Click Wisely

A MINI TRAINING SESSION FOR LOSS PREVENTION

Quick Take on Data Security

Phishing and Social Engineering

TRAINING OVERVIEW AND OBJECTIVES

Overview: Covers definition of social engineering—including phishing—common attacks, and methods to identify and avoid them.

Purpose: Train employees about the basics of phishing and other social engineering attacks to help prevent data compromises or breaches.

Preparation:
- Read and become familiar with this Quick Take. *Change as needed to reflect procedures and personnel in your department.*
- Review your current IT practices and recommendations if a suspicious message occurs and revise the Quick Take script to follow those procedures.
- Consideration should be given to situations where IT may not be available for contact.

Handouts: Quick Review of Data Security: Phishing and Social Engineering

What Is Social Engineering?

Social engineering is the use of social skills and psychology to trick individuals into sharing sensitive, valuable or private information. One of the most common social engineering attacks, called phishing, uses email. But social engineering attacks can also be by phone, called vishing, or in person. An example of a phone attack could be someone claiming to be a member of IT asking for your password to update a system to prevent data loss. In person cons often involve tricking someone into giving passwords or plugging in flash drives to a computer and the like.

However, the most common social engineering attack is phishing, the one carried out via email. It usually refers to deceptive messages sent with the intent to trick people into clicking on malicious links that install viruses or other malware, or into responding with sensitive information. A common example is someone sending a message pretending to be from IT asking for a password or to click on a link to update equipment. [*Instructor Prompt:* Ask the group to offer additional examples]

Numerous cases of data breaches have occurred where hackers gain unauthorized access to systems. Local government entities are a main target. Hackers want to steal citizens' and employees' personal data, disrupt government websites from functioning and even desire to affect election results, among other aims.

IT professionals work to protect our systems, but it takes all of us doing our part to keep our systems and data secure. Please pay attention.

Recognizing Social Engineering Attacks

To prevent social engineering attacks, they must be identified. Fortunately, most attacks have the same characteristics. If a message or conversation has one or more of these features, you should carefully review it.

Social engineering attacks often include:

- **Requests that require a fast response or crucial time window:** Social engineering attacks rely upon a person not asking for confirmation or checking with others prior to acting. Therefore, immediate responses are demanded.
- **Threats:** This goes along with rushed requests. There are often negative consequences implied if the request is not completed quickly. Threats of fines, denied access, missed opportunities for easy money or employment termination are common.
- **Unsolicited messages:** Social engineering attacks are not typically in response to a request or other previous communication. Receiving an unsolicited communication should raise suspicions.
- **Requests for sensitive information:** Most attacks ask for passwords, login information, Social Security numbers, bank account numbers, credit card information or other data that is typically kept private or confidential. Requests for this information from any source should be treated with suspicion.
- **For emails specifically, the following should be treated with suspicion if:**
  - The sender's address is in a different format than the rest of the organization. For example, all emails within the organization follow the format of "firstname.lastname@countymn.gov," but the message claiming to be from someone within the organization is different.
  - There are frequent misspellings and poor grammar. Many attacks originate in non-English speaking parts of the world, so English mistakes are common in these attacks.
  - The message asks users to click on links or open attachments.
  - If anything sounds too good or too bad to be true. For instance: "Claim your tax return now," "We have your kids," and so on.
  - The message contains outrageous or sensational headlines or imagery that entices you to click on them. Avoid clicking on any of these "clickbait" items if you receive them in an email or encounter them online.
  - It is in a spam/junk email folder. Spam refers to junk email that typically consists of unsolicited bulk commercial emails. Many IT departments and email providers have filters that automatically screen spam messages. If a message is in the spam folder, it can be a clue that it may not be legitimate.
  - There is a vague greeting and sender. Often bulk phishing attempts do not send messages directed to individual people. Messages may start with the "attention" or other generic words or phrases. Similarly, messages that end with a title or vague location should also be viewed with suspicion, for example, "web administrator" or "help desk."
- Hovering the mouse cursor over the link shows a different Web address than the indicated link. [*Instructor Prompt:* Can use the handout for the additional activity as an example]

Prevention

If a message has one or more of the elements above you should:

- Contact IT
- Follow IT directions
- Do not open the message, click on any links or items or follow any instructions in the message, such as to send confidential information or passwords.
- Forward requests for private information to the responsible authority for your organization.

DISCUSSION QUESTIONS

- To whom should we report suspicious messages or conversations?
- What do we do if we cannot contact IT or if they are not available?

ADDITIONAL ACTIVITY

- Review Sample Phishing Attack activity together to find the common warning signs.

Phishing and Social Engineering Session Planning and Review

Trainer	Training Date
Department(s)	

TRAINING GOALS

- Employees understand what phishing and social engineering is.
- Employees are aware of methods to recognize and prevent phishing and social engineering attempts.
- Employees know what to do if they encounter a suspicious message or request.

RESOURCES

- "Trustworthy Email (Publication 800-177)," National Institute of Standards and Technology, NIST.gov
- "Security Tip: Avoiding Social Engineering and Phishing Attacks," United States Computer Emergency Readiness Team, US-CERT.gov
- Report Phishing Sites, United States Computer Emergency Readiness Team, US-CERT.gov
- "Phishing," Federal Trade Commission Consumer Information, Consumer.FTC.gov
- "Malware" produced by Federal Trade Commission Consumer Information, Consumer.FTC.gov

REVIEW

Did the training meet the stated goals?

[add comments here]

How can the training be improved?

[add comments here]

TRAINER COMMENTS

[add comments here]

Attendance Record

Training Session Phishing and Social Engineering

Trainer Training Date

Participant Name (printed)	Participant Signature