Risk Mitigation Best Practices for Mobile and Online Banking Consumers

The FFIEC Supplement to Guidance on Authentication in an Online Banking Environment calls on institutions to extend customer awareness and education efforts to both retail and commercial customers. Among other things, these efforts are to include "[a] listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found."

In this increasingly connected world, consumers must take proactive steps to safeguard their data. Channels (such as online and mobile banking) and tools (such as social networks) have become a part of our daily landscape. Due to increased risk of personal data being compromised and also increased probability for fraudulent transactions from these added conveniences, consumers should take the time to review the following recommendations for risk mitigation:

Applicable to both Online Banking and Mobile banking

1) Be vigilant in reviewing your financial statements and monitoring your transactions. Develop the good habit of monitoring your financial accounts (e.g. bank, credit card, retirement etc.) at least weekly through online, mobile, voice banking or the ATM.

2) Never leave your computer, tablet or mobile phone unattended when using any Online Banking, mobile banking or other financial services.

3) After you have completed your Internet or mobile banking session, it is good practice to always log off to ensure that the session is disconnected.

4) It is also good practice to lock your computer or mobile device whenever you plan to leave it unattended.

5) Never use publicly available information to create your password. Examples to avoid are common names or phrases, birthdates, social security numbers, etc. And of course, it goes without saying that you should never reveal your password to anyone.

6) Change your passwords frequently. Establish a routine where you change your password frequently to reduce the risk of a compromised account.

7) Avoid using password managers. Even though they may be convenient, password managers create a habit of not changing your passwords regularly and therefore make it easy to forget your passwords over time.

8) Never click on links or applications that you receive in emails or text messages, as those are common ways viruses, malware and malicious software are installed. If you get an email with links claiming to be from State Bank of Belle Plaine, please visit State Bank of Belle Plaine's main website through your browser or call State Bank of Belle Plaine to verify legitimacy. Keep your passwords/pin confidential. Under no circumstance will you be asked to provide it to State Bank of Belle Plaine.

9) While using the Internet, verify use of a secure session (https:// and lock icon, and not http://) in your browser's address bar. This is your indication that the data being transmitted between your browser and State Bank of Belle Plaine's systems is securely encrypted.

10) Install anti-virus and anti-malware software. There are many good applications available for both your computer and your mobile device. Some are even free. Also, remember to keep these products updated regularly so they can be most effective.

11) Avoid using unsecured public wireless connections. If you must, then use VPN software to provide a secure "tunnel" within which to work.

12) Be aware of the types of information that you post to social networking sites. Ensure you know who your "friends" are on such sites and do not accept "friend" requests from unverified parties. Statistics show that users of such sites experience a higher incidence of fraud. Use privacy settings on social networking sites to control who is able to access your personal information.

13) Your Internet and mobile banking service has extensive alerts available for your use, be sure to take advantage of these alerts. Once you set up the alerts you need, you will be notified of activity on your accounts.

14) Checks and your financial statements all have your private financial information on them. Request electronic statements (eStatements) and use online bill pay whenever possible to reduce the paper trail and the risk of your account information being compromised.

15) Be aware of your surroundings when speaking on your phone. If you absolutely have to relay social security numbers, account numbers or other personal information, be very aware of who may be able to hear you.

16) Never post any personal information about your accounts such as account numbers, passwords, balances etc. to anyone on social media such as Facebook, Twitter, Google +, Linkedin, Pinterest etc.

17) If you suspect fraudulent activity or have doubts about the authenticity of a site or communication you have received via any medium, please call State Bank of Belle Plaine at 952-873-2296.

Mobile Phone and Tablet Specific (The above are also applicable to mobile)

1) Ensure that you install software capable of remotely wiping the device should it get stolen or lost.

2) Enable any remote locating features of your mobile operating system or install “find me” software on your devices.

3) The minute you suspect that your device is lost or stolen, notify your mobile carrier and suspend your service. If you have downloaded a mobile banking application, promptly notify State Bank of Belle Plaine as well.

4) Install mobile software only from the Google Play Store, Apple App Store or Windows 8 Store and never a 3rd party site. Read the permissions requested by the application carefully and determine whether the permissions coincide with the alleged function of the application.

5) Do not install any “financial” apps on your device without first verifying them with State Bank of Belle Plaine, so that you can be certain that you are installing the genuine downloadable app.

6) Do not “jailbreak” your iPhone/iPad or “root” your Android device. Tampering with your device could unintentionally open “backdoors” for malicious software. Android and Windows users should avoid installing (side-loading) applications that did not come from the official app stores or markets. Side-loading will make the device more vulnerable to attacks.

7) If you purchased or received a used or refurbished device, be sure to “wipe” or factory reset it to be certain that the device is free of any pre-loaded malware or viruses that could be used to steal your data.

8) Turn off wireless device services such as Wi-Fi, Bluetooth and GPS when they are not being used.

9) Use screen locks and passcodes to protect your information when your device is idle or unattended.

10) Keep your device up-to-date with the latest operating system patches and releases from your mobile network provider.

11) Never store your sign on, password, and answers to your challenge questions on your mobile device.

12) Regularly run anti-virus and anti-spyware programs on your smartphone or tablet, just as you would on your PC.

13) Never send any information about your accounts such as account numbers, passwords, balances etc. to anyone via a text message, as it is not secure.