Discovering Computers 2016 Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Safety and Security

Objectives Overview

Define the term, digital security risks, and briefly describe the types of cybercriminals

Describe various types of Internet and network attacks, and explain ways to safeguard against these attacks

Discuss techniques to prevent unauthorized computer access and use

Explain the ways that software manufacturers protect against software piracy

Discuss how encryption, digital signatures, and digital certificates work

See Page 202
for Detailed Objectives

Objectives Overview

Identify safeguards against hardware theft, vandalism, and failure

Explain the options available for backing up

Identify risks and safeguards associated with wireless communications

Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing

Discuss issues surrounding information privacy

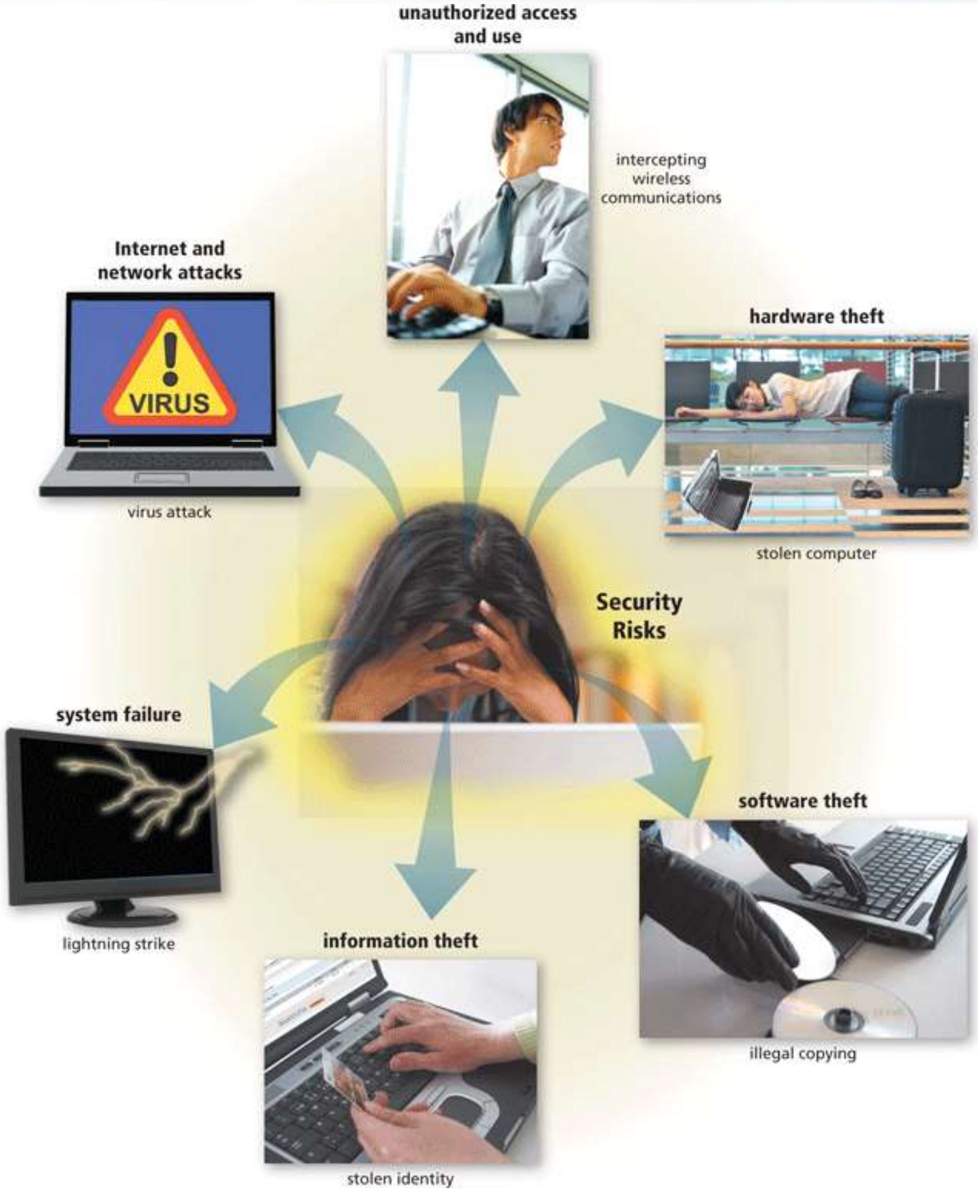
See Page 202
for Detailed Objectives

Digital Security Risks

- A **digital security risk** is any event or action that could cause a loss of or damage to a computer or mobile device hardware, software, data, information, or processing capability
  數位安全風險是指任何可能損害電腦或行動裝置硬體、軟體、資料、資訊、或處理能力的事件或動作。
- Any illegal act involving the use of a computer or related devices generally is referred to as a **computer crime電腦犯罪**
- A **cybercrime** is an online or Internet-based illegal act
  網路犯罪是一種線上或以網路為基礎的不合法行為

Page 212

Digital Security Risks



Page 203
Figure 5-1

Digital Security Risks

- Perpetrators of cybercrime and other intrusion fall into seven basic categories:

Hackers
駭客

Crackers
怪客

Script Kiddies

Corporate Spies
公司間諜

Unethical Employees
不道德的員工

