Security Awareness and Fraud Education

Computer

- Use operating systems that are currently supported by the software vendor.
- Stay up-to-date with current service packs and security patches on all installed software.
- Make sure you computer is password protected.
- Make sure you have an up-to-date antivirus/antispyware application and its set to automatically update and scan your computer. Don't trust "free" security software. Purchase security software from well known reputable software vendors. Make sure the software package you purchase includes anti-virus, anti-spy- ware, anti-phishing, and anti-spam protection.
- Do not disable the computer firewall.
- Use a reputable third party router/modem with firewall capabilities instead of connecting your computer directly to the internet.
- Avoid downloading programs or files from unknown sources.
- Computers used for business online banking should be used for business related functions only. These computers should not be used for personal use or personal web browsing.
- Mobile computers/laptops should have disk encryption enabled and strong password or biometrics authentication.
- If your home or business computer is connected via wireless network, make sure the SSID is hidden and a wireless security password is required.
- If you feel your computer is infected with malware or compromised, disconnect it from the internet immediately. Resolve the issue on your own or have it repaired by a reputable service technician prior to connecting it back to internet access.

Online Banking

- Commercial online banking customers should perform a periodic risk assessment and controls evaluation to include, but not limited to, employee access rights and roles, dual control requirements and transaction/activity alerts.
- Always access online banking by typing the address directly into the internet browser or by using a favorite link. Avoid clicking on links in emails to access your financial web sites.
- Verify the web address starts with https:// and the full address is correct.
- Be alert and aware about anything out of the normal about the website.
- Verify site encryption by making sure the lock icon is locked in the internet browser.
- Avoid accessing your online banking on public computers.
- Avoid accessing your online banking on public WIFI networks.
- Set responsibility specific roles in the company and define those roles per user account.
- Require dual authentication/approval for business related activities.
- When possible, implement a restricted funds transfer recipient list (whitelist).
- Implement time of day restrictions on employee online banking accounts.
- Avoid sending financial account information in unencrypted email.
- Always log off from online banking and any websites you enter financial and personal information into.

Web Browsing

- Use updated internet browsers to access online banking.
- Turn popup blocker on.
- Keep internet browser security settings at recommended levels or higher.
- Delete "tracking" cookies on a regular basis (usually under tools and settings or options in internet browsers).
- Avoid clicking on pop-ups or ads.
- Avoid posting personally identifiable information (PII) on social network websites.
- Make it a habit to only visit well known reputable web sites.
- Verify all addresses begin with https:// and the secure lock icon is locked before entering any personal or financial information on a website.
- Don't fall for scams that may pop up (in an internet browser) alerting you of computer infections or free computer scans.
- Always use well known reputable online payment processors to purchase products or services.
- Be alert of multiple tabs that are open in your internet browser. Close unneeded/unused tabs to avoid "tabnabbing". Fraudsters will unknowingly duplicate your online banking session in another browser tab to commit fraudulent activity.
- Close your internet browser when you are not using it.

Email

- Be alert for suspicious emails claiming to be from a reputable person or company.
- Never open attachments, respond or click on links from unknown senders.
- Never send personal or financial information over email. All email is unencrypted unless you have an encryption device or subscribe to an encryption service.
- If you receive a suspicious email claiming to be from First Federal Bank Littlefield Texas ssb please forward it to us.
- If you accidently respond to a suspicious email with personal or financial information in it please contact the bank.
- Before you click on any link in an email, hover your pointer over the link and it will display the "actual" address it contains. Review the address carefully to verify it is correct.
- Avoid posting your email address on social networking websites.
- First Federal Bank Littlefield Texas ssb will never request personal or financial information via email.

Username and Password

- Use complex passwords that include a combination of letters, numbers and special characters or use sentence based passwords such as (MybirthdayisThursdayJune20!)
- Avoid using the same passwords for online banking that are used at other websites
- Avoid using your social security number as your username
- Change your usernames and password regularly
- Remember your username and password. Do not write them down or share them with anyone. This is extremely important for commercial customers who have transactions that require dual authentication/ authorization.
- Keep your security questions and answers private. When possible use questions and answers

that are not public knowledge
- First Federal Bank Littlefield Texas ssb will never ask you for your passwords.

