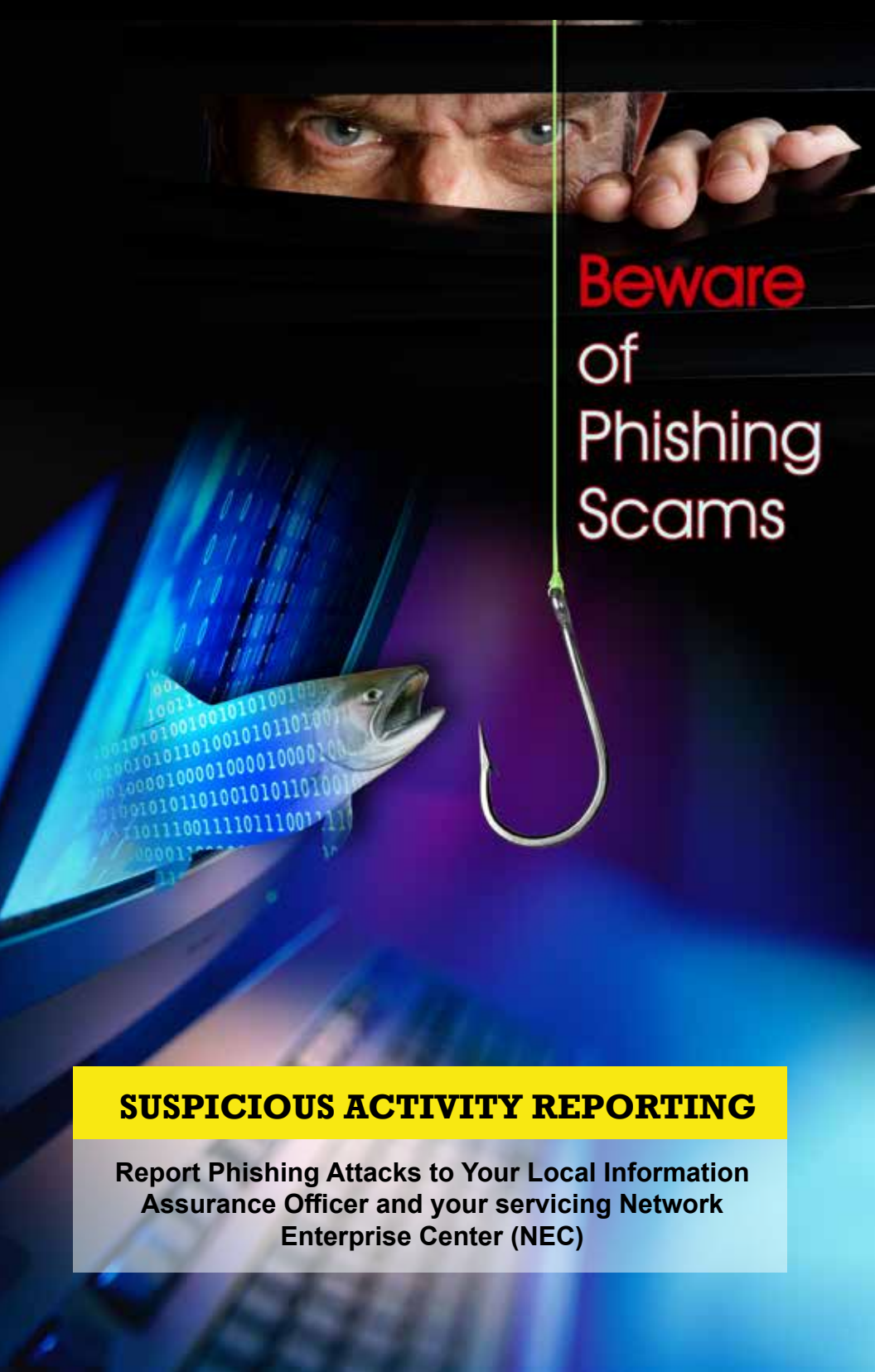


SUSPICIOUS ACTIVITY REPORTING

Report Phishing Attacks to Your Local Information Assurance Officer and your servicing Network Enterprise Center (NEC)

What is Phishing?

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques (i.e., manipulating people into performing actions or divulging confidential information). Phishing emails are crafted to appear as if they were sent from a legitimate organization or known individual. These emails often attempt to attract users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords that can further expose them, their network, and their unit to future compromises.

In order to fully understand phishing and how it can impact you and your unit, you should be aware that there are different types of phishing:

Phishing is usually an e-mail sent to a large group of people that attempts to scam the recipients. The people the message is sent to often do not have anything in common.

Spear phishing is a message sent to a smaller, more select group of targeted people or to a single individual.