Cyberextortionists
勒索者

Cyberterrorists
恐怖分子

Page 214

網路罪犯

- Hacker
  - Who accesses a computer or network illegally
    非法使用電腦或網路的人
  - Hackers often claim the intent of their security breaches is to improve security
    駭客宣稱他們入侵有安全漏洞系統的目的是為了提高安全性
- Cracker
  - Who accesses a computer or network illegally
  - Has the intent of destroying data, stealing information or other malicious action
    怪客具有破舊資料，竊取資訊或其他惡意的行為的意圖
- Both hackers and crackers have advanced computer and network skills.

Page 214

Cracker VS Hacker

- 1970年代後期，史丹福和麻省理工學院的分時電腦，吸引了一群自稱**駭客Hacker**的電腦狂熱者。當時**駭客**意指享受學習電腦細節與撰寫聰明程式的人，大部份是充滿好奇熱情聰明具有理想而且無害的。這些早期的駭客，實際上很多是微電腦革命的設計者。
- Cracker(怪客)喜歡侵入他人的電腦系統中。這是Hacker駭客族在1980年代中期創造的新詞
- **駭客族本身只是喜歡偷偷跑進系統有漏洞之處，有時搞一點無傷大雅的玩笑。但怪客則是惡意入侵系統，做出破壞的舉動。**
- 雖然 Hacker 總認為他們與 cracker 有所不同，不過一般大眾媒體還是搞不清楚他們之間的區別，因此還是將與cracker放在一起使用。

White hat hacker

- People who break into a computer system and inform the company that they have done so.
- They are either concerned employees or security professionals who are paid to find vulnerabilities.
- White hat hackers are the "good guys." Contrast with black hat hacker and blue hat hacker.
- 這些是懂得安全弱點的駭客，同時也知道如何找出並且利用弱點的人，script kiddle 所利用的工具，大多出於這些駭客之手。
  這些人具備道德的良知，在企業或資安公司裡，默默協助資訊安全的強化，幫助甚大，異於那些亂搞卻不知其然的小朋友。

White hat hacker

- **黑帽駭客（Black Hats）**

  與白帽駭客相同，差別在於他們不具備道德良知，只關注於利益或炫耀其技術。最可怕的莫於利用自身具備的能力，勒索他人。

網路罪犯

- Script kiddie
  - Someone with the same intent as a cracker but **without the technical skills and knowledge**
- Cyberextortionist 勒索者
  - Is someone who uses e-mail as a vehicle for extortion
- Cyberterrorist 恐怖分子
  - Is someone who uses the Internet or network to destroy or damage computers for political reasons.

