United States Army
Criminal Investigation Command

Media contact: CID Public Affairs Office
571-305-4041

FOR IMMEDIATE RELEASE

CID Major Cybercrime Unit: Detect, Protect, Report Phishing Scams

QUANTICO, Va. (Aug. 24, 2020) – The U.S. Army Criminal Investigation Command's Major Cybercrime Unit has seen an increase in phishing and spoofing scams and reminds the Army community to be cautious when opening emails and to take extra precautions to protect personal information.

The Director of CID's Major Cybercrime Unit, Edward Labarge, said, there has been a "massive increase" in the number of phishing attempts since the outbreak of COVID-19.

"Cybercriminals and nation-state actors continue to exploit the fears related to the pandemic," said Labarge.
The MCU reports the main goal of a phishing attack is for cybercriminals or foreign adversaries to "compromise a business network."

A phishing email is an email designed to convince the recipient to divulge personal information, banking or credit card information, or passwords. Whereas, spoofing occurs when a criminal disguises an email address, sender name, phone number, or website URL to make it appear the user is interacting with a trusted source. Generally, there is only a subtle difference by only changing one letter or a number. For example, the email received appears to be from supervisor, family member or business associate. The cybercriminal attempts to manipulate the user into believing the spoofed communications are real.

"The end goal of these campaigns is to obtain login credentials such as usernames and passwords to compromise systems and steal propriety and sensitive data," said Labarge.

MCU official's state combining both phishing and email spoofing allows cybercriminals to use deception to convince recipients into believing an email was sent from a legitimate and reputable organization or company. Typically, the email states a specific action is required. The sender's

email address looks authentic, the subject line appears valid, and the email body contains a simple and somewhat convincing message usually accompanied by a website link.

Phishing may occur on both personal and business or government emails. However, it is more likely to occur in personal email.

“From a government side of the house, DISA (Defense Information Systems Agency) does a great job protecting the enterprise by filtering millions of phishing emails every month,” said Labarge. “From a personal perspective, phishing emails are more apt to get through free email filters. However, phishing is one of the most effective attack vectors out there and regardless whether you are using a personal email or business email, you must always be on your ‘A’ game.”

Phishing is not a new scam and his been around for a long time. However, criminals are constantly changing their approach by using various techniques to gain access. This includes: vishing scams over the phone, voice email, or VoIP (voice over Internet Protocol) calls; smishing scams via SMS (text) messages; and pharming scams by installing malicious code on your computer redirecting you to fake websites.

CID officials warn users to be cautious when opening emails and clicking on links in those emails. Email service providers cannot detect all phishing and spoofed emails. Here are some steps you can take to detect, protect, and report phishing and spoofed emails.

Detect

- Keep an eye out for incorrect spelling and poor grammar in emails.
- Pay close attention to the sender email address; click on the display name if the email address is not visible.
- Be extra cautious if an email asks for personally identifiable information, financial account information, or passwords.
- Be suspicious of emails asking you to click a link to change a password, especially if password change request was not initiated.

Protect

- If the email seems suspicious, but you recognize the display name, contact the sender offline, via call or text, to verify they sent the email. Do not use any phone numbers provided in the email.
- Never click an unfamiliar link or download an attachment if you suspect the email is spoofed.
- Type in URLs or use a search engine to locate websites, if you have to log into an account.
- Turn on spam filtering to stop the majority of phishing and spoofed emails. Keep in mind, legitimate emails are sometimes flagged as spam emails.
- Scan your computer for malware regularly.
- Check account settings. If any accounts offer multifactor authentication, enable it for an additional layer of security.

Report

- Report phishing and spoofed emails to your email service provider for personal email accounts. For official government and military email accounts, report them to your system administrator or security representative.

- If you become a fraud, identity theft, or deceptive business practice victim, file a report with your local CID office, the Federal Trade Commission and the Internet Crime Complaint Center.

The Internet Crime Complaint Center has identified phishing and spoofing in the top five methods cybercriminals used during 2019, to cause more than $350 million in victim losses.

Basic protective measures will aid in the reduction of compromised information and losses.

Important User Tips to Protect Against Cybercrimes

- Companies generally don't contact you to ask for your username or password.
- Don't click on anything in an unsolicited email or text message. Look up the company's phone number vice using the one provided in email and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it
- Be careful with what information is being shared online or on social media. By openly sharing things like pet names, schools attended, family members, and birthday, a scammer gains the information they need to guess password or answer security questions.

"When it comes to protecting against these types of attacks, you really need to incorporate everything from the list," said Labarge. "However, if you had to pick one, don't click on links in your email."

MCU recommends hovering over the hypertext of the link in the email to show where the actual link is going.

Army personnel or their families who are victims of an Internet-based crime should report the crime to their local CID office. Individuals can also report crime tips to CID anonymously via a specialized application at https://www.cid.army.mil/report-a-crime.html.

-30-

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil