Subject :- Fake Antivirus

What is fake antivirus?

Fake antivirus is malicious software (malware) designed to steal information from unsuspecting users by mimicking legitimate security software. The malware makes numerous system modifications making it extremely difficult to terminate unauthorized activities and remove the program. It also causes realistic, interactive security warnings to be displayed to the computer user.

How can my computer become infected with fake antivirus?

Criminals distribute this type of malware using search engines, emails, social networking sites, internet advertisements and other malware. They leverage advanced social engineering methodologies and popular technologies to maximize number of infected computers.

How will I know if I am infected?

The presence of pop-ups displaying unusual security warnings and asking for credit card or personal information is the most obvious method of identifying a fake antivirus infection.

What can I do to protect myself?

- Be cautious when visiting web links or opening attachments from unknown senders. See Using Caution with Email Attachments for more information.
- Keep software patched and updated. See Understanding Patches for more information on the importance of software patching.
- To purchase or renew software subscriptions, visit the vendor sites directly.
- Monitor your credit cards for unauthorized activity.
- To report Internet crime or fraud, contact the Internet Crime Complaint Center. http://cybercrimecomplaints.com/