

Internet Security Issues: Tips to Keep You & Your Information Safe

Introduction

THE INTERNET. WE ENJOY ITS UNCEASING POSSIBILITIES WITHOUT BOUNDS. We gather invaluable information, visit with distant friends and family, elevate our careers, shop 'til we drop, download and listen to music, and gallivant the world over. The vast opportunities the universe has to offer seem to be set before our fingertips. Unfortunately, the opportunities can be hindered by some that use the Internet as a means to gather personal and profitable information from fellow Internet users. As you are aware, this is not a new issue. It is a security issue that continues to raise concern amongst all that use and enable the Internet. Specifically, and in this case, for Digital Subscriber Line (DSL), cable modem and dial-up Internet Service Providers (ISPs).

Covad is the nation's leading broadband services provider of high-speed Internet and network access utilizing DSL technology. Covad provides its broadband services to ISPs, who use Covad's DSL services to offer high-speed, "always-on" broadband access to small and medium-sized businesses and home users. Covad also provides its broadband services to large enterprise customers with remote workforces. This document describes security issues surrounding DSL and what can be done to reduce security risks. Covad's goal is to minimize the potential security risks by informing you about: the issues, the extent to which Covad goes to resolve them, how other technologies compare, and how businesses and home users can be proactive in maximizing their own security.

What are the security issues?

The press has published articles on the security of cable and DSL networks. These articles usually center around the "always on" property of these technologies. Always on is a great convenience, at the same time it also provides a greater "window of opportunity" for potential hackers. Dial-up users are equally exposed while they are logged on, but their exposure is proportionately less. One of the reasons for this is because hackers "sweep" the known IP address space looking for users who are connected.

Once a hacker locates you, what do they do? Of course everyone is worried that the hacker will get into their PC and start deleting files or otherwise doing serious damage. This *could* happen, but that is a very small fraction of the cases. Measuring the extent of hacking is difficult. No analyst firms or government agencies track specific data on security crimes against individuals. The Social Security Administration recently reported that it received more than 30,000 complaints in 1999 relating to abuse of Social Security numbers, compared with 11,000 in 1998. The agency attributes the rise to the ease with which the Internet can distribute information, but it seems that most of the net-related incidents were emailed across the world or posted on web sites, rather than stolen from PCs.

The prominent Internet security issues are snooping, impersonation and information theft. We'll talk more about those in a bit. First of, course, you want to know how to keep the hacker out altogether. Think of keeping your computer secure as you would keep your house secure. Do you usually leave your house unlocked? No. What could happen if you left it unlocked? Most often, nothing. Sometimes someone may wander in and look around, but not do anything. Other times someone may steal things, maybe paint some graffiti. Occasionally, they may get nasty.

Many people leave their PC's "unlocked". Things that allow others into your computer are also things that you may use yourself: file sharing with another PC, printer sharing, etc. These are the "doors and windows" on your PC that hackers use to get in. Just as you lock the doors and windows on your house, you should lock the doors and windows on your PC. Do you have passwords set on all file sharing? Printer sharing? Do you allow access to your PC via the file transfer program "ftp"? Is it password protected?

Locks on doors and windows are effective against casual intruders, but not against people who are intent on breaking and entering. Just so, passwords are effective against casual intrusion by hackers. For your home, you

may install an alarm system to detect intrusion or even hire a security firm. Similarly there are various degrees to which you can secure your PC.

There are programs that you can purchase that will effectively provide an “alarm” against intruders. These programs log various activities that occur on your PC and allow you to determine (later) that someone might have hacked into your PC. While these are interesting facts, what you’d really like to do is prevent the hacker from gaining entry in the first place. You can purchase other programs or external equipment called “firewalls” that are the computing equivalent of building a security fence around your home. Their purpose is to prevent access to the “doors” and “windows” of your PC in the first place.

Now let’s look at what most hackers are trying to do.

SNOOPING

Snooping is when someone monitors your Internet connection to see what you’re sending and receiving, and what web sites you frequent. It is used as a means of capturing both personal and profitable information from unsuspecting Internet users. Snooping can be performed both intentionally and unintentionally. When it is intentional, it requires someone who is computer savvy and unethical. When it is unintentional, it is often due to the shared nature of cable modem access. Cable modem subscribers can often easily stumble across their neighbor’s hard drive by merely using their own cable modem to surf the net.

IMPERSONATION

Impersonation is when intruders mask themselves with your identity to carry out attacks aimed at other Internet users. For example, an intruder might impersonate you to send email that looks as if it came from you. An intruder may want to impersonate you specifically, or may simply want to conceal their own identity to make it look like someone else is guilty of the activities they are conducting.

