Anthelio Healthcare Solutions
Global Information Security Group
Security Awareness Bulletin - Vol. 01

anthelio®

A higher aim. A newer standard.

Malware – What Is It and How Do I Avoid It?

Short for “malicious software,” malware is software that exploits or takes action on your computer or mobile device without your consent. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware. Creators of malware have various intentions and objectives for their software, but none are good. These include:

- Granting an attacker remote control to access and use an infected machine to launch attacks etc.
- Collecting and stealing sensitive and personal information
- Sending spam emails from the infected machine to unsuspecting targets
- Investigating the infected user’s local network

There are a number of ways that malware can get “on” your computer or mobile device. You might click a link in the body of an email or on a social networking site that automatically downloads a virus. You might even click an ad banner on a website and end up downloading a virus or malware (known as “malvertising”). In some cases your computer can even be infected just by visiting an infected website; this is called a ‘drive-by download’. Malware can also spread by sharing files, USB drives and other portable media.

While security is everyone’s responsibility, here are some personal Do’s and Don’ts to help **<u>you</u>** protect your device and the data on it, as well as company and client data.

DO

- Verify Anti-Virus software is installed, active, updates automatically and is never disabled.
- Keep your computer up-to-date with all vendor patches and security updates.
- Avoid suspicious or unknown websites when using the Internet.
- Only install software from trusted vendors and sources.
- Avoid using flash drives and other removable media.

DON’T

- Click on web pop-ups claiming to be anti-virus protection, to speed up your internet, or other advertisements.
- Click on hyper-links or open email attachments from unknown or unsolicited senders without verifying the sender.
- Use accounts with Administrative privileges for daily computing, i.e surfing the web, checking email, etc.
- Use peer-to-peer file sharing such as Kazza and Bit-Torrent.
- Use “cracked” or pirated software, music, or movies.

www.antheliohealth.com