Sherwood State Bank
SSB A COMMUNITY BANK
MEMBER FDIC EQUAL HOUSING LENDER

FRAUD PHISHING AND SMISHING

Cybercriminals are out to lure you in. Don't take the bait.

Online scams that take advantage of consumers are on the rise. Watch out for bogus spam emails and rogue websites that "phish" for your account information.

Avoid Email, Internet and V.O.I.P. Scams

Phishing and smishing scams can be difficult to detect because fraudsters have become very skilled at misrepresenting the businesses you know and trust. Emails created to phish information may contain stolen business logos or other visuals to mislead you into believing they are from legitimate sources. In spear-phishing attacks, cyber criminals target victims because of their involvement in an industry or organization they wish to compromise.

Information that is phished includes:

- Credit card numbers
- Social security numbers
- Deposit account numbers
- User names and passwords

Fraudsters can also smish for your personal information using Voice Over Internet Protocol (V.O.I.P.) technology that can send text or voice mail messages to your phone that appear to be legitimate providers.

Take action

The Federal Trade Commission, a national consumer protection agency, recommends these tips to avoid phishing/smishing scams:

- Do not reply to emails or pop-up messages that ask for personal or financial information.
- Do not follow a link from an email. If you wish to check the validity of your website, type in the site name.

- Keep in mind that online businesses, including banks and merchants, typically will not ask for personal information, such as usernames, PINs and passwords, via e-mail. When in doubt, call the company.
- Do not send personal or financial information in an email or email attachment.
- Be sure to make on-line transaction only on websites that use the https protocol. Look for a sign that indicates that the site is secure (e.g., a padlock on the address bar).
- Do not open attachments or download files unless you are confident of the source.
- Keep your computer's anti-virus software and firewalls updated. Many of the latest browsers have a built-in phishing filter that should be enabled for additional protection.

The cost of cyber-espionage and cybercrime to the U.S. is as much as $100 billion each year.*

Be wary of any email that:

- Tells you there is a problem with your account.
- Directs you to a website where you are asked to provide sensitive information.
- Does not include a phone number you recognize to be genuine.

If you think you have been phished, quickly contact your financial institution and/or debit card company to alert them of potential fraud. You should also contact the three major credit bureaus to request that a fraud alert be placed on your credit report:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241P.O.	Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
800.685.1111	888.397.3742	800.888.4213

"Phishing" is a popular form of computer fraud that uses deception to get personal financial information from targeted individuals. The cybercriminal lures victims by creating emails, pop-up windows and websites that appear to represent a legitimate business in order to obtain private information. "Smishing" is a similar phish for personal financial information that is completed by sending a single message over a cell phone in the form of text or voice mail.

The Federal Trade Commission (FTC) also investigates consumer fraud through the Bureau of Consumer Protection. You can forward unsolicited commercial email (spam), including phishing messages, directly to the FTC at spam@uce.gov.

* Source:"Annual U.S. Cybercrime Costs Estimated at $100 Billion", Siobhan Gorman, Wall Street Journal, July 2013