FIFTH DISTRICT SAVINGS BANK

Online Safety

Federal Regulators have reported that online threats have changed in recent years. Criminals use various methods to gain access to personal information. Understanding these threats is the first step to building a good defense.

- Phishing – Fraudulent emails claiming to be from your bank, or another trusted source, that provide a link to a website that looks legitimate. You are then asked to verify or enter personal information that is used to access your online account.
- Pharming – Internet traffic is intercepted and rerouted to a fraudulent website.
- Malware – Software designed to damage a computer system without the owner's knowledge. Examples include viruses, worms, Trojan horses, spyware, and adware.

Fifth District understands the importance of having a safe and secure environment when accessing your accounts online and has taken several steps to ensure your personal account information is protected.

- Password Protection – Be sure not to share your password with anyone. Most frauds involving stolen accounts start with someone the victim knows.
- Encryption – When accessing your accounts online, your transactions and personal information are encrypted so that it is readable by only you and the Bank.
- Watermark – This is a picture that is selected by you. It will display throughout the website to show that you are in a secure location.
- Privacy Policies – The Bank has established policies and procedures to protect your personal information.
- Account Information – Account information is never stored on the computer or device used to access online banking.

When using online banking, there are several precautions that you can take to help protect your personal information.

- Passwords – Security begins with a strong password. Experts suggest a strong password include a combination of letters and numbers.
- Anti-virus Protection – Make sure the anti-virus software on your computer is current and scans your email as it is received.
- Email Communication – Email is usually not encrypted. Be careful when sending personal information. If you receive a suspicious email, contact the Bank immediately.
- Be Aware – Do not respond to any unusual requests for personal information. When you are unsure, call the Bank.

Mobile Banking is a fast and easy way to access your account from a mobile device. While mobile banking is similar to online banking in several ways, there are additional actions you can take to help ensure a safe mobile banking environment.

- Enable password protection on your mobile device. This will increase security if your mobile device is lost or stolen.

- Do not connect to mobile banking through a public wireless (WiFi) network. Data transmitted over wireless networks is not encrypted and can be easily intercepted.
- Turn off the Bluetooth connection when not in use. This will reduce the risk of someone using Bluetooth to connect to your mobile device.
- Regularly install operating system and software updates on your mobile device.
- Consider installing mobile antivirus software on your mobile device.
- Try to download mobile applications from verified sources. This will reduce the risk of downloading malicious applications.

If you would like additional information about online safety, you may visit one of the following websites.

- Internet Crime Complaint Center – www.ic3.gov
- Consumer Fraud (Department of Justice Homepage) – www.usdoj.gov
- Federal Trade Commission Consumer Response Center – www.ftc.gov
- Consumer Guides and Protection – www.usa.gov
- Financial Fraud Enforcement Task Force – www.stopfraud.gov
- On Guard Online – www.onguardonline.gov

Thank you for choosing to bank with Fifth District. If you have any questions, please contact the Customer Service Department at 504-363-6513.