Online Banking Safety Tips

Online Banking

State Bank takes the security of your personal information very seriously. Online Banking eliminates paper statements and reduces the number of checks written helping to prevent identity theft via mail.

Online Banking Safety Tips

- Never share or reveal your login info to anyone. State Bank does not store or retain your online banking password or ATM PIN and will never ask you for it.
- Create passwords that contain a variety of capital and lowercase letters, numbers, and symbols. Avoid easy to guess things like your child's name, pet's name, birthdays, or your address.
- Log out completely when you finish an online banking session.
- Avoid storing passwords and SSNs on your mobile devices.
- Password protect your mobile devices and lock them when you aren't using them.
- Read your monthly statements to verify all transactions are correct.

"Phishing"

Phishing involves the use of fraudulent emails and copy-cat websites to trick you into revealing valuable personal information. "Phishers" often lure their targets into a false sense of security by hijacking the familiar, trusted logos of established, legitimate companies. A typical phishing scam starts with a fraudster sending out millions of emails that appear to come from a high-profile financial services provider and ask you to "verify" information you previously provided when you established your online account.[1]

Phishing Safety Tips

- **DO NOT** respond to any emails that request personal or financial information. If you have reason to believe that a financial institution actually does need your personal information, pick up the phone and call them.
- Be wary of emails that look suspicious or aren't from someone you know.
- Don't click on link's provided in emails. Type the web address in your browser yourself.
- Make sure your PC's firewalls and security software are installed and up to date.
- Keep up to date on phishing tactics and scams. Visit www.antiphishing.org for a list of current attacks and phishing news.

[1]Source: www.sec.gov/investor/pubs/phishing.htm