

## Tips for right online behaviors

### 1. Protect yourself and your family on the web

- a. Configure a strong password – password allows the safe access to personal information and data, exactly like accessing the house with the key. Therefore you should use a password or a passphrase that is easy to remember and change. Strong passwords consist of at least eight characters containing letters, numbers and marks such as punctuation marks.
- b. Don't post your information and pictures on the web - it's as if you post them on a big banner in a market crowded with thousands and millions of people to read it. Therefore you should keep your personal data for yourself in order to protect your identity, privacy and family from hackers and insiders.
- c. Don't arrange for a personal meeting - insiders and criminals on the web will try to deceive you into meeting them in person by the illusion that they are friends who care for you. Take care of those anonymous to you and don't be an example for the proverb "Don't be a cheap in the house of wolves".
- d. Always consider the information you read on the internet is incorrect (unless the poster is a trusted organization) - many people write and post incorrect information in order to spread rumors, create stories, changing of pictures and imitating fake characters. It's more likely that you won't believe or trust any person knocks your door or any story narrated by him. So why do you believe and trust anyone on the web?
- e. Talk to one of the elders if you feel offended or afraid of anything you see or hear on the web - use on the internet the same methods you use to prevent anyone from harassing and annoying you in the school or suburb. Tell a school teacher or your parents in case you read or hear something offensive, frightful or provoking.
- f. Encourage your family members to separate their user accounts – each of us must have a private room or a private corner in the room shared by all family members in order to keep our privacy. Parents for example keep important documents in a closed place. We should all follow this behavior when keeping our information such as diaries, bank accounts data, or any important data.
- g. Share what you know about safety on the internet with your family – many of you may have a wider knowledge about computing and internet safety compared to your parents or brothers. Therefore you should take sometime to teach them how to protect themselves and data from the threats on the internet.

### 2. Protect you data

- a. Always consider that your email, discussions on the online forums and email messages are read on the public. Most web pages are public forums as all what is written on them can be read by millions with no ability to delete it.
- b. Be careful when opening the email - anonymous emails or unexpected emails from persons you know are mostly infected with viruses and repeated viruses. Therefore you should delete such emails before opening them. If you think that a friend of you has sent you an unexpected email, Call him before opening the mail.

- c. Backup your data – backup all your important files, information and software every time you change them (at least once a week). Store these backups in a safe place.
- d. Take care of using of shared files or using of a computer with others – shared files allow several users to download files through the internet from a computer to another. These shared files allow you to download files from the computers of others to your computer and also allow others to access your computer and data to scan them and download what they like from software and data on your computer.
- e. Don't share the password with anyone. Do you share your house key with your friends? If the answer is no. why do you share the password with them?

### 3. Protect your properties

- a. Update antivirus and antispyware software – they delete from the computer memory the files that indicate patterns of infection and corruption. It's therefore important to update antivirus and antispyware software in order to have recent definitions of computer viruses and spywares.
- b. Use and maintain firewall software – firewall is a bodyguard that doesn't allow any dangerous files, commands or software to access your computer, and allows proper ones to perform in-goings and out-goings. You can customize the firewall to prevent access to some sites and allow it for others.
- c. Disconnect the computer from the internet when not using it. Some kinds of fraudulent viruses are programmed to destroy your computer when you stop using it while it's still connected to the internet. Some others are programmed to me when the computer is in standby mode.
- d. Take care when opening the attachments that you receive by emails, online forums or SMS - attached files may contain viruses, worms or spywares. Therefore you should delete attached files without opening them. Don't open attached files sent by persons you don't know or with meaningless addresses and names.
- e. Download the latest batches and security updates to the computer systems frequently – many of the computer software and hardware vendors continuously release updates for the vulnerabilities in their software. These updates fix security problems in the operating systems, web pages, or software. Some companies such as Microsoft release regular updates every month. We advice you to check web pages of operating system's vendors such as Microsoft and Apple. You can also visit Q-CERT's web page to find necessary information about internet security updates and vulnerabilities.