PHISHING PREVENTION

What you need to know

Take the PHISHING training class @ https://cyber.mil/ | Use your government issued computer

What IS PHISHING?

Phishing is a form of cybercrime in which a target or targets are contacted through the use of email, phone, or text message by someone impersonating a legitimate institution in order to trick individuals into providing sensitive data such as personally identifiable information, banking and credit card information, and passwords.

What are THEY AFTER?

Usernames & Passwords

Financial Information

Identity

Money

What is the probability that a PHISHING ATTACK SUCCEEDS? 1 OUT OF 10!

I've been PHISHED. WHAT DO I DO?

► **Get your computer completely offline.** That way you won't inadvertently send phishing links to everyone on your email list, for example.

► **Save everything on a NEW USB drive.** If you've been hit by ransomware, it's best to have as much of your documents saved as possible. It may be tempting to save everything on an external hard drive, but ransomware can infect that, too, so use a new jump drive that doesn't have anything on it.

► **Change passwords for your apps, but do it from a phone or a different laptop.** Don't change them from the computer that got hit (which should be offline anyway) in case there's a keylogger on there scooping up said passwords.

► **Restore your original operating software.** Installing to its original factory image will get rid of any modifications you don't want to be there.

► **Run anti-virus software.**

► **Restore your latest backup.**

► **Inform the company.** After you've done what you can to mitigate damage, reach out to the company that the phishing email appeared to come from. Let them know what happened so they can investigate.

► **Beware of identity theft.** If your personal information was accessed, you'll want to monitor things like account activity and credit reporting.

WATCH FOR:

- ► **Spelling and Grammar Errors**
- ► **Sender Address**
- ► **Things that sound too good to be true**
- ► **Asking or demanding personal information over the phone**
- ► **Phone calls from an "Unknown Number"**

Beware of UNSOLICITED PHONE CALLS:

If you receive a phone call from an individual claiming to be from the Defense Finance and Accounting Service (DFAS), U.S. Army Human Resources Command (HRC), United Services Automobile Association (USAA) or any other organization, these calls should be handled with caution. Ask for official contact information and call them back through business contact numbers. Do not give out any personal information over the phone.

Beware of UNSOLICITED MESSAGES:

Every day, 3.4 billion phishing emails are sent around the world. According to recent phishing assault research, 25% of emails from brands contain phishing emails. Microsoft, Amazon, the banking and financial industries, and shipping corporations such as DHL, FedEx, and UPS are all examples of well-known brands.

Beware of ATTACHMENTS:

94% of malware is delivered by email, 48% of malicious email attachments are Office files

Beware of LINKS:

Hover over link to ensure it is legitimate, be wary of shortened links or URLs

Beware of LOGIN PAGES:

Always type the web address or go to the company's official website, do not login into a web site from a link in an email.

Make yourself a DIFFICULT TARGET:

Phishing occurs when cybercriminals seek to mislead someone into doing "the wrong thing," such as following a link to a malicious website.

Phishing can occur by text message, social media, or phone, however the term "phishing" is most commonly used to denote email-based attack. Cyber Criminals send phishing emails to millions of people, requesting sensitive information (such as bank account information) or providing links to malicious websites. Some phishing emails may contain viruses disguised as harmless attachments that, when opened, activate the infection.

The detection of a phishing email is becoming increasingly complex, and even the most cautious user might be duped. Here are some red flags that could point to a phishing effort. Information from your website or social media accounts leaves a 'digital footprint' that fraudsters can exploit. You can reduce your chances of being phished by performing the following.

- ► **Keep Informed About Phishing Techniques**
- ► **Think Before You Click!**
- ► **Install an Anti-Phishing Toolbar**
- ► **Verify a Site's Security -** secure websites always start with "https".
- ► **Use Firewalls and consider using a Virtual Private Network (VPN) service**
- ► **Use Antivirus Software**
- ► **Never Give Out Personal Information**
- ► **Be Wary of Pop-Ups**
- ► **Keep Your Browser Up to Date**
- ► **Check Your Online Accounts Regularly**