, the damage is done; there’s no way to return the information or undo that click. It only takes one successful phishing attack to compromise your network and steal your data, so it’s crucial to “*Think Before You Click*” and avoid falling for phishing attempts in the first place!

## What to Do When Something Smells Phish-y

Phishers use emotions like fear, curiosity, urgency, and greed to compel you to open attachments or click on links. The attacks appear to come from real companies or individuals because cybercriminals are becoming more sophisticated every day. Never reveal personal or financial information in an email, don’t respond to email solicitations for information, and don’t follow links in emails that you don’t trust. If you’re unsure whether an email is real, try to verify it by contacting the company or sender directly.

Before sending or entering sensitive info in forms or websites online, check the security of the site. Make sure you see **https://** in the address; the “s” stands for “secure.” You should also pay close attention to the website’s URL. Malicious websites may look identical to a legitimate site, but the URL may vary in spelling or be sourced from a different domain.

Some other helpful tips to keep in mind:

* Use multi-factor authentication on all apps, accounts, and social platforms that offer it
* Monitor your online accounts regularly
* Keep your browser, installed programs, and security software updated
* Don’t click on email links from unknown sources
* Never give out personal information over email
* Block pop-up windows in your browser and never click links in them
* Track the latest phishing attacks so you know what to expect