

# Information Sheet On Internet Security

## 1. Introduction

The Internet has brought many changes in our life, and not all of these changes are positive ones. Cyber crime activities are on the rise as the online world is growing. Users have to be aware about the security risks facing them online and what appropriate measures they have to take in order to minimize the risk of being a victim to these Cyber crimes.

## 2. Security Risks Facing Internet Users

### a. E-Mail Viruses

Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address.

Malicious code might be distributed in amusing or enticing programs. Never run a program unless you know it to be authored by a person or company that you trust. Do not send programs of unknown origin to your friends simply because they are amusing -- they might contain a virus.

### b. Trojan Horse Programs

Trojan horse programs are a common way for intruders to trick you into installing "back door" programs. It can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

### c. Denial of Service Attacks

This type of attack causes your computer to crash or to become so busy processing data that you are unable to use it. In most cases, the latest patches will prevent the attack.

It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

### d. E-Mail Spoofing

E-mail spoofing is the forgery of an e-mail [header](#) so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of [spam](#) often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

### e. Packet Sniffing

A packet sniffer is a program that captures data from information packets as they travel over the network. The data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the packet sniffer, intruders can launch widespread attacks on systems.

### f. Mobile code (Java/JavaScript/ActiveX)

These are programming languages that let web developers write code that is executed by your web browser. Although the code is generally useful, it can be used by intruders to gather information (such as which web sites you visit) or to run malicious code on your computer. Also be aware of the risks involved in the use of mobile code within email programs. Many email programs use the same code as web browsers to display HTML. Thus, vulnerabilities that affect Java, JavaScript, and ActiveX are often applicable to email as well as web pages.

### g. Spamming

Spamming refers to the sending of unsolicited electronic communications over e-mail, mobile (SMS, MMS) and instant messaging services, usually with the objective of marketing products or services. The content of these

## Information Sheet On Internet Security

messages can range from advertisements to offensive pornographic materials.

While this description covers most kinds of spam, a rising phenomenon is the use of spam to support fraudulent and criminal activities including attempts to capture financial information (e.g account numbers and passwords) by masquerading messages as originating from trusted companies, so called phishing attacks.

### h. Phishing

Phishing (also known as phising) is the practice whereby someone who is pretending to be from a legitimate organisation, sends misleading emails requesting personal and financial details from people.

## 3. Security Tips for Home Users

### a. Use virus protection software and keep it up to date

It is recommended to use of anti-virus software on all Internet-connected computers. Be sure to keep your anti-virus software up-to-date. Many anti-virus packages support automatic updates of virus definitions. We recommend the use of these automatic updates when available.

### b. Do not open unknown E-Mail attachments

Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs.

If you must open an attachment before you can verify the source, we suggest the following procedure:

- be sure your virus definitions are up-to-date
- save the file to your hard disk
- scan the file using your antivirus software

- open the file

### c. Do not run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or colleagues simply because they are amusing -- they might contain a Trojan horse program.

### d. Disable Java, JavaScript and ActiveX if possible

Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser.

## 4. Legislation

**The Computer Misuse and Cybercrime Act 2003** has been introduced to protect businesses and individuals from criminal activities perpetrated through computer systems by providing for the creation, investigation and prosecution of computer-related offences. The following offences are punishable in the Act:-

- Unauthorised access to a computer system;
- Unauthorised access to and interception of a computer service;
- Unauthorised modification of computer data;
- Damaging or denying access to a computer system (e.g through Denial of Service attack, spamming);
- Unauthorised disclosure of password;
- Unlawful possession of devices and data; and
- Electronic Fraud