Defend Yourself!

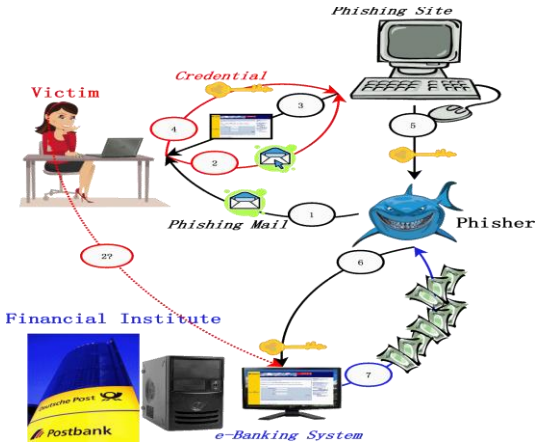
Fraudulent solicitations are now being spread using the power, speed, and reach of the Internet.

Don't Be a Target: When in doubt, **delete!** Be suspicious of unsolicited e-mail—even if it appears to be from someone you know. Scammers have tricks and tools with which they are actively trying to defraud you. Defend yourself!

Don't Take the Bait: Best wishes for love and prosperity? Don't be fooled. Defend yourself!

Dodge the Net: Use your work e-mail at work and your personal e-mail at home. Create a free e-mail account for any questionable communication; keep your primary e-mail account clean. Defend yourself!

Don't Get Hooked: Never reveal personal information, give money, or thoughtlessly divulge your identity. Defend yourself!



Questions? Need More Info?

Visit these websites:

AE-ITT
Army in Europe Information Technology Training

United States Army Europe
Information Technology Training
Program
https://aeitt.ext.eur.army.mil

Information Assurance Program
Management
https://intranet.eur.army.mil/hq/iassure/SitePages/Home.aspx

U.S.ARMY
EUROPE

United States Army Europe
http://www.eur.army.mil

This publication is available at
https://aepubs.army.mil

AE MISC PUB 25-2A ● 18 JUL 16

Cybersecurity Program Management

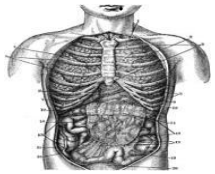
"Defend Yourself!"

Internet Fraud

Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command, Europe Region
Sembach, Germany

Anatomy of an Internet Scam



- **Phishing Grounds:** Scammers choose their targets. Often the target audience is everyone who has an e-mail account or a Facebook profile. Sometimes a scam artist will be more selective.

- **The Bait:** Internet scams are effective only when someone is ready to take the bait. As long as there are people who are overly trusting, lonely, or greedy, there are potential victims, given the appropriate bait.

- **Casting the Net:** Scammers may format e-mail messages to look legitimate (that is, as if they were coming from a good friend or coworker). They may also "spoof" a website that looks like another legitimate website and program it to accept your data, your passwords, and your bank-account number.

- **Hooking the Prey:** You are "hooked" once you click on a link and enter personal information, click on a link that activates malware, reply to a spoofed e-mail message and transfer funds to a distant account, or enter your credit-card number and the security code.

- **Reeling It In:** Scammers receive and use your information, use your credit, make cash withdrawals from your bank accounts, and assume your identity.

Phishing Grounds

Internet Fraud occurs in chatrooms, on dating sites, in e-mail, on message boards, on websites—essentially any location with social interaction and the potential for information exchange between two or more people. The group targeted may be very general. With *Spear Phishing*, the scam artist targets specific groups such as Government workers, deployed Soldiers, or the employees of a corporation. In these cases, the scammer will design an attack that is most effective against the target audience and supports the scammer's goals (for example, to obtain money or information).

The Scam may involve just a website on the Internet that draws in victims, but usually e-mail messages are sent to bait victims. Scammers harvest e-mail addresses to reach the largest audience possible. Many tools are available to harvest e-mail addresses, but the simplest method is to purchase e-mail addresses from spammers or to trade lists with them. Once you use your ".mil" e-mail account to reach out to a non-Government network (for example, when sending a reminder from work to your personal e-mail address), your .mil e-mail account becomes vulnerable.

Love—The old con-artist trick, the *sweetheart swindle*, takes on a new personality when carried out on Internet dating sites. The perpetrator forms a relationship with victims and convinces them to send money or provide private information. On a dating site, it is not unreasonable to assume that some, if not most, members have some degree of loneliness. The scammer needs only a few members who are also overly trusting. The victim may submit because of the promise of companionship and perhaps love.

Money—*Greed* makes many web users

careless. The promise that some (previously unknown) rich uncle has died and left millions (just for you!) is enough to push some to take a chance and send the $1,000 "handling fee" to an unknown address. The thought of millions just around the corner will convince some to overlook the misspellings in the e-mail message or the fact that neither your mother nor father had a brother. Maybe it's an uncle who no one wanted to talk about—because he was RICH!

Cast the Net, Hook the Prey, and Reel Them in

Using the harvested e-mail, sent to most people with spoofed websites in place, the scammer has all the pieces in place. Only a small percentage of people need to fall for the scam. Multiplied by the sheer magnitude of spam e-mail sent, the fraudster has potential for great success and ample incentive to spam and scam again. ***The net is cast!***