NIRMA
Serving County Government

TODAY'S SAFETY TALK – TRAINING SESSIONS TO PREVENT INJURIES AND INCIDENTS

TAKE A MINUTE FOR YOUR SAFETY

PHISHING AND SOCIAL ENGINEERING

Social engineering is the art of deceiving, manipulating or influencing a person into sharing information or taking action that is not in their best interest or the best interest of their organization. The social engineer will then use the sensitive information for nefarious purposes or to gain access to your network and install viruses or malware. Ransomware attacks are becoming more prevalent and organizations are forced to pay a ransom to recover access to their data. Local government has become a target of hackers. This safety minute will help you identify and avoid phishing attacks.

Types of Attacks

Phishing is email-based social engineering targeting an organization. Spear Phishing is similar, but it is aimed at a specific person or role.

USB attacks are when a person uses a thumb drive to install malware on your computer. This can be done in person if your computer is left unsecured or they can simply leave thumb drive lying around near a business and hope someone plugs it in to see what is on it.

Tailgating is when a hacker bypasses physical security by following an authorized person inside.

Text-based social engineering is referred to as Smishing, while over-the-phone-based social engineering is referred to as Vishing.

Red Flags

Red flags are signs of danger or that something is wrong. Trust your gut instincts. If something doesn't seem right, don't click the link, don't download the item, don't open the attachment. Call the sender to verify. We are going to cover some common red flags that occur in social engineering emails.

From

An email from an address you do not recognize or an email from a person you recognize but the email is unexpected or out of character.

To

You are one of multiple people copied on an email and you don't recognize any of the other people it was sent to.

Date/Time

An email you normally receive during business hours was sent in the middle of the night and the person sending it has never sent you an email at that time.

Subject

The subject of the email does not match the content of the message or is irrelevant. It's an email about something you never requested or a receipt for something you didn't purchase. The subject line simply says "Re:". Again, trust your instincts.

Hyperlinks

Look very closely at hyperlinks for misspellings or for a hyperlink asking you to take an action. When you hover your cursor over the hyperlink, the link address is for a different website.

Content

The sender is asking you to click on a link or open an attachment. The email is asking you to look at a compromising or embarrassing picture of yourself of someone you know. You have an uncomfortable feeling, or it just seems wrong. Again, trust your instincts.

Attachments

Any attachments that you were not expecting or are included in an email containing any of the red flags listed above.

We've all heard the term a "culture of safety." Cyber security experts are now recommending a "culture of security." What they mean is this, from now on we need to scrutinize every email we get, look at each email as if it is a scam or a phishing attempt until we can prove that it isn't. Before you click on any link, open an attachment, or download anything, you need to consider the fact that it could be malicious and act accordingly.

NiRMA
Serving County Government

TAKE A MINUTE FOR YOUR SAFETY
SIGN-IN SHEET

COUNTY/AGENCY: ______________________________

DATE OF TRAINING: ______________ **PRESENTER:** ______________

TOPIC(S):______________________________

Print Name	**Signature**
1______________	______________
2______________	______________
3______________	______________
4______________	______________
5______________	______________
6______________	______________
7______________	______________
8______________	______________
9______________	______________
10______________	______________
11______________	______________
12______________	______________
13______________	______________

14________________________________ ________________________________

15________________________________ ________________________________

16________________________________ ________________________________

17________________________________ ________________________________

18________________________________ ________________________________

19________________________________ ________________________________

20________________________________ ________________________________

21________________________________ ________________________________

22________________________________ ________________________________

23________________________________ ________________________________

24________________________________ ________________________________

25________________________________ ________________________________

26________________________________ ________________________________

27________________________________ ________________________________

28________________________________ ________________________________

29________________________________ ________________________________

31________________________________ ________________________________

32________________________________ ________________________________

33________________________________ ________________________________

34________________________________ ________________________________