Our Customer's Information:

At First Southern Bank, the security of our customers' information is a priority. We are strongly committed to the safety and confidentiality of your records. Because of this, First Southern Bank will NEVER ask you for any private information (such as account numbers, passwords, PINs, social security numbers, etc.) for any of our products through an e-mail. If you feel that you have been victimized by someone pretending to be First Southern Bank, please contact us immediately at (912) 490-1010. You should also contact your local law enforcement agency and complete a complaint form with the Internet Crime Complaint Center at www.ic3.gov and the Federal Trade Commission at www.onguardonline.gov/file-complaint.

Identity Theft:

Identity Theft is one of the fastest growing crimes in America. Scammers, hackers and identity thieves are always looking for methods to steal your personal information. However, there are steps you can take to help protect yourself, such as keeping your computer software to update and giving out your personal information only when you have a good reason. Below are some general banking security tips to help protect your information;

- Sign up for online banking and review your statements and your activity on a regular basis
- Use hard to guess unique passwords and change them regularly
- Sign up for direct deposit whenever possible
- If your account activity looks suspicious or if important mail is delayed, check with the merchant or biller immediately
- Shred receipts, bank statements and unused credit card offers before throwing them away
- Do not give your social security number or other personal information about yourself to anyone who calls you.
- Don't pre-print your social security number on anything.
- When conducting business with a government agency, only fill in the required pieces of information. Certain government agency records are public record and anyone can access the information you disclose to the agency within that record.
- Check your credit report at least once a year to look for suspicious activity. If fraud is detected, contact the all three credit bureaus and take advantage of all recourse and protection periods. The three credit report agencies and the numbers and websites are as follows:
    - Equifax 1-800-685-1111 or www.equifax.com
    - Experian 1-888-397-3742 or www.experian.com
    - Transunion 1-888-909-8872 or www.transunion.com
- Report the loss of any credit cards, debit cards or your driver's license immediately.
- For both businesses and consumers, it is recommended that
    - The computer should be running a supported operating system that is regularly patched with critical vendor updates.
    - The computer should run anti-virus that is regularly updated.
    - A firewall should be located between the internet and the computer.

Internet Fraud:

With the growth of the Internet, scams that had previously been limited to telephone or mail are now being perpetrated via the computer. There are now variants of the fake contest, debt consolidation, business opportunity, miracle cures, and charity scams that are committed with false or misleading websites, or through e-mail solicitations. In addition to the Internet variations of telephone and mail scams, there are new scams that have recently appeared that are unique to the world of computers. While it is impossible to document all of these scams, these are some of the most common:

Non-delivery of Merchandise or Payment

This was the most widely reported type of fraud in 2010. This is when a purchaser does not receive the items purchased over the Internet or telephone, or when a seller does not receive payment for items sold. Sometimes, this crime occurs in the context of an online auction site.

Phishing

This type of fraud is the sending of a false e-mail that claims to be from a legitimate business or government agency. Often times the e-mail claims to be from a financial institution, the Social Security Administration, or the FBI. Often the e-mail claims that billing or account information needs to be updated, or that the victim's help is needed to catch a dishonest employee. Sometimes there is a claim that the individual's account will be frozen or liquidated, if information is not provided. This fraud attempts to get the recipient to reveal personal information, passwords, credit card numbers, or account information. Once this information is obtained, identity theft occurs and the thief uses the information to perpetrate other crimes without the knowledge of the victim.

The Stranded Victim

This occurs when the criminal hacks into an individual's e-mail address book. The criminal then sends an e-mail to contacts in the address book claiming to be stranded in a foreign country and in desperate need of help. The e-mail appears to be from a friend because it comes from his or her e-mail account. The criminal asks for money to be wired to help them out of their bad situation, but it is actually a fictitious story.

Overpayment Fraud

This can occur over the Internet or by mail or phone when the victim receives a payment which is significantly larger than the original sum agreed upon for a product or service. Often this is used when the victim is advertising an apartment rental or the purchase of a vehicle. The victim is then asked to deposit the payment into his or her account and pay back the difference. In actuality, the original payment is counterfeit and the individual is being scammed.