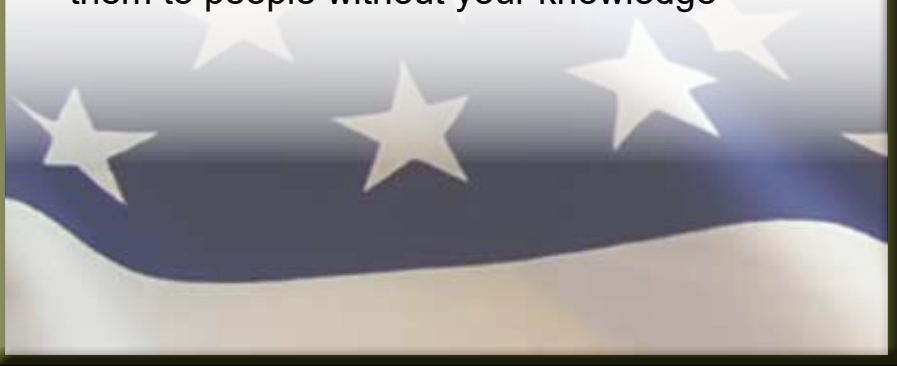
Whaling or whale phishing is a highly personalized message sent to senior executives, high-level officials ,or their personal executive staff members.

Why Phishing Works

- We are easily enticed —we trust known brands/logos
- Lack of user education and awareness
- Lack of Information Assurance knowledge and warning indicators
- Visually deceptive text
- Image masking
- Image mimicking Windows

User Awareness

- Most phishing attempts are for identity theft, but phishing is also being used to gain access to online banking, federal, and DoD information
- Phishing Attacks can be geared to collect personal information such as: SSN, mother's maiden name, date of birth, passwords, credit card numbers, etc.
- Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software
- Malicious software can be viruses and other computer code designed to allow a hacker to use your computer for illegal Internet activity, or to access your unit's network to gather DoD information
- Malicious code may capture your keystrokes or capture your personal and work files and send them to people without your knowledge



Protect Yourself and Your Organization

DO

- Watch out for phishing
- Delete suspicious emails
- Contact your Information Assurance Officer or your servicing Network Enterprise Center (NEC) if you have questions about emails
- Report any potential incidents

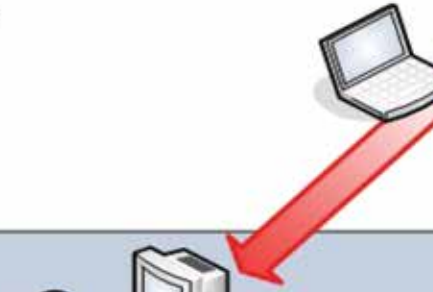
DO NOT

- Open suspicious emails
- Click on suspicious links in emails or pop-up windows
- Call telephone numbers provided in suspicious emails
- Disclose any information

How Phish

A hacker sends a fake or "spoofed" email that appears to be from a trusted company.

The email usually instructs the user to login to verify information, and contains a link.

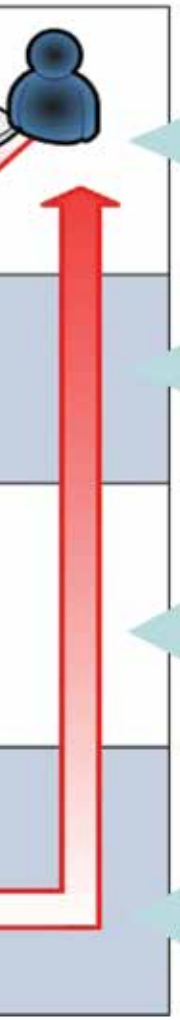


The link in the email directs the user's web browser to a fake website operated by the hacker.

The fake website looks exactly like a companies real website, and requires the user to login.

Any information the user enters into the fake website is immediately delivered to the hacker, which they can use to access the user's accounts.

hing Works



Exploiting people's trust

Websites are easy to set up and register a believable Domain name

Website publication can be done with tools that can be found on the internet, or a simple web browser

"Phished" information can be used by hacker before victims are aware personal information was stolen

Help!
I think I've been Phished!

Anti Phishing Quick Reaction Drill

- Change your password immediately at the real website:
  - Type the website name in your browser's address bar.
  - Sign into your account and click the "user profile" or "change password" link.
  - Follow the website's instructions to change your account information and password.
- Click the "contact us" link found on most websites and inform them about the phishing attack you just experienced.
- If you are using a government computer, contact your local Information Assurance Officer and servicing Network Enterprise Center (NEC).

Recognizing & Avoiding Email Scams
https://www.cisa.gov/sites/default/files/publications/emailscams_0905.pdf

HQDA Antiterrorism Division
Email: usarmy.pentagon.hqda.list.aoc-at-division@army.mil