Eastern Kentucky University
Information Technology

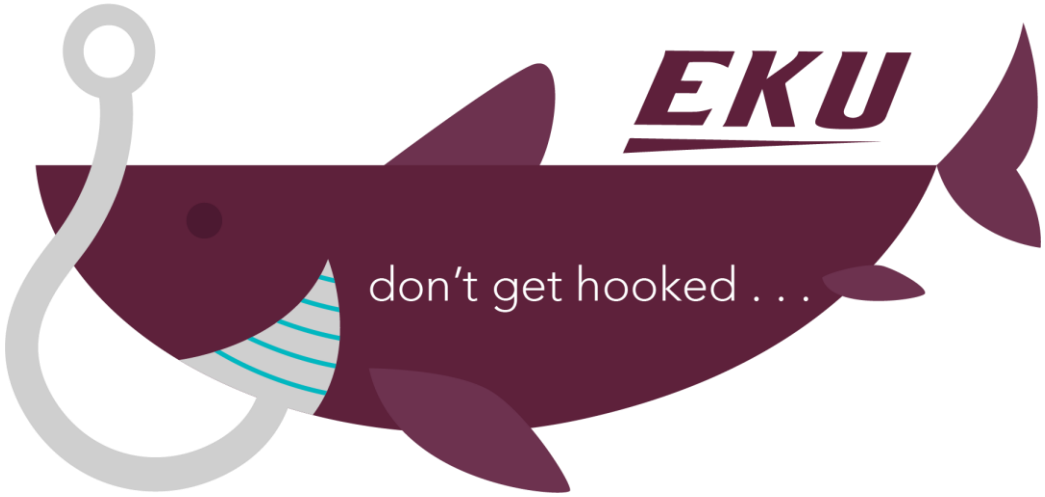
Phishing Training:
You have the power and are our main line of defense!

Last Updated: 5/25/2021

Training Outline

- Section 1: What is phishing?
  - Why this is important
  - Types of phishing
  - Campaigns and themes
- Section 2: How to recognize phishing
- Section 3: How to avoid phishing
  - EKU security measures
- Section 4: How to handle phishing
  - Spam@eku.edu
  - What is you accidently get “caught”?

Section 1: What is phishing?



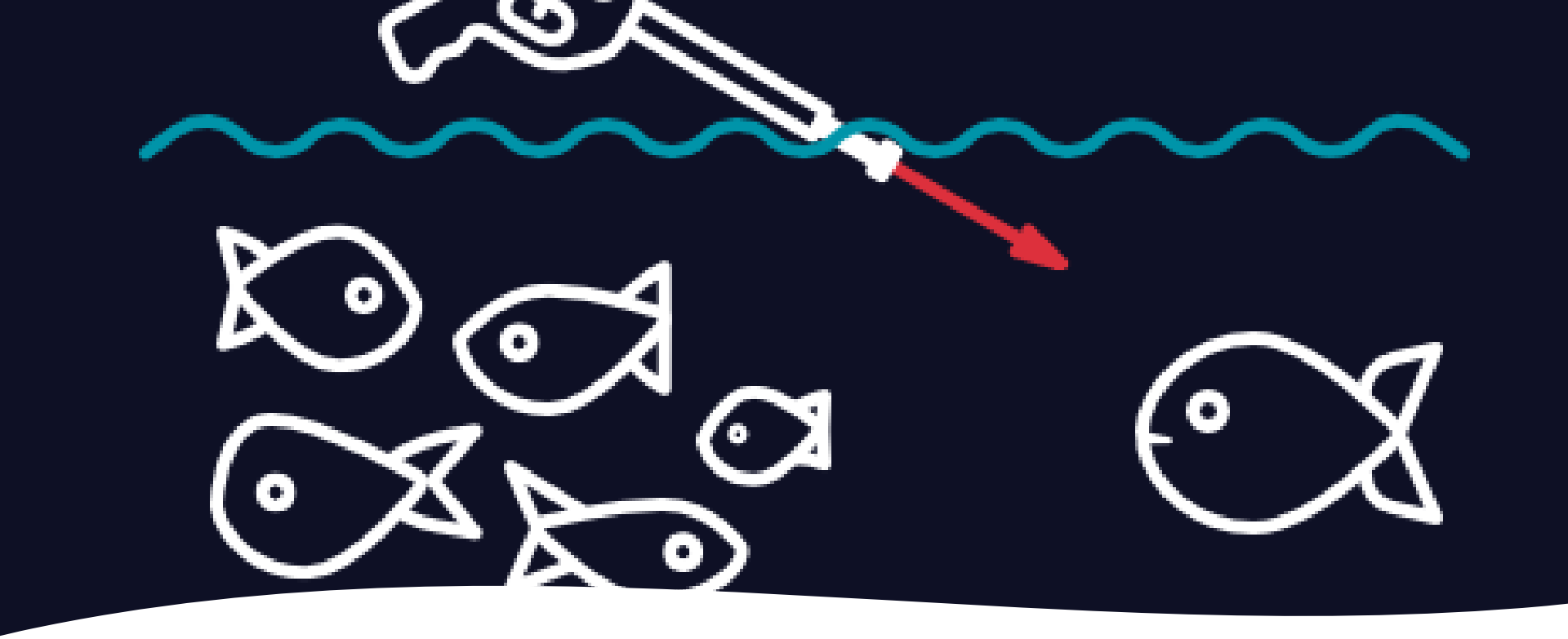
Why is this training important and why should you care?

