

From: UTech Security

RE: UTech Security Awareness Bulletin – **Beware of Fake Antivirus Scams**

Malware posing as antivirus software has been spreading fast in recent months through popular sites such as Facebook, Twitter, and other social networking sites. Malware is malicious software that is designed to damage or do other unwanted actions on a computer system.

Web users fall prey to the scam when they click on links, pop-ups or flashing advertisements warning them that their computer is infected. The fake program then appears to run a virus check which tells the user that their PC is infected and asks them to pay for it to be cleaned up.

Here are ways to combat the problem and avoid being a victim:

- Make sure that your computer has legitimate antivirus software and keep it up-to-date.
- If you see an antivirus popup for a product that you don't recognize as being installed on your computer, **do not** click on the link and **do not** give out your credit card number. Simply close your web browser and use your existing antivirus software to scan your PC.
- Make sure that your system has the latest Windows Updates from Microsoft.