Quarterly Cybersecurity Awareness Newsletter

Value of Data

Have you ever looked at what kind of data you have stored only on your computer's hard drive? Have you make a backup of that data? Computer hard drives can wear out and fail and it may take time to retrieve data. Worse, the internet harbors potential threats to your data such as viruses and Trojans – these can corrupt or steal your data. There is also the rising threat of "ransomware" that can be installed by simply clicking on a link in a seemingly innocuous email. If you lost access to data on your computer – would you be able to recover everything you need?

This may be a good time to use OneDrive. OneDrive is a secure, cloud-based location for storing important data. That way, if something happens to your computer, you will still be able to access all of your files as soon as you log into your replacement computer and your OneDrive. Here are some tips for keeping important data protected and available.

Remain Cyber Safe

1. **Back up your data –** You should always back up files and projects that cannot be easily replaced. This does not mean to put the data on a removable flash drive. Flash drives are intended as temporary storage not a backup. There is little protection offered for flash drives and they can be easily lost or stolen.
2. **Determine what data is still relevant –** This may also be a good time to delete old data that is no longer needed. Old data may contain sensitive personally identifiable information (PII) that a cybercriminal could access and exploit if your computer becomes compromised.
3. **Determine where to store your information –** OneDrive is an excellent place to store your information that doesn't need to be shared. However, if the information needs to be shared with team members, a department Teams channel is another great option. Using Teams alleviates the need to email documents and provides version control and security features as well.

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**