Page 214

指令小子（Script Kiddie）

- Script Kiddie許多中文翻譯為指令小子，顧名思義他們會利用網路上現成的**自動攻擊程式**，以這些程式掃瞄出系統的許多弱點，讓這些人可以在未獲得授權的狀況下，取得系統權限。
- 這些人通常不具備相關知識，對這些系統弱點及掃瞄與運作方式都不熟悉，所以入侵經常無法成功，但是萬一得手，卻又不曉得已經造成重大危害

Internet and Network Attacks

Information transmitted over networks has a higher degree of security risk than information kept on an organization’s premises

在網路上傳輸信息相較於在企業的辦公室有更高程度的風險

Internet and network attacks that jeopardize security include malware, botnets, denial of service attacks, back doors, and spoofing.

網路上危害安全性包含了惡意軟體、殭屍網路、阻斷服務攻擊、後門、網路詐騙

Page 215

Internet and Network Attacks

- Malware, short for malicious software, consists of programs that act without a user’s knowledge and deliberately alter the operations of computers and mobile devices
  惡意軟體在使用者不知的情況下故意（惡意）改變電腦和行動裝置的運作

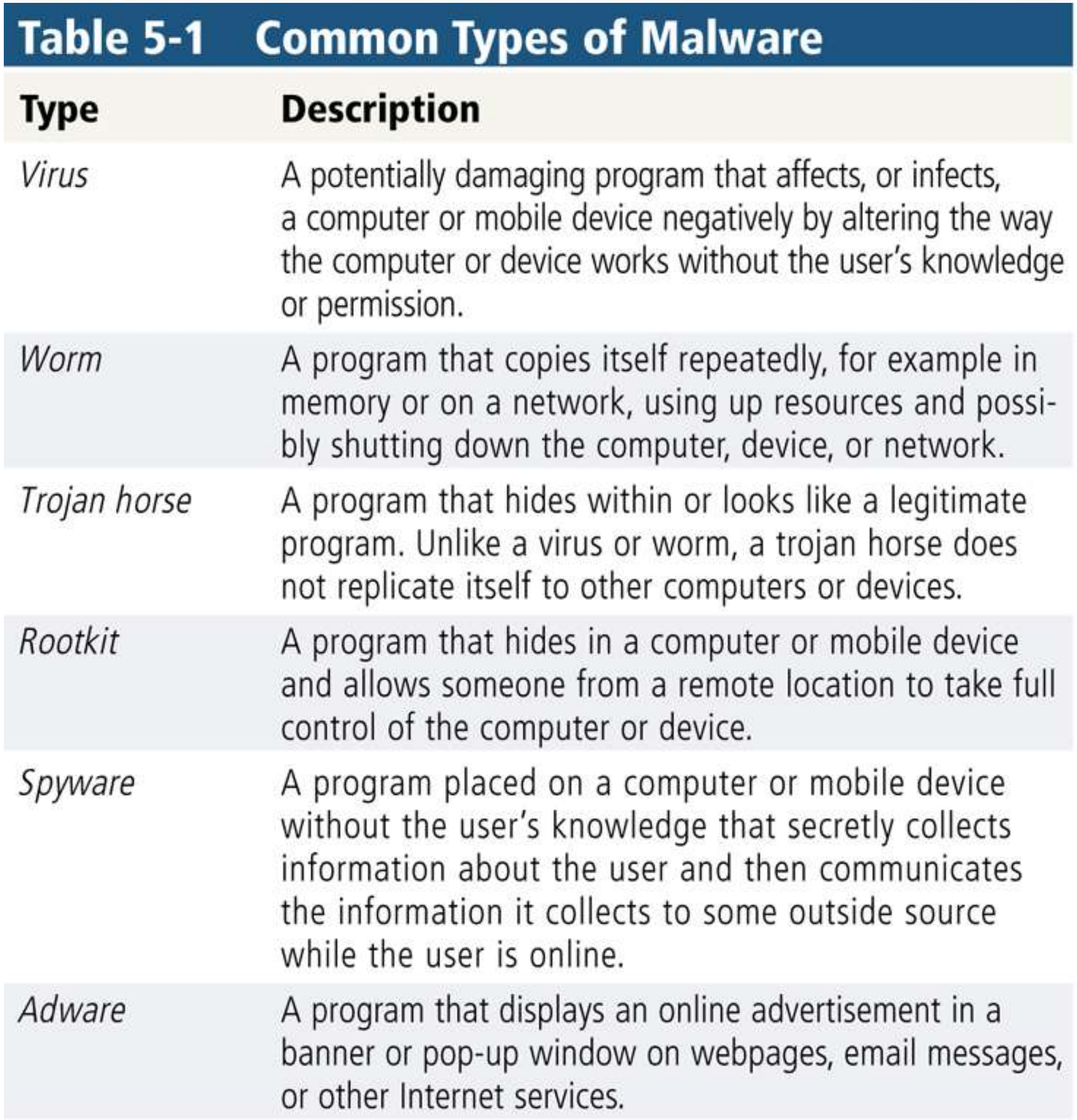


Table 5-1 Common Types of Malware

Type	Description
Virus	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user’s knowledge or permission.
Worm	A program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer, device, or network.
Trojan horse	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
