Computer Services
www.tsgcs.ca

TECH-info

NOVEMBER

Security

As it turns out, November is **"Child Safety and Protection Month."** So it's fitting that this month's newsletter is also about Safety & Security..... for your computer.

Computer & Network Security are often overlooked as integral parts of business today.
This is because security isn't an *in-your-face* measurable threat. Unfortunately, many businesses become victims for this reason alone.

There are many things which can be done that don't require a degree in **Information Technology (I.T.)** , which will *harden your Security Gates and fend off attackers.*

This includes:

- Install and Use Anti-Virus Programs
- Keep Your System Patched
- Use Care When Reading Email with Attachments
- Install and Use a Firewall Program or Hardware Firewall
- Use Strong Passwords
- Use Care When Downloading and Installing Programs
- Make Backups of Important Files and Folders

According to U.S. Security Statistics, there have been over 140 million confidential files compromised in the U.S. since Jan 1st, 2008. ©

PrivacyRights.org

Install and Use Anti-Virus Programs
AntiVirus programs are an essential part of every computer system, and need to be treated as such. Make sure you have AntiVirus software running onboard, and that it is up to date. Simply having AntiVirus Software on your computer, isn't enough. There are always new threats being released, and therefore, your AntiVirus program needs to be constantly updated. Most AntiVirus programs on the market today have an Auto-Update feature, which retrieves the latest updates for your particular program, and automatically installs them. If however, your AntiVirus program is old & outdated, or the Subscription has run out, then you will need to Upgrade, not just Update. What is the difference between Upgrading & Updating? Upgrading involved purchasing the latest version of the software. Updating simply refers to making sure the Virus Definition files on your computer are up to date.

- Upgrade or Update your AntiVirus Software
- Run a complete System Scan to remove any Viruses on your Computer
- Systems Scans should be done at least Once-a-Month, if not more.

Keep Your System Patched
Keeping your system patched and up-to-date with the latest security fixes is relatively easy. If you are using Windows XP or Windows Vista, and if they are setup correctly, the Operating System will go out, get the updates, and install them without needing your intervention. However, some people like to install the updates themselves, and be in control of what updates to install and when to install them. Unless you are the type of person who is able keep on top of what updates are coming *"down the pipe"*, then I advise against doing this. This is because it is possible to get a virus that exploits the vulnerability in the Operating System before the appropriate patch gets installed. This often causes so much damage to the Operating system, that a complete reinstall is the only remedy.

- Ensure your computer is fully patched with the latest Security Fixes, and that **"Automatic Updates"** is enabled.

Use Care When Reading Email with Attachments
With email being used everyday at work and at home, it is more important than ever to be vigilant when sending and receiving

messages. There are 5 tests that can help you to identify whether you have sufficient email security.
These five tests can can be summarized by the word **"KRESAV"**.

- **K** - Do you **KNOW** the sender of the email?
- **R** - Have you **RECEIVED** email from this person before?
- **E** - Were you **EXPECTING** an email with an attachment from this sender?
- **S** - Does the email make **SENSE**? Is the content of the email relevant to the email's subject line? Are there purposely misspelled words?
- **AV** - If an **ATTACHMENT** was included. Is the attachment infected by a **VIRUS**?

In the first half of 2008, the share of spam on the internet averaged 85.3% of all mail traffic .

© VirusList.com

Install and Use a Firewall Program or Hardware Firewall
A firewall in your network is the equivalent to having a security guard at your office. Just like the security guard protects the office, the firewall ascertains whether the outside computer trying to access your network is supposed to be there or not. But instead of simply turning back intruders like the security guard does, the firewall hides the network (or makes it invisible to would be attackers) thereby preventing the attackers from getting to your door in the first place.

This is not the only aspect of what a firewall can do. In addition to preventing people from accessing your internal network, firewalls are also capable of monitoring programs on computers within the network, and allowing or preventing program access to the internet. This is highly invaluable. You do not want to be the one who is responsible for sending viruses out into the internet! With the firewall setup to monitor your programs, you can quickly extinguish any attempt by rogue programs to send data or files from your computer.

For more information on how to setup a router, click here

Use Strong Passwords
Passwords are the first line of defence when someone is sitting at your computer without your knowledge. Most people make 2 crucial mistakes when operating a PC.

- Users use the ADMINISTRATOR account for general day-to-day computer usage. This opens up many of the computer's backdoors. This is a substantial security risk.
- Users often use accounts with poor passwords or worse, no passwords. This is particularly dangerous, especially if your computer contains sensitive company information.

Passwords should be no less than 8 charcacters comprised of letters, numbers and special characters.
Regular Password: alligator
Proper Password: A11ig@t0r

There is one test that you can use to determine whether your passwords are safe or not. It is called the **"SUPR"** test.
SUPR stands for:

- **(S)TRONG** - Is the password as strong as the rules allow?
- **(U)NIQUE** - Is the password unique and unrelated to any of your other passwords?
- **(P)RACTICAL** - Can you remember it without having to write it down?
- **(R)ECENT** - Have you changed the password recently?

Regardless of how well you implement the **SUPR** test, you should be aware that passwords are only a preventative measure against computer invasion, and there is no way to completely prevent someone from getting into your computer (especially if they are in posession of it).

You should never use one password for everything, simply because once your password is leaked, then it is good for everything. It's equivalent to having one key for your house, your car, your office, your safety-deposit box, etc. It sounds stupid, but that is what you have if you insist on using one password.

There are programs out there that essentially are password vaults. These password vaults store all your passwords that you want to enter into it. The upside to this is that you can still have a different password for every website you visit, but you only need to remember the password to the vault.

Over 79 per cent of people asked, reported using the same password for multiple websites or applications. A practice that means one stolen password could jeopardize multiple accounts.

© theregister

Use Care When Downloading and Installing Programs
Software purchases have increased to 62.7 billion in 2007, up 26% from the year before. With these kind of statistics for e-commerce, it is crucial that you do your due-diligence when thinking of making an online purchase.
This can be done by asking yourself these 3 question before making a purchase.

- Did you learn as much as you could about the product and what it does?
- Do you understand the refund/return policy?
- Can you get it from a local store that you already know, or from a National Chain Online?

Answering these 3 simply questions can save you hours of frustration if the product doesn't live up to your expectations.

Make Backups of Important Files and Folders
Whether you realize it or not, your computer is divided into 2 types of files, replacable and non-replacable. Replacable files are files such as your Operating System or programs. Essentially replacable files are files that are easily replacable. That brings us to non-replacable files. These are files that can't be replaced easily such as documents you've created, photos you've taken, emails, address book contacts & internet bookmarks, etc. Essentially any file that would be difficult to replace is considered non-replacable.

Many people don't put much stock in computer backups. Backups are, to your computer, what a spare tire is to your car. People would thinking twice about owning a car without a spare tire, yet people don't give a moments thought to a computer backup system. Imagine that your computer's Hard Drive crashed, and that you had all your university documents save on the computer. Now let's say that your paper is due tomorrow. If you had a backup, you would still need a second computer to finish your paper, but who doesn't have a second computer to use or access. Now if you didn't have a backup, I'g say that you are in a bit of a bind

You can also check out our WebSite at www.tsgcs.ca.

Have a fantastic week!

Chad Rushka
Computer Services
604-272-3607
604-803-2824
chad@tsgcs.ca