Techno Tips

Advice to prevent computer hacking

by Marc Y Touitou, WHO Global IT Director

With the authorization of AFSM Geneva, we are including the following summary of Jean-Paul Menu from the July issue of the Global AFSM newsletter. He was quoting from an information circular issued by Mr. Marc Touitou and referred to the bad experience of one AFSM member who had to obtain bit coins and pay a ransom for unlocking his files.

- Do not open any suspicious, unexpected emails, and in particular attachments and/or links to other websites.
- Do not be tempted to open attachments assuming your antivirus will take care of any malicious software. This is a common mistake - new viruses are always out before countermeasures are in place.
- Do not assume it is safe to open suspicious emails on your phone.
- Do not disclose your personal information after clicking on suspicious links.
- Should your computer become infected, do not pay any ransom demanded.
- For Ransomware in particular, if you have a Windows computer, make sure you have Microsoft's monthly security update for October, November and December 2017 installed and your antivirus software is up to date. The best way to make sure your computer is up-to-date is to configure it to check for and install Windows updates automatically.

Please keep in mind that antivirus software is about 90% effective and does not offer full protection. You should also make backup of the most important information on your computer, as all can be lost in matter of minutes.