Protecting You and Your Business

FIRST CITIZENS Community Bank

Malware – Malicious Software

Malware, short for "malicious software," includes any software (such as a virus, Trojan, or spyware) that is installed on your computer or mobile device. The software is then used, usually covertly, to compromise the integrity of your device. Most commonly, malware is designed to give attackers access to your infected computer. That access may allow others to monitor and control your online activity or steal your personal information or other sensitive data.

There are *many* unique types of malware that can infect your computer:

- ✓ **Adware:** a type of software that downloads or displays unwanted ads when a user is online or redirects search requests to certain advertising websites.
- ✓ **Botnets:** networks of computers infected by malware and controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Many botnets are designed to harvest data, such as passwords, Social Security numbers, credit card numbers, and other personal information.
- ✓ **Ransomware:** a type of malware that infects a computer and restricts access to it until a ransom is paid by the user to unlock it.
- ✓ **Rootkit**: a type of malware that opens a permanent "back door" into a computer system. Once installed, a rootkit will allow additional viruses to infect a computer.
- ✓ **Spyware:** a type of malware that quietly gathers a user's sensitive information (including browsing and computing habits) and reports it to unauthorized third parties.
- ✓ **Trojan**: a type of malware that disguises itself as a normal file to trick a user into downloading it in order to gain unauthorized access to a computer.
- ✓ **Virus:** a program that spreads by first infecting files or the system areas of a computer or network router's hard drive and then making copies of itself.
- ✓ **Worm**: a type of malware that replicates itself over and over within a computer.

If you've been compromised…

Infections can be devastating to an individual or organization, and recovery can be a difficult process that may require the services of a reputable data recovery specialist. If your computer has been compromised by malware, you can either consult with a reputable security expert to assist in removing the malware or use a legitimate program to help eliminate the infection. Some legitimate programs are:

- ✓ F-Secure: http://www.f-secure.com/en/web/home_global/ online-scanner
- ✓ McAfee: http://www.mcafee.com/stinger
- ✓ Microsoft: http://www.microsoft.com/security/scanner/en-us/ default.aspx
- ✓ Sophos: http://www.sophos.com/VirusRremoval

Member FDIC