

Best Practice

“Best practice”, in the context of security, is a phrase used to describe the habits and methods computer users should employ to make it more difficult for common attacks and threats to your data to be successful.

E-Mail Attachments

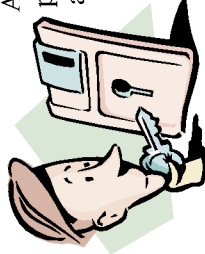
Worth repeating is the “best practice” advice to be especially careful opening e-mail attachments. Knowing just who sent a particular attachment is not always sufficient. There are many viruses, more specifically, worms that fall into a class called “mass mailers”. As the name implies, this worm infiltrates address books and e-mails a copy of itself to every address it can find. If you receive such an e-mail, notify the sender immediately so that immediate action must be taken to prevent further damage.

Avoid Spyware/Adware

Avoid haphazardly downloading freeware or shareware applications on the Internet. While there are a great many useful applications, ensure that you research software you wish to download and install. Chances are high that if it contains spyware or adware, information to that effect will be posted in numerous places on the Internet. With some operating systems, if you happen to have a number of employees, you can actually deny permission to install software at all. It is also important to always read any security dialogues that come up. Be careful before clicking **allow** or **yes**.

Change Your Passwords

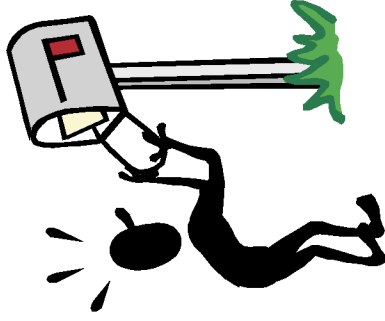
An often overlooked “best practice” is to change your important passwords on a regular basis. Ensure, also, that your passwords are not names or words that can be found in dictionaries. It is best to use completely different passwords for each service that requires one; this way if someone hacks the password for your e-mail account, for example, he or she will not automatically have access to your online bank account. It is best if you don’t write down your passwords however, if you must, make sure that they are kept in a secure location where only you have access.



Stay Current!

Most important among best practice methods is to persistently keep your software current. Ensure that you have applied all security patches to your operating system, web browser, e-mail client, and that your anti-virus software is up-to-date.

IT Security Basics for Small Offices



Designed by

CEONET

Communities of Eastern Ontario Network

Reseau des communautés de l'est de l'Ontario

Tel: (613) 525-2151 Fax: (613) 525-2417 eMail: info@ceonet.on.ca

Web: www.ceonet.on.ca

Risks and Threats

Depending on the sensitivity of the data with which you work daily, the risks associated with overlooking information security can be quite serious. The same risks that home users face are present within all small offices; the consequences, however, are much higher. Information compromised from within a business can be quite costly in terms of data loss, data recovery, breach of customer privacy, and the possibility of legal liability.

Network Intrusion

A connection to the internet is a great tool for business but it can be a dangerous one if it isn't properly secured. Just as you have a connection to anyone or anything on the internet, anyone with the right skills, can connect to an online desktop computer or network. Some attackers are simply curious and mean no harm, while others are vindictive, intending to steal or destroy as much as they can. What can be confusing is that sometimes a computer or network may simply be randomly selected for this type of attack even by a stranger from another continent.



Viruses, Worms and Trojan Horses

While some malicious users on the internet might wish to steal or exploit your data, there are others who are quite content to write viruses to destroy it, worms to infect and further propagate, or trojan horses in an attempt to leave your system open to backdoor intrusion.



Spyware/Adware

Spyware is written to record what you do while on your computer. For example, the websites you visit may be subsequently transmitted back to a third party for market research and targeted advertising.

Adware is written to show you advertisements from the internet within a downloaded application or on its own. These advertisements are for the financial benefit of the author.



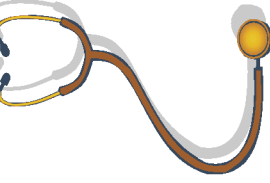
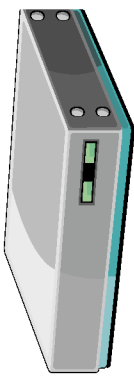
The main issue with either iteration of this nuisance/threat is that the software can be in constant communication with a third party using your internet connection. It is a huge assumption to trust that your privacy is safe when connected to the internet by DSL, cable wireless or other services that are "always on".

Preventive and Recovery Measures

Small offices generally lack IT-trained staff to look after security. Thankfully, there are easy-to-use solutions available in the common marketplace. While the products available do require a working knowledge of some of the basics, the process of securing your office's local area network is now reasonably manageable.

Router/Switch

The most straight-forward way to secure a local area network against intrusion is by installing an inexpensive router/switch. This is a device into which all computers, other network devices, and your connection to the internet connect. The router's firewall can be configured using a web browser on a connected PC to allow or deny certain traffic coming into or out of your network.

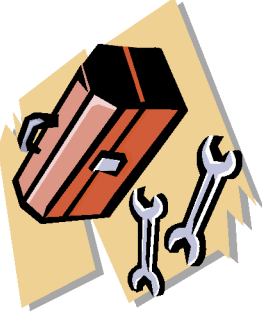


Anti-Virus Software

The best layer of protection against viruses, worms and the like, in tandem with best-practice methods, is to have up-to-date anti-virus software running on each personal computer with updates being downloaded on a regular basis. While anti-virus software protects each computer it is installed on, it is also capable, with relative ease, of removing infections that may slip past.

Adware/Spyware Removal Tools

The best way to get rid of spyware and adware is not to have it installed on your computer in the first place as getting rid of spyware and adware isn't always a simple matter. There are tools that can be freely downloaded online that can help you keep on top of the situation. Two highly recommended tools are Spybot Search & Destroy, and HijackThis. Details can be found online.



AdAware - www.lavasoft.de

HijackThis - www.hijackthis.nl

SpyBot Search & Destroy - www.safer-networking.org