Trainers - keep this page and provide only the following page to your staff

Bulletin Guidance for Managers & Supervisors

This bulletin is provided to facilitate talking with your employees about their data security responsibilities. Often, the best time to review the subject is during regular weekly or monthly meetings. This month's data security topic is phishing attacks.

Trainer Notes

Phishing attacks are used to both solicit sensitive information directly and to entice victims into unknowingly downloading and installing malware. Cyber thieves are using more sophisticated tactics making it more difficult to distinguish phishing emails, phone calls, and text messages from legitimate ones. The scams are commonly designed to appear to be from, among others,

- Banks, financial Institutions, or creditors
- E-mail service providers
- Charitable organizations
- Friends in need
- The IRS
- The police
- The USPS, Fedex or UPS
- C-Level executives within your organization

The message often includes:

- A legitimate-looking design that mimics the spoofed organization
- An urgent request for information, often sensitive
- A promise of reward if instructions are followed, or penalty or punishment if they are not

On next page we provide guidance to help defend against such attacks.

Talking Points

- Remind employees about malware dangers (keyloggers, compromised systems, etc.) and how to avoid becoming a victim. Remind employees to inform IT immediately if they suspect an attack.
- Have employees share their own experiences with the group, such as what kind of phishing messages have they received, how they recognized them, etc. This helps build awareness throughout your team.

Additional Resources

Information about known phishing attacks is available online from groups such as the Anti-Phishing Working Group, www.antiphishing.org.

How to Recognize Scams

Over time, phishing attempts have become more sophisticated with increased quality of imitating a genuine email. Be aware of these warning signs:

- The message is unsolicited and asks you to update, confirm, or reveal personal identity information (e.g., SSN, account numbers, passwords, protected health information).
- The message creates a sense of urgency.
- The message has an unusual “From” address or an unusual “Reply-To” address.
- The (malicious) website URL doesn’t match the name of the institution that it allegedly represents.
- The message is not personalized. Valid messages from banks and other legitimate sources usually refer to you by name.
- The message contains grammatical errors.

Phishing Email Dos and Don’ts:

DO call a company that you received a suspicious email from to see if it is legitimate, but DO NOT use the phone number contained in the email. Check a recent statement from the company to get a legitimate phone number.

DO look for a digital signature/certificate as another level of assurance that senders are legitimate. Digitally signed messages will have a special image/icon at the subject.

DO adjust your spam filters to protect against unwanted spam.

DO use common sense. If you have any doubts, DON’T respond. Ask your department IT representative.

DON’T open email that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try other means.

DON’T ever send credit card or other sensitive information via email.

DON’T click the link. Instead, phone the company or conduct an Internet search for the company’s true web address.

DON’T open email or attachments from unknown sources. Many viruses arrive as executable files that are harmless until you start running them.