Art courtesy of Freepik

Guide for Parents - Computers

1. Wherever possible, position home computers in common areas.
2. Talk to your children about expectations for safety and use of computers when gaming or using the internet. Set guidelines for use that include what should and should not be accessed, and when access is allowed. Follow up with your children regularly to talk about their activities online. Constant communication is the key to prevention of potential risks.
2. Consider installing monitoring software and or content filters. Many are available as both paid and free services.
3. Understand that communication with others using desktops can occur not only in the more typical chat room, or social media site, but additionally within applications, games, and direct client software. These applications may not always bear the same restrictions that content filters applied to browsers can or will protect.
4. Desktops and Laptops offer a lot more flexibility in the applications available out there. This allows for the potential to download applications that can cause greater risk to personal data security. Invest in Antivirus and Internet Security software if it is not included with the Operating System. Even Mac which is considered a relatively secure Operating System is not outside of risk.
5. Be aware of downloading habits to ensure safe browsing is occurring. A quick look through internet history or the downloads folder may be simple enough if your child isn’t actively attempting to mask activities. Be wary of discovering any software on your computer or digital content that you did not specifically purchase. Digital Piracy can lead to both legal and data security risks. Often, compromised software allows for backdoor viruses or access to be granted to your pc.
6. Be on the look out for torrent files (*.torrent), or torrent downloading clients on your pc as they are typical of activities used to download software and content illegally.
7. Consider restricting access to the computer for various activities and various times per day/week. Allotting time for homework is necessary, but limiting recreational use could help prevent addictive habits from forming.
8. Do not automatically save usernames and passwords to your browsers, especially when it comes to accounts that provide access to your financial data. The convenience comes at the cost of your potential security.
9. If you are concerned that your computer is compromised, for example if you notice advertisements appearing unwarranted, and even when a browser is not open, do not access personal accounts until you have had a professional perform virus/ malware removal. Additionally, any software that pops up claiming that you have a virus, and it not software that you installed yourself, or asks you for additional funding is most likely a virus. People also have begun to trust phone callers, since a person speaking seems less likely to be a virus initiator. Scams, even over the phone, still exist. Microsoft will never call you to inform you that your Operating System is invalid, and ask for a credit card to reconfirm it.