CYBER SECURITY AWARENESS MONTH

WEEK 3: Recognizing and Combating Cybercrime

Phishing Emails:

How to Avoid the Hook When It Looks So Trustworthy

Phishing (pronounced "fishing") is a term used to describe a certain type of identity theft. Criminals send out emails as bait for unsuspecting consumers designed to resemble popular or trustworthy sites and companies. The goal is to lure the victim into clicking a malicious link or opening an email attachment. The link or attachment may threaten that an account will be deleted or altered if personal information is not verified, thus luring the individual to divulge personal information. Some attachments may contain a virus or malware for hackers to exploit in the future. And it's not just computers that are vulnerable; there are even some reported cases of mobile phones being attacked through phishing emails. Many are very convincing and well loaded with data, graphics, or even personal information to look as legitimate and enticing as possible. Some phishing emails even use a target's name, title, company, work phone number, and more.

Many phishing emails include some sort of threat to grab the reader's attention and cause concern. One example may be a threat that your account will be terminated or deleted if you do not respond.

A link in the email may take the victim to a legitimate *looking* website that asks for personal information in order to "verify" the user. Other times it may list a phone number to call. In reality, the criminals are gathering information to use for malicious purposes.

The following is a hypothetical example of a phishing email:

```
Dear ABC Email Subscriber.

This mail is to inform all our users that we will be maintaining and upgrading
our website in a couple of days from now. As a subscriber you are required to
send us your email account details to enable us know if you are still making
use of your mailbox. Be informed that we will be deleting all mail account that
is not functioning to enable us create more space for new users. Click on the
following link abcemailservice.com and send your mail account details which are
as follows:

*User Name:

*Password:

*Date of birth:

Failure to do this will imediately render your email address deactivated from
our database.

Thank you for using ABC Email Services
```

Cyber criminals are counting on users acting out of urgency and fear (loss aversion) that this type of message will normally produce. The reader reacts by clicking on the link or calling a given phone number in order to protect their account. As a result, the victim gives up personal information that is then used by the criminal to steal the victim's identity and may cause serious damage.

Every email you receive should be read with discretion, especially if that email is asking for information.

Phishing emails look legitimate because they are designed to deceive. They may appear to come from companies you frequent or have accounts with, or even from your friends. Many even include company logos, graphics, or quotes to add to the deception. Here are some things to look for to protect yourself and make a better decision.

1. **Is there a threat?** Many phishing scams hook the reader by threatening some sort of action such as deleting your account if you do not respond. In the example above, th email service is threatening to delete the account if the subscriber does not respond.
2. **Are there links in the email?** Always be suspicious of links embedded in the email. Without clicking, hover your mouse over the link. A pop up window should appear with the link's web address. If the web address does not match the company or website, DO NOT CLICK!
3. **Are there spelling errors?** Notice in the last sentence that the word immediately is misspelled. Large companies usually have staff that are hired to edit and correct such mistakes. Criminals are not normally known for their grammar skills.
4. **Is it asking for personal information?** Are you being asked to provide personal account information? Even if the email lists a phone number to call, do not give out personal information unless you are absolutely positive that the person you are dealing with is legitimate.

So how can you know if an email is truly legitimate and a threat is real?

1. **Call the source.** If you get an email from a financial institution that you do business with, call the company directly. This way you can be certain that you are talking to a representative from the actual corporation. They can answer any questions you might have and let you know if there is an issue. Most legitimate banks and financial institutions will not request information via email.
2. **Check the business's website.** If a company has been hacked or realizes that a threat has been made to users using the company's logo or name, a statement may be posted on the company's website.
3. **Report it!** It is important to stop the crime as soon as possible to protect yourself and others. If possible, you should inform the company being impersonated that the scam is taking place. Another way is to report it to the government-operated website http://www.us-cert.gov/nav/report_phishing.html. This site provides a way to send a copy of the email or the URL to the website so that they can be examined by experts.

What if you receive a phishing email? The answer is simple, delete it and don't click on any links. If possible, report the email as noted above so the criminals are identified and others may not fall victim.

The following video offers more information on recognizing and avoiding phishing emails.

https://www.youtube.com/watch?v=9TRR6lHviQc

CLASSROOM EXTENSIONS

Read over the following websites and answer the questions below. (These sites are safe, trust me)

- https://www.microsoft.com/en-us/safety/online-privacy/phishing-faq.aspx
- https://www.cnet.com/how-to/how-to-check-if-a-web-site-is-safe/
- http://www.phishing.org/history-of-phishing/

1. What is meant by phishing? Why is it spelled this way?
2. According to Internet records, when was the first published mention of "phishing"?
3. What can you do to prevent identity theft from a phishing email scam?
4. If you receive an email that appears to be from your bank and has the bank's official logos and graphics, can you assume that it is legitimate and safe to respond? Explain.
5. What are some ways you can tell that an email is potentially a phishing scam?
6. What should you do if you believe an email may be a phishing scam?
7. If you were asked to speak at the next PTA/PTO meeting and discuss what you have learned about phishing emails, what would you say in your speech?