INFORMATION THEFT

Information theft is when someone breaks into your computer and steals valuable information. This might include personal information such as credit card numbers, passwords, or your top-secret chocolate chip cookie recipe (if you keep such information online). Business and professional information can also be targeted for access to confidential, proprietary or sensitive documents.

In general, lack of privacy on the Internet can place all Internet users at risk of unintentionally sharing personal, proprietary and financial information. These security issues require measures from both network providers (such as Covad) and Internet users to achieve the maximum level of security technologically available.

How does Covad address these issues?

The Covad broadband network employs technological measures that reduce the vulnerability of DSL end-users to security issues. These primary measures are as follows:

Private physical connection per end-user

Each Covad DSL end-user receives their own dedicated private physical connection to the Covad network, rather than sharing a physical cable with all their neighbors, as cable modem subscribers do. Thus, Covad DSL end-users are much less vulnerable to snooping (because there are no shared lines for attackers to snoop on) and impersonation (because Covad and your Internet Service Provider (ISP) or employer can determine who the data is really coming from by determining which DSL line it came over).

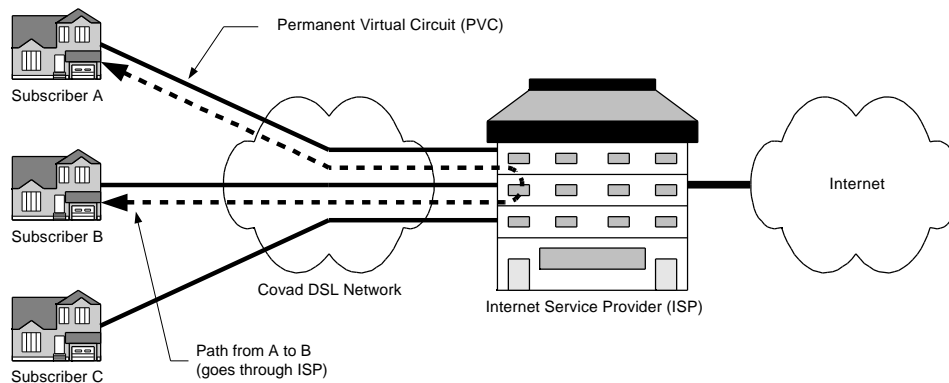
Being less vulnerable to snooping and impersonation also makes Covad DSL end-users less vulnerable to information theft. Being unable to snoop on your connection makes it more difficult for attackers to steal private information (or the passwords and such needed to access the information) as it crosses the network.

Being unable to impersonate you makes it more difficult for attackers to successfully use any passwords. If they do somehow manage to obtain or guess your password, it is easier for your ISP or employer to track any such attempts back to the attacker.

Private Permanent Virtual Circuit (PVC) per end-user

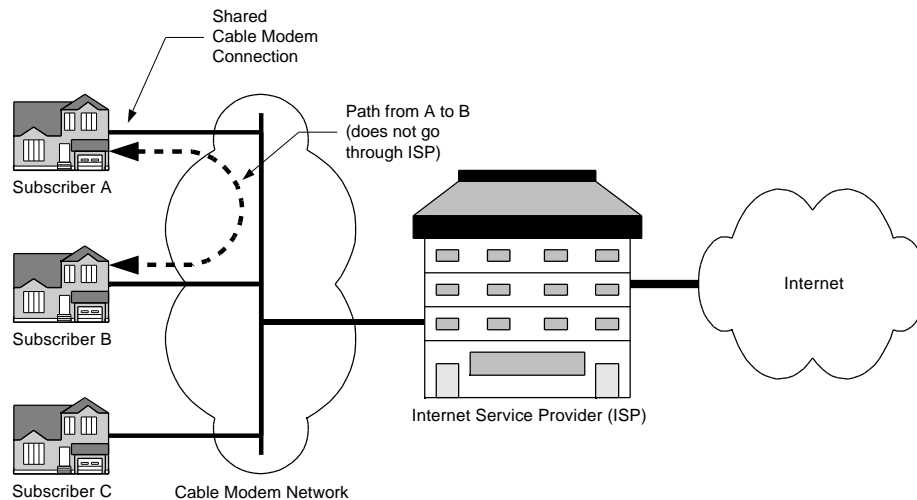
In addition to the private physical connection to the Covad network, Covad DSL end-users also get a private PVC) from their DSL device all the way through the Covad network, and back to their ISP or employer. Covad's secure Layer 2 packet-based network uses Asynchronous Transfer Mode (ATM) and frame relay Permanent Virtual Circuits (PVCs) to encapsulate and transport user data. The PVC imposes no restrictions on IP addressing and provides a private path between the ISP or employer and the end-user's PC. Covad does not use the public Internet to transport data. These added levels of privacy make Covad DSL end-users that much less vulnerable to Internet related intrusions.

