IDENTITY THEFT

Protect your valuable information

State Bank is committed to maintaining the privacy of your confidential information. We want you to know we do not solicit your confidential, personal or financial information through email. If you suspect an email is fraudulent, please inform State Bank or a government agency. If you suspect you have been a victim of identity theft or you see unauthorized charges on your accounts, please contact State Bank immediately. We would also advise calling the police to file a police report or case number for later reference.

Please read on to learn about different types of fraud and how you can protect yourself from becoming a victim of fraud or identity theft. For additional information, please contact a State Bank Representative at 815-297-0900.

State Bank
Freeport, IL
1718 S Dirck Dr. - Freeport, IL 61032
815.297.0900 - Member FDIC
www.statebankfreeport.com

Report Suspicious Activity

Report emails or calls to the Federal Trade Commission at www.consumer.gov/idtheft or by calling 1-877-IDTHEFT.

Report suspicious websites to the Internet Crime Complaint Center at www.ifccfbi.gov.

Phishing: The fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an email or website. Phishing is typically carried out by email or instant messaging, and it often directs users to enter details at a fake website that has a look and feel almost identical to the legitimate one.

Twishing: The act of sending a message to a Twitter user in an attempt to obtain his or her name and password.

Vishing: The criminal practice of using features facilitated by Voice over IP (VoIP) phone systems, to gain access to private information.

Smishing: The phishing type derived from "SMS Phishing," SMS (Short Message Service) using cell phone text messaging technology.

Malware: Malware is software designed to secretly access a computer system without the owner's informed consent. Malware is commonly obtained through fraudulent software updates, banner ads, downloadable documents, and key stroke recording.

Mobile Fraud: Mobile devices have opened a new door for fraudsters. Use the tips below to keep your information secure:

- Set a password or PIN so your phone can't be used if it's lost or stolen.
- Don't download software until you verify its security and privacy features.
- Install anti-spyware software specifically designed for your device.
- Be suspicious if you get many unsolicited emails or text messages. It could mean you have a spyware program on your phone.
- Install security software to protect your mobile phone from viruses, some of which can give fraudsters access to your personal information.
- Keep your mobile software up to date.
- Don't let people use your mobile phone until you've logged out of secure sites such as Mobile Banking.

You Can Fight Identity Theft

Protect your information with these tips:

Never provide personal information, including your Social Security number, account numbers or passwords over the phone or Internet if you didn't initiate the contact.

Never click on links within an email you believe to be fraudulent. They may contain a virus that can contaminate your computer.

Do not be intimidated by an email or caller who suggest dire consequences if you do not immediately provide or verify financial information.

If you believe an email contact is legitimate, go to the company's website by typing in the site address directly or using a page you have previously bookmarked instead of a link provided in the email.

If you fall victim to an attack, act immediately to protect yourself. Alert State Bank and place fraud alerts on your credit files. Monitor your credit files and account statements closely.

Credit Bureau Fraud Alert

Call to place alerts on your credit files by contacting the three major bureaus:

Equifax: 800-525-6285

Experian: 888-397-3742

TransUnion: 800-680-7289