- This is NOT just a work-related issue
- 97% of users cannot identify sophisticated phishing emails
- The #1 way malware is delivered is via email
- 1.6M is the average amount lost in a successful spear phishing campaign
- 96% of phishing is delivered via email
- FBI's Internet Crime Complaint Center (IC3) found phishing, including vishing, SMiShing, and pharming, was the most prevalent threat in the US in 2020
- 75% of organizations around the world experienced a phishing attack in 2020
- More than 50% of those with a work-related device grant access to their family and friends!

Phishing is…

Phishing is a social engineering scam that "appears" to come from a "trusted" source but "tricks" you into "giving them" personal (private) information or "performing" risky actions.

Social engineering is the art of manipulating people so they give up information or perform risky actions. This can also occur in person.



Types of Phishing

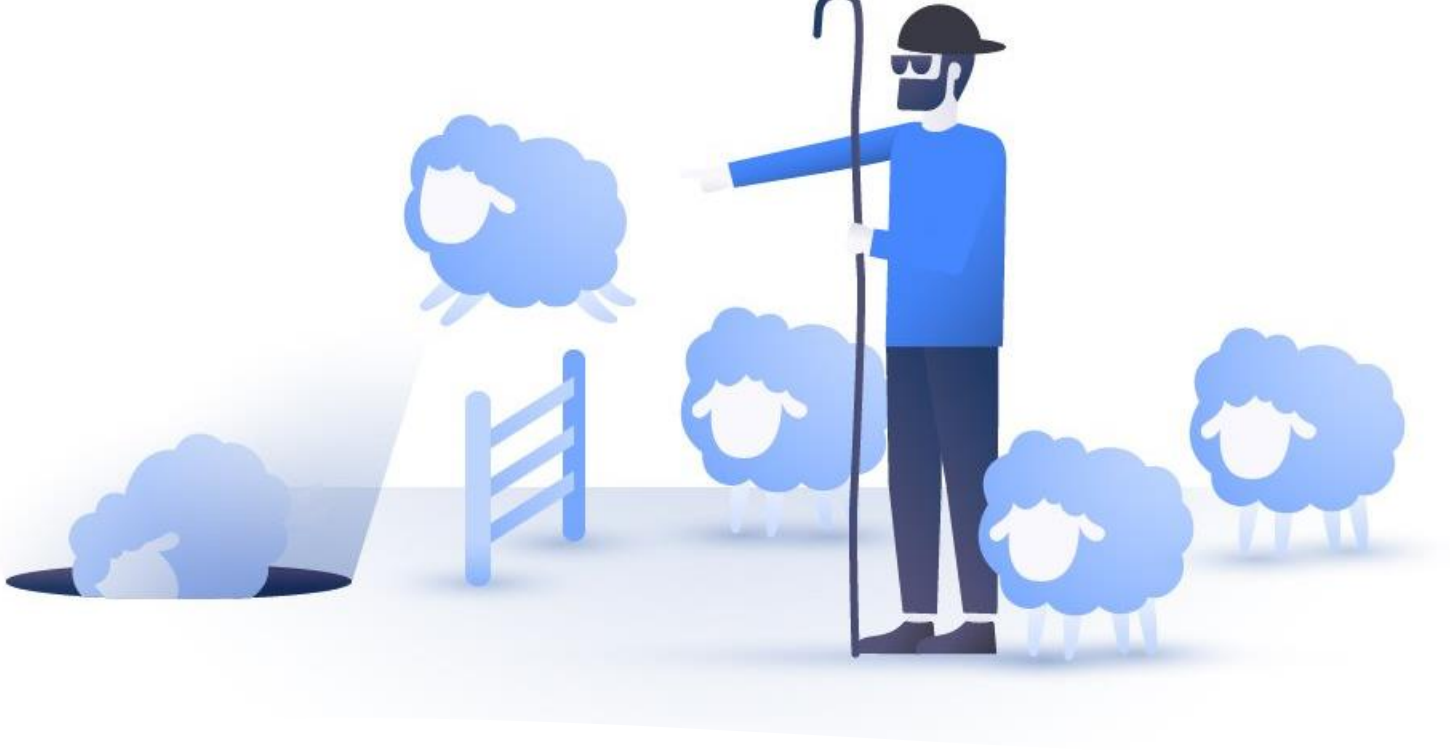
- **Spear phishing**- targets one user at a time. The attackers put a lot more effort into learning about their victims, including the details of their job role and the people they connect with regularly. This enables the attacker to send a highly personalized email that's much more difficult to detect.
- **Whaling**- similar to spear phishing, where it targets top-level executives in your organization (e.g., CIO, CFO, President, VPs) and manipulates THEM into sending high-value wire transfers to the attackers.

