Security is Everyone's Responsibility

The one thing cybersecurity threats have in common is that they are harmful and the cybercriminal is committed to destroying, stealing, or disrupting data, critical systems, and digital life in general. Commercial Bank uses numerous security applications and incorporates processes to keep your financial information and assets secure and to comply with regulatory guidelines.

However, security is everyone's responsibility, and you can do the following three things to help safeguard your assets.

1. Educate yourself about the various tactics, techniques, and processes (TTP) cybercriminals use to steal from you. TTPs are like fashion, what's in style one month is out of date the next-so cybercrimes change over time.
2. Install security applications on your personal computers and mobile devices. Those applications, especially anti-virus and content-blocking applications, are an additional layer of protection for devices connected to the outside world. It's important to secure all your devices, especially those used by your whole family.
3. Regularly monitor your account activity and let Commercial Bank know about any suspicious activity.

Tips To Help You Remain on Guard

- Don't reveal personal or financial information in a text or email, and don't respond to email solicitations for this information.
- Don't click on links sent in a text or email-you might wind up in a scam site built by a cybercriminal.
- Don't send sensitive information over the internet without checking the website's security. Look for URLs that begin with "https"- the 's' stands for secure-rather than "http". A website safety check like Google Safe Browsing helps, too.

If You're a Victim?
Immediately change any passwords you might have revealed. Contact Commercial Bank immediately. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.