SOUTHERN INDEPENDENT BANK

Your Online Safety Is Important To Us.

Online Banking brings a great deal of convenience to your banking experience. At Southern Independent Bank, we're pleased to offer this service, but we want you to be informed about online safety and security. While we work diligently to incorporate firewalls to ensure your privacy and security, your awareness and education can help prevent ID theft. Please take a moment to access any of these resources listed and to review the FDIC guidelines shown below.

- The FDIC Link *Don't Be An Online Victim: How To Guard Against Internet Thieves And Electronic Scams*

- YouTube line: *Don't Be An Online Victim*

- ThinkStop Connect website to help all *digital citizens stay safe and more secure online*

- RSA website for *Tips For Staying Safe Online*

- McAfee website *Guide to Online Banking Safety for Carefree, Confident and Conservative Consumers*

These Guidelines And Advice Are Offered Directly From The FDIC Website *"Safe Internet Banking"*

The Internet is a public network. Therefore, it is important to learn how to safeguard your banking information, credit card numbers, Social Security Number and other personal data.

Look at your bank's Web site for information about its security practices, or contact the bank directly.

Also learn about and take advantage of security features. Some examples are:

- Encryption is the process of scrambling private information to prevent unauthorized access. To show that your transmission is encrypted, some browsers display a small icon on your screen that looks like a "lock" or a "key" whenever you conduct secure transactions online. Avoid sending sensitive information, such as account numbers, through unsecured e-mail.

- Passwords or personal identification numbers (PINs) should be used when accessing an account online. Your password should be unique to you and you should change it regularly. Do not use birthdates or other numbers or words that may be easy for others to guess. Always carefully control to whom you give your password. For example, if you use a financial company that requires your passwords in order to gather your financial data from various sources, make sure you learn about the company's privacy and security practices.

- General security over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers or Internet service provider to ensure you have the latest in security updates.

If you have a security concern about your online accounts, contact your bank to discuss possible problems and remedies. Remember that nonfinancial Web sites that are linked to your bank's site are not FDIC-insured.

As an added convenience to their customers, some banks offer online links to merchants, retail stores, travel agents and other nonfinancial sites. An outside company's products and services are not insured by the FDIC, and your bank may not guarantee the products and services. As in everyday business, before you order a product or service online, make sure you are comfortable with the reputation of the company making the offer. Only then should you give out your credit card or debit card number. And never give the number unless you initiated the transaction.