PREVENTIVE MEASURES – AVOID CYBERCRIME

Cybercriminals target everyone with access to the internet, and already, almost two thirds of internet users have been victims of some sort of cybercrime. Nevertheless, most cybercriminals are opportunistic – they will only attack easy and vulnerable targets. Therefore, the harder your computer is to crack, the less likely it is to be attacked by cybercriminals.

While it is impossible to make yourself impervious to all cyber attacks, there are some very basic strategies that can be employed to reduce the chance of becoming a target – or at least limit the damage that a successful attack may cause:

Keep your computer updated with the latest security software

Just like it is necessary to lock your front door at home, it is imperative to ensure your computer is secure by installing anti-virus, anti-spyware and a firewall, or a package including all three. Regularly install new updates when they become available, otherwise hackers will exploit any existing flaws to break into your system. Take advantage of 'auto-update' features to ensure you receive the updates as soon as they are released.

Configure your computer's security settings

Make sure that the security settings on your computer are set to the right level, particularly with regard to your internet browser and email software, as they will be able to warn you of potential risks when visiting dubious or suspicious websites.

Be responsible when using passwords online

Passwords are a necessary security measure to perform various functions on the internet. If used and chosen improperly, they can make an internet user extremely vulnerable to attacks. When required to select a password, make sure you choose a secure password that:

- Has at least eight characters or more (with a combination of letters, numbers and symbols if possible)
- Is not related to personal information such as birthdays or login names
- Is not the same password you use for other internet functions

Furthermore, try to change your password regularly – about every two months– and always keep your password information in a secure place.

Keep an eye out for suspicious e-mails

If an e-mail displays any of the following, approach it with care:

- Misspellings
- Poor grammar or odd phrasing
- A suspicious web address – such as one made up of predominantly numbers rather than words
- Instructions requiring you to provide information (particularly e-mails which ask you to provide details quickly to avoid something bad happening).

If the e-mail is from an unknown source, try to avoid opening it, and definitely avoid opening any attached files or links as they may contain harmful viruses or worms.

Keep your personal information protected

Many online services (for purchasing goods, using social networking services etc.) require you to enter at least some personal information on a website. Before doing so ensure that the website is in fact authentic – for instance a shopping or banking website requiring sensitive information should begin with 'https://www', with the extra 's' standing for 'secure.' Also, read the privacy policies of websites, and understand how the website may use or share your personal information in the future. Always guard your e-mail address when possible, and do not unnecessarily post it on any online blogs, chatrooms, or newsgroups, or you may become susceptible to spammers and phishers.

Steer clear of pirated materials

The use of pirated software, or the downloading of pirated material, is not only illegal but is also dangerous for your computer. Many files contain hidden Trojan horses that will download themselves onto your computer along with the stolen file.

Regularly check your financial accounts

By regularly checking your accounts for unauthorized transactions, you may greatly reduce the damage a cybercriminal could inflict on your financial assets. If there are any suspicious looking actions on your account, report them immediately to your bank.

And always remember: if an online offer looks too good to be true, it is likely fraudulent.

Online Protection of Children

The internet is used by all types of criminals, and there is no doubt that many individual internet users view cyberspace as an ideal forum to prey on the vulnerabilities of children. While the internet allows children to experience new and exciting sources of knowledge, it is vital that they are protected from internet users who seek to exploit them.

Different surveys purport different statistics on the issue, but according to the Virtual Global taskforce, roughly 1 in 5 children using the internet have received sexual advances while online. Furthermore, about nine out of ten sexual advances towards children take place in internet chat rooms.

Children can be targeted by offenders through many different online venues:

- Instant Messaging platforms (such as MSN messenger etc.) – often a user's details, including age, can be viewed publicly, unless the user specifically chooses otherwise.
- Gaming websites – which, aside from providing gaming services, also allow communication between players from all over the world.
- Chat rooms and forums – where offenders can target children with flattery or other deceitful tactics and encourage them to communicate more privately through sms or instant messaging services.
- Email – offenders sometimes send fraudulent emails in which they pretend to represent an organization a child may be interested in, with the hope of establishing communication.

Child Online Safety: Guidelines for Parents

There are some guidelines that can be followed to increase your child's online safety:

- Openly communicate with your child about sexual victimization and the potential for danger online – make sure they understand not to be embarrassed or ashamed of being inappropriately approached online, but to come to you immediately and tell you about it. Let them know it is never too late for them to tell someone they feel uncomfortable about something.

- Keep the computer in an open space of the house (and not in the child's bedroom) where you can easily view your child's online activities. Encourage your children to be open about their internet activities, and learn how they enjoy spending their time online.
- Utilize parental controls and blocking software to monitor your child's online activities.
- Help your child understand that when online they should never give out personal details and explain to them what sort of information is personal (their email address, mobile number, home address, school details, photos or videos of family and friends etc.) In addition, make sure your child is aware of what posting items online in profiles or on forums implicates – it is easy to forget the internet is not a private place, and children need to understand this.
- Instruct your child not to open files or images from people they do not know, as they may contain harmful material like worms, viruses or sexually explicit material.
- Explain to your child never to arrange a face-to-face meeting with anyone they have met online, even if the other person claims to be another child.

Potential Signs that your Child is at Risk

Most children have never been abused online, and never will be, but there are some potential signs that you look to look out for, namely:

- Your child is becoming very secretive about his or her online activities (perhaps deleting their history, using encryption software, or quickly flicking the screen display when you come into a room).
- Your child is spending a large amount of time on the internet, predominantly in chat rooms and forums.
- Your child is using an online account that belongs to someone else.
- Your child is withdrawing from the family and is beginning to isolate his/herself.
- Your child receives packages or gifts from unknown sources.
- Your child is making phone calls to unidentified and unusual phone numbers.

Remember, however, that these behaviors may simply be signs of your child growing up – therefore, always try to be open with your child and establish the reasons behind why your child may be changing their behavior.