Foreign Lottery Scam

In this scam, you receive a call, email or letter — usually from a foreign country — telling you about a way to select winning lottery numbers, and you need to call a toll-free number to find out more. There is no need to call that number. All the con criminal has is a winning way to take your money.

Beware of Debit Card Scams

Protect yourself from debit card scams.

Criminals are soliciting and contacting customers via cell phone text messages and voice recordings, in an effort to con customers by illegally obtaining personal information.

- These text messages and voice recordings may look and sound authentic.
- They may resemble those sent by legitimate financial institutions, but they are fraudulent.
- Recordings will claim that the customer's Debit Card has been deactivated and to reactivate, the customer must enter their Debit Card number followed by the Personal Identification Number (PIN).

Should you receive a text or voice recording like this, do not provide your Debit Card number or PIN. Contact your Personal Banker immediately to receive guidance on blocking fraudulent transactions.

Password Protection

Take proactive steps to insure your passwords are protected.

In our day and age, we use passwords for everything. Passwords are designed to protect our devices and information, but we also must learn to protect our passwords to prevent hacking from outside parties or individuals. Compromised passwords could potentially result in identity theft or stolen funds, so it is vital to use password protection strategies.

Click on the below tips to learn more.

Avoid using common passwords.

Birthdates, children names, favorite team, and anniversaries are some common passwords that hackers will try first. Avoid passwords like these, as most hackers can access this information from your social media page. Also, avoid using passwords that can be found in the dictionary. Instead, use a mysterious and unique password that mixes letters (upper and lowercase), numbers, and special characters. Here are some tips to help you build a strong password.

Tip 1 Spell a word backwards.

Tip 2 Replace a letter with a special character.

Tip 3 Randomly use capital letters.

Tip 4 Add a number.

If you find that this type of password is hard to remember, then consider making a phrase. For example, the password “I<3FS.” stands for “I love First Southern."

Keep your password a secret.

Never share your password with anyone and also avoid writing your passwords down. If you must have a document of all your passwords and accounts, make sure to keep it in a secure location such as a safe.

Use different passwords each login.

If your password is compromised for one login, the hacker will attempt to use this same password on all your other logins. If the password is the same, the hacker has access to all your accounts and information. By using a different password for each login, this will help block the hacker from getting access to your other accounts.

To help remember each password, first establish a strong base password. Next, add the first three letters of the login service provider to the end of the password.

For example if your base password was "“I<3FS ": Your Amazon password could be I<3FS.AMA. Your Gmail password could be I<3FS.GMA. Your Frist Southern online banking password could be I<3FS.FS.

Business Security:

Corporate Account Takeover is a form of corporate identity theft where a business' online credentials are stolen by malware. Criminal entities can then initiate fraudulent banking activity. For business customers, a risk analysis and control evaluation may need to be performed periodically to help identify weaknesses and minimize the risk of corporate account takeover. Education about cybercrimes to all employees that utilize the company's computers is recommended so that each employee understands that even one infected computer can jeopardize the business and its computer network. A business should advise its employees to

- Not open suspicious emails from unknown persons.
- Be suspicious of emails that appear to be from financial institutions or government agencies or any emails requesting personal information or the business's confidential information. If one of these emails is identified, the business should contact the financial institution or government agency to verify the legitimacy. The business, however, should not call the phone number included in the email, or click on any links or reply to the sender.
- For websites, businesses should block unnecessary or high risk websites and prevent access to websites that employees should not visit during work hours.
- User Accounts:
    a. Each employee that has access to a computer should be set up with a user account and limit the amount of administrative rights on those users.
    b. Require the employees that have user accounts to employ strong passwords and change their passwords frequently.
    c. Deactivate or remove access rights of employees who no longer require access.
- Initiate payments under dual control, with assigned responsibility for transaction origination and authorization. Dual control involves file creation by one employee with file approval and release by another employee on a different computer. Avoid having employees initiate and authorize payment transactions with administrator credentials.