Quarterly Cybersecurity Awareness Newsletter

Your Digital Self-Defense within the Cyber Threat Landscape

Cybercriminals use various methods and tools to breach your device, get into the network, or steal valuable information. All these different attack methods are known by the cyber term "Threat Landscape." This quarter's newsletter focuses on how we navigate this threat landscape while defending ourselves, otherwise known as Digital Self-Defense.

Threat Landscape	Digital Self-Defense
Phishing – Sending out generic email messages to large groups of individuals enticing them to click on a link, image, or attachment. Phishing has led to 64% of all ransomware attacks.	**Remember Red Flags –** Being able to accurately identify the various red flag warnings of an email message is your first and best defense. Use the *Phish Alert* button in Outlook or report it to security@cabrini.edu.
Social Engineering – The act of manipulating people into performing acts or divulging information. Social engineering has led to 33% of all ransomware attacks.	**Validate for Yourself** – If called, emailed, or even sent something through the mail. Never take it for face value and always validate it for yourself. Perform a separate web search, locate the business, and contact them directly.
Spear-Phishing – Similar to Phishing, but attackers do some research and know more about you, your position, and your peers. Messages typically appear to be from someone you know, or peers.	**External Email Flags** – The external email flag is the best defense against a spear-phishing attack, helping you identify that this may not be the person you think it is.
Websites – Websites with an adult theme or content most often contain malicious links and applications, but other more popular websites also can become infected.	**Safe Surfing** – When surfing the web, be wary of any application download that is not from the original site. Remember to hover over links to validate that they go where you believe they should go.
File Types – It is common to receive attachments via email or download files from websites. But which ones are safe?	**.TXT Files** – The text file is the only file type that is always safe to open. All others should be opened with caution.

Malware – This is the umbrella term used to describe the wide variety of programs attackers use to steal information or control your device.	**Antimalware and Patching** – Keeping your virus definitions in antimalware and your system up to date (patching) is essential to malware defense.

Reporting or Reacting to Threats

If you're lured in by a phishing attempt, do the following!

1. Contact the ITR to change your password **IMMEDIATELY!**
    a. The faster you react, the less likely the attackers will leverage your information against you.
2. Contact IT Security: security@cabrini.edu
    a. Be sure to include as much information as possible to begin the investigation.

Reporting Emails with Phish Alert Button

With the suspected email message selected in Outlook, find the Phish Alert button on the ribbon:
Once you have click Phish alert, and then **Report**. The email will auto-generate a support ticket, and the suspected messages are moved to your trash.

Reporting Emails without the Phish Alert Button

To assist in the investigation, please forward a copy of the malicious email directly to security@cabrini.edu.
To forward a copy of an email message:

1. Select the suspicious email message in Outlook
2. Select **More** within the respond section of the ribbon, and then choose **Forward as Attachment.**
    a. (You may also press CTRL+ALT+F)
3. Address this message to security@cabrini.edu and use the subject: **Malicious Message**