GO safeonline
A monthly infocomm security newsletter

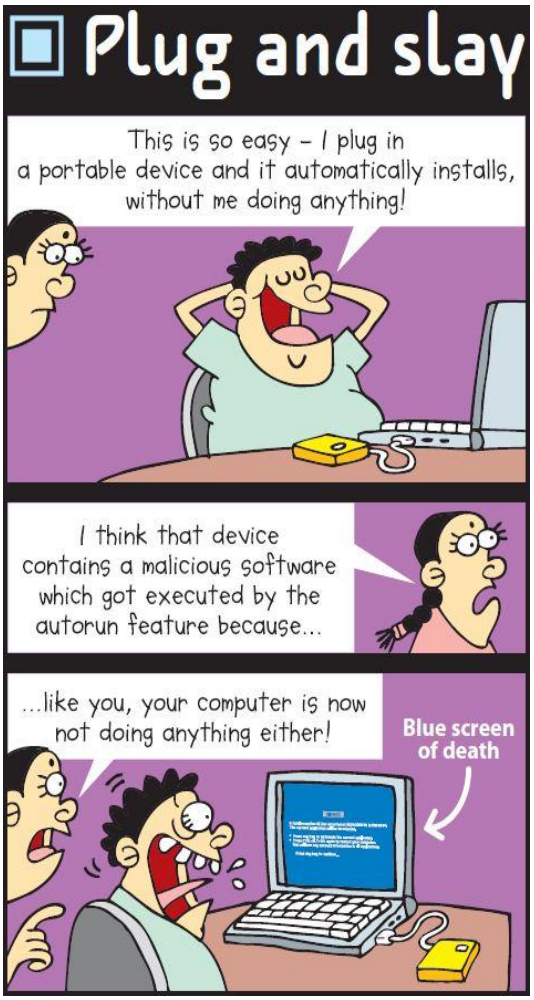
Monthly Newsletter – Issue No. 2013-05

Computer Security – Usage of Computing Peripherals

Computing peripherals are devices that connect to and work with the host computer to enhance its capabilities. External peripherals are connected to, but not part of the host computer. There are three types of external peripherals:

- **Input:** Provide input to the computer from the user, such as mice, webcams and keyboards
- **Output:** Provide output from the computer to the user, such as monitors, projectors and printers
- **Storage:** Provide data storage, such as hard drives, thumb drives and memory cards

Internal devices such as video card, sound card, internal modem, internal hard disk and random access memory (RAM) are installed inside the host computer.



How Are Peripherals Connected?

Internal peripherals are connected to the motherboard directly via the ports or the expansion slots. External devices can be connected using wired or wireless connection. A wired connection requires a cable to be plugged into the computer through a parallel port, PS/2 port, network port or the commonly used Universal Serial Bus (USB) port connector. There may be several other types of connectors used, depending on the computer and the type of peripherals.

On the other hand, a wireless connection has its portability advantage since it does not require a cable. Bluetooth or WiFi are the common technologies used to connect peripherals to devices wirelessly. Bluetooth is commonly used in peripherals such as mouse or keyboard due to its short range connectivity. WiFi is ideal for longer distance connectivity such as for a wireless printer.

Tips On Using Peripherals

Peripherals are essential for a computer to function and perform its duties. Most of us may have take for granted the ease of using the peripherals and overlooked the security issues. Let's look at some tips to better secure the use of peripherals.

Wired	✓ Scan all plug and play devices with antivirus software prior to usage. ✓ Disable the autorun feature to reduce the risk of malware spreading. ✓ Enable encryption on the removable storage device, where possible. ✓ Update firmware of device to eliminate the bugs and vulnerabilities that have been detected. ✓ Use software from reputable source when installing your devices to prevent malicious codes and back doors from being introduced. ✓ Install and configure firewalls to filter out unwanted content or suspicious traffic. ✓ Install and update antivirus software to detect and remove the latest malware from your computer.
Wireless	✓ For Bluetooth connection, turn off the 'discoverable' mode when the pairing process is done. ✓ Use encryption to protect the information you send and receive over your wireless network by scrambling the information using a passphrase only known by you. Turn on the encryption feature such as Wi-Fi Protected Access 2 (WPA2) in your wireless router to secure the privacy of your wireless network. ✓ Disable Service Set Identifier (SSID) and change the default password of your wireless network to prevent attacker from sniffing information and impersonate you. ✓ Install and configure firewalls to prevent unauthorised connections or suspicious traffic. ✓ Install and update antivirus software to detect and remove the malware from your computer.

Interesting Reads

- Peripherals:

  http://en.wikipedia.org/wiki/Peripheral

- How Peripherals are connected:

  http://education-portal.com/academy/lesson/what-are-peripheral-devices-of-a-computer---definition-examples-types.html

- Wired versus wireless peripherals:

  http://www.dell.com/content/topics/topic.aspx/global/learn/network/plan_vs?c=us&l=en&cs=19

www.gosafeonline.sg

www.facebook.com/gosafeonline

Published by: iDA SINGAPORE

A member of: gosafeonline.sg Cyber Security Awareness Alliance

In the next issue...

Learn about how QR code becomes the falling prey of malicious websites.

Let us know what you like about this newsletter and what we can do to better serve your infocomm security awareness needs.

If you have any enquiries or feedback for our newsletter, do write to us at contact_us@gosafeonline.sg.

BE AWARE, RESPONSIBLE AND SECURE!