Bulletin Guidance

Trainer Notes

This month's bulletin reminds employees of the importance of understanding the threat that can come from emails and the steps employees can take to keep their organization's data secure.

Talking Points

- Remind employees that email addresses and phone numbers can be spoofed (faked). If someone contacts you via text, email, or phone, the address or phone number alone cannot be relied on to identify the true identity of the person or organization.
- Contact IT immediately if they suspect an attack.
- Have employees share their own attack experiences with the group. What kind of phishing messages have they received, how did they recognize them, etc.? This helps build awareness within your team.

DATA SECURITY TRAINING BULLETIN

Best Practices for Email

Social engineering and phishing attacks have become commonplace and effective. Phishing attacks rely on human tendencies to trick people into revealing sensitive information, downloading malware, or committing financial fraud. Phishing emails and other social engineering schemes are increasingly sophisticated and harder to recognize.

With the advent of “spear-phishing” thieves are diligent in gathering background information on their targets from social media, blogs, and other websites to appear more credible when crafting their scams. Attackers then play on emotional triggers including fear, urgency, and authority to trick their target into making impulsive decisions without thinking.

Common phishing examples frequently come from sources with authority, such as: Banks, financial institutions, the IRS, police, FBO, UPS, or executives within the organization.

Best practices to use when surfing through daily emails:

Critical Thinking

Don’t take everything at face value. Before you open and click an email, go through these questions:

- Is the email from someone I recognize?
- Am I expecting the email?
- Are the requests of the email reasonable?
- Is the email using emotional gauges like fear or urgency to entice an action?

Always Hover

Before clicking any links in the email, hover your mouse over the link and the actual URL will appear. Double check to make sure the real URL is leading you to the right place. You don’t want to be clicking a link to ju-spandoo.de/82359/index.html. Hackers will also try to spoof the URL to look like the legitimate address. You want to investigate to make sure the domain is the same as the sender of the email.

Do Not

- Copy and paste the link into the URL section of your browser to check it. That’s the same as clicking the link.
- Forward a suspected malicious email to other people. You don’t want to further the potential damage, especially within your organization.
- Open the malicious email on your mobile devices. They are not immune to malware and viruses.
- Solely rely on antivirus software. AVs protect against viruses with known signatures, but are susceptible to new malware that goes undetected.