KCSB

KALAMAZOO COUNTY STATE BANK

Cybersecurity Awareness Basics

Consumers increasingly rely on computers and the Internet for everything from shopping and communicating to banking and bill-paying. But while the benefits of faster and more convenient cyber services for bank customers are clear, the risks posed by these services as well as the strategies for preventing or recovering from cyber-related crimes may not be as well-known by the average consumer and small business owner.

Common cyber-related crimes include identity theft, frauds, and scams. Identity theft involves a crime in which someone wrongfully obtains and uses another person's personal data to open fraudulent credit card accounts, charge existing credit card accounts, withdraw funds from deposit accounts, or obtain new loans. A victim's losses may include not only out-of-pocket financial losses but also substantial costs to restore credit history and to correct erroneous information in their credit reports.

In addition to identity theft, every year millions of people are victims of frauds and scams, which often start with an e-mail, text message, or phone message that appears to be from a legitimate, trusted organization. The message typically asks consumers to verify or update personal information. Similarly, criminals create bogus websites for such things as credit repair services in the hopes that consumers will enter personal information.

If you think you are a victim of a fraud or scam, contact your state, local, or federal consumer protection agency. Local law enforcement may be able to provide advice and assistance. By promptly reporting fraud, you improve your chances of recovering what you have lost and you help law enforcement. The agency you contact first may take action directly or refer you to another agency better positioned to protect you.

Violations of federal laws should be reported to the federal agency responsible for enforcement. Consumer complaints are used to document patterns of abuse, allowing the agency to take action against a company.

People who have no intention of delivering what is sold, who misrepresent items, send counterfeit goods or otherwise try to trick you out of your money are committing fraud. If you suspect fraud, there are some additional steps to take:

- Contact the Federal Trade Commission (FTC). The FTC enters internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
-
- If the fraud involved mail or an interstate delivery service, contact the U.S. Postal Inspection Service (https://postalinspectors.uspis.gov/). It is illegal to use the mail to misrepresent or steal money.

How to Avoid Identity Theft

- Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with;

- Kalamazoo County State Bank will NOT contact you by phone, email, text, or any other means and ask for your online banking credentials;

- Be suspicious if someone contacts you unexpectedly online and asks for your personal information. It doesn't matter how legitimate the e-mail or website may look. Only open e-mails that look like they are from people or organizations you know, and even then, be cautious if they look questionable. Be especially wary of fraudulent e-mails or websites that have typos or other obvious mistakes;

- Don't give out valuable personal information in response to unsolicited requests. Social Security numbers, financial account information and your driver's license number are some of the details that should be kept confidential;

- Shred old receipts, account statements, and unused credit card offers;

- Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your social security number, or phone numbers;

- Pay attention to billing cycles and account statements and contact your bank if you don't receive a monthly bill or statement since identity thieves often divert account documentation;

- Review account statements thoroughly to ensure all transactions are authorized;

- Guard your mail from theft, promptly remove incoming mail, and do not leave bill payment envelopes in your mailbox with the flag up for pick up by mail carrier;

- Obtain your free credit report annually and review your credit history to ensure it is accurate;

- Use an updated security program to protect your computer; and

- Be careful about where and how you conduct financial transactions, for example don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.

How to Avoid Frauds & Scams

There are numerous scams presented daily to consumers so you must always exercise caution when it comes to your personal and financial information. The following tips may help prevent you from becoming a fraud victim:

- ➢ Be aware of incoming e-mail or text messages that ask you to click on a link because the link may install malware that allows thieves to spy on your computer and gain access to your information;

- ➢ Be suspicious of any e-mail or phone requests to update or verify your personal information because a legitimate organization would not solicit updates in an unsecured manner for information it already has;

- ➢ Confirm a message is legitimate by contacting the sender (it is best to look up the sender's contact information yourself instead of using contact information in the message);

- ➢ Assume any offer that seems too good to be true, is probably fraudulent;

- ➢ Be on guard against fraudulent checks, cashier's checks, money orders, or electronic fund transfers sent to you with requests for you to wire back part of the money;

- ➢ Be wary of unsolicited offers that require you to act fast;

- ➢ Check your security settings on social network sites. Make sure they block out people who you don't want seeing your page;

- ➢ Research any "apps" before downloading and don't assume an "app" is legitimate just because it resembles the name of your bank or other company you are familiar with;

- ➢ Be leery of any offers that pressure you to send funds quickly by wire transfer or involve another party who insists on secrecy; and

- ➢ Beware of Disaster-Related Financial Scams. Con artists take advantage of people after catastrophic events by claiming to be from legitimate charitable organizations when, in fact, they are attempting to steal money or valuable personal information.

To report suspicious activity or other security-related events, please contact one of our branches:

Schoolcraft – (269) 679-5291 or schoolcraft@kcsbank.com
Mattawan – (269) 668-3386 or mattawan@kcsbank.com
Vicksburg – (269) 649-0001 or vicksburg@kcsbank.com

Additional Cybersecurity Resources

FFIEC www.ffiec.gov/cybersecurity.htm

The White House www.whitehouse.gov/issues/technology www.whitehouse.gov/issues/foreign-policy/cybersecurity

Department of Homeland Security www.dhs.gov/topic/cybersecurity www.dhs.gov/stopthinkconnect www.us-cert.gov

Federal Bureau of Investigation www.fbi.gov/about-us/investigate/cyber http://www.ic3.gov/default.aspx

U.S. Secret Service www.secretservice.gov/ectf.shtml www.secretservice.gov/ntac.shtml

SANS Institute www.sans.org

Financial Services Information Sharing and Analysis Center www.fsisac.com

ISACA www.isaca.org

Open Web Application Security Project (OWASP) www.owasp.org

Software Engineering Institute CERT Division www.cert.org/resilience/ www.cert.org/cybersecurity-engineering/

National Institute of Standards and Technology www.nist.gov/cyberframework/index.cfm http://csrc.nist.gov/publications/