Training Bulletin Guidance— Phishing

Trainer Notes:

Phishing emails remain the most common way hackers access your organization's environment.

Why? Because it's easier to get past humans than technology. Software manufacturers are releasing more secure software and it's increasingly difficult and expensive for hackers to exploit software vulnerabilities. On the other hand, it's cheaper (and easier) to simply trick a user into clicking a malicious link or opening an attachment in a phishing email to gain access into your organization's environment. Therefore, hackers are focusing on making their phishing emails harder to spot.

To help prevent successful phishing attacks on your organization, train your employees to spot a phishing email. Also, implement a social engineering awareness policy which, among other things, requires employees to take regular training on how to spot and report social engineering attacks like phishing emails. Organizations can also perform company-wide mock phishing exercises and conspicuously mark all external emails to aid employees in identifying a potential phishing email.

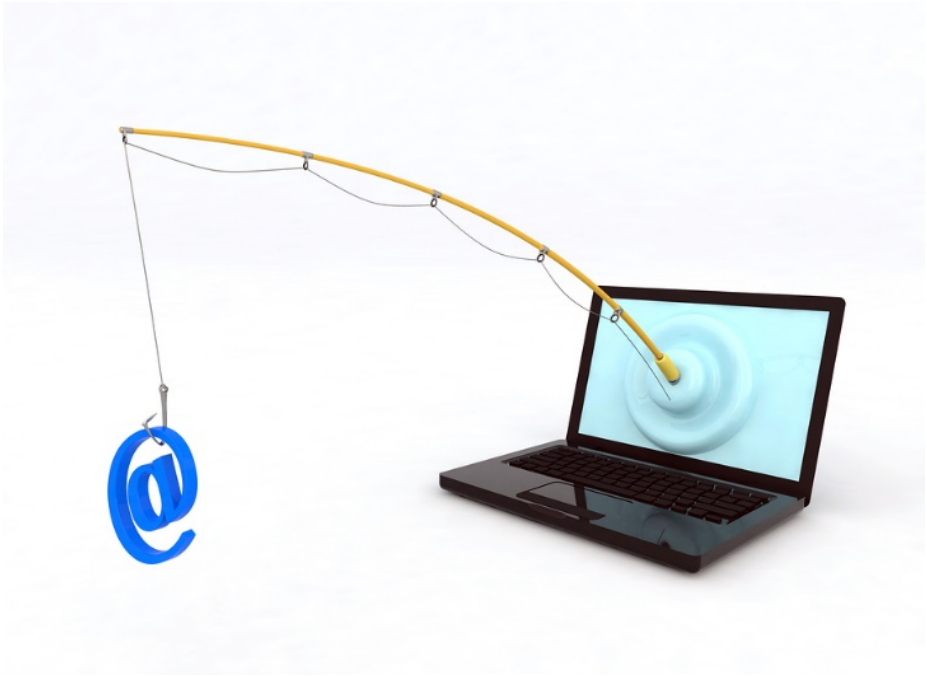
IMPORTANTLY, no one is perfect and even the most vigilant employees may fall victim to a phishing email. Enabling multi-factor authentication will help protect against account takeover even if credentials are compromised in a phishing attack.

Distribute the following page to your employees and discuss the below talking points to train them to recognize a phishing email!

Talking Points for Your Employees:

- Explain social engineering and phishing to your employees.
- Describe the damages that phishing emails can cause your organization.
- Tell employees the procedures to follow after receiving a suspected phishing email.
- Remind employees that cybersecurity is a team effort. Every employee counts, and participation from everyone is needed to maintain a good security posture.

CYBERSECURITY TRAINING BULLETIN



THE IMPORTANCE OF RECOGNIZING PHISHING EMAILS

Phishing emails remain the most common way hackers access your organization's environment. So – recognizing phishing emails is important!

Common Signs of a Phishing Email

- Your name is missing as an addressee in the email.
- Be suspicious of any email that requests your username/password or any personal information.
- Bad grammar and poor spelling.
- Short emails that threaten or otherwise create urgency to act.
- Hover your mouse over any website links and you should see the actual hyperlinked address. If the actual address is different from the displayed address, the message is likely malicious.
- Use common sense. If it's too good to be true, then it's likely not!
- Phishing emails are getting harder to spot. When in doubt, **ASK** before clicking on a link or opening an attachment.
- If you get an unusual email from a co-worker, call the sender and verify the email.

What if you get a phishing email?

Follow your company's policy on reporting phishing emails. If you don't know what to do, ask your supervisor or someone from IT. If you think you received a phishing email, report the email to the appropriate company personnel. Reporting a phishing email might prevent a co-worker from falling victim to the same email!