identity theft

If someone starts phishing don't take the bait!

CALLS ■ E-MAILS ■ TEXTS

Scammers will try any method to get your personal information!

Protect Your Identity. ***Never give out sensitive personal information to any request made via these methods, no matter how legitimate those requests may appear.***

South Side Bank

Member FDIC Since 1922

southsidebank.com

PEORIA | EAST PEORIA | WEST PEORIA | CHILLICOTHE
BARTONVILLE | WASHINGTON | PEKIN

important reminder to our valued customers!

Internet, telephone and text messaging scams fraudulently attempting to obtain and use your personal or financial information referred to as "Phishing" (E-mail), "Vishing" (Telephone), and "Smishing" (Text) are on the rise. These scams encourage you to verify, re-submit, or update personal or confidential information such as ATM, credit card (card number, expiration date, security code) or debit card numbers as well as social security numbers, Personal Identification Numbers (PIN), user IDs, passwords, and bank account information.

These e-mails, telephone calls, and text messages will probably warn you of a problem that requires your immediate attention. The e-mails, telephone calls, and text messages look and sound very legitimate. Please do not give out any such information to anyone who contacts you either via e-mail or telephone.

If you receive an e-mail or text requesting you to "click on" an Internet link that purports to be the South Side Bank website, please do not do so. This will take you to a look-a-like website in an effort to encourage you to divulge sensitive personal information and could contain a virus that can contaminate your computer. Please do not click on any links embedded in unsolicited e-mails or text messages as they may also contain viruses. In a similar way telephone calls are made advising you to call a local or toll-free number where again sensitive personal information is being requested. **Please do not call the number even if your caller ID is showing a local or bank telephone number. Please simply delete the e-mail or hang up.**

As a reminder…if you receive a call, text, or e-mail directing you to act immediately to avoid your account from being blocked, do not respond. **South Side Bank will never ask for personal or confidential information in these manners. If you have any questions, please don't hesitate to contact us!** Report any suspicious phishing/vishing/smishing scam telephone number or e-mail address to your local law enforcement agency.

Act immediately if you have been hooked by a phisher. If you believe you've been scammed into providing sensitive financial information you should:

- Immediately contact your financial institution. (If ATM, Debit, or Credit Card information was given call the telephone number on the back of the card.)
- Contact your local law enforcement agency.
- Contact these three major credit bureaus and request a fraud alert be placed on your credit report: Equifax, 1-800-525-6285; Experian, 1-888-397-3742; and TransUnion, 1-800-680-7289.