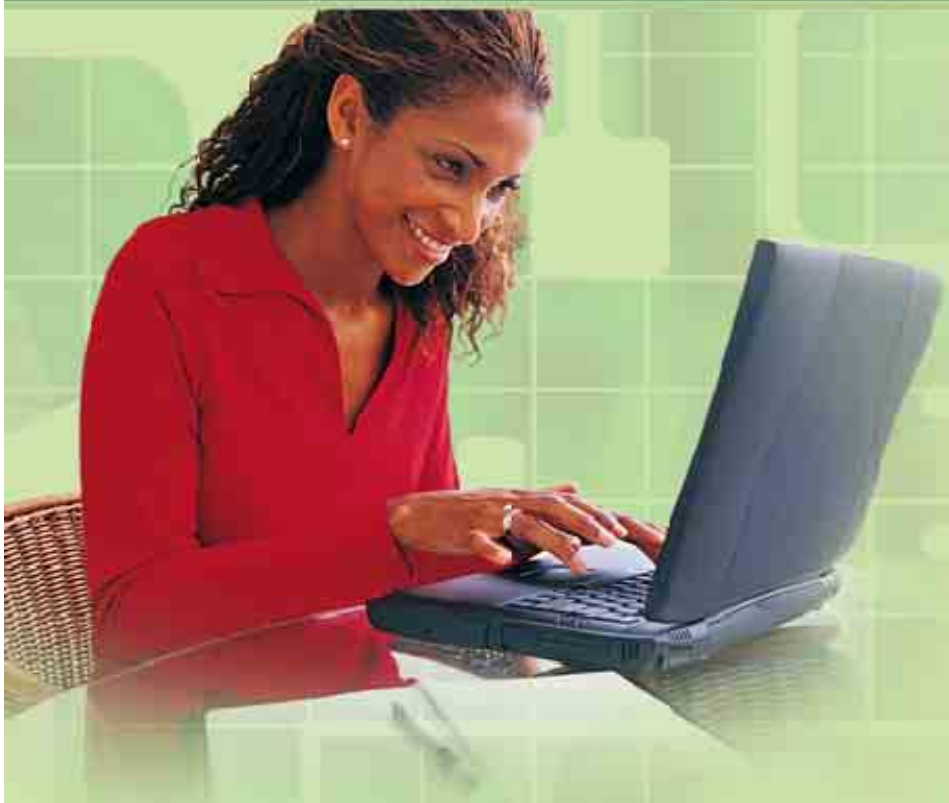
ALBERTA efuturecentre



Internet Security

An initiative of:

THE BUSINESSLINK Alberta's Business Information Service

Funded by:

Western Economic Diversification Canada | Diversification de l'économie de l'Ouest Canada | Canada

Introduction

As the Internet becomes a mission-critical component of more and more small businesses, security is possibly the single greatest concern they face. When security breaches and large-scale viral attacks make national headlines, consumers typically feel helpless. This guide will introduce you to the topics of computer security on the Internet and provide practical tips to defend yourself.

Physical Security

People panic at the thought of "hackers" breaking into their computer and stealing their identity, yet it is far easier to just walk down a back lane on trash day and get all the personal information one would ever need.

Perhaps the most overlooked topic when discussing security is that of offline security. People panic at the thought of "hackers" breaking into their computer and stealing their identity, yet it is far easier to walk down a back lane on trash day and get all the personal information one would ever need. Similarly, there are numerous cases of companies selling off old computers without properly deleting sensitive information on the hard drive.

All businesses in Canada are now subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), and one of the Act's ten principles is that of safeguards. It is your responsibility to protect the physical safety of the personal information your organization collects, and to dispose of it responsibly.

Data Isolation and Backup

If you are familiar with computers, you know that inevitably you will need to reinstall your operating system. Hardware can fail; systems become sluggish and bloated with unnecessary and partially uninstalled programs; and despite your best efforts, viruses and spyware can infect your system beyond repair. The downtime of mission-critical systems during an operating system reinstall can be very costly to an organization.

Storing all of your documents in one well-known place will reduce the time and risk associated with reinstalls.

Get into the practice of separating your documents and data from the applications being used. An ideal system would have one main directory (with any number of subdirectories) containing all of the company's documents that could be transferred from one computer to another if necessary. Some applications, especially older ones, like to save files to the same directory as the application, so pay attention.

Storing all of your business documents in one place will significantly reduce the time and risk associated with reinstalls and data recovery.

