



# **Cyber Security Workshop**

**for Students  
in the 6th – 12th grades**

# Q-CERT

## Cyber Security Workshop for Students in the 6th – 12th grades

Wiam Younes

### What is cyber security?

---

Cyber security is a set of principles and practices designed to teach you how to safeguard your computing assets and online information from threats.

### Cyber crimes and security risks

---

Cyber crime is defined as any criminal or illegal behavior that is facilitated by computers. This can range from illegal behavior intended to harm people, such as cyber bullying or cyber stalking, to using malicious software or exploiting vulnerabilities to steal assets such as credit card or identity information. Cyber crime also includes fraud or the deliberate destruction of data on an individual computer or network. Other computer crimes and security risks include the following:

- a. Piracy – illegal use of copyrighted material such as plagiarism or illegal downloading of music, movies, text, or other types of files
- b. Intrusion – unauthorized individuals trying to gain access to computer systems in order to steal information, corrupt files, illegitimately view data, or gain control of the computer
- c. Identity theft – computer intruders intent on stealing your personal information to commit fraud or theft
- d. Predatory behavior – online behavior that targets some aspect of your online information in order to steal or destroy it
- e. Virus – a self-replicating program that spreads by inserting copies of itself into other computer code or into documents
- f. Spam – often automated programs designed to send a message to multiple users, mailing lists, or email groups
- g. Worm – a self-replicating, self-spreading malicious computer program
- h. Trojan horse – a malicious program disguised as legitimate software
- i. Malware – programs that are designed to harm your computer
- j. Spyware – software that sends information from your computer to a third party without your consent

### Cyber crime has serious consequences!

---

Anyone who commits a cyber crime may encounter a variety of serious, negative consequences. Cyber criminals can end up in prison, face legal action, find themselves pursued by national or international law enforcement, and face severe financial loss and social rejection.

# Behavior tips for responsible cyber citizens

---

## Protect yourself and your family online.

- a. Create a “strong” password. A password provides secure access to personal information and data in a way similar to the key for your house. Use a unique password or passphrase that you can remember, and change it often. A strong password consists of at least eight characters and should include letters, numbers, and special characters such as punctuation marks.
- b. Do not post information or pictures about yourself online - it is like posting to an electronic bulletin board in a busy market where thousands, if not millions, of people can view it. Keep your personal information to yourself in order to protect the identity and privacy of you and your family from predators and thieves.
- c. Do not arrange to meet in person. Online predators and criminals will try and trick you into meeting with them, posing as friends or caring people. There is an old proverb that applies: “Beware of wolves in sheep’s clothing.”
- d. Always assume information you read or hear online is not true. People can write false things, spread rumors, fabricate stories, alter pictures, and assume false personalities online. You would not believe or trust a stranger knocking at your door with a story, so why do so on the internet?
- e. Talk to an adult if you feel uncomfortable or afraid of anything you see or hear online. In the same way you don’t allow people to bully you and harass you in school or the neighborhood, be sure not to allow it online either. Talk to your teachers or parents if you read, see, or hear something that makes you uncomfortable, fearful, or angry.
- f. Encourage your family members to have separate user accounts. We all like to have our own room or a personal corner in a shared room to keep a few things to ourselves. Parents keep important documents locked away. This is a behavior we all should follow with our own information such as journals, bank account information, or other important data.
- g. Share your knowledge of cyber security with your family. Many of you may know more about computers and cyber security than your parents or siblings. Take the time to teach them how to protect themselves and their data from danger.

## Protect your data.

- a. Always assume your emails, chat sessions, and text messages are read in public. Most of the internet is a public forum where anything you post online could potentially be viewed by millions and will not be erased.
- b. Use caution when opening emails. Emails from people you don’t know, or unexpected email from someone you do know, are likely the result of a spam or are infected with a virus. Delete these emails without opening them. If you think a friend is emailing you unexpectedly, call them to ask.
- c. Make backups of your data. Back up all important files, information, programs, and folders every time a change is made (or at least once a week). Keep your backups in a safe place.

- d. Be wary of file sharing or sharing your computer with others. File sharing is the practice of making files available for other users to download over the internet from one computer to another (sometimes called a “peer to peer [P2P] model”). File sharing will allow you to download files from another person’s computer and gives them access to your computer and data in turn.
- e. Do not share your password with anyone. Do you share your house keys with your friends? If not, then why share your password?

## Protect your assets.

- a. Update your anti-virus program and virus definitions as well as your anti-spyware software. Anti-virus and anti-spyware software scans files in your computer’s memory for certain patterns that may indicate an infection. It is important to update your anti-virus and anti-spyware software frequently to have the latest virus definitions or spyware profiles available on your computer.
- b. Use and maintain a firewall. A firewall acts like a guard, keeping potentially dangerous files, requests, or programs from accessing your computer. You can also set up your firewall to block access to certain websites and allow others.
- c. Disconnect your computer from the internet when not in use. Some types of malware are programmed to destroy your computer after you log off but remain connected to the internet; others trigger malicious actions when the computer is in screen-saver mode.
- d. Take care when opening an attachment you receive through email, chat rooms, or SMS. Attachments can contain viruses, worms, or spyware, so scan your attachments before opening them. Do not open an attachment sent by someone you don’t know or that has a name or subject title that does not make sense to you.
- e. Patch your computer with the latest security updates for the software you use. Software and hardware companies frequently issue updates to correct vulnerabilities. These updates fix the problem found in their operating system, browser, or software. Check for updates by visiting the website of the company that makes your computer’s operating system or web browser. Some companies issue a security update regularly; for example, Microsoft issues one once a month. You can also visit the Q-CERT website to find information about computer security updates and vulnerabilities.

## References

---

[www.qcert.org](http://www.qcert.org)

[www.cert.org](http://www.cert.org)

[www.mysecurecyberspace.com](http://www.mysecurecyberspace.com)

[www.us-cert.gov](http://www.us-cert.gov)

- Security Tips for Non-Technical Users (<http://www.us-cert.gov/cas/tips/>)
- “Home Computer Security” ([http://www.us-cert.gov/reading\\_room/HomeComputerSecurity/](http://www.us-cert.gov/reading_room/HomeComputerSecurity/))

[www.netSMARTZ.org](http://www.netSMARTZ.org)



For more information about Q-CERT, contact [info@qcert.org](mailto:info@qcert.org)

