Cyber Security

with Lou Palumbo

“With the ever-increasing integration of technology into our personal lives, consumers have to be engaged and take an active role protecting their sensitive information.”

– Lou Palumbo, CISA, CISM, CRISC, CISSP
SVP / Chief Information Officer
NexTier Bank

CYBER SECURITY
TIPS & TRICKS

By Lou Palumbo

1. **Create different user names and passwords for each application**. If a company is breached and your information is exposed, criminals tend to use those credentials to attempt to gain access at other websites.

2. **Create strong passwords.** Passwords should not contain easily obtainable information such as a spouse, child, or pet's name. Fraudsters scour the internet and social media to profile potential targets.

3. **Utilize multi-factor authentication.** Most websites allow you to utilize one-time codes that are sent via text message to your cell phone in conjunction with a username and password to access their sites. This makes it harder for criminals to utilize stolen credentials.

4. **Think before you click.** The easiest way for criminals to circumvent security controls is to trick you into clicking on a link or downloading an attachment in an email. If you are unaware of a message's authenticity, contact the sender via phone call, text message, or even snail mail to ensure they meant to send you that message. If you reply to the email, it is possible you may be corresponding directly with the fraudster if their account was compromised.

5. **Practice Safe Web Browsing.** If you are performing sensitive browsing such as banking or shopping, use secure networks such as your home Wi-Fi or cell phone network. Public networks like coffee shops, hotels, and public spaces are rife with fraudsters that will intercept and steal your data.

6. **Keep Your Systems Up To Date.** Patches for your computers, laptops, and even smart phones are important. Fraudsters target out of date devices because they are the "low hanging fruit."

7. **Use Anti-Virus and Firewalls.** Anti-virus software is readily available for free for computers AND smart phones. Firewalls are embedded in most operating systems like Windows and enabled by default.

8. **Back Up Your Information.** In the event your information is lost or stolen, a backup may be your only lifeline to restore your critical information. Many providers such as Apple, Google, and Microsoft gives their users free online storage for just that purpose. Keeping an "offline" copy of files on a flash drive or external hard drive in a safe deposit box protects your information from a house fire or other natural disaster.

9. **Be Your Own Security Officer.** Review your online accounts and credit reports regularly for changes. Many fraudulently opened credit cards and accounts are opened for 30 days or more on average before the victim is aware there has been a breach of their information.

10. **The Power of No.** You are in control with what information you share. If you are uncomfortable with providing any information just say no. No reputable company or entity will ask for personally identifiable information over the phone, by email, or through text message. When in doubt, call the company using known avenues like a web search to verify authenticity before giving out any information.

NexTier Bank