Cyber Directorate
Department of the Army
Criminal Investigation Division

Cybercrime Prevention Flyer

CPF 0006-2023-CID461 **3 March 2023**

Scam Awareness

Scammers – those determined to steal money, personal information, and identities from anyone – continuously evolve their scam strategies. Staying abreast of the latest scams and following some easy best practices is key to avoid becoming the next victim.

Defense Finance and Accounting Service (DFAS) Scam

Pretending to be from the DFAS, scammers contact soldiers via text and phone calls and claim the soldier has been overpaid by the military. Knowing military terminology, the scammers easily convince the soldier of a legitimate pay problem and threaten the soldier with punishment if the excess funds are not returned via a money transfer application.

Pig Butchering Scams

Pig butchering scams rely on a scammer – the butcherer – building an online relationship and level of trust, often over a long period, with a victim – the pig. The scammer then convinces the victim to invest large sums of money or cryptocurrency in a bogus investment platform or account, essentially fattening up the victim with opportunities for increased wealth while feeding the scammer-controlled account. The victim, eventually attempting to withdraw funds, will have no success because the scammer has taken everything.

Tax Season Scams

Tax season is here, and the Internal Revenue Service (IRS) warns that cybercriminals are more intent during this time of year to steal taxpayer's money and data. Taxpayers are reminded that the IRS will not initiate contact via email, text message, social media, or other digital applications to notify a taxpayer of an overdue tax bill, unfiled return, tax filing error, or for personal or financial information. The IRS will initiate contact with taxpayers through official correspondence delivered by the United States Postal Service (USPS).

Multifactor Authentication (MFA) Prompt Bombing

MFA requires a combination of two or more credentials to access an account, such as a password and an additional authentication request sent to the account owner via email, text, or phone call. MFA prompt bombing involves an unauthorized individual using the stolen credentials, username and password, on an account with the hope the legitimate user mistakenly authorizes the second authentication request. Once authorization is granted, the unauthorized user has complete access to the account.

Verification Code Scam

Selling household goods is a popular practice for relocating military personnel, which the military does often. Feigning an interest in purchasing a particular item, the scammer contacts the seller and requests the seller verify their identity by providing the scammer with the six-digit Google Voice verification number texted to the seller's

Report a crime to the Department of the Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

phone. If provided by the seller, the scammer then uses the six-digit verification number to create a Google Voice number linked to the seller's phone number. Now the scammer uses the new Google Voice phone number to hide their identity to cheat other people.

Scam Prevention Best Practices

- Questions regarding pay issues should be handled in-person at the supporting military pay office or directly contact DFAS.
- Resist the pressure to act immediately or respond to threats of disciplinary action.
- Never send money, trade, or invest based on the guidance received from someone you have only met online.
- Do not be lured by promises of high returns with no risk or very little risk.
- Personalized messages do not make the sender trustworthy.
- Do not accept an unsolicited request for account authentication.
- Do not approve authentication requests you do not recognize.
- Do not provide a verification code to anyone if you did not contact them first.
- Use strong passwords, change them often, and do not use the same password for all your devices and accounts.
- Every time you sign up for a new account, download a new app or get a new device, immediately configure the privacy and security settings.

Report

If you suspect you have been victimized, regardless of the type of scam, contact the local CID office and submit a report to the Federal Trade Commission (FTC) or Internet Crime Complaint Center (IC3).

Resources

Army Warns of Scam Targeting New Soldiers

Association of Certified Fraud Examiners

Reclaim your Google Voice Number

Test Your Scam Knowledge

Tax Season Cyber Fraud

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF