Cybersecurity Awareness Month

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.

This October we are focusing on risky behaviors and will provide some tips on how to identify them and things you can do.

Thank you and hope you have enjoyed Cybersecurity Awareness Month.

To wrap up the month we will take a lesson from the 1950s about being “thoughtful”. What does that mean? Well, watch this video and find out why from “Billy” (StaySafeOnline.org)

We hope you had some fun while learning something new about cybersecurity and ways to stay secure.

Some key points to remember:

Use sound judgment and avoid human errors. Updating to the latest security software, web browser, and operating systems. Understand at least the basic security settings for all your apps and devices. (Mimecast Human Error vs Sound Judgement)

Create strong, unique passphrases, and do not Re-Use those passwords. Change default passwords for all your devices. (Jimmy Kimmel Live - What's Your Password)

Be aware and on the lookout for phishy things. (Phishing It Wasn't Me)

Want to see if you can spot a phish?

Visit the google phishing quiz site. 
https://phishingquiz.withgoogle.com/

Human Error vs Sound Judgement?

Continuing with risky behaviors, we balance it against sound judgment. Human Error has been identified as the leading reason for most security incidents. 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 activities.
Tips on how to reduce Human Error:

Avoid using weak passwords or storing passwords in unreliable places; such as plain text (word, excel, email, phone, google) or even on sticky notes on the office desk or around the house.

Understand what sensitive data is and how to handle sensitive data in paper or digitally. Be aware of accidentally deleting sensitive files. Understand how to encrypt or protect sensitive data. Be careful not to send sensitive data to the wrong recipients. Make sure you back up and secure important data.

Do not use outdated (or unauthorized) software: Do not ignore software updates. Do not download unknown or illegal software they could be malicious or have an adverse impact on your machine.

Pay attention to opening email links or attachments. Make sure it was something you expected, and you know who sent it.

Do not plug in insecure devices, like unknown USB storage devices they could contain viruses. Do not connect to open public Wi-Fi it could be malicious. Use a VPN (Virtual Private Network) or connect to your own private hot spot.

Passwords - Are they strong?

Continuing with risky behaviors. Passwords are still important to be strong even with a second-factor authentication, which adds an additional layer of security to your login process. Why is it still important? Because if your password is in the hands of bad guys it puts them one step closer to gaining access. The bad guys will try additional tricks to get you to approve their login attempts even with your second factor.

Please watch a funny video about Passwords (Jimmy Kimmel Live Jan 2015). What do you think, is still true today? (spoiler alert the answer is yes)
Creating a strong password is an essential step to protecting yourself online and at Suffolk. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime. Creating a strong password is easier than you think. Follow these simple tips to shake up your password protocol:

(The second factor, sometimes called multifactor or two factor, is where you have a password along with a second factor like your phone, text, or mobile app.)

SIMPLE TIPS to a better Password

Don’t make passwords easy to guess. Do not include personal information in your passwords such as your name or pets’ names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.

Use a long passphrase. Consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a part of the sentence, four random words, or even the title of the last book you read. Then add in some punctuation and capitalization.

Avoid using common words in your password. Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter “A” and an exclamation point (!) can replace the letters “I” or “L.”

Get creative. Use phonetic replacements, such as “PH” instead of “F.” Or make deliberate, but obvious misspellings, such as “enjin” instead of “engine.”

Keep your passwords on the down low. Don’t tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.

Unique account, unique password. Having different passwords for various accounts helps prevent cybercriminals from gaining access to these accounts and protects you in the event of a breach. It’s important to mix things up—find easy-to-remember ways to customize your standard password for different sites.

Utilize a password manager to remember all your long passwords. The most secure way to store all of your unique passwords is by using a password manager. With just one master password, a computer can generate and retrieve passwords for every account that you have – protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions, and more.

For more information on Passwords please visit https://wikis.suffolk.edu/display/ITSEC/Strong+Password

Phishing - It Wasn’t Me?

Even when it is not October (or Halloween) bad 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 messages.

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 phishing attempts send links that may take you to a spoofed website that looks real but isn’t. If you log in, the scammers can then steal your username and password.

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 by 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 will 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 it 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?

Visit the google phishing quiz site.
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.