Cyber Security Awareness Basics (source: fdic.gov)

Consumers increasingly rely on computers and the Internet — the "cyber" world — 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. Also, a local law enforcement officer 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. 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.