Now that all of your important files are in one place, backing up your business data should be much simpler. With the low cost of CD and DVD burners, you should be backing up this data to removable media like read/writable discs on a regular basis. There are excellent backup and recovery software packages available, but sticking to a schedule of manually backing up data should suffice for most. As an extra precaution, if your burning software allows for it, data can be verified after writing to a disc for additional peace of mind.

Critical Systems and the Internet

What is the easiest way to limit online attacks against a critical business system? The answer is simple – do not connect it to an external network. This may not be practical in a small business where one computer is used to do the accounting, word processing, file storage, and web browsing. On the other hand, if your home office computer is the same one the kids cruise the web and play games on, eventually you can count on having a serious security issue. With computers being relatively inexpensive, perhaps it is cheaper in the long run to have separate machines for these purposes.

Passwords

Systems are often hijacked by guessing a simple password.

Is your bank card's PIN your birthday? Is your password the same word as your username, a simple word in an English dictionary, or even worse, a blank? Do you use the same password for everything? If you answered yes to any of these questions, rethink your strategy. "Strong passwords," consisting of at least 6-8 random alphanumeric characters, should be used at *all* times. You should not use one multi-purpose password. No one carries around a single key on their keychain that starts their car, opens their house, and gets into their safety deposit boxes.

Keeping Your System Up To Date

New security vulnerabilities appear constantly within operating systems and software. Minimize these potentially devastating threats by keeping your system as up to date as possible. There is always the risk that a system may lose stability after

upgrades, but this risk is usually smaller than the potential of a severe security hole in a particular application. Operating system vendors usually provide free mailing lists that notify subscribers of security upgrades so that you can try to stay ahead of the game.

Firewalls

A firewall is hardware or software (or both) that inspects, allows, and/or blocks traffic along a particular network, usually between yourself and the Internet. The hardware that typically connects two networks together is called a router, and part of its function can be to serve as a firewall between networks. Software firewalls running on personal computers are becoming more and more common, with many becoming simple enough for ordinary users to deploy.

Think of firewalls as the locked door to your house, and anitvirus software as your alarm system.

Firewalls are often your best defense against intrusions over the Internet. Therefore, their configuration and maintenance is best left to the professionals. The standard approach is to lock down everything initially, then gradually open "holes" in the firewall for Internet services you either use or provide to the outside.

Malicious Software

What most people call computer viruses are actually several distinct types of malicious software.

When most people think of malicious software, the term virus is often used. This is not entirely accurate, because computer viruses have distinct behaviours. **Malware** is the general term that refers to any type of malicious software, including:

- **Viruses** – While there is still some debate on the exact definition of a computer virus, most agree that a virus refers to a program whose primary purpose is to replicate existing files, usually with a malicious result.
- **Worms** – Instead of infecting existing files, a worm replicates itself and infests a network, consuming system resources in the process. For example, an e-mail worm will spread from an infected computer by sending itself to all email addresses in the infected machine's address book.
- **Trojans** – Like the Trojan Horse from Greek mythology, trojans attack by masquerading as legitimate programs hoping to obtain sensitive information from an unsuspecting user.

- **Adware** – This potential type of malware forces users to display ads for software that is very difficult to remove from your system.
- **Spyware** – Spyware collects marketing information behind the scenes while you use your computer. Malicious spyware attempts to obtain sensitive information without your knowledge.

Protection from Malware

Viruses can corrupt operating systems, physically affect hard drives, destroy files, and spread like wildfire. Internet worms have been responsible for shutting down major corporations. Trojans can give hackers backdoor access to your system. Worse yet, most attacks are now combinations of all three. Your single best defense against such threats is to prevent getting infected in the first place.

Through painful experience, most people now see the benefit of having antivirus software. Antivirus software continually scans your system behind the scenes. It monitors programs running in system memory, files being saved to your hard drive, and incoming email. When malware is detected, the antivirus will identify, isolate, and try to remove the offending software. If you want to think of firewalls as a locked door to your house, then antivirus software is the house's alarm system.

Antivirus software has become commonplace, but many entrepreneurs still do not update their virus definitions. The software needs to be continually updated as new threats emerge daily. Most programs give you the ability to automate virus definition updates, so be sure to update your software regularly. For computers that are not connected to the Internet, virus definitions should be manually updated along with your online systems.

Adware and spyware are slowly being considered as threats by antivirus software, but protection is still limited. Fortunately, most spyware and adware can be removed by scanning with removal tools developed specifically for this threat. Until antivirus and spyware removal tools are merged into one, you will need to run both types of software protection.

SSL Encryption

SSL is the most common way to secure communications on the Internet.

