Malware

WHAT IS MALWARE?

Malware or "malicious software" is designed to infiltrate or damage a computer system without the owner's knowledge or informed consent. Software is considered Malware based on the creator's perceived intent rather than any particular features the software may include. The term Malware covers a host of software including computer viruses, worms, Trojan horses, spyware, and other malicious software.

HOW DOES MALWARE WORK?

Malware is a significant problem. Malicious programs are now considered aggressive and sophisticated, often using a combination of techniques to accomplish their objective. Malware that combines exploitation of a flaw in operating system, browser software, or other applications (e.g., iTunes, Adobe, etc.) with viruses and other Malware is quickly growing in popularity.

Malware for personal digital assistants (PDAs), smart phones and other portable computer-based tools has now entered the market as well. As portable devices continue to grow in popularity, so too will this form of Malware.

Spyware, Trojan horses, and key loggers are becoming increasingly popular with criminals, including organized crime. These programs can be used to obtain confidential information about the user of the infected computer, such as account numbers and PINs, login credentials, the contents of email, even Internet habits, and the resulting data can easily be sold or used directly to perpetrate fraud.

As a result of Malware, users may find that their computers have become part of a botnet. A botnet is a collection of software robots, or bots, that run autonomously and automatically. While the term "botnet" can be used to refer to any group of bots, this word is generally used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed via worms, Trojan horses, or backdoors, under a common command-and-control infrastructure. If you take the necessary steps to limit your exposure to Malware, your computer will be less likely to become part of a botnet.

WHAT SHOULD I BE LOOKING FOR?

Although the phishing attacks that lead to Malware are designed to be nearly impossible to distinguish from legitimate emails messages, there are some common signs you can look for.

- Attackers urge the recipient to click on the link to update or verify account information, re-activate an account, or cancel an order.

- Attackers convey a sense of urgency and often mention negative consequences for failing to respond.
- Attacks are not consistent with other email messages from the business.
- Messages do not contain any personalization: the recipient's name, the last four digits of their account number, or other information that shows that the sender knows something about the recipient's account.
- Attacks often contain spelling errors and bad grammar.
- Messages often claim the user has ordered something that they never ordered.

WHAT SHOULD YOU DO IF YOU RECEIVE A SUSPICIOUS EMAIL?

- Do not respond.
- If you are unsure of its authenticity, call a phone number you trust such as the one on your most recent statement.
- If it is an email message that appears to be from Fifth Third Bank, you can forward it to 53investigation@security.53.com to help track the phishers and shut down the fraudulent sites or disconnect fraudulent phone numbers.
- If it appears to be from another company or financial institution, you can forward it to the Anti-Phishing Working Group at reportphishing@antiphishing.org.
- Delete the message from your Inbox.
- If you responded to the message and provided information, contact Fifth Third Bank Customer Service immediately at **1-800-676-5869**.

HOW CAN I PROTECT MYSELF/MY BUSINESS?

- Don't open attachments from unsolicited emails at work or at home. This is the most common way computers become infected with malware.
- Install a firewall to prevent unauthorized access.
- Install and run anti-virus and anti-spyware software on your computer and keep them up-to-date.
- Try to avoid spyware altogether by taking the following steps before loading software onto your home computer:
  - Read the license agreement. Learn what to look for at http://grc.com/oo/fineprint.htm.
  - Search the Internet for spyware reports. Use the software's name and the word 'spyware' as your search keywords.
- Do not allow anyone to access your computer without your knowledge. Keep your computer turned off or locked when you're not using it.
- Never use the "save ID and password" option.
- Never write your user ID and/or password on a piece of paper and leave it near your computer.
- Install updates and patches for your home computer's operating system and all of your installed applications (e.g., iTunes, etc.).
- Download Trusteer Rapport from the http://www.53.com Online Security Center onto your home and business computer.

FIFTH THIRD BANK