Regularly Update Security Systems

One of the best ways to keep cyber attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.

While keeping your computer up to date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere.

Most companies release software that can be configured to download and apply updates automatically so that you do not have to remember to check for the latest software. Taking advantage of "auto-update" features in your software is a great start toward keeping yourself safe online.

Other Key Points to Note

Be wary of "free" software such as screensavers, secret investment tricks and contests that you have surprisingly won without entering. These are enticing hooks used by cyber criminals to grab your attention and lure you into submitting personal information.

In addition, while you may not directly pay for the software or service with money, the free software or service you asked for may have been bundled with advertising software ("adware") that tracks your behavior and displays unwanted advertisements. If an offer looks so good it's hard to believe, ask for someone else's opinion, read the fine print, or even better, simply ignore it.

Keep an eye out for phony email messages. Messages may be fraudulent if they contain misspellings, poor grammar, odd phrasings, URLs with strange extensions or that consist entirely of numbers, and anything else out of the ordinary.

Don't respond to email messages that ask for personal information. Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company's web address into your browser. Do not click on the links in these messages as they often take you to fraudulent and malicious websites.

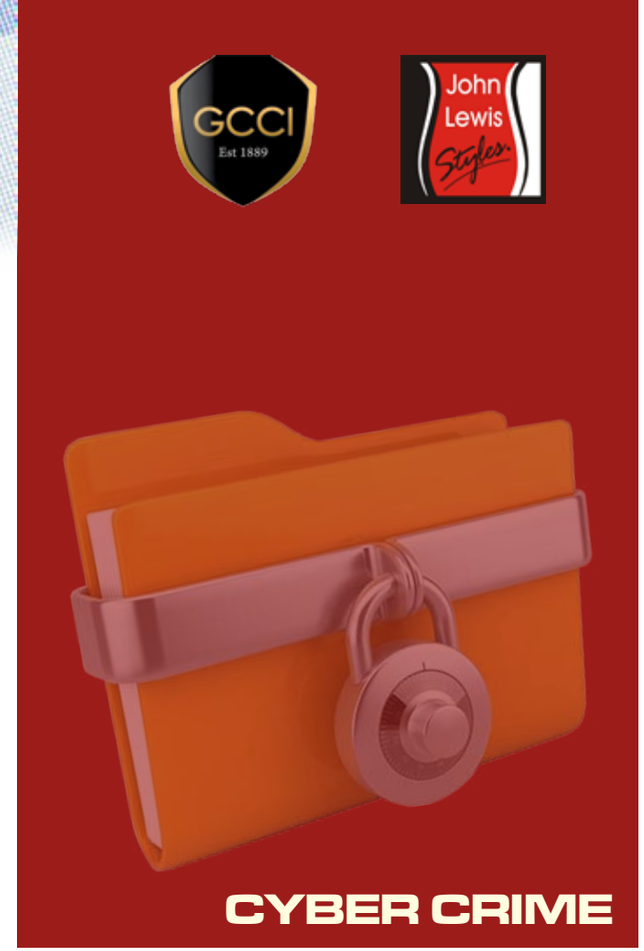
A shopping, banking, or any other website that requires your sensitive information should begin with "https:" (i.e., https://www.yourbank.com), not "http:" (i.e., http://www.yourbank.com). The "s" stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner).

Pay attention to privacy policies on websites and in software. It is important to understand how an organization might collect and use your personal information before you share it with them.

The Georgetown Chamber of Commerce & Industry
156 Waterloo Street
North Cummingsburg
Georgetown, Guyana

Tel: + 592 225-5846 or + 592 227-6441
Tele/Fax: + 592 226-3519

Email: gccicommerce2009@gmail.com
Website: http://www.gcci.gy



CYBER CRIME

STAY SECURE

What is Cyber Crime?

The Guyanese business community is moving rapidly towards the use of digital technology applications to run and operate their businesses. This development makes them vulnerable to the pernicious effects of Cyber Crimes.

Cyber crime is a term that covers a broad scope of criminal activity using a computer. Some common examples of cyber crimes include identity theft, financial fraud, website defacements and cyber bullying. At an organizational level, cyber crimes may involve the hacking of customer databases and theft of intellectual property. As cyber criminals gradually become more sophisticated in their bid to target companies and individuals, so should be the effort of potential victims to thwart their efforts. This involves not just finding comfort in anti-spyware and anti-virus software, but by becoming actively involved and practicing sound prevention strategies.

Effects of Cyber Crime

The effects of a single, successful cyber attack can have far-reaching implications including but not limited to financial losses, theft of intellectual property and loss of consumer confidence and trust.

The Way Forward - Prevention Is Better Than cure

Training and awareness are important and can go a long way towards limiting attacks. Individuals and businesses should be aware of cyber threats and take preventative actions to safeguard their digital application.

Securing your WiFi Networks

Use a strong password to prevent unauthorized access to your wireless (Wi-Fi) network. Wi-Fi networks are vulnerable to intrusion if they are not properly protected after installation.

Use wireless hotspots with care

Do not connect to "free" wireless hotspots in public places unless you know the source, such as a verified hotel or airport run access point. Many hackers will set up free hotspots to intercept information as you surf the web and type in passwords or account numbers.

Create strong passwords

For password selection, avoid obvious personal references that can be linked to you through social networks. This means avoiding birth dates, anniversaries and names. Also, we encourage the use of complicated passwords by combining letters, numbers and special characters.

Moreover, passwords should be updated regularly, never written down and the practice of using different passwords for different accounts is greatly recommended.

Download applications with care

Be wary of downloading free applications and programs unless you know who provided and developed them, and whether they were properly tested.

Store Sensitive information offline

If you have highly sensitive information, it should be stored on a device that is not connected to the Internet so as to limit the chances of it being compromised.

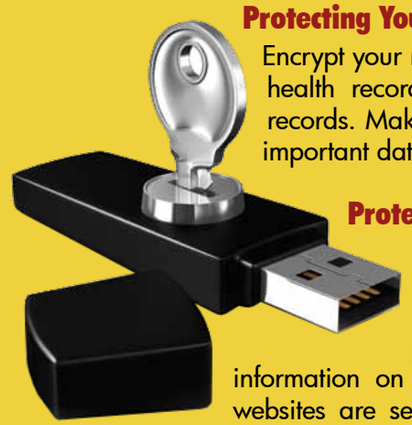
Careful what you post on the internet

The personal information individuals post on social networks can greatly assist cybercriminals. These details can be used for a whole slew of illegal purposes, including figuring out answers to security questions for online accounts, tracking personal activities and even figuring out when people won't be home for an extended period of time.

Enable and maintain your firewall

A firewall is usually your computer's first line of defense as it controls who and what can communicate with your computer online. You could think of a firewall as a sort of "traffic cop" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic, such as attacks, from ever reaching your computer.

Protecting Your Data



Encrypt your most sensitive files such as health records, tax returns and financial records. Make regular back-ups of all your important data.

Protect your e-identity

Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure especially when making online purchases, or that you have enabled privacy settings (e.g., when accessing/using social networking sites, such as Facebook, Twitter, YouTube, etc.). Information posted on the internet can have long lasting consequences.

Secure your mobile devices

Be aware that your mobile device is vulnerable to viruses and hackers. Do not store unnecessary or sensitive information on your mobile device. It is also important to keep the device physically secured as it can be easily lost or stolen. If you do lose your device, it should immediately be reported to your carrier and/or organization. There are some devices that allow remote erasing of data. Be sure to keep your mobile device password protected.

Review bank and credit card statements regularly

The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.