CUSTOMER SECURITY AWARENESS AND EDUCATION

Banking online can be a way to save you, the customer, time and money. At First State Bank & Trust Company, we want you to know that our online banking system is secure and your personal and financial information are protected. We are committed to protecting your personal information. We will never request personal information by telephone, mail, e-mail, or text messaging including account numbers, personal identification information, passwords, or any other confidential information. The bank's goal is to safeguard your confidential information and we will continue to work diligently to do so.

INTERNET BANKING SECURITY

The following are some tips to protect your confidential information:

- Never share or give out your user name, password, or security challenge questions and answers.
- Do not use personal information as your access ID, user name or password.
- Create difficult passwords that include letters, numbers, upper and lower case letters (case – sensitive) and special characters.
- Change your password frequently.
- Avoid using public computers and Wi-Fi to access your internet banking.
- Do not provide any personal information to web sites that do not use encryption or other secure methods of protection.
- Ensure that your computer is equipped with updated anti-virus and malware software protection.
- Ensure that your computer and mobile devices are updated with the latest operating system software version available.

MOBILE BANKING SECURITY

Managing your finances using a smartphone or tablet can be very convenient. However, you should consider these safety tips to protect your account information:

1. NEVER SHARE YOUR LOG-IN INFORMATION: Never share or give out your User Name, Password or Security challenge questions to anyone.
2. LOCK YOUR PHONE: Locking your phone with a PIN or security code, makes it more difficult for others to access the device. If you lose your phone or if it's stolen, your data is safer. Use an auto-lock or time–out feature so your device will lock when it is left unused for a certain period of time.
3. CREATE STRONG PASSWORDS: Create a strong password or PIN for your device and mobile app and do not save them. Enter your password every time you need to access accounts rather than storing them automatically. When banking on your cell phone, it is essential to protect the data you access from it. Manually entering user ids and passwords might be more time-consuming, but you'll thank yourself if your phone is ever stolen.
4. SUBSCRIBE TO REMOTE WIPING PROGRAMS: Some phone providers offer remote wiping services that can be used to erase all data if your phone is ever lost or stolen. Since banking on your cell phone can leave personal information on the device, these services create peace of mind.
5. PROTECT YOUR DEVICE: Be proactive in protecting your smartphone and/or tablet by installing anti-malware software on the device and keep your device upgraded to the latest operating system version.

6. FOLLOW NORMAL SECURITY PROCEDURES: One of the dangers of banking from your cell phone is the ease with which you can access account features. It becomes second nature, an afterthought, and this is where people get in trouble. Follow basic security procedures whenever you use mobile banking features. Don't give your passwords to anyone, use complex passwords, and store your phone in safe place.

YOUR PROTECTIONS UNDER "REG E"

First State Bank & Trust Company follows specific rules known as Regulation E, issued by the Federal Reserve Board for electronic transfers. These rules cover all kinds of situations regarding transfers made electronically. Under the consumer protections provided by Reg E, you can recover internet banking losses according to how soon you detect and report them. For a complete detailed explanation of protections provided under Regulation E; please visit the Consumer Financial Protection Bureau's (CFPB's) website: http://www.consumerfinance.gov/eregulations/1005

COMMERCIAL BANKING INTERNET SECURITY

Business and Commercial (non-consumer) customers using internet banking and/or bill pay are not protected under Reg E. Special consideration should be made by the business customer to ensure adequate internal security controls are in place that are commensurate with the risk level that the customer is willing to accept.

As a non-consumer customer you should perform periodic assessments to evaluate the security and risk controls you have in place. The risk assessment should be used to determine the risk level associated with any internet activities you perform and any controls you have in place to mitigate these risks. You should also ensure all company computers are equipped with up to date anti-virus protection.

CUSTOMER VIGILANCE

Watch out for suspicious emails that ask for your personal information. If you receive an email from us and are unsure whether it is legitimate, please contact us and we will be glad to assist you.

Neither this Institution nor its service providers will contact you via telephone or email requesting personal information, access ID, or your passcode. If you are contacted by anyone requesting this information, please contact us immediately. If you notice suspicious activity within your account or experience security-related events (such as a phishing email from someone purporting to be from First State Bank & Trust Company) you can contact any employee at the bank and report such issues.

You can also learn more about online safety and security at these websites:

- Avoiding ID Theft: http://www.FDIC.gov
- Internet Crime Complaint Center: https://www.ic3.gov
- U.S. Department of Justice: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
- Protecting your Workplace: https://www.us-cert.gov/security-publications
- Securing Your PC and Protecting Kids Online: https://www.consumer.ftc.gov
- Federal Trade Commission: http://www.ftc.gov/
- Federal Bureau of Investigation: http://fbi.gov/