Each end-user's private PVC to their ISP is shown in the following diagram. As you can see, the only way for traffic to go from one end-user to another is through the ISP; there is no way for end-users to snoop on each others' traffic, or impersonate one another (the ISP can see from which PVC the data originated).



How does cable modem security compare?

Cable modem subscribers are especially vulnerable to security issues since their cable modem is connected to a cable that they share with all their neighbors (up to thousands of homes, in some cases), as shown in the following diagram:



These shared connections make cable modem subscribers especially vulnerable to:

- Snooping, because someone can use an older cable modem (or a modified current cable modem) and intentionally snoop on their neighbors' Internet connections.
- Impersonation, because a malicious subscriber can easily modify or reconfigure their cable modem to allow them to appear to be another subscriber. Cable modem ISPs do not have a reliable way to differentiate subscribers on a shared cable, thereby enabling attackers to carry out untraceable attacks on other Internet users. Cable modem ISPs have to rely on all their subscribers to be forthcoming about their identities, and not all subscribers are worthy of such trust.
- Information theft, for two reasons. First, as discussed above, cable modem subscribers are more vulnerable to snooping, which enables an intruder to get information as you send it to and from your computer. In addition, an intruder can intercept passwords or other keys that will let them explore your system and obtain information later at their leisure. Second, as discussed above, cable modem subscribers are more vulnerable to impersonation. As a result, it is easier for an intruder to pretend to be you in order to get access to something that you have access to.

How do dial-up and ISDN security compare?

There is a myth that dial-up and/or ISDN Internet connections are somehow more secure than DSL and cable modem connections, because they are intermittent (the subscriber isn't continuously connected to the Internet) and because the subscriber gets a different IP address each time they connect via dial-up.

While a user is connected to the Internet via dial-up or ISDN, they are just as vulnerable to most attacks as they are when connected via DSL or cable modem. Many of these attacks are fully automated, and can be carried out in seconds. When the attacks are that fast, it doesn't matter whether you're connected continuously, or "only" for a few hours each day; either way, there's enough time for an attack to occur.

It's true that dial-up and ISDN subscribers are assigned a different IP address each time they connect to their ISP, and that DSL and cable modem subscribers tend to use the same IP address for days, weeks, or months on end. However, it's also irrelevant to security. It would be relevant if attackers were targeting a particular subscriber; however, most attacks are directed at whoever is using a particular IP address at the moment, rather than at a particular subscriber. It doesn't matter to the attacker if the subscriber has been using that address for months, or for only a few minutes; the attacker generally doesn't even learn whom the subscriber is until after they've broken into the subscriber's machine, if ever.

What can businesses and home users do?

All business and home Internet users are vulnerable to loss of privacy. All business and home Internet users can also be proactive in elevating their own Internet security by taking the following precautions:

As a business:

Use passwords that are difficult to guess

Most users think that using easily remembered passwords, like their cat's name or a common word is okay for a password. Don't. Hackers can easily guess these sorts of passwords. They have lists of commonly used words and names that people use as passwords and they program their computers to simply run through these lists (even through a whole dictionary of words) trying to "guess" your password. The best way to protect yourself is to mix numbers and other special characters, like " !#%\$&* " in with letters. A simple way to do this is to use letter translation. For example if your "usual" passwords are "Garfield" and "Gaspar", replace the "a" character whenever there is an "a". So the passwords become "G%rfield" and "G%sp%r". Much less guessable, but still memorable.

Use a firewall

A firewall is a security system that usually separates an internal network from the Internet. A firewall restricts access between the Internet and your internal network. A firewall is typically installed at the point of maximum leverage, the point where your network connects to the Internet. The existence of a firewall can greatly reduce the odds that outside attackers will penetrate your internal systems and networks. A firewall can be implemented by a contractor or by your own staff, depending on your needs and your resources. You might want to contact your ISP about firewall products or services that they offer.

Have security policies in place

A security policy sets explicit expectations and responsibilities among users and management; it lets everyone know what to expect from one another in regards to your business' security. It concentrates on what all users need to do (and avoid doing) to keep your business systems secure.

Resources for Internet security can be found at the following web sites:

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 62,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for challenges they face. Check out their web site at <<http://www.sans.org>>, and in particular take a look at the "Fundamentals of Effective Network Security" document in their "Resources" section (currently at <<http://www.sans.org/newlook/resources/esa.htm>>).

COAST (Computer Operations, Audit, and Security Technology) is a group based at Purdue University that maintains a very useful set of free computer security tools. You can visit their web site at <<http://www.cs.purdue.edu/coast/coast.html>>.