Phone

- Do not rely on caller id to verify the identity of a person or business. Caller id can be spoofed.
- Do not give out personal information when you did not initiate the call.
- First Federal Bank will never initiate a call to ask for personal information, financial information or ebanking credentials. Hang up and call back with a known good phone number.

Mobile

- Always require a password to access your mobile device
- Enable an automatic screen lock to lock your device when it is not in use
- Use encryption software to protect your mobile device
- If possible purchase a mobile antivirus software
- Avoid saving passwords in your mobile device apps and browsers
- If possible setup a remote wipe account. This will allow you to erase all data on your mobile device in the event it is lost or stolen.
- In the event you're mobile device is lost or stolen have the SIM card/phone number deactivated immediately.
- Make it a habit to delete text messages frequently from the bank.
- Never reply to a text message claiming to be from First Federal Bank Littlefield Texas ssb requesting personal or financial information. First Federal Bank Littlefield Texas ssb will never initiate a text message requesting this information.
- Never divulge personal or financial information from a caller claiming to be from First Federal Bank Littlefield Texas ssb. First Federal Bank Littlefield Texas ssb will never initiate a call requesting this information.
- Never use caller id to verify the identity of a person or business. Caller id can be spoofed.
- Always download mobile apps from well known reputable software companies.
- Never "jail break" your mobile device. Jail breaking typically opens the device up to vulnerabilities outside the original manufacturer's control.
- Make sure to sign off of your mobile apps instead of closing them.
- Be alert of fraudulent or spoofed apps claiming to be from First Federal Bank Littlefield Texas ssb. Notify the bank immediately if you suspect fraud.
- Notify the bank immediately if your mobile device gets lost or stolen. This will allow the bank to unenroll your accounts from web access.

Mail

- Avoid responding to "to good to be true" mail scams. Never supply personal financial information in a reply to someone that is pressuring you to respond to a sweepstakes or money wire request to claim a prize.
- Never discard paper that has personal or financial information on it. Shred all documents containing this information.

Debit/Credit Card

- Always keep your debit or credit card in a secure place.
- Remember your PIN. Do not write it on your card or anywhere else.
- Do not share your PIN number with anyone.
- Never give your debit or credit card number to anyone unless you initiate the contact.
- Sign the back of the card to help protect you on signature based transactions.
- Cancel and cut up unused cards.
- Review your transactions regularly, contact the bank immediately if you notice fraudulent/unauthorized transactions.
- Keep your receipts safe or make sure to shred them.
- Do not let any website store your credit card information.
- Report lost or stolen cards to the bank immediately.

Check

- Keep unused and canceled checks in a secure place.
- Do not discard checks, make sure to shred all unwanted checks.
- Limit the amount of personal information printed on checks.
- Review your transactions regularly, contact the bank immediately if you notice fraudulent transactions.

ATM

- Always pay close attention to the ATM and your surroundings. Do your automated banking in a public, well-lighted location that is free of shrubbery and obstructions.
- Maintain an awareness of your surroundings throughout the entire transaction.
- Be wary of people trying to help you with ATM transactions.
- When leaving an ATM make sure you are not being followed. If you are, drive immediately to a police or fire station, or to a crowded, well-lighted location or business. Call 911.
- Do not use an ATM that appears unusual looking and be alert of skimming devices that may be attached.
- Do not allow people to look over your shoulder as you enter your PIN.
- Never count cash at the machine or in public.
- Take your ATM receipt with you.
- Prepare all transaction paperwork prior to your arrival at the ATM. This will minimize the amount of time spent at the machine.
- If you are in a situation where someone demands your money, comply and report it immediately to the local authorities and bank.
- When possible have a friend or family member along
- Keep your engine running, the doors locked and the windows up at all times when waiting in line at an ATM.