

Canaudit Perspective

March 2005
Volume 6, Issue 3

Topics of Interest:

- Break in via the Internet
- Virus or Trojan
- Spyware
- Wireless Networks
- Online Transactions

“Your computer is more vulnerable directly connected to the Internet than if it was behind a router.”

Home Networks, Safe or Sane?



People always ask me if their home computer can be hacked. Unfortunately this is not an easy question to answer because many factors exist that can make our home computer more or less secure. Although there is no such thing as a completely secure system there are many things a home user can do to make their system and network more secure. Is their system up-to-date on patches? Does the user have an up-to-date anti-virus program? Is a personal firewall being used? Is their system behind a router? Are their any wireless devices attached to the network? The answer I usually receive to some of these questions is “I’m not sure.”

The Internet Storm Center’s latest study concluded that an unpatched Windows system will get compromised in 20 minutes. The following are different ways a hacker can access your home computer, in much the same way as they can use to access your corporate computers.

Break in via the Internet

Your computer is more vulnerable directly connected to the Internet than if it was behind a router. Most home users have their system set up with an administrator account without a password or with an easily guessed password such as “password.” When this is the case, all an attacker needs to do is type “\\yourIP\c\$” into their Internet Explorer and they will have access to the entire C:\ drive. This type of attack is not possible against default installations of Windows XP because the administrator account does not have remote access.

Is it possible for an attacker to access your computer even if you have a strong password on your account? Absolutely. If you have not patched your system recently, then all an attacker needs to do is run an exploit against your computer and BAM, they now have access. I can almost guarantee that your system has been attacked if you don’t have a firewall, your anti-virus is not up to date and you have not recently patched your system. One of the most common exploits is DCOM. All an attacker needs to do is run this exploit code and they will have complete access to your computer even if you have a strong password.

The following simple steps will help to prevent the above attacks: have a strong password on all accounts, keep your system up to date on patches, keep your anti-virus up to date, and most importantly, have a personal firewall. A personal firewall prevents an attacker from ever reaching your computer and thus the attacker cannot use a weak password or recent exploit. However...you are **NOT** fully protected even if you have a personal firewall. Recently, a vulnerability was found for those running Internet Security System’s (ISS) BlackIce. A worm called Witty attacked un-patched versions of BlackIce. The Witty worm would connect to your system and write random 65k files on your computer. Thus, more damage was done the longer you were infected. This goes to show you that layers of security are needed to properly protect your home computer.

Virus or Trojan

This type of attack usually requires the user to perform a certain action, such as opening an infected email or visiting a vulnerable website. In either case, a personal firewall may not protect you unless your personal firewall blocks outbound connections as well as inbound ones. Most people do not know what connections to allow so they end up blocking everything, causing their computer to misbehave or they allow everything to connect out which makes their computer more vulnerable. Users of personal firewalls complain about all of the pop-up alerts they get, so they end up turning the alert off, or they disable the firewall so they don't get any alerts. That's like turning up the radio when your car starts to make a noise.

There are three ways to protect yourself from these types of attacks. First, keep your system up to date on patches. Second, keep your anti-virus properly patched. Third, use a personal firewall at all times. I personally will not connect my computer to **ANY** network (the Internet, a client's network, and even my home network) without a personal firewall running.

Spyware

Spyware is fast becoming an issue these days. Studies have shown that 80 to 90% of all computers are infected with some form of Spyware. But what exactly is Spyware? There are different opinions on this, but for this article, we will use any tool that a remote attacker can use to get personal information. Spyware can range from simple cookies that track where you have been on the Internet to key loggers that track everything you type, including your banking password. These programs get on your computer usually by one of two ways. First, you may have downloaded a free program and installed it on your computer. If you read the terms of use agreement, you may see that you are also agreeing to load the Spyware. Second, you may have visited a website which uses a vulnerability in your browser to load Spyware.

There are two steps to help prevent this type of an attack.