Types of Phishing

- **Vishing (voice phishing)** – a type of phishing attack using a phone to trick victims into handing over sensitive information rather than through an email.
- **SMiShing (SMS phishing)** – a type of phishing that uses text messages, tricking victims into handing over sensitive information or clicking malicious links in a text message.

Types of Phishing

- **Angler phishing** – commonly used on social media—fake URLs, ads, websites, posts, tweets, and IMs to persuade people to divulge sensitive information or download malware. This one is commonly used to masquerade as customer service on social media.



Types of Phishing

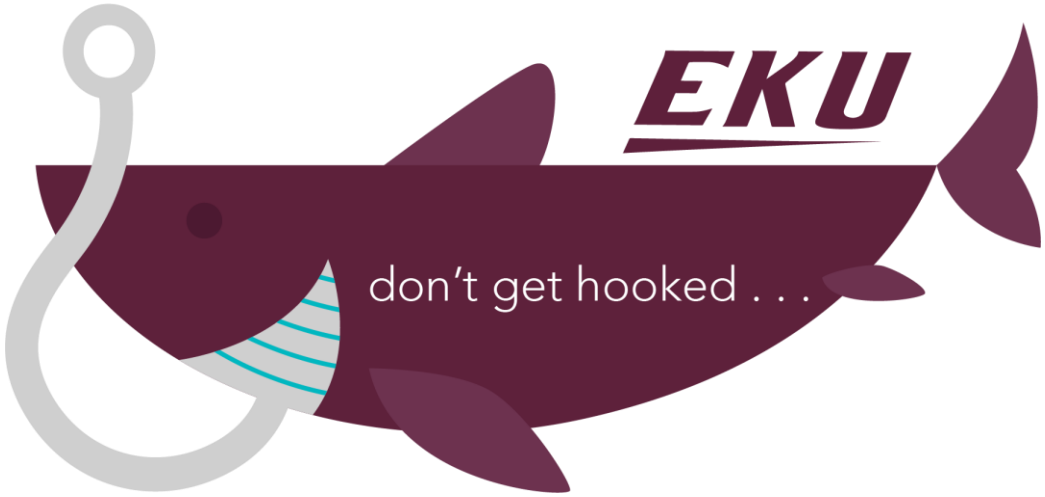
- **Pharming** – a phishing attack without a lure. It is an advanced form of social engineering in which the attackers create a fake website, such as “Microsoft” login portal, and then trick the web server into redirecting targets to their website. This type of attack doesn’t target one person specifically.

Campaigns and Themes

Phishing is often associated with “campaigns” or “themes” with lures commonly around:

- Microsoft requests (Teams, Office 365, OneDrive)
- US or Worldwide disasters\events (Coronavirus advisories, WHO Coronavirus information, 2020 Olympics, earthquakes)
- Shipping notices (USPS, UPS, FedEx, Amazon)
- Sweepstakes
- Other lures (Free month of Netflix; Vacation rentals; Starbucks pumpkin spice; Overdue invoice; Notice of moving violation)

Section 2: How to Recognize Phishing?



Steps to Recognize Phishing

- **Step 1:** Look at the sender's address
  - Hover over or double-click to open it
    - Is it the same email as what you see displayed?
      - No: The message is probably fraudulent or malicious.
      - Yes: Do you know the sender, and are they family, friend, or a co-worker?
        - » How are they contacting you? Work email? Social media? Text? Phone Call?
        - » Attackers have access to families, friends, and co-workers they have attacked successfully or from your social media (or other internet sites) or your address book.

