

Qatar K-12 Schools
Cyber Security Tips for Parents
Wiam Younes
Contribution; Eric Hayes

What is cyber security?

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

Why do I need to know about cyber security?

You probably use many kinds of current technology such as internet-connected computers, cell phones, personal digital assistants (PDAs), digital cable or satellite television, ATM machines, credit/debit cards, and more. Given how much a part of your daily life this technology has become, it is imperative that you learn to protect yourself from cyber crimes by arming yourself with cyber security knowledge.

An Analogy: Learning to use a computer safely is like learning to drive.

Most of us require a vehicle in order to facilitate daily life. Driving can be great fun when you first learn how to drive. We expect that the first time teenagers sit behind the wheel of a car, someone will be next to them, teaching them how to drive with skill and safety. As parents, we want our children to become safe drivers, so we provide them with driving lessons and driver's education classes that emphasize safety, skill, and knowledge. We encourage them to drive safely by sharing lessons from our driving experience. We make sure the automobile they drive is in good condition and has all required safety devices such as seat belts, airbags, turn signals, and effective brakes. Without this effort on our part as teachers, teenagers would learn from each other or through trial and error and probably make many mistakes. Unfortunately, a driving mistake could cost them their lives!

While it is unlikely that the uneducated use of computers and the internet could lead to a threat to physical safety, there are many other serious threats in the cyber world. Communication and computing technology are the "vehicles" that we use to create, transport, exchange, extract, and store all kinds of information. When we allow our children to use these sophisticated tools without proper training and preparation or with no warning about the dangers, it is no surprise that they will often inadvertently cause damage, expose themselves to inappropriate content, or encounter malicious individuals. This is why you must teach your children about cyber security, similar to the way you would if they were learning to drive.

Are we in any danger when we use the internet through a personal computer?

You and your family are not in danger as long as you are aware of the types and severity of various threats, have the knowledge to protect against these threats, and monitor your computer's behavior and your family's internet use.

How can I protect myself, my family, and my resources?

Here are ten tips to protect yourself and your family when you use a computer to access a network:

1. Understand cyber security risks.
2. Create "strong" passwords.
3. Use and maintain anti-virus and anti-spyware software.
4. Use and maintain a firewall.
5. Use care when reading email that contains attached files.
6. Make secure backups of your important files and folders.
7. Use care when downloading and installing programs, files, or software.
8. Establish user accounts when sharing your computer.
9. Establish security guidelines for anyone who uses your computer.
10. Protect your children by educating them about online threats.

Scenario: AbdulAziz family learns about cybersecurity the hard way.

AbdulAziz is a civil engineer and a father of four. AbdulAziz's wife Sarah is a high school teacher, his eldest son Mohamed is in 11th grade, his second son Rakan is in 9th grade, his daughter Hafssa is in 7th grade, and his second daughter Huda is in 5th grade.

AbdulAziz has a busy work schedule, so he often takes documents home and works on them using a home office computer. His wife Sarah also takes work home to prepare lesson plans and to grade students' papers using the home office computer. The AbdulAziz family has a second family computer for general use.

AbdulAziz stores some client information and project specifications on his home office computer to use when he works there. His wife Sarah stores her lesson plans, student roster, and information such as their age, addresses, parents' names, contact information, and their grades on the office computer's hard drive.

Mohamed, their eldest son, uses the family computer to download music, learn about cars, follow his favorite soccer team, and to chat with friends. Rakan, the 9th grader, spends most of his time surfing the web; he browses the website Orkut to check email from friends and to trade gossip. He also sends text messages to his friends, reads the latest news about pop culture, and updates his music library with files sent from friends or that he downloads.

Hafssa, on the other hand, is not interested much in using the home computer, other than

as a tool for homework and to research school projects. She prefers to phone her friends and chat for hours. Her cell phone enables her to exchange text messages with her friends and they frequently share pictures, funny animations, and ring tones. Huda, the youngest daughter, likes to play games online and follow fashion for her age group. She often uses the home computer to chat with her friends and talk about school, movies, and TV shows.

One day, Rakan had a school project which required him use the internet to find information about ancient Egypt. His brother Mohamed was typing an essay using their home computer, and was taking a long time doing so. Rakan asked his mother's permission to use the office computer to do his project. Once Rakan was online, he logged on to MSN messenger to discuss his progress with friends and share tips. One friend directed him to a website that had information about ancient Egypt and also to a site with a link to a free download of a song they had wanted to listen to for some time.

Rakan jumped at the opportunity. He visited the website and started to download his favorite song while still browsing other pages in his search for information on ancient Egypt. Several pop-up windows appeared, and the computer froze. Rakan did not know what to do, so he asked his brother Mohamed to help. Mohamed tried to close all open windows but could not, so he unplugged the computer and then rebooted. In the process, Rakan lost the paper he was writing and angrily realized he would have to write it all over again.

After they turned the computer back on, they noticed that it did not function the same as it had before; it opened the start-up programs more slowly, then odd web pages would pop up rapidly, and finally the computer would freeze.

