Anti-virus scam

Has this ever happened to you? You are browsing online when a pop-up ad appears on your screen warning you that your computer is infected with dozens of viruses.

This is what you should look for:

Rogue anti-virus / spyware programmes often generate more "alerts" than the software made by reputable companies.

You may be bombarded with pop-ups, even when you are not online.

High-pressure sales copy will try to convince you to buy immediately.

Other signs of infection include new desktop icons, new wallpaper,or having your default homepage redirected to another site.

If you have been infected, your computer may dramatically slow down.

The issues it finds can only be fixed by purchasing an upgraded subscription or additional software.

Your antivirus software keeps detecting issues and displaying pop-up windows.

Your computer is working at a low Internet speed and slow system performance as the software uses the Internet connectivity to install junk malware – with the result that the efficiency of the system also decreases gradually.

Another likely sign that you are being scammed is when the name of the antivirus software being hawked onto you is one you do not recognise.

The easiest way to know if you have a rogue programme installed on your system is when you find that your homepage within the web browser is changed.

You cannot shut down or uninstall your antivirus software.

eSkills
eSkills Malta Foundation

GEMMA
know, plan, act.

/ESkillsMalta

@eSkills_Malta

www
eskills.org.mt

Anti-virus scam

Action you should take:

Keep your computer updated with the latest anti-virus and anti-spyware software, and be sure to use a good firewall.

Never open an email attachment unless you are positive about the source.

Do not click on any pop-up that advertises anti-virus or anti-spyware software.

Remember that anti-virus scams mimic the design of well-known brands such as Grisoft AVG, Norton and McAfee. Do not buy it because of a pop-up ad on your browser. Go to the actual brand's site and buy it at your convenience – ideally looking first at what is out in the market.

If a virus alert appears on your screen, do not touch it. Do not use your mouse to eliminate or scan for viruses, and do not use your mouse to close the window. Instead, hit control + alt + delete to view a list of programmes currently running. Delete the "rogue" from the list of running programmes and call your computer maker's phone or online tech support service to learn if you can safely use your computer.

Install a pop-up blocker and keep it turned on.

Some scareware is difficult to close and is designed to trick you into accidentally starting a download. It is best to close your browser rather than the individual pop-up ad. If the pop-up ad will not let you close the browser on your PC, try Ctrl-Alt-Delete to shut things down (if you are a Mac user, try Command-Option-Esc to open the Force Quit applications window). If you cannot close your browser, do a hard shutdown of your computer.

Do not download freeware or shareware, such as a torrent site, unless you know it is from a reputable source. Unfortunately, freeware and shareware programmes often come bundled with spyware, adware or fake anti-virus programmes.

Reset your current security settings to a higher level and clear your cache.

eSkills
eSkills Malta Foundation
GEMMA
know, plan, act.