Steps to Recognize Phishing

- **Step 2:** Is there an attachment or link
  - If there is a link\attachment, were you expecting a link\attachment from the sender?
    - Yes: You should be safe to open it
    - No: Reach out to the sender via another method to check if the attachment is legitimate. For example, if they send in a social media IM, email them about it. Don't use the same method because if they are hacked, you'll simply reach the hacker.

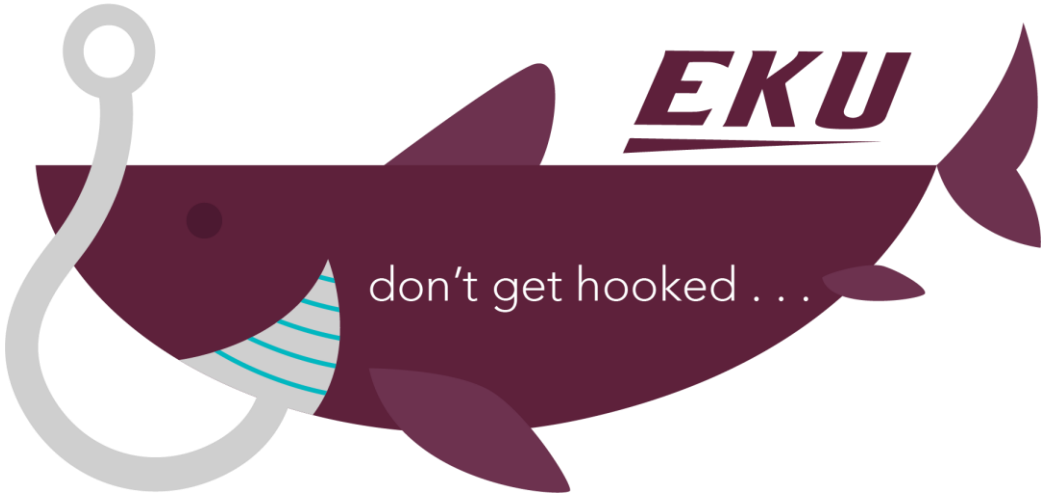
Steps to Recognize Phishing

- **Step 3:** Are they asking for immediate help or actions be taken (giving personal information, performing a risky action)?
  - Yes. Stop and slow down. Reach out (with another method) and ask! Do not be rushed into doing anything!!
  - No. Proceed.

Steps to Recognize Phishing

- **Step 4:** Are they obviously after passwords, financial information, your identity information, or money? Yes, it is phishing.
- **Step 5:** Are they itching one or more of these desires: urgency, desire to please, greed, curiosity, complacency, or fear? Yes, it is probably phishing.
- **Step 6:** Do they have spelling and grammar errors? Offer things that sound too good to be true? Yes, it is possibly phishing.

Section 3: How to Avoid Phishing



EKU Measures

- **Spam Filter.** EKU's spam filter takes out a lot of the spam and phishing before it ever reaches your inbox.
- **[EXTERNAL] Email Tag**. This alerts users that the email did not originate from an EKU email address.
- **Multifactor/Two-Factor Authentication**. Asking users to verify they are who they say they are, helps too.
- **Safe Links and Attachments.** If a link or attachment is known to be malicious, they are automatically blocked.
- **Impersonation Settings Policy.** This setting is enabled at the university C-level (EKU President, VPs) to protect users from email spoofing and spear phishing and whaling that comes along with it. Email spoofing is when someone creates a fake email, for example, in Gmail, with a familiar name but uses the Gmail email account and is sent to staff reports. These spoofed messages usually ask the sender to purchase gift cards, take pictures of the codes on the cards, and return the images to the sender's email address. Enabling the impersonation setting will automatically redirect all such emails to our spam account, bypassing staff.

Risky Business

Do you do any of these personal activities on a work-issued device?

- Check/respond to personal emails?
- Read news sites?
- Research (new products, travel destinations, homework topics, etc.)?
- View/post on “personal” social media sites?
- Shop online?
- Stream media (movies, TV shows, videos, music)?
- Play games?

Risky Business

Do you use your work email when signing up for or using any of these?

- Sign up for streaming services?
- Sign up for shopping services?
- Joining an online community like Reddit?
- Joining a social media site?
- Sign up for anything NOT related to your position at EKU?

Risky Business

If you answered yes to one or more of those questions, you are putting your work and personal lives at risk of

- Account hijacking (if hackers gain access to your email and password, the results can be ginormous)
- Spear phishing attacks (attackers will use your “hacked” account(s) against others you know)
- Credential stuffing attacks (since people reuse passwords, if they get one of your passwords, often they have access to all your passwords on all your accounts)
- You can others can be infected with malware*

*Malware

Malware is the catch-all term for any type of malicious software designed to harm or exploit any programmable device, service, or network. It includes:

- **Ransomware**-one of the most profitable and most popular types of malware. Once installed on a victim's machine, it encrypts their computer files and then demands a ransom (usually in the form of bitcoins) to return the data to the user.

