CITY NATIONAL BANK
AN RBC COMPANY

11 Ways to Protect Yourself Online

Thanks to the Internet, life is easier than it used to be. Recent headlines remind us, however, that technological progress has also created new opportunities for fraud (and much worse). Government agencies and companies like City National devote major resources to combat Internet fraud, but these efforts will have limited effectiveness until all consumers and businesses actively join the fight. Here are some of the steps you should take to protect yourself from online crime:

1. Install an anti-virus program that will help fight viruses and malicious software on your computers, tablets, mobile phones and other devices. Use firewalls to secure and protect your home and/or office network.
2. Be conscientious about installing critical updates for your computer's operating system. Better yet, set it up for automatic updates. The bad guys don't stand still and you shouldn't either.
3. Keep your mobile devices with you or lock them away when they're not needed. Password-protect them to protect against unauthorized use. And, when it comes to apps, be careful before you click. Only download from legitimate online stores.
4. Is your computer set up to "auto-load" removable media (e.g., USB drives, SD cards)? If so, disable this feature. Play it safe by scanning these items before you open them.
5. When it comes to your passwords, be extra diligent. Passwords should be complex, frequently changed, and unshared. And be sure to password-protect your router and other wireless connections.
6. Never open email attachments or click on links from unknown or suspicious sources, including social media sites.
7. Don't be manipulated. Disregard in-person, phone, text message, email or Web requests that ask you to share your personal or account information unless you are sure the request and requestor are legitimate.
8. Be careful on social media. Avoid posting too much personal information. At the very least, utilize privacy controls to limit who can see what.
9. Be disciplined in the management of your financial accounts. Check them daily and report suspicious activity to the bank right away.
10. ACH transactions and wire transfer security is especially critical. Use security tokens only when releasing an ACH or wire transaction, never at login. City National Bank will never initiate a communication to request entry of security tokens. If you enter a token to complete a transaction and you receive an error message, you are logged off the system or you do not receive a confirmation, contact the Bank IMMEDIATELY. There is increased likelihood your computer has been hacked.
11. Internet security is a family affair. Make sure all Internet users in your home are educated about online safety and know what needs to be done.

continues

For Business Owners

If you are a business owner, here are a few additional steps you should take:

- Provide cyber-security training and share fraud protection and other important information with all company users.
- Monitor security threats and periodically assess network and security risks. Develop a cyber-incident response plan and test it regularly.
- Maintain "cyber insurance" appropriate to your financial risks.
- Take full advantage of bank-related security products and alerts (e.g., Positive Pay and ACH blocks and filters).
- Encrypt sensitive data, whether transmitting or simply storing it.
- Review transaction information throughout the day and let the bank know right away if something doesn't look right.
- Confirm that your System Administrator effectively communicates warnings, security messages and other information we may send to you.

Learn more about protecting yourself online by visiting City National's Fraud Prevention Center at **cnb.com/fraud**, as well as sites provided by the National Cyber Security Alliance (staysafeonline.org) and the Department of Homeland Security (dhs.gov/cybersecurity).

This guide is intended to be your first step toward a more secure online environment. It is not intended to be an all-inclusive and comprehensive approach to cyber security. We encourage you to conduct your own due diligence and develop a cyber-security plan based on your perceived risks.