

How Can I Secure My Computer Systems?

For most, it is no surprise that the Internet can be a dangerous place, full of malicious attacks that can slow down, take over, or completely ruin any system. But there is good news. There are various ways that individual users and companies can keep their systems safe.

Balancing Act

Computer networking is a balancing act. Assessing the tradeoffs between functionality and security can be a daunting task for anyone. It can be said that the only truly safe computer is a computer never connected to the Internet. But for most users, simply disconnecting is not an option. Therefore, you must balance your desired amount and type of Internet usage with the types and degrees of security you implement. After all, solid security mechanisms are rarely free and always take time to implement and maintain. Over-securing can waste more than it saves.



Buzzword Definitions

Spam – Spam is unsolicited e-mail on the Internet. From the sender's point-of-view, spam is a form of bulk mail, often sent to a list obtained by companies that specialize in creating huge e-mail distribution lists. To the receiver, it usually seems like junk e-mail. Spam is roughly equivalent to unsolicited telemarketing calls. Spammers typically send a piece of e-mail to a distribution list in the millions, expecting that only a tiny number of readers will respond to their offer. It has become a major problem for all Internet users.

Hackers – A hacker is someone (a very smart computer programmer) who attempts to crack someone else's system or otherwise uses programming or expert knowledge to act maliciously. Hackers have been known to break into impenetrable networks such as the military, large banks, and international media giants – causing widespread panic & costing millions for better security and damage control.

Spoofing – also known as IP address forgery is a hijacking technique in which a hacker masquerades as a trusted host to conceal his identity, hijack browsers, or gain access to a network. The hijacker obtains the IP address of a legitimate host and alters it so that the legitimate host appears to be the source. For example, if the hijacker spoofed the Library of Congress Web site, then any Internet user who typed in the URL www.loc.gov would see spoofed content created by the hijacker. If a user interacts with dynamic content on a spoofed page, the hijacker can gain access to sensitive information such as a credit card number or password. The hijacker would also be able to take control of a compromised computer in order to send out spam.

Virus – A computer virus is a program or code that replicates by being copied to another program, or document. Viruses can be transmitted as attachments to an e-mail or in a downloaded file, or be present on a CD. The immediate source of the e-mail note, downloaded file, or CD you've received is usually unaware that it contains a virus. Some viruses wreak their havoc as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are benign or playful in intent and some can be quite harmful, erasing data, crashing systems, or causing your hard disk to require reformatting.

Cookies – A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time. Cookies are commonly used to rotate the banner ads that a site sends so that it doesn't keep sending the same ad as it sends you a succession of requested pages. They can also be used to customize pages for you based on your browser type or other information you may have provided the Web site. Web users must agree to let cookies be saved for them, but, in general, it helps Web sites to serve users better.

Spyware – Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

Pop-ups – Pop-up ads are a form of online advertising intended to increase web traffic or capture email addresses. It works when certain web sites open a new web browser window to display advertisements. A less intrusive variation on the pop-up window is the **pop-under** advertisement. This opens a new browser window, behind the active window. Pop-unders interrupt the user less, but are not seen until the desired windows are closed, making it more difficult for the user to determine which Web site opened them.

Pieces of the Puzzle

All computers and networks consist of three major mechanisms:

- Software and hardware components
- Users
- Procedures

Securing a system entails:

- Securing the software and hardware through various means
- Evaluating the trustworthiness of system users and administrators
- Bolstering the reliability of established procedures for using and managing the system

How can you possibly minimize all of these risks, especially as attackers invent new threats? Implementing a good password policy (i.e., making passwords complex and keeping them secret) is always an important first line of defense, but don't rely solely on it.

There are other types of computer and network security that will help prevent and deter security holes:

Securing Large Networks

For any company, protecting certain data is essential. Company leaders must define a Security Policy, implement it company-wide, then enforce those policies through communication, tools, automation, and reporting. An additional security mechanism is for management to establish expectations for all users and to maintain safety by tracking network usage.

No matter how knowledgeable and careful users are, attackers can still find their way into systems without ample security mechanisms. Large, network security appliances (think **SonicWall**) are often required to provide sufficient protection for medium-to-large networks.

These types of security systems apply a layered security model, including any combination of the following (depending on the use and needs of the network):

- Establish security policies and implement company-wide
- Comprehensive firewalls
- Anti-virus systems
- Intrusion, prevention, detection, and automated reporting
- Routers

Internet-borne threats constantly become increasingly complex. In response, the technology needed to protect against these threats must continually evolve.

Never assume that your systems are well-protected forever, even if you use all of the best security measures. Every organization must continually assess the threatening state of the Internet and evaluate their security accordingly. Schedule periodic risk assessments and never wait to act when you find a weakness.

However, evaluating your system and defining your security needs does not need to be daunting. You can get help from a professional security implementation team. Companies such as ITX can design, install, and provide support for a security system that meets your needs.

Personal Computer Security

Though an individual rarely risks as much as an organization, anyone that connects a computer to the Internet should understand the basics of Internet threats and security.

The instant that your computer is connected to the Internet or to another computer that has been connected to the Internet, attackers may be knocking at your ports, attempting to break into your system.

Attacks can go undetected for long periods of time before inflicting damage. Furthermore, even if you have ample protection against an attack that has found its way onto your system, you could unknowingly pass the threat along if you connect to another computer.

ITX recommends that any computer that connects to the Internet, if even rarely and for short periods of time, should have at least the following security mechanisms in place:

- **Antivirus** implemented via hardware or software: Prevents, detects, and removes viruses, worms, and other threats
- **Email scanner**: Usually included with antivirus products and help detect and prevent threats transmitted via email messages, and to prevent spoofing
- **Anti-spyware** implemented via hardware or software: Detects and/or removes spyware that can share your information with unauthorized users and slow down your system
- **Firewall**: Either a hardware solution for a small office, or (as a last resort and not as reliable) a software solution
- **Routers**: If you plan to connect two or more computers with Internet access, use a router. Some single-computer users also choose to take advantage of the strong hardware firewall that most routers include.

Some Internet service providers (ISPs) offer security features like server-side antivirus and anti-spyware mechanisms. These are beneficial, but should not be substituted for client-side security.

Updates and Patches

The need to stay current with updates and patches cannot be overstressed. They are often released in response to new threats, or those increasing in frequency, so not obtaining a security update can leave you more exposed than ever. When possible, use automatic updates.

In general, updates are essential for:

- Your operating system
- Security applications
- Any application that has the ability to access the Internet. This includes most applications, and attackers can use your word processing program or media player to break into your system.

Finally, don't count on your computer or applications to come out of the box with sufficient security mechanisms in place. Apply all updates as soon as possible after receiving any new hardware or software.

Can your business afford to be down for days, or worse, to lose your critical customer information due to a virus or a hacker? Make sure your business systems are secure. Get a **security audit** by calling the experts at ITX at (970) 282-7333, visit <http://www.itxfc.com/>, or e-mail sales@itxfc.com.