SECURITY AWARENESS

COMMERCIAL BANK
Member FDIC

When sending sensitive information via the Internet, make sure “https:” appears in the address bar. This means the information you are transmitting is encrypted.

Ensure the wireless network you use is password protected. Choose a strong password and update it frequently for your work and home wireless networks. Likewise, always use a passcode on your mobile phone or tablet to stop an unauthorized user from accessing your device.

Don’t enter sensitive information into your phone or computer when others can see what you’re entering, or when using public Wifi.

Set the privacy settings on frequented social network sites. Cyber-criminals often learn about people and their families and friends via social media in an attempt to spoof or phish you and your network.

Set-up and use two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

Remain cautious of someone who isn’t who they say they are or if the name and area don’t match what appears on caller ID. This is often how spoofing occurs.

Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight variations on legitimate email addresses and websites to trick your eye and gain your trust.

Be careful what you download. Never open an email attachment that you weren’t expecting or from someone you don’t know.

Similarly, don’t click on links or scan QR codes sent to you from unknown sources via text message or email, because they could be spyware, malware, or ransomware. Use caution when making payments through a QR code, and download apps from the app store instead of scanning a QR code.

Never respond to text messages, emails, or phone calls from companies alleging to be your bank, government officials, or business representatives that request your account numbers, user names, passwords, or PINs. Be wary of individuals who press you to act or respond quickly.

Always choose a strong password for banking accounts or online payment apps. It should be a mix of uppercase and lowercase letters, numbers, and special characters.

Keep track of what transactions you have conducted, and check your bank statements frequently for unauthorized charges. Also monitor your credit reports.

If you feel like your email, computer, or sensitive information has been compromised, it is important to act quickly to minimize risks and effects.