AbdulAziz came home that day at 6 p.m. and needed to work on one of his projects. He had promised the company CEO he would send some files to him before midnight. The CEO had an important client meeting early in the morning and needed the information beforehand. AbdulAziz logged on to his office computer in order to retrieve some of the data he had stored on the hard drive. He could not find the data, and every time he attempted to open a file the computer froze after web pages popped up.

AbdulAziz called his colleague Ahmed in the company IT department to ask for help. Ahmed gave AbdulAziz instructions but nothing worked. Ahmed said he would visit AbdulAziz's house before going home and came by two hours later. Ahmed discovered that a Trojan horse had infected AbdulAziz's office computer and that the program enabled some computer intruder to access it remotely.

The intruder appeared to have accessed the data and then destroyed files stored on the hard drive. Not only did AbdulAziz not have backups of his stored company project data, he had also lost his wife's school files, as well as their personal financial investment data. He now had to worry about the possibility of identity theft and of the intruder accessing their financial accounts.

There was also a risk that other families at his children's school could now become

victims of identity theft. He was upset on two counts — not only had he lost critical work and personal data with no back-up, but now, via the internet and the unwitting actions of his children, some malicious individual possessed critical data and could use it any way they chose.

After reading this scenario, ask yourself the following questions:

1. What risks could have been mitigated in advance?
2. What protective measures could AbdulAziz and his family have taken to protect their data and their computer?
3. Do I share any vulnerable aspects of this scenario?

To address these questions, let us revisit the ten tips for safe computing:

1. Understand cyber security risks. Here are some definitions you should understand:
 - Virus - self-replicating code that spreads by inserting copies of itself into other software programs or documents
 - Trojan horse - a malicious program disguised as legitimate software
 - Worm - a self-replicating, self-spreading malicious program
 - Spyware - software that sends information from your computer to a third party without your consent
 - Malware - programs designed to harm your computer
 - Intrusion - trying to gain privileged access to computer systems in order to steal, corrupt, or illegitimately view data
 - Identity theft - the theft of personal information to commit fraud
2. Create “strong” passwords.
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. As an aid to memory, you can use a phrase or sentence. Letters should be both connected and disconnected (if the password is written in Arabic).
Examples of strong passwords:

Abdul19!21Aziz
mysOnisra&Kan5*

Do not write your password down anywhere, instead, if you need to, record some hint that will help you recall if you forget.

3. Use and maintain anti-virus and 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.
4. Use and maintain a firewall.
The firewall acts like a guard, keeping potentially dangerous files, requests, or programs from accessing your computer. It permits only appropriate traffic to enter and leave the computer. You can also set-up your firewall to block access to certain websites and allow others.
5. Use care when reading email that contains attached files.
Email can contain worms and viruses in an attachment, so before you open an email, ask yourself the following questions:
 - a. Is the email from someone you know?
 - b. Have you received email from this sender before?
 - c. Were you expecting email with an attachment from this sender?
 - d. Does the subject and name of the attachment make sense?
 - e. Should you scan the attachment before opening it?
6. Make backups of important files and folders.
Back up all important files, information, programs, and folders every time a change is made (or at least once a week). Just as you protect your irreplaceable valuables, back up the files you cannot replace. Keep your backups in a safe place such as with other valuables in your house or, even better, in a secure location different from you home.
7. Use care when downloading and installing programs.
Make sure you do the following:
 - a. Buy software and programs from vendors that you trust or who are well-known nationally.
 - b. Learn about the software and the programs you are purchasing.
 - c. Make sure that software you use has been used safely by others or recommended to you from a knowledgeable, trusted individual.
 - d. Install programs that will not take all available space on your hard drive and that do not negatively affect other programs you rely on.
8. Establish user accounts when sharing your computer.
When sharing your computer, do the following:
 - a. Create a separate account for each user.
 - b. Limit privileges for some accounts, such as children or guests.
 - c. Lock your computer when you are away from it.
 - d. Choose restrictive options in your security settings for hardware and for programs such as web browsers and email programs.
 - e. Disconnect your computer from the internet when you are not using it.

9. Establish security guidelines for anyone who uses your computer.
 - a. Create a family contract with clear rules for using the computer and make sure everyone understands and agrees.
 - b. Keep a list of internet access guidelines and good computing practices close to your home computer for all to see.
 - c. Stay aware of the security aspects of any new technology or software used at home, learn about any associated threats and how to handle them, and share this knowledge with your family.

10. Protect your children online.
 - a. Keep the family computer in a centrally-located place where an adult can easily observe what is happening.
 - b. Discuss guidelines for computer use.
 - c. Use the internet with your children sometimes.
 - d. Stay informed about potential cyber threats against children and protective measures you can take.
 - e. Implement parental control tools.
 - f. Know your children's online friends.
 - g. Teach your child never to give personal information to anyone online.
 - h. Teach your child never to trust people online they do not know personally.
 - i. Provide separate user accounts for each child and control their access.
 - j. Consider installing software that allows you to monitor your children's activity on the internet.

What could AbdulAziz and his family have done differently to protect their computer and their data?