The dangers of free WiFi

With the explosion of free, public WiFi networks, students have been handed the key to freedom, being allowed to search the web, carry out research and correspond with peers on projects from any location possible, be it a café, a restaurant or an airport. Yet this freedom also comes at a price in the form of a list of dangers that goes on and on and will have you running to bestonlinereviews.com for the best antivirus software or VPN service on the market.

The issue that arises with the popularity of public WiFi networks is that, just as users can easily log on and connect, so too can hackers. The fact that these networks require no authentication means that unsecured device using the networks are easily accessible to anyone with hacking skills on the same network.

This can be done with hackers placing themselves between the user and the connection point. Therefore, every time the user sends an email, enters a word in a search engine or provides any data to a website or social network site, it would be as if the user went up to the hacker and handed that information over to him himself. This is particularly dangerous when making purchases, as the hacker is able to steal directly from the users bank account he posing as that individual while making online purchases. Besides this, the hacker might also control the electronic device remotely, disrupting workflow and the device's functionality.

However, with access to personal files, a hacker may also decide to distribute malware. This could mean a number of things, such as the files on a device being locked up until a ransom is paid, or even the computer's data storage being wiped

clean.

The most highly skilled hackers might even be able to infect the network itself, resulting in anyone who connects to the public WiFi becoming infected with the virus.

Students may be prone to shrug off warnings under the impression that hackers normally aim for more profitable victims. Yet, at an age when data is almost more valuable than money, this might not be so. By withholding a user's files or by accessing personal emails, the hacker is in a position to syphon money from his victims.

Nevertheless, not all is lost. There are precautions one could take when using a public WiFi network to deter hackers, who normally seek the easiest targets on the system.

Using encrypted websites by enable the 'Always Use HTTPS' option or forking out money for a virtual private network (VPN) will allow a user to surf the web under the radar, going unnoticed by hackers. Also, if a student is using a WiFi network solely for research purposes, or even simply for personal use, and data sharing is not required, it would be advisable to disable the sharing function by going to system preferences or on control panel.

Lastly, even when not actively connected, devices tend to continue to communicate with networks within range. Thus, when not using the internet, it would be best to turn off the WiFi setting.