



## TIP SHEET SERIES NO.8

# Bots and Botnets

### What is Bot and Botnet?

There is no doubt that the Internet provides great opportunities for human life. Because it makes human life easier and connects people to the rest of the world. Unfortunately, there are malicious people who want to take control of these technologies that make life easier. Some of the common types of cybercriminals turn these technologies into slaves (bot) with malware that they infect computers.

After a device turns into a bots, it usually becomes part of a botnet. Botnet is a large network of all other infected devices and is remotely controlled by hackers. Cybercriminals use these bots to send spam and attack more devices or attack various sites. A botnet (robot network) can have hundreds or even thousands of devices.

### What can we do?

In the light of the following suggestions, we can protect ourselves and others against the attacks of various malicious software.

#### ■ Better password creation

A strong password must contain at least 12 characters. Strong passwords should be created by focusing on proverbs, favorable positive sentences, idioms, proverbs.

#### ■ Keep your machine clean

One of the best defenses against viruses, malware and other online threats is the latest security software, web browsers and operating systems.

#### ■ Delete if you are in doubt

Cybercriminals often steal personal information via links in e-mail, social media messages, or online advertisements. Even if the source is known, it should be removed immediately when something seems suspicious.

#### ■ Plug & Scan

USBs and other external devices may be infected by viruses or other malicious software. Security software must be used to scan these devices.

#### ■ Backup

Electronic copies of valuable works, music, photographs and other digital information must be regularly stored and safeguarded.