Rootkit	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device.
Spyware	A program placed on a computer or mobile device without the user’s knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
Adware	A program that displays an online advertisement in a banner or pop-up window on webpages, email messages, or other Internet services.

Pages 215
Table 5-1

Internet and Network Attacks

Virus
病毒

- Affects a computer negatively by altering the way the computer works
- 電腦病毒藉由改變電腦的工作方式對電腦產生負面作用具傳染性，受感染的程式或是磁碟會複製更多的分身

Can spread and damage files

Worm
蠕蟲

- Copies itself repeatedly, using up resources and possibly shutting down the computer or network
蠕蟲會自行不斷複製以耗光電腦資源可能會使電腦或網路當機(記憶體或磁碟空間不足而停擺)

Internet and Network Attacks

Trojan Horse
木馬程式

- A malicious program that hides within or looks like a legitimate program
  木馬會隱藏自己或是看起來像是合法程式直到有事件觸發，不會在其它電腦上自行複製

Does not replicate itself on other computers

Rootkit

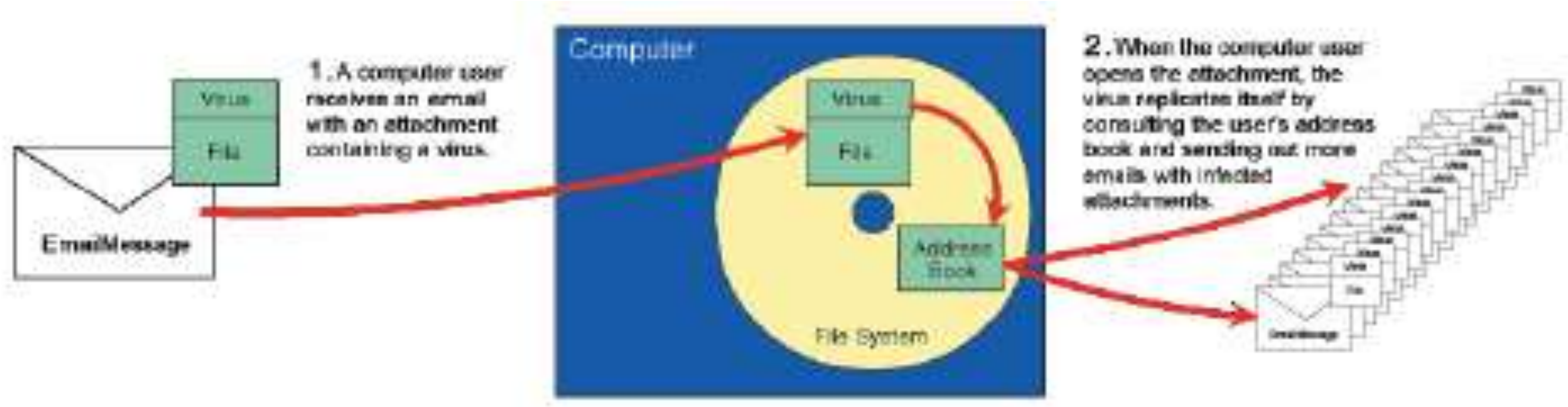
- Program that hides in a computer and allows someone from a **remote** location to take full control
  Rootkit是隱藏在電腦中的一種程式，允許某人從遠方全面監控