*Malware

- **Viruses** – performs malicious action on an infected device
- **Worms** – malicious code that can copy itself from machine to machine, usually by exploiting some security weakness in software, app, or operating system (This is why keeping your devices and their software up-to-date is so important!)
- **Trojans**-applications masquerading as harmless applications trick users into downloading and installing them to steal data, crash devices, spy on activities, or launch other attacks.

*Malware

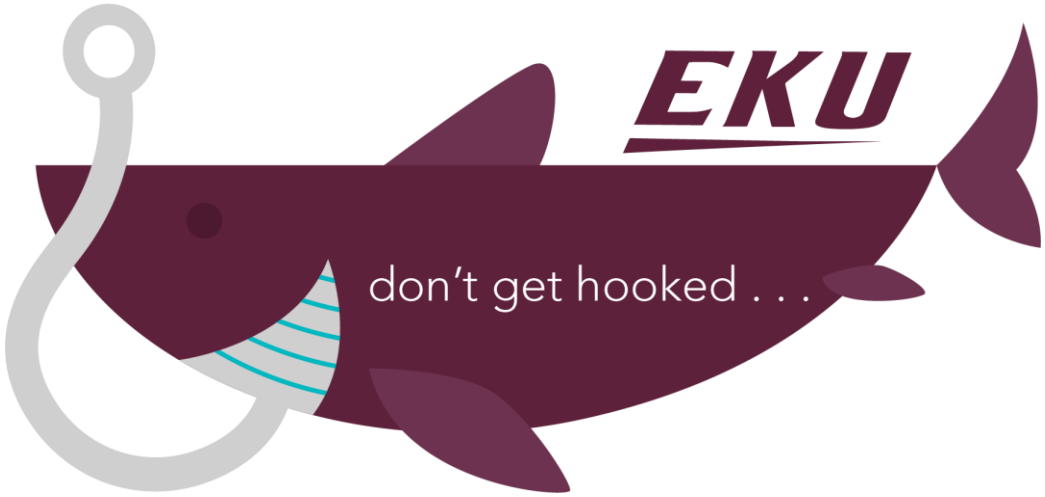
- **Scareware** – this scares us into thinking we are infected, so we download or buy fake software or apps to clean up the problem
- **Spyware** – programs installed, usually without the user's knowledge, capture and transmit personal information, browser habits, and other details to a hacker.
- **Adware** – programs used to push unwanted ads to users to display ads or popups on a personal device or while using a software program

*Malware

How are we commonly infected? (Remember, so it is hard to see happen!)

- Email attachments
- Text messages
- Malware ads on popular sites (malvertising)
- Fake software installs
- Infected USB drives
- Infected apps
- Phishing emails

Section 4: How to Handle Phishing



Before you interact with the email (phone call or text)

- If you see something suspicious—email, text, voicemail, person—report it!
- For spam or phishing emails and voicemails, you can forward them to IT: spam@eku.edu
  - We look at EVERY email
    - If the sender is from EKU, we reset their account
    - If the sender is non-EKU, we block them as most of the time it is originating from a made-up email account
    - If there is a link, we usually block on-campus access to those (we can't block off-campus user's actions)
    - If there is an attachment, we examine it
  - In the unlikely event it is legitimate (less than 99%), we will respond and tell you
- If the spam is from another legitimate organization/company, you should go to their website (not from a link in the suspicious email but a Google search) and see if they have an email you can forward it to.

What if you fall victim?

If you accidentally get caught:

- Forward the message to: spam@eku.edu
- Then contact the IT Service Desk:
  - 1-859-622-3000
- If this is concerning another account (e.g., Amazon, Bank of America) then open their webpage and contact them too
- You can also report at a state or federal level here:
  - Forward here: reportphishing@apwg.org (Anti-Phishing Workgroup)
  - File an FTC complaint here: https://reportfraud.ftc.gov
  - State Consumer Protection Offices: https://www.usa.gov/state-consumer
  - Internet Crime Complaint Center (IC3): https://www.ic3.gov/

Wrap Up

Remember…

- **You** (the user) are our best line of defense!
- **Be suspicious** of any unexpected/unsolicited emails, text messages, and phone calls.
- **Don't be bullied or rushed** into reacting without thinking first.
- **Be more suspicious** if passwords, financial information, your identity, or money are involved.
- **If you see something, report it!**

it.eku.edu