Keep your systems up-to-date

It's important to keep up-to-date with the latest releases of security software packages (for example encryption, virus protection, personal firewall, etc). Intruders know of many security problems that can be exploited in out-of-date systems; one of the major reasons for most software updates is to fix security problems that have been discovered since the previous release.

Keep yourself up-to-date

It's much easier to keep your systems up-to-date if you keep yourself up-to-date. To increase your understanding and reduce your vulnerability to Internet security risks, you need to find ways to become and remain informed about computer and Internet security.

As a home user:

Use passwords that are difficult to guess

Most users think that using easily remembered passwords, like their cat's name or a common word is okay for a password. Don't. Hackers can easily guess these sorts of passwords. They have lists of commonly used words and names that people use as passwords and they program their computers to simply run through these lists (even through a whole dictionary of words) trying to "guess" your password. The best way to protect yourself is to mix numbers and other special characters, like "!"#\$%&*'" in with letters. A simple way to do this is to use letter translation. For example if your "usual" passwords are "Garfield" and "Gaspar", replace the "a" character whenever there is an "a". So the passwords become "G%rfield" and "G%sp%r". Much less guessable, but still memorable.

Disable file sharing

One of the best things that a user can do to protect themselves is to disable file sharing, so that an intruder cannot take a leisurely stroll through the contents of their hard disk drives. Many systems come with file sharing enabled by default, and many users enable it for a specific purpose (such as moving a file from one system to another), but forget to disable it when they're done. If you use file sharing regularly and need to leave it enabled, then you should set up passwords for all users and disable "guest" access.

Consult your operating system manuals for assistance or see appendix of this document for specific guidance.

Don't keep sensitive information unencrypted on disk

If you have sensitive information (account numbers, passwords, private files, etc.) on your system, keep them encrypted when they are not in use. There are a number of good encryption packages available for little or no cost; try searching for "personal encryption" on your favorite Internet search engine (www.altavista.com or www.zdnet.com, for example).

Don't pass sensitive information unencrypted across the Internet

Similarly, if you're passing sensitive information across the Internet, it should be encrypted. If you're sending and receiving files, you can probably use the same packages discussed above. When accessing web sites, use "secure" connections whenever the site offers them.

Use a personal firewall

A firewall is a security system that sits between your computer and the Internet, and guards you against potential privacy threats on the Internet. There are hundreds of firewall products on the market today, covering a broad range of capabilities and prices (including free). To find some of them, try searching for "personal firewall" on your favorite Internet search engine (www.altavista.com or www.zdnet.com, for example).

Keep your systems up-to-date

It's important to keep your home system up-to-date with the latest releases of security software packages (for example encryption, virus protection, personal firewall, etc). Intruders know of many security problems that can be exploited in out-of-date systems; one of the major reasons for most software updates is to fix security problems that have been discovered since the previous release.

Keep yourself up-to-date

It's much easier to keep your systems up-to-date if you keep yourself up-to-date. To increase your understanding and reduce your vulnerability to Internet security risks, you need to find ways to become and remain informed about computer and Internet security.

Conclusion

The intention of this paper is to not scare Internet users, but to help educate home and business Internet users about the issues surrounding security and the precautionary measures users can take to minimize security threats. Unfortunately, we live in a world where there are people who find it "fun" to invade other people's private information, whether it's a PC, car, home, etc. Just like people take precautionary measures to protect their cars and homes from being broken into, people need to be aware and take the necessary measures to safeguard themselves in the online world. The Internet is here to stay and will increasingly become a more essential and critical component to the way people live, work and play. In fact, various industry analysts expect that the U.S. online population will reach 137 million in 2000 ⁽¹⁾ and the average time spent online in the U.S. will increase to 8.2 hours per week up from 7.6 hours in 1999 ⁽²⁾. Therefore, the more time people spend online and depend on the Internet for business and/or pleasure, the greater the chances of a security threat. Being the nation's leading broadband provider utilizing DSL technology, Covad recognizes the importance of addressing Internet security issues and informing online users about how to keep their information safe.

Appendix on MS Windows 98

How to check to see if you have file sharing or printer sharing on. How to turn file sharing or printer sharing off.

1. Click on the Start button and follow the menus through Start->Settings->Control Panel.
2. Double click on the "Network" control panel.
3. Click on the "Configuration" tab.
4. Click on the "File and Print Sharing..." button.
5. Uncheck the boxes to turn off file and/or print sharing.

To allow file and/or print sharing, but to add a password.

1. Go to the "Network" control panel as above.
2. Click on the "Access Control" tab.
3. Check the "Share-level access control"
4. When you share a "resource" (file, folder, or printer) you will be asked to supply a password, which will be required to "map the network drive" or use the printer.