# PREVENTING CYBER ATTACKS

## *KEEPING YOUR INFORMATION SAFE*

Did you know that the term Email Phishing is a general term given to any malicious electronic message intended to entice users to disclose private information. Attackers typically aim to steal account credentials, personally identifiable information, and company trade secrets.

## FACTS

- A legitimate business will not ask a user to send sensitive personal information via email.
- The less information you post, the less data you make available to a cybercriminal to use in developing a potential attack or scam.

## TIPS TO STAY SAFE

- Be vigilant about any communication requesting personal or financial information.
- Use and memorize strong passwords or passphrases.
- Take time to verify offers that seem too good to be true.
- Be wary of unexpected and high-pressure requests claiming to be from legitimate institutions. Contact the organization or person via different communication methods if in doubt.
- Hover over email addresses to verify the authenticity of email addresses and links.
- Pay attention to the legitimacy of each email by checking the sender's identity and layout errors.

## DO NOT

- Do not open attachments or links in unsolicited emails.
- Avoid sharing passwords or sensitive information on third-party sites or applications.
- Do not use external storage devices found in public places.
- Do not leave your devices unattended with open sessions.
- Do not simply close the browser when you have finished the current session, always log out.
- Do not enter personal information after clicking on a link without hovering over the email address; always type the web address directly if you doubt the legitimacy of a request.