FACTS Schemes, Scams & Frauds

Your bank has security measures to protect your account information, but they can't be effective without your help and cooperation. Many threats come as a result of hacking into individual computers or obtaining account information and security codes from individuals.

WHAT:	**Phishing –** a criminal attempt to steal your personal information through fraudulent emails or smart-phone texts. They are often very believable, luring the victim to a site that asks them to provide (or "verify") personal financial details such as account numbers and social security numbers.
Protect Yourself:	OSB Community Bank will not send emails or phone asking for your personal information – we already have it.
WHAT:	**Spyware –** a term used for criminal software that a victim unknowingly loads on a personal computer. Once there, the spyware collects personal information and sends it to the criminal.
Protect Yourself:	Up-to-date security software is the best defense

TIPS to minimize the risk of fraud:

- Monitor bank statements and credit card bills for signs of ID fraud.
- Use up-to-date firewalls and antivirus/antispyware software on all computers.
- Be especially cautious when using remote devices (such as Smart Phones, Tablets, Laptops) to ensure you are using a secure connection.
- Shred or tear up unwanted documents that contain personal information before discarding contact.
- Review your free consumer credit reports annually.
- Review your bank account activity daily.
- Never give personal information over the phone or the Internet unless you initiated the contact.
- Public connections are not secure.
- A secure (or "encrypted") transaction will have these two features:
    - An icon of a lock appears in the bottom strip of the web browser.
    - The URL address for the Web page changes from "http" to "https' for the page at which you input the personal data.
- Beware of spending time on unknown websites.
- For added security, it is recommended that you exit the browser completely when you are finished. You may also want to consider clearing your browser's cache and deleting any temporary files.

- Memorize your social security number and passwords; don't carry them with you. Don't use your birth date as your password.

FREE CREDIT REPORTS – THE BEST DEFENSE OF ALL: When it comes to guarding against Identity Theft and Account Hijacking, perhaps the most important tool at your deposal is your credit report. It details all your credit transaction accounts, and will be the first place that unusual charges or entirely new accounts will appear. The good news is that you can monitor your credit report for FREE! But you must exercise this option through specific channels. Since you are entitled to a free report from each of the three major credit reporting agencies, security experts advise you get a free report from each one every four months. That way, you can keep an eye on your personal account safety year round. To order your free credit report go to: www.annualcreditreport.com 1-877-322-8228.

Web sites for credit reporting agencies:

Equifax 800-525-6285 www.equifax.com
Experian 888-397-3742 www.experian.com
TransUnion 800-680-7289 www.transunion.com

Web sites for credit card companies:

American Express www10.americanexpress.com
Discover www.discovercard.com/discover/data/products
MasterCard www.mastercard.com/education/fraud
Visa www.usa.visa.com/personal

RESOURCES:

The Michigan State Police (MSP) Region I Special Investigation Division: www.michigan.gov/identity-theft
Federal Deposit Insurance Corporation: www.fdic.gov/comsumers
U.S. Secret Service: www.secretservice.gov
U.S. Postal Inspection Service: www.usps.com/postalinspectors
Internet Crime Complaint Center: www.ic3.gov
Consumer Fraud (Department of Justice Homepage): www.usdoj.gov
Federal Trade Commission (FTC) Consumer Response Center: www.ftc.gov
Consumer Guides and Protection: www.usa.gov
Financial Fraud Enforcement Task Force: www.stopfraud.gov

Suggested ways businesses can avoid fraud

- Review transaction reports daily to confirm the validity of transactions originated.
- Use the 'alert' function of internet banking to verify daily activity.
- Delete or request that the Bank delete the user-names for terminated employees.
- Periodically review the risks your company takes when originating electronic transactions and take action to reduce identified risks.
- Use a dedicated, highly-secured computer for banking.
- Adopt good internal security policies.

Report fraudulent activity

Law enforcement agencies and many financial institutions around the world work together to stop scammers and provide consumers with the information they need to avoid fraud. If you observe suspicious account activity or fraudulent emails or websites, contact customersupport@osbcb.com or OSB Community Bank at 1-800-466-2990 or 1-517-592-3205.

If you believe you have been the victim of a scam, you can also file a complaint with the Federal Trade Commission at www.ftc.gov, or call 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4621. If you are outside the U.S., file a complaint at www.econsumer.gov.

All complaints are entered into the Consumer Sentinel Network, a secure online database used by hundreds of law enforcement agencies in the U.S. and abroad.