Objective 13

Recognizing Phishing and Other Internet Scams

GETTING STARTED WITH TECHNOLOGY

WHAT YOU NEED TO KNOW

What is phishing?

Phishing (sometimes referred to as “spoofing”) targets individuals (or groups) and contacts them by phone, text, email, or social media. Phishing uses this communication to pose as a legitimate business or institution. The attempt typically is to get the individual to provide sensitive data. The information they’ll look for could be personally identifiable information, bank or credit card details, or passwords. Some will attempt to get their targets to download malicious software (malware) to infect a device or infiltrate the entire network.

Cybercriminals using phishing are highly successful. Nearly 20% of individuals contacted by a phishing attack through email can get their victim to click on a link within the body of the message. By clicking the link, an individual may inadvertently provide access to a local computer or even an entire network.

In a business environment, one individual opening a nefarious email or clicking the wrong link in a message can breach an entire business network. Phishing accounts for 90% of all breaches that organizations face.

THINGS TO KEEP IN MIND

Scammers and other cybercriminals have gotten more sophisticated in their digital attacks, but that does not mean that all are flawless. Because such a great deal of phishing attacks stem from email messaging, there are some common red flags to look for.

Below are some of the warning signs AT&T uses to help consumers avoid falling victim to a phishing scheme.

- An unfamiliar tone or greeting or unusual request
- Grammar and spelling errors
- Generic customer names or undisclosed recipients
- Inconsistencies in email addresses, links & domain names
- Suspicious attachment links in email
- Recipient did not initiate the conversation
- Request for credentials, payment information or other personal details

BEST PRACTICES

Avoiding phishing scams

- **Educate yourself:** Becoming familiar with what a phishing attempt looks like can help avoid many of the traps.
- **Add a layer of technology:** Add an antivirus software to help increase the level of protection for a network or personal information
- **Be a smart web browser:** If a website is questionable and you are unsure of the legitimacy of the destination, using a tool like McAfee® SiteAdvisor® will show search results and whether sites are safe to visit.
- **Check link and image destinations:** By right clicking a link (image or text) and pasting it into a word processor or generic note application, the actual destination website can be viewed without actually pasting the malicious link into a web browser.

What should be done if a suspicious email or message is received?

- **Report it:** If you believe you've received a phishing attempt, report the incident. Reporting potential phishing attacks can help others not fall victim.
- **Consider your logins:** If the scam attempt makes you feel uncomfortable with your data, consider changing any potentially compromised passwords. Updating passwords can eliminate some stress in scamming instances where online data has been breached.
- **Delete it:** After you've reported the message, delete it, and add the sender's email address to a junk category. This should eliminate that specific email address from sending messages. Don't click on any links or images in the message.

RESOURCES

Report Phishing Campaigns to
reportphishing@antiphishing.org

Federal Trade Commission Report Fraud Site
https://reportfraud.ftc.gov/#/assistant

How to Recognize and Avoid Phishing Scams
https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Identity Theft Website
https://www.identitytheft.gov/#/Info-Lost-or-Stolen