Computer-related crimes affecting businesses and consumers are frequently in the news. While Federally insured financial institutions are required to have vigorous information security programs to safeguard financial data, financial institution customers also need to know how to steer clear of the fraudsters.

The following are some suggestions on how to protect your information.

- **Protect computers and networks**: Install security and antivirus software that protects against malware, or malicious software, which can access a computer system without the owner's consent for a variety of uses, including theft of information.
- **Require strong authentication**: Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices and online accounts by using combinations of upper - and lower-case letters, numbers, and symbols that are hard to guess and changed regularly.
- **Control access to data and computers and create user accounts for each employee**: Take measures to limit access or use of business computers to authorized individuals. Only give employees access to the specific data systems they need to do their jobs, and don't let them install software without permission.
- **Learn the basics**: Establish security practices and policies for employees, such as appropriate Internet usage guidelines, and set expectations and consequences for policy violations. Stress the importance of strong cybersecurity, especially when it comes to handling and protecting customer information.
- **Be careful where and how you connect to the Internet**: Public computers, such as at an Internet café, hotel business center, or public library, may not be secure. You shouldn't connect to a network if you are unsure about the wireless connection you are using, as in the case with many free "Wi-Fi" networks at public "hotspots."
- **The dangers of suspicious emails**: Be suspicious of unsolicited e-mails asking you to click on a link, open an attachment, or provide account information. It's easy for cyber criminals to copy a reputable company's or organization's logo into a phishing e-mail. By complying with what appears to be a simple request, you may be installing malware on your network. The safest strategy is to ignore unsolicited requests, no matter how legitimate they appear.
- **Patch software in a timely manner**: Software vendors regularly provide patches or updates to their products to correct security flaws and improve functionality.
- **Make backup copies of system and data**: Regularly backup the data from computers. Apply security measures such as encryption to the data.
- **Pay attention to your bank accounts**: Put in additional controls, such as confirmation calls before financial transfers are authorized with the financial institution.

Cybersecurity:

A Beginner's Vocabulary

Antivirus Software. Most Internet users are well aware of these programs since nearly every computer sold today provides at least short – term access to this type of software. In a nutshell, these programs protect your computer from Internet viruses or codes that can quickly disable your computer (or an entire network). When functioning properly with all necessary updates, this software will constantly monitor your computer to prevent viruses from "infecting" it.

Back Door. Sometimes used interchangeably with the term "trap door," a software or hardware designer makes ones of these to allow herself (or privileged others) to circumvent computer security.

A Key-logger. This type of harmful or malicious program is used to infiltrate your computer to record information about all of your computer keyboard activities, including all Internet browsing activities, e-mail usage and instant messaging communications.

Phishing. These Internet scam programs often contact unsuspecting people via e-mail, urging them to visit *fake* websites designed to look like those run by well-known banks or other financial institutions. Perpetrators then try to obtain private information by telling users it's time to update their account passwords or usernames. If unwitting people comply, all types of fraud, including identity theft, may result.

Trojan Horse. This type of harmful computer program can be easily installed on your computer while you're downloading unknown programs or files off the Internet (or simply opening up unfamiliar email attachments). A Trojan horse will nearly always damage your computer in some way.

Spyware. This type of software is installed on a network of computers without the owner's knowledge. Its main purpose is to gather personal/group information and communicate it to an unknown third party. Spyware can monitor your activities and even pick up critical information like credit card numbers, usernames and passwords.