Security threats faced by Telecommuters while connected to the Internet

By: **Richard A. Bassett**

Asst. Professor MIS – Western Connecticut State University

Email: bassettr@wcsu.edu

Overview

The pervasiveness of the Internet has enabled remote workers and their employers to enjoy Telecommuter arrangements at unprecedented levels within the past several years. Contributing factors such as the dropping price of technology, increasing functionality of systems and bandwidth becoming more affordable and available have all helped companies to overcome the previously significant technological barriers in setting up remote workers.

Many of the remote Telecommuters use the Internet as a transport vehicle to access corporate information resources. As such it is important for these remote computer users to have at least a basic understanding of the security risks that they face while they are connected to the Internet.

Security Threats

A great number of users that access the Internet from their home computers are unaware of the many security risks that they are exposed to while they are connected to the Internet. Certainly most computer users have heard of computer viruses and acknowledge their existence, as there always seems to be a news story featuring the virus of the day. Still, the vast majority of computer users lack a detailed understanding of the potential payload damage that viruses can deliver to their system as well as understanding the other potential computer security risks that they are exposed to.

Computer viruses are commonly delivered to unsuspecting users via the receipt of a file that is attached to an email message. The attached files are often disguised with enticing file names or messages that encourage the user to open the attachment. Sometimes these messages appear to come from trusted sources but are actually spoofed. Once the unsuspecting user opens or executes the harmful attachment, the full wrath of the virus can be released onto the users computer.

There are no standard requirements on the havoc that a virus can wreak on a users computer system. The wrath, or payload, of the virus is determined by the virus's creator and can vary greatly from being slightly annoying to causing the total destruction of the users storage system. New viruses appear on a very regular basis and the authors of anti-virus scanning software are pretty attentive about getting new definition files out soon after new strains are discovered. Definition files contain the telltale signs of what to look for in new viruses.

While email is the greatest potential source of viruses there are other sources in which computer users can obtain viruses as well such as downloading files and software from the Internet and through the copying of files on diskettes and other media such as CD's.

One possible effect of a virus is in the potential for a Trojan horse program to be secretly installed. A Trojan horse program is a backdoor program that hides in disguise seeming to be a normal and harmless part of your computers operations. Like viruses, the risk created by Trojan horse programs is entirely up to the author. Once these back door or remote administration programs are installed, the unauthorized intruder can gain access control to your computer to change your system configuration settings, potentially steal confidential information stored from the hard drive, perform Denial of Service attacks or to enlist your computer to be an intermediary for an attack on another computer system.

A Denial of Service (DoS) attack can cause a users computer to crash or to become so bound up by processing data and instructions that the system becomes locked up and unusable. Being an unwilling intermediary for another attack is referred to as a Distributed Denial of Service (DDoS) attack. In this situation, a hacker may install an "agent" that runs on the violated computer awaiting further instructions. Then a single "handler" can instruct a number of similarly hacked computer systems to launch a coordinated DoS attack on another system. Intruding attackers will frequently use multiple compromised computers as a base for launching coordinated attacks on other systems.

The security threats are magnified when a user accesses their employers network from their home system, as there is a greater incentive for hackers to use the home system as a gateway into the corporate network for more wide scale mischief. Recognizing this risk, a number of companies have established technology security plans to combat these potential attack risks.

Cable modems and DSL connections can raise security risks. They are always connected to the Internet exposing subscribers to threats for extended periods of time. This makes it easier for users computers to be discovered by hackers that might be running automated port scans or packet sniffers as they are looking for vulnerable machines. Cable modem services pose an additional security risk over DSL or dial-up connections as the technology shares connections among multiple subscribers and often maintain the same IP address for prolonged periods of time thus exposing a subscriber's data via packet sniffers to any other user on the connection in the same way that a LAN shares data among multiple PCs.

A packet-sniffing program installed on a computer in a neighborhood of cable modem users may be able to capture data or information transmitted by any other cable modem in the same neighborhood. A packet sniffer is a program that captures data from transmitted information packets as they travel over the network. Captured data may include user names, passwords, and personal information that traverse the network in clear text.

The combination of "Always-Connected" Internet access and ignored or poorly assigned personal software security settings (such as, not disabling or protecting the shared file feature in Windows), create an opportunity for hackers to jump in and gain access to a users computer under the pretext of posing as legitimate employee access.

Windows users have the ability to share their drives, folders and files with other users by enabling some rather simple settings in the Control Panel. Shared drives without designating specific users and passwords for the shares open the users computer up to intruders as unprotected windows shares can easily be exploited.

The use of seemingly harmless applications such as music sharing programs and instant messaging programs make it easy for hackers to find and exploit an unprotected computer system. These applications provide for information to be transmitted synchronously between users computers on the Internet. Chat clients provide groups of individuals with the means to exchange dialog and files of virtually any type. Music sharing programs provide a peer-to-peer network method for users to swap MP3 files. In this environment computer users may download MP3 files from other users computers and they open up their computers to anonymous Web surfers who select music files to download to their systems. The risks associated with this application include the possibility that a downloaded MP3 file might really be a virus or a Trojan horse program in disguise and that a users system is now opened up to potential DoS hacks.

Rouge mobile code (such as Java, JavaScript, and ActiveX) can also present security risks as these programming languages allow malicious web developers to write dangerous code that is executed through the web browser. This rouge code can be used to collect information about the user such as which web sites were visited or in some cases to run malicious code or script on the users computer. A user can potentially expose their web browser to malicious code or scripts by following rouge links in web pages, email messages, or newsgroup postings.

Conclusion

It is important for computer users to have at least a basic understanding of the security risks that they face while they are connected to the Internet.

Installing up to date anti-virus software and firewall protection are two important components in protecting against potential security risks. Updating these technologies on a regular basis with new definition files and patches are critical as new viruses and hack methods are constantly evolving.

The proper configuration of the computer users system has a great deal to do with how much security exposure a user faces as anti-virus and firewall protection alone do not solve all of the potential security threats. Small configuration settings errors such as leaving a folder shared with no access control can allow an intruder to take control of a system and install programs or steal information.

Knowledge is the best weapon against potential security threats and periodically updating that knowledge helps a computer user to understand the ever-changing risks associated with being connected to the Internet. The Internet itself contains a great deal of information and many resources that computer users can utilize in protecting their systems from hacks and intrusions.

About the author

Richard Bassett is a full time faculty member of management information systems at Western CT State University and part of the team of consultants, which provides technology analysis and assessments to the clients of Telecommuter CT!