Cyber Security

Protecting your personal information and ensuring your account information is secure is a top priority at Southeast National Bank.

REMEMBER: Southeast National Bank will **NEVER** ask you to provide or verify account or login information by email, phone or text message. This includes account numbers, User IDs, passwords, and debit or credit card information.

Unfortunately, the convenience of electronic communication brings with it vulnerability to criminal activity and it is critical for Southeast National Bank and its customers to partner-up to keep scammers at bay. This includes not only personal computers but also your smartphones.

Phishing: Fraudulent email usually containing an urgent message regarding account status and a link directing the recipient to a fraudulent website. Remember, Southeast National Bank will NEVER send out an email requesting personal information.

Vishing: A variation of Phishing, combining "voice" and "phishing" and often involves an automated recording made to the victim alerting the customer their account or credit /debit card has been compromised and directing them to call a phone number immediately. Automated instructions require entry of private information such as PIN, date of birth, etc.

Malware: Malicious software criminals use to access your computer without your consent – or even your knowledge – and is often delivered via fraudulent emails.

While these are the most common forms of fraud it is important to be constantly vigilant to any suspicious activity on your computer or smartphone.

PROTECT YOURSELF:

- Don't respond in **any way** to any email concerning any aspect of your account.
- Avoid sending personal or financial information in an email.
- Review your credit card and bank account statements as soon as you receive them.
- Keep login credentials confidential and change your password periodically.
- Install virus protection software on your computer(s) and run full system scans often.
- Use extreme caution when on social network sites.
- Password protect your smartphone; enable an automatic screen-locking mechanism to lock the device when it's not being actively used.
- Consider using a remote wipe program that gives you the ability to send a command to your device that will delete any data.
- Clear data from your smart phone frequently.
- Always download apps from reputable sources.
- Remove personal information before replacing your smartphone.

REPORT:

If, despite taking precautions, you do become a victim of fraud report it immediately to Southeast National Bank. We're here to help you.