Computer Security

Solutions

What is the Problem?

In general, the security issues we are trying to prevent include:

- illegal or unwanted access to your computer
- access to your personal information
- loss or damage of information
- loss or damage of computer programs
- loss of control over computer operations

Anti-Virus

Viruses (and worms, and trojan horses) are the most publicized type of threat. They are also generally the most harmful and destructive given the chance to infect your computer.

The tools to combat these threats have been around the longest, and fall into the general software category of “anti-virus”.

Anti-Virus
Detecting & Treating the Virus

A biological virus has a genetic code, or signature, that our immune system learns to identify and defeat.

Computer viruses also have (computer) codes which form a signature.

Each virus generally needs its own “cure,” so security companies maintain large databases with information on each virus (signature and cure).

Anti-Virus
"Always on" software

Most anti-virus software runs on your computer at all times. It actively scans files for virus signatures, and if a virus is detected, it is neutralized (cured) or quarantined (incurable).

Some software only scans new or external files (e.g., email attachments). Other software might scan any program running on the computer.

Anti-Virus
Using System Resources

Having a program running all the time, and checking many files on the system, can cause performance problems (i.e., computer runs slow).

In addition, there are cases of “false-positives”, where anti-virus software will incorrectly identify a legitimate program as a virus.

On the flip-side, a poor, old, or out-of-date program might not recognize a new virus, so the computer might get infected anyway.

Spyware Cleaners

The line between viruses and spyware is becoming blurry. More and more anti-virus programs also detect and remove spyware.

There are also many software products that will find and remove spyware already installed on a system.

These are similar to anti-virus, in that they look for a signature files and then remove the spyware file(s).

Firewalls

A firewall is a piece of software running on your computer or other network hardware (e.g., router) that acts as a barrier between a computer and the rest of the world.

At the most basic level, a firewall is a complete barrier, meaning no information passes the firewall. This type of “lockdown” is not practical for most computer use.

Firewalls

In a more useful mode, firewalls act as filters that allow the authorized flow of data over specific channels (ports) on the computer system.

By limiting the type of traffic, and the routes it can use, a firewall can significantly reduce the ability of hostile programs to access a computer.

In addition, some firewalls will also prevent unauthorized software (e.g., worms, spyware) already on the computer from communicating with the outside world.

System Updates

As security flaws are identified in their products, manufacturers will usually release a patch or update to close the security vulnerability.

Many systems are infected simply because the owners did not keep their software up to date (particularly the operating system).

Modern systems are generally very active about notifying users of critical updates, and can usually be placed into an automated update mode.

Popularity Contest

Some security breaches are targeted (e.g., against a specific organization). In those cases, the target is whatever system is used by the organization.

In most cases, however, security threats are more generic. They want to target as many systems as possible, so their efforts to develop malware turn into a popularity contest.

It is possible to improve security by avoiding more popular targets.

Popularity Contest

- Operating Systems:
  - Windows (90%)
  - MacOS (8%)
  - Linux (2%)
- Web Browsers
  - Chrome (45%)
  - Windows (20%)
  - Firefox (15%)
- Mobile Devices
  - Android (49%)
  - iOS (11%)
  - Windows (14%)