Cybersecurity Awareness Month

**Phishing - It Wasn't Me?**

Even when it is not October (Halloween) buy guys try to get you to fall for their tricks. They may not be wearing a costume but they are pretending to be something they aren't. Sometimes they pretend to be your bank or even a member of Suffolk. Sending you a request through email, social media, or even text message.

Check out this video with a twist on Shaggy's song "It wasn't me" (Emirates NBD 2019)

The bad guys, scammers, use a variety of ever-changing stories to lure you in:

- Promise free prizes, gift cards, or coupons
- Promise to help you pay off your student loans
- Send fake messages that say they have some information about your account or a transaction.
- Say they've noticed some suspicious activity on your account
- Claim there’s a problem with your payment information
- Send a fake invoice and tell you to contact them if you didn’t authorize the purchase
- Send a fake package delivery notification

They may even be so bold as to ask you to give some personal information — like how much money you make, how much you owe, or your bank account, credit card, or Social Security number — to claim your gift or pursue the offer.

Some recent examples have been seen here at the University.

A phishing message that appears to be from someone you know (email or text): "I am on vacation and need your help", "I am out of the office and need your help".

Then they follow-up saying it is urgent: "Are you available?", "Text/Call this number", "Click this link".

What comes next is a call to action: "Can you purchase gift cards, I will pay you back", "I will send you a check, you send me the difference and keep the rest"; "log in to this site to restore your access"

This is when you will have to decide if you are going to just do what they ask or take a CLOSER LOOK. Will you give away your personal information? Will you purchase a gift card? What should you do... Pause and if it appears phishy it probably is. Just delete the message. If in doubt forward to the Service Desk. If it is someone from Suffolk or another business that you know and you think it is real. Use their official contact information to reach back to them. If the message came in through text, send them an email or pick up the phone and call their official number from their official website.

Want to see if you can spot a phish?
**Human Error vs. Sound Judgment**

The leading security issue, Human Error. Cybercriminals rely on human error and are always looking at new and creative ways to leverage it to make money. From using social media posts, text messages, emails to phone calls.

Watch this Mimecast sketch and see where Human Error should be replaced with Sound Judgment. After watching see if you can reduce Human Error with your day-to-day online activities.

Some SIMPLE TIPS to prevent Human Error.

- **Strong Unique Passwords.** Most people use weak passwords and then re-use passwords for multiple accounts. The bad guys know this. Create a strong memorable password unique for each account and protect yourself. Visit [Strong Password](#) to learn more about how to create a strong memorable password hard for others to guess. Then make sure to NEVER share your password.

- **Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks “phishy,” reach out to them via customer service to verify the communication. If in doubt don’t click just delete the message.

- **Make sure you update your software and apps.** On your smartphone and computers make sure you keep the Operating System (OS) up-to-date and keep your phone apps and/or computer applications up-to-date. Remove apps you no longer use. Additionally, your computers, always make sure you have Antivirus software running and up-to-date.

Want to see if you can spot a phish?

Visit the google phishing quiz site.
[https://phishingquiz.withgoogle.com/](https://phishingquiz.withgoogle.com/)
Observed every October, the annual Cyber Security Awareness Month is committed to encouraging personal accountability, securing behaviors, and maintaining digital privacy in the cybersecurity landscape. This initiative was created as a joint effort between government and industry providing resources to stay safe and secure online.