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 keeping it simple and following good security habits.

It's your lucky day.

Take a look at this video (from Mimecast) of an unexpected call .. just pay for shipping and it can be all yours.

(this link plays on YouTube)

It's nice to be recognized, but if it happens to you will you recognize the scam?

The gift-giving season is just around the corner. Be on the alert for a scam that asks you for your personal information and too-good-to-be-true offers over the phone, through text or email asking you just to pay the shipping and asking for your credit card or the mention of gift cards.

Magic Words and Passwords

Take a look at this video twist on how Passwords are similar to Magic Words (by Wizer) that shows just like having a single Magic Word having a single Password to open everything is not a good idea.

(this video plays directly on the wizer website)

Passwords are like a "Magic Word". Here are some tips on how to have a strong unique "Magic Word" and its use.

Having a unique long and strong Magic Word (Password) is important. Did you know that a computer can crack an 8-character password in seconds whereas a 14-character password with complexity (upper and lower case, a number, and a special character) takes centuries to crack? You ask, how can anyone remember a long complex Magic Word (Password)? Use a Passphrase. A Passphrase is a string of words, it can be just as simple as 4 random words together to make a memorable Magic Word (Password). Below are tips on how to make it memorable, unique, and strong.

How to create a strong memorable Magic Word (Password) *Here are some tips*

Make your passphrase funny so it will be easier to remember (do not use this example as your password)

dogridingsmallbicycle

Now add in complexity (upper and lower case, a number, and a special character)

dog RIDING 24 small bicycles

Great. Now you have a strong memorable Magic Word (Password).

However, there are a few things to keep in mind.

Don't use personal information like your name, birthday, or pet name.

Don't use known phrases from a song, common saying, or book. You would need to change part of it to make it unique.

The idea is to have a unique Magic Word (Password) for every login. Have trouble with all those unique Magic Words (Passwords)? Use a password manager to remember all of your Magic Words (Passwords).

If you are reusing Magic Words (Passwords) it is time to stop and update the most sensitive ones first. Like your bank, Suffolk credentials, email, and social media accounts.

Lastly, regardless of how strong your Magic Words (Passwords) are, you should enable Multifactor Authentication (two-factor or 2 step authentication) wherever it is available, so if anyone steals your Magic Word (Password) it will not be enough to log in to your account.

Phishing

Watch this funny video Phishing Song (by GetCyberSafe CSE) that talks about how to spot a phishing attempt and what you can do to "ruin a cyber criminal's day".

GetCyberSafe-PhishingSong.mp4

Before you Delete a Phishing Message, please Report it using the Report Phishing button in Outlook

How to Report Phishing

Suffolk email filters remove most malicious emails but some get through. This is where we need your help to spot phishing and report it.

What you can do when you know or think an email is phishing is to please report the message in Outlook. Reporting a message as phishing updates our filtering and can potentially protect other users' inboxes from the same or similar message.

To report phishing in Outlook online and desktop Outlook on Windows and Mac.

Select the email you want to report as phishing,
then click the Report button in your toolbar,
then select Report phishing.
(You can find the toolbar directly above your inbox which includes commonly used actions like deleting or marking items as read. See the image below)

blocked URL

Can't find the report button? Depending on your toolbar's layout, Report may be hidden under a three-dots menu or dropdown menu. Also note you can customize your toolbar to rearrange your toolbar buttons to make it easier in the future to find.

If you are using Outlook mobile app, tap the three-dots menu at the top of the message. In the dropdown menu, tap "Report" then select "Report Phishing"

What's the difference between junk and phishing and what happens when I report it?

If you have this question, you're not alone.

"Junk" is another email word for spam or unsolicited unwanted email. Phishing, on the other hand, is malicious email meant to steal or trick you into sharing credentials, personal information, installing malicious software, or taking your money.

When you "Report Junk" the message is moved to your Junk Email folder. You still have access to the email and future similar emails are routed to your Junk Email folder.

When you "Report Phishing" Outlook deletes the message from your inbox and it is reported to our Office 365 environment for tuning our filtering potential new similar bad messages.

Want to see if you can spot a phish?

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

SUFFOLK
UNIVERSITY
BOSTON

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.