破壞性軟體：病毒和其他惡意軟體

- ***Viruses*** 病毒
  - replicate themselves into uninfected programs
    具傳染性，受感染的程式或是磁碟會複製更多的分身
  - 多半隱藏在電腦的作業系統或應用程式中
  - 針對特定的作業系統
  - 例外，**巨集病毒(Macro virus)**，會附在含有巨集的文件上，若文件以跨平台的應用程式建立，巨集就會散佈到不同的作平台上；有時也會藉由電子郵件附件檔案散佈。
    - **1999 Melissa 電子郵件病毒**，以VB所撰寫的巨集病毒，一旦文件被開啓，病毒就啓動，再自動轉寄給outlook通訊錄中50個名字，因大量郵件造成郵件伺服器檔機和網路擁塞。

破壞性軟體：病毒和其他惡意軟體

- Examples: Macro viruses and email viruses
  - 1991 Melissa virus
  - Chernoby 1
  - Love bug---I love you attachments
  - Sobig



1. A computer user receives an email with an attachment containing a virus.

2. When the computer user opens the attachment, the virus replicates itself by consulting the user's address book and sending out more emails with infected attachments.

10.5 How a virus spreads via email.

破壞性軟體：病毒和其他惡意軟體

- 蠕蟲　Worms
  - 遊走於電腦網路的獨立程式，尋找未受感染的工作站
  - 第一個造成轟動的蠕蟲，是1988年由一名康乃爾大學的研究生所撰寫的
  - 2001年夏天，一隻名為**紅色警戒 (Code Red)** 的蠕蟲上了全球頭條新聞
    - Code Red病毒的主要攻擊對象為**Microsoft的IIS Web Server**
  - 2010年 Stuxnet 蠕蟲，是世界上首個專門針對工業控制系統編寫的破壞性病毒，癱瘓或損毀發電廠，管線和其他重要設備
    - Stuxnet 病毒已經感染了全球超過 45000個網路，伊朗、印尼、美國、台灣等多地均不能倖免，其中，以伊朗遭到的攻擊最為嚴重

Code Red紅色警戒

- **Code Red** was a computer worm observed on the Internet on **July 13, 2001**. It attacked computers running **Microsoft's IIS web server.**
- The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permeh.

- They named it "Code Red" because **Code Red Mountain Dew was what they were drinking at the time.**
- Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001. On this day, the number of infected hosts reached 359,000.

補充

Code Red紅色警戒

- Code Red病毒的主要攻擊對象為 **Microsoft的IIS Web Server**，更精確地說，是IIS Web Server的一隻 ISAPI Extension程式。這隻程式（可以把它想像成是一隻CGI程式）是用來作為IIS和Windows的 Indexing Service所使用的。
- 這裡所謂的Indexing Service，即是每台電腦上面都會有的「搜尋功能」，利用這隻ISAPI Extension， IIS可以提供簡單的網頁搜尋功能，但是由於這隻程式係存在**緩衝區溢位**（Buffer Overflow）的漏洞裡，所以可以讓病毒有機會取得機器的控制權。

Chernoby 1

- 台灣大同工學院（現大同大學）學生陳盈豪的名字拼音（**Chen Ing-hau**）縮寫
- 技術名稱 Win32.CIH, Win95.CIH
- 系統病毒
- CIH病毒的1.2和1.3版發作日期為4月26日（第一版本病毒創造出來的時間），正好是前蘇聯（位於今日烏克蘭）核電廠災害「車諾比核事故」的紀念日，故曾被認為病毒作者撰寫動機和車諾比事件有關，因此CIH病毒也被稱作車諾比（Chernobyl）病毒。

破壞性軟體：病毒和其他惡意軟體

- **Trojan horses木馬程式**
  - carry a hidden destructive program
    在執行有用工作的同時，暗中進行秘密破壞行為的程式
- **Logic bomb** can be programmed to respond to an event
  邏輯炸彈是設定成因某特定事件而進行攻擊
- **Time bombs** are triggered by a time-related event
  定時炸彈由時間相關事件而啟動
  - 發病日Michelangelo’s birthday
    1992年 3月6日米開朗基羅病毒製造了一次數位大災難。

Software Sabotage: Viruses and Other Malware (cont.)

