Prevention - Phishing Teachers Guide

Disclaimer – This was prepared as a guide to the slides. If it does not suit your students' learning style feel free to change it up. It is intended to help lead the discussion around password safety

Show: Slide 1: Phishing Prevention Title Slide

Say: "Today we are going to go over Phishing, what it is and what dangers it poses."

Show: Slide 2 – Warm Up

Ask: When you hear the work Phishing, what comes to mind?

Expect answers like

*catching fish at the lake

*fishing for answers (phrase)

Ask: Do you notice that it is spelled differently from what we would normally think of?

Ask: This is so we know this is something relating to computers. Does anyone know how it could tie in?

Show: Slide 3 – Today's Goals

Say: Today we are working towards three different goals: Identify features of a phishing attempt in an email/text message, Differentiate between legitimate communications and phishing attempts, Execute the steps necessary to report and delete phishing attempts.

Show: Slide 4 – Phishing Overview

Say: To give us a brief overview of phishing, let's watch this video

Show: Slide 5 – Social Engineering Overview

Ask: So what is social engineering?

Say: From the video we learned that social engineering is when someone tricks you into sharing personal information about yourself. Another important thing to know is that phishing, today's learning goal, is a form of social engineering.

Show: Slide 6 – What is Phishing?

Ask: Now that we know a little background, what is phishing exactly?

Say: Tying back to our opening question, remember when some of you said you like to go fishing with your family? Well, online phishing is when the attacker sends a fake message designed to "bait" (just like fishing) a human into revealing sensitive information or to install a nasty program on their computer.

Show: Slide 7 – Ways attacks are delivered
Say: That sounds scary, right? There are many different types of communication we need to watch out for. These include phone calls, emails, text messages, calendar invites, and even game server chats.
Ask: Has anyone in this room received a type of phishing attack before?

Show: Slide 8 – Tactics and techniques
Say: Within the types of attacks, specifically emails and text messages, there is usually a link or download that the message is trying to get you, as a user, to click.

Show: Slide 9 – Phishing consequences
Say: If you do click one of these links or documents, it could add malware to your device, steal your personal information, or steal your password.

Show: Slide 10 – Recognizing phishing attempts
Ask: How do we distinguish a real email/text from a phishing email attempt?

Show: Slide 11 – How to Build a URL
Say: As you can see we have three pictures of the same url with different parts highlighted. The first part of a URL is what is called the protocol. Most commonly you will see HTTPS, but sometimes you will see HTTP. Be careful without the S, this means the website is not secure and could be malicious.

The second part of the URL is our main focus, which is the domain name. In this case it is Kinsta.com but other common domain names are google.com, amazon.com, gmail.com. This can also be known as the website name. When you see a website name, you want to make sure that you can read it and that the name is spelled correctly.

The third part of the url is what is called the path. If you are familiar with a file explorer when you choose documents and then Readme.txt this would be the path. It works the same way for websites; each page

is stored on a different path. This is also important when trying to detect phishing attempts. You also want to be able to somewhat read what the path says. Safe websites will name their pages “cart” verses “x8ew9hd”.

Now that we know the very basics of how a url is made let's jump into more ways to detect phishing attempts.

Show: Slide 12 – Links/URLs
Say: The first thing to check in a suspicious email or text is a link. On the left you can see that the link looks like it would take you to Amazon.
Ask: If we look closer at the domain name, like we learned about on the last slide, what can you see?
Say: That's right, there are two N's in the word Amazon. That is an immediate red flag even though the website looks real. The next type of links to watch out for are shortened or unreadable links. On the right you can see we have a bit.ly link. The bit.ly is the domain name. The “1vfEgl” is the path.
Ask: Who can remind me of what we learned about paths on the slide before this?
Say: Sometimes these are safe, but you should be wary of them and do not click on them.

Show: Slide 13 – Immediate action
Say: Another red flag when looking at an email or text is if it wants immediate action. Here we can see that it says if you do not click on their link within 24 hours your account will be terminated. You should know that Amazon and other companies will not ever close your account if you do not complete an action. The only time that an account is usually removed is if you, as the customer, ask for it to be removed or closed. If a company is making a change, they will send out mass emails that say something such as “We are making this change on Dec 15th; please watch for this email and follow instructions at that time.” There is no pressure in this and they are giving you lots of advance warning.

Show: Slide 14 – Downloads and documents
Say: Downloads and documents are always suspicious unless you are expecting a friend or family member to send you one. In this example you can see that the text says their account is restricted (red flag) and to click on this random file download (red flag). Why would they not direct you to their actual website?

If you are unsure if this message is real or not, a good option is to go to Global Pay's website and call their customer service phone number.

Show: Slide 15 – Grammar

Say: This example points out many red flags.

Let's start with number one.

Ask: Does anyone know why this would be a red flag?

Say: This is a red flag because they do not know your name. It is a hint that this was sent to many different people. Next we have number two.

Ask: Who can tell me what is wrong here based on what we have just learned?

Say: It is saying that our account is restricted, which we discussed on the Immediate action slide. Numbers three and four go together.

Ask: Can we see what is wrong here?

Say: The grammar is incorrect. Accounts need an apostrophe, and in English we do not put "has need" instead we would put needs. For number five we discussed how to build the URL's. If you look at the link it looks like it points us to the muccu website. However, if we hover over it we can see that it takes us to a completely different link. This is a red flag and you should always hover over links before clicking on them. Finally this email is generically signed whereas usually you see a customer service representative's name.

Show: Slide 16 – Text messages

Say: Text message phishing is becoming more and more popular. The first thing that should set you off is if you have not ordered from Fedex recently and are not expecting a package. The next flag is the URL which we have discussed a couple of times.

Ask: Why is this URL bad?

Say: You are right, we cannot read this url and have no idea what page it will take us to. We would expect a fedex tracking link.

Show: Slide 17 – What can YOU do?

Say: That was tons of information! What can you do as an everyday user to combat fishing and keep from being "baited"? The first step is to always be on the lookout. Remember all of the tips that we just went over. These are the things you want to always keep in the back of your mind. The second is to set

up multi factor authentication. This helps if your password is stolen then they have to go through two steps to steal your information. Finally if you receive a phishing email, you should report it to your school/email provider. This helps them to watch out for more attempts from the same email or to let others know there were phishing attempts sent out.

Show: Slide 18 – How to report Phishing/Junk Mail
Say: Depending on your email provider, there are different spots to look for the place to report a phishing email. Using gmail as an example, on the left you have to click on the three dots from within the email to report it as phishing. In Outlook they have a top bar that includes a Junk dropdown where you can then click phishing to report your email.

Show: Slide 19 – Activity
Teacher choose TestDrive or Kahoo (Online):
https://app.socialmediatestdrive.org/intro/phishing
Kahoot - https://create.kahoot.it/share/phishing-practice/28e1e3e2-8329-45d2-8d0d-3ffd7a5b84d4

Fishing Pole Activity (Unplugged)- See Teacher Instructions

Show: Slide 20 - Wrap Up
Say: You now know how to identify phishing emails and texts, differentiate between real and phishing attempts, and how to report a phishing email.