Quarterly Cybersecurity Awareness Newsletter

Practicing Digital Self-Defense When Working Remotely

Our physical world has made some changes this past month, but it is important to note that the digital world is the same. With one exception, now most workers are remote and relying on their home internet connections to perform their much-needed work activities and projects. Due to this change, the data that we process each day is now more vulnerable to attackers. Hackers understand this and are working overtime on ways to infiltrate your device and gain access to this data. The focus today is on being ever vigilant in our efforts to secure the data entrusted to us while remote.

Defending Against Cyber Scams

The nation's Cybersecurity and Infrastructure Security Agency (CISA) has several warnings related to the Coronavirus.

- Avoid clicking on links in unsolicited emails and be wary of attachments.
    - We have early alerts such as the External Email notification, and our training on spotting the red flags in an email message.
- Use Trusted Sources – such as legitimate, government websites for up-to-date, fact-based information.
- Do not reveal personal or financial information in an email or on phone calls. Go to the source separate from the email or call and look at this information yourself.

Blocking Social Engineering Attacks

Everyone is trying to stay connected, and today, more than ever, social engineering threats are more aggressive as well. Here's some tips on how to be safe. Preparedness is key.

- Phishing, Vishing, and Smishing
    - Phishing – Watching for those red flags and being wary of malicious emails.
    - Vishing – Voice calls asking for information such as financials, tax, or login information. (Remember the IRS has explicitly stated they WILL NOT contact individuals via the phone.)
    - Smishing – SMS phishing or text phishing. Especially now that we are doing more on our remote devices, watch out for any links sent on text messages.

VPN Connection

Stay Connected, Patched and Up-to-Date

Everyone with company issued equipment, please connect to the VPN at least once per week for about 4 or 5 hours. By doing so, your computer will receive much-needed patches and updates. If you don't regularly leverage the VPN, you can simply log in at the end of the week and leave your computer running overnight.

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 in 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**