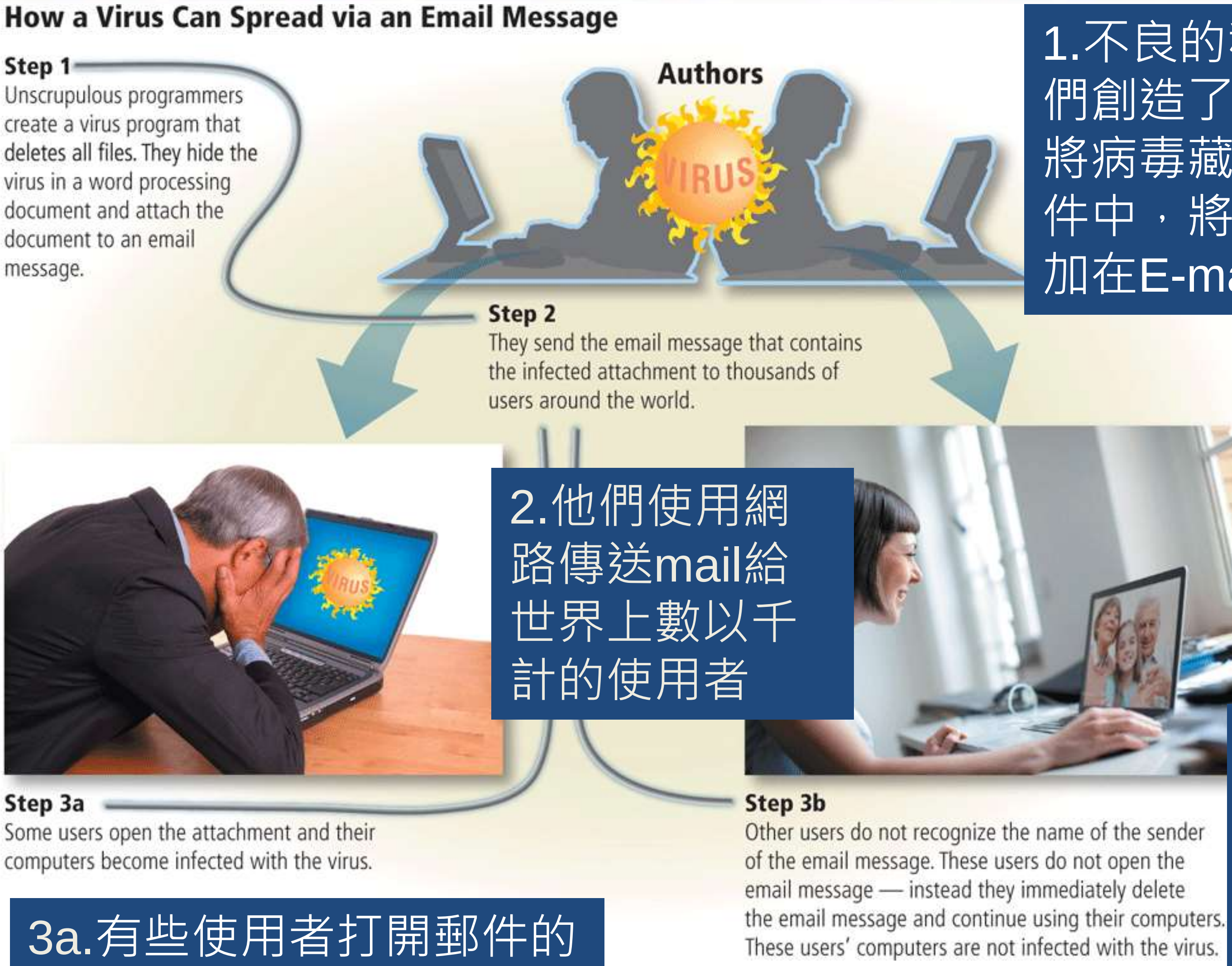
- **Spyware間諜軟體**
  - collects information without users knowledge
  - Also called: *Tracking software* or *Spybot*
  - communicate data to others via the Internet
    - Your keystrokes could be monitored
    - Web sites which you visit are recorded
    - Snapshots of your screen are taken
    - Cause pop-ups to appear
  - In drive-by downloads 路過式下載just visiting a Web site can cause a download
  - 間諜軟體可能對使用者隱私造成威脅，也可能因暗地裡做別的事而讓PC降低效能

