AVOIDING MALWARE: VIRUSES, TROJANS AND WORMS

In recent years, malicious software—malware—has become increasingly sophisticated, both in terms of how it is used and what it can do. By understanding the tools being used by criminals, we can better defend ourselves.

Did you know? Many people who think their computer must be broken because it’s running so slowly are simply the victims of malware.

**Viruses**
The term "computer virus" is sometimes erroneously used as a catch-all phrase to include all types of malware, such as Trojans and worms, which are technically different. A computer virus is a computer program that can replicate itself and spread from one computer to another (in some form of executable code) when a user unwittingly sends it over a network or the Internet, or carries it on a removable medium such as a floppy disk, CD, DVD, or USB drive. In order to replicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to executable files that may be part of legitimate programs. If a user attempts to launch an infected program, the virus’ code may be executed simultaneously.

Similar to a computer virus, a mobile virus targets mobile phones or wireless-enabled PDAs. Security companies, cellular operators and phone makers are moving to quash these threats before they spiral out of control.

**Trojan horses**
A Trojan horse is a program that purports to be useful but actually harbors hidden malicious code. Just like the horse from the Trojan War, its function is to deceive the user into bringing an intruder inside. A Trojan horse can be used to set up a back door in a computer system so that the intruder can gain access later. A back door is a method of bypassing normal authentication and securing remote access to a computer, while attempting to remain undetected.

Unlike viruses, Trojan horses do not replicate themselves, but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to get rid of viruses but instead introduces viruses onto the computer. Fake antivirus software programs (called Fake AV) that pop up when browsing, often carry a Trojan horse. Trojan-type malware accounts for a large percentage of the malware detected around the world.

**Worms**
Self-replicating code that automatically spreads across a network is called a worm. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that appears harmless but hides malicious functions. Worms and Trojan horses, like viruses, may harm a computer system’s data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are sneaky doing nothing to call attention to themselves.

What can I do to prevent my computer from becoming infected?
Malware gets secretly installed on computers in many different ways, making it difficult to protect against. While there is no method that can 100% guarantee that your computer will not be infected with malware, there are a number of steps that you can take to lessen the probability of this happening.

**10 Ways to Protect Your Computer from Malware**

1. Keep your firewall turned on. A firewall puts a protective barrier between your computer and the Internet. Turning it off for even a minute increases the risk that your PC will be infected with malware.
2. **Install or update anti-virus & anti-malware software from a trusted source.** You need both to prevent malicious software programs from embedding themselves on your computer. Set them to update automatically.

3. **Install or update your antispyware technology.** Some spyware collects information about you without your consent; others produce unwanted pop-up ads on your web browser.

4. **Keep your operating system up to date.** Updates are needed to fix security holes.

5. **Be careful what you download.** Careless downloading can beat even the most vigilant anti-virus/anti-malware software. Investigate any free software before downloading.

6. **Use flash drives cautiously.** Putting your flash drive (sometimes called a thumb drive) in a computer that is infected could corrupt the drive, and ultimately your computer.

7. **Close your browser when you’re done working.** Delete the cache, history and passwords each time. Also, turn off your computer. Being "always on" leaves you connected to the crooks. Turning the computer off effectively severs an attacker’s connection.

8. **Ignore scareware.** Scareware pop-ups may look like actual warnings from your system, but they are not. Made to appear authentic, they often deliver malicious payloads. Close them with the “X” button.

9. **Review your bank and credit card statements.** It’s one of the easiest ways to get the tip-off that something is wrong. Also, monitor your credit reports. For even more protection, you might consider a credit monitoring service that will alert you when there’s an entry in your credit file.

10. **Choose strong passwords.** Create at least an eight-digit complex password to protect activities like online financial transactions and don’t use that password anywhere else. Change your most critical passwords every 90 days.

Remember, it’s much easier to stop the shopping spree before it ever begins.

Your financial institution has taken strong measures to ensure the security and safety of your account and its overall online banking system. By staying alert to potential security threats and keeping in mind the suggestions listed above, you can help us keep online banking extremely safe and secure. Follow the good practices and use the knowledge we’ve provided here, and you will be much more prepared to enjoy the conveniences of online services with peace of mind!