1. Don't download free programs or visit websites that install Spyware
2. Use an anti-spyware program.

Unfortunately, these solutions are unrealistic, since you don't know if a web site is loading Spyware and you really like those free programs you downloaded. To minimize the risks use a browser that does not have any vulnerabilities, which attackers can use. Again, is this realistic? Even if you use a "secure" browser, such as Firefox, attackers and spammers are constantly looking for vulnerabilities in each browser. The best you can do to protect yourself is to browse safely, e.g. don't go to hacker or porn sites, use a browser with fewer vulnerabilities, such as Firefox, Mozilla or Opera and use an anti-spyware program. Keep in mind that anti-spyware programs are a new market and not all programs are created equal. Surprisingly some of the best Spyware removal tools I have found are free. I personally use two programs to help protect myself. First, I use Ad-aware (<http://www.lavasoft.com>), which has been around longer than most and is generally good at finding Spyware. The second program I use is Spybot – Search & Destroy (<http://www.safer-networking.org>). This program, which is free, usually finds Spyware that Ad-aware does not. It can also immunize your computer to reject certain types of Spyware automatically.

Wireless Networks

Everyone has heard that wireless is insecure, but is it really that big of a security risk when used at home? You are at risk if you have a wireless network at home, a neighbor that lives within 500 feet and you have not taken any security measures. But the main risk is not necessarily the risk of your computer getting hacked, after all you have a personal firewall on your home computer like I do, right? The risk I am most concerned about, at home, is someone using my Internet connection to commit a crime. If I was a teenager today and I wanted to download illegal copies of movies and music, I would use my neighbor's wireless network. After all, it's the neighbors that will get the notice from the RIAA (Recording Industry Association of America) that they have been downloading illegal music and not me. How are you going to prove that you did not download music when it was your IP address that did?

I am sure you are like most people and not logging traffic on your home network. You might want to consider whether having a wireless network at home is a good idea depending on your position. Do you think it's prudent that your CEO have a wireless network at home?

To protect yourself from a wireless attack at home is not difficult, but it is also not guaranteed. You need to enable Wired Equivalent Privacy (WEP) or Wireless Protected Access (WPA) security. If you are not using WEP or WPA then anyone can easily connect to your home network. I disconnect my wireless network when I'm not using it, and of course, I have personal firewalls on all of my systems. It is possible for a determined attacker, such as the teenager next door, to bypass WEP or WPA security, especially if you are using WEP. WEP has a flaw in its implementation of encryption, which allows an attacker to crack the encryption key used to encrypt the data, whereas WPA does not have this flaw, but an attacker could try to guess the password, which was used to generate the key.

Online Transactions

Many people are reluctant to purchase items on the Internet because they have heard of hackers stealing credit card data. A big mistake people make is thinking that hackers can not steal their information if they never buy anything on the Internet. Unfortunately this is not the case. I have audited many companies that do not perform online transactions and I was able to see credit card numbers, social security numbers and other personal information. In fact, I could make an argument that says you are safer performing transactions over the Internet than in person. For example, it is highly unlikely you will get mugged while performing a banking transaction from home and what happens to your credit card when you use it at a restaurant? Your waiter or waitress could easily "swipe" it with a portable reader before they process the charge.

Whenever you decide to perform a transaction over the Internet, the first thing you must do is ensure it is a reputable and legitimate website. Many people are being duped these days by phishing scams. Phishing is where someone makes you believe you are at the website of a legitimate company when in reality you are at their website. Sometimes identifying phishing scams can be difficult. A good rule of thumb to follow is if a company you have done transactions with, such as your bank, sends you an email saying you need to change your password and asks you to retype it in a form, then it is probably a phishing scam.

You can also look at the address that you are visiting. If it looks like the following, then it is definitely a bogus website: <https://www.canaudit.com:ac%398HAAA9UWDTYAZJWVWAAA9pYWwgc2l6ZT00PjxTVgc2l6ZT00PjxT@www.phishing-site/Images/logo/bay/index.html>

The previous URL will go to <http://phishing-site.com>, but the URL in the Address bar or the Status bar in Internet Explorer may appear as <http://www.canaudit.com>.

Conclusion

You can reduce the likelihood of your computer being hacked or your personal information from being stolen if you follow safe computing practices. Do not assume that it won't happen to you. History and recent statistics prove that, given enough time, you will eventually get hacked unless you take reasonable measures to prevent it.

As always, the comments in this article are mine and mine alone. I invite you to send your comments to me (Chris@Canaudit.com).

Chris Schroeder
Senior Manager

1376 Erringer Road, Simi Valley, CA, 93065
Telephone: (805) 583-3723 – Fax: (805) 582-2676 – Web site: www.canaudit.com