Bank of South Texas

Checklist for Cyber Crime Prevention.

Personal information is the currency of the 21st century digital economy. Cyber criminals who obtain your personal data can sell it to a variety of buyers, including spammers, identity thieves, botnet operators, and organized crime rings. These criminals use your personal information to commit identity theft or other fraudulent activities.

How cyber criminals can damage you:

1. Establish credit in your name and utilize the assets involved in the crime.

2. Sell your information to others, which results in an avalanche of email or text messages.

3. Purchase goods or services using your debit or credit card.

4. Access your bank accounts and transfer your funds.

5. Acquire healthcare services using your insurance, resulting in future harm to you.

6. Lock your computer and require you to pay a ransom to get access to your data.

7. Use your information from social media to commit crimes against you.

8. Ruin your identity and credit by using your information to commit crimes.

9. Send text messages using your account, costing you additional fees.

10. Steal your tax refund or create liability by filing false returns utilizing your information.

See reverse side for tips on prevention and mitigation.

Preventing and Mitigating Cyber Crime:

1. Put freezes on your personal credit files at all three bureaus. See contact information below.
2. Do not click on links, photos, or attachements in email or text messages without verifying them first. Use: **redirectdetective.com**
3. Do not click on pop up ads or messages on the internet.
4. Sign up for text alerts for your debit and credit cards.
5. Use a firewall and anti-virus service for all of your devices.
6. Secure your home WiFi with the latest encryption and password protection.
7. Do not post specific personal or business information on social media sites.
8. Do not use unknown WiFi hotspots without protecting your connection with a VPN product.
9. Sign up for alerts regarding password compromises of email accounts.
10. Request that financial institutions put passwords on your accounts to better secure your information.
11. Do not download apps for your devices unless they are from a trusted source.
12. Use a password manager like Roboform or Dashlane.
13. Promptly verify your periodic statements and report any irregularities.
14. Maintain a firewall and anti-virus software on your computing equipment.
15. Keep the operating system and anti-virus software up to date. Turn on “Automatic Updates”.
16. For business computers, use a dedicated computer for banking and do not allow internet surfing on it.
17. Ask your bank about products and services that can help your assets.

Resources:

The Three Credit Bureaus
Website: http://www.equifax.com/home/en_us (tel: 888-298-0045)
Website: www.experian.com/consumer/security_freeze.html (tel: 888-397-3742)
Website: www.transunion.com (tel: 888-909-8872)

If you are a victim of Identity Theft
http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft

Has your email address been compromised?
https://breachalarm.com