The security of your computer is extremely important, but you also need to secure your communications with the outside world. Imagine the secrets someone could learn if they were able to eavesdrop on all of your telephone calls. Secure Sockets Layer, known as SSL, has become the most common technology used for encrypting data sent over a network.

Most people encounter SSL encryption when they are asked to enter sensitive information on "secure websites." These websites' URL begins with *https://* instead of the usual *http://*. Your browser may inform you that any data sent to this website will be encrypted. While SSL can be used with other Internet services, secure websites use this technology most frequently.

Another important aspect of SSL is that it can be used to authenticate the identity of both the sender and receiver. This rather amazing feature is a basic component of the public-key encryption algorithm used by SSL. Cryptography is an extremely advanced subject, but in layman's terms, it provides the ability for users to digitally "sign" their messages, in much the same way that your handwritten signature can identify you. These digital signatures are often referred to as certificates. Website certificates are called Server IDs, and personal certificates are called Digital IDs.

For those of you who are still not bored to tears with this technical stuff, you may have realized that something is still missing when it comes to establishing trust between two unknown parties. Seeing someone's signature is meaningless unless someone you already trust can vouch for its validity. We encounter this situation offline when we use public notaries to officially attest to a person's identity.

A certificate authority is the online equivalent of a public notary.

The equivalent to a "public notary" on the Internet is a Certificate Authority (CA). If a CA has put their signature on a verified SSL certificate, you can trust that the CA vouches for this person's or website's identity. There are relatively few well-known Certificate Authorities that are trusted by your browser. VeriSign is the most widely known CA to the public.

So now let's put the whole process together. When you visit a secure website, the website sends its certificate to your browser, which includes the domain name for verification signed by a recognized CA. If the domain name in the certificate does not match the name in the URL, your browser will generate a warning before allowing you to continue. This warning is also generated if the certificate is not signed by a trusted CA, or if the certificate has expired (a certificate signed by a CA is typically valid for only a year or two, and must be renewed). If you ever encounter this warning, you cannot trust that the website is who they say they are and you should stop communications with it.

Trust is considered to be one-way with secure websites, as they almost never require that you have a Digital ID. Most user authentication is done by other means, such as having a user account with an associated password. Requiring users to authenticate with Digital IDs is a powerful technique, but this would require consumers to pay for their own Digital IDs to be signed by a CA at a certain cost to the consumer. One of the few places Digital IDs are currently used is with secure e-mail. Secure e-mail, however, has been slow to be adopted by the general public. Until fundamental business, government, and logistical issues are sorted out, Digital IDs will continue to be rarely used by the general public.

Summary

Internet security is not something that should be taken lightly. You need to be proactive in identifying ways to protect your clients' personal information and your sensitive business files and communications. Following secure procedures is the most important thing you can do to keep threats to a minimum. You may consider having an experienced security expert audit your system, jus as you would a chartered accountant your financial statements. We hope this guide has increased your awareness of Internet security issues and will help you develop an action plan to deal with them in your small business.

Resources

- About.Com - "Antivirus Software"
  http://antivirus.about.com
- CIO.com: Internet Security
  www.cio.com/research/security
- Microsoft - "Trustworthy Computing: Security"
  www.microsoft.com/security
- Office of the Privacy Commissioner of Canada
  www.privcom.gc.ca
- Operations: Security
  www.operationsecurity.com
- Soltrus Inc
  www.soltrus.com/english/corporate/library.html
- Symantec Security Response
  www.sarc.com
- Thawte: Digital Certificates
  www.thawte.com
- Verisign: Digital Certificates
  www.verisign.com

Contact Us

The Alberta E-Future Centre, a service initiative of The Business Link, is your first stop for e-business information in Alberta. We offer free, impartial, and easy-to-understand e-business advice and information for small and medium-sized businesses. Our goal is to help entrepreneurs make more informed decisions as they adapt to technological change. If you have any questions, we are only a visit, click or a call away!

The Business Link's Alberta E-Future Centre

Business Information Line: 1-800-272-9675

Edmonton: 100 – 10237 104 Street NW, Edmonton, Alberta T5J 1B1

Tel: (780) 422-7722 **Fax:** (780) 422-0055

Calgary: 250 – 639 5 Avenue SW, Calgary, Alberta T2P 0M9

Tel: (403) 221-7800 **Fax:** (403) 221-7817

E-mail: info@e-future.ca **Website:** www.e-future.ca/alberta

This guide was prepared by the Manitoba E-Future Centre
www.e-future.ca/manitoba

A member of the Pan-Western E-Business Team