Internet and Network Attacks

- The **Payload** is the destructive event or prank the program is intended to deliver.
  在當你開啟文件，執行被感染的程式時發生，或用已感染的磁片開機

P215

Internet and Network Attacks



How a Virus Can Spread via an Email Message

Step 1
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an email message.

Step 2
They send the email message that contains the infected attachment to thousands of users around the world.

Step 3a
Some users open the attachment and their computers become infected with the virus.

Step 3b
Other users do not recognize the name of the sender of the email message. These users do not open the email message — instead they immediately delete the email message and continue using their computers. These users' computers are not infected with the virus.

1.不良的程式設計師們創造了一個病毒。將病毒藏在Word的文件中，將Word文件附加在E-mail

2.他們使用網路傳送mail給世界上數以千計的使用者

3a.有些使用者打開郵件的附件，電腦就會感染病毒

3b其他使用不認識寄信者，便沒打開信件，反而刪除，便不會感染到病毒

Page 205
Figure 5-2

Internet and Network Attacks

- A **botnet** is a group of compromised computers or mobile devices connected to a network
  - A compromised computer or device is known as a **zombie**
    被病毒或其他工具劫持進行惡意行為的Internet連線電腦形成的網路
- A compromised computer, known as a **zombie**, is one whose owner is unaware the computer is being **controlled remotely** by an outsider.
  一台受感染的電腦被稱作**殭屍**，電腦的擁有者不知他的電腦已被別人由遠端控制
- **僵屍電腦**個人電腦在不自知的情形下被植入後門程式而變成僵屍電腦，這些受害的電腦被集合成千上萬的僵屍電腦大軍，它們集結而成的力量，被用來執行許多非法的網路活動

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

Pages 216

什麼是「Botnet傀儡殭屍網路」？ | 資安趨勢

Internet and Network Attacks

- A **denial of service attack** (**DoS attack**) disrupts computer access to Internet services

  阻斷式服務攻擊(DOS攻擊)中斷電腦存取網路服務，如阻斷web或e-mail不斷轟炸伺服器和網站，過多的假造流量造成系統停擺，無法提供服務給合法用戶
- Distributed denial-of-service (DDoS)**分散式阻斷攻擊**
  - The flood of messages comes from botnets.
- 2000年2月，在一個星期內Yahoo! 、eBay、 Amazon都被阻斷服務攻擊癱瘓損失數百萬美元
- 2009年Twitter、 Facebook也因受數個DDos攻擊而停擺數小時

Pages 217

阻斷服務攻擊

- Dos是**一對一**的網路攻擊方式，攻擊者藉由不當方式佔用系統分享資源(CPU、網路、硬碟...)，達到干擾正常系統運作的進行。
- 不同於一般網路入侵，DoS 不一定需要取得系統使用的權力，即可達到目的。
- 最常見的DoS方式即是透過所謂的**訊息洪泛(Message Flood)**，向攻擊對象送出大量且無意義的網路訊息，不管被攻擊對象是否回應，都會因頻寬的被佔用，而導致不正常運作。

阻斷服務攻擊

- **DDoS**算是DoS的一種，只是攻擊的模式並非一對一，而是以**多對一**的方式，同時對一個攻擊目標發動攻擊，而這些發動攻擊的點，通常是已遭受入侵而不自知的電腦系統。
- 由於這種攻擊方式多數係以遙控方式，利用替死鬼行兇，因此不僅難以防範，追查更是不易。

http://www.synnex.com.tw/asp/newsdetail.asp?seqno=17678&page=&csfilter=

Internet and Network Attacks

- A **back door** is a program or set of instructions in a program that allow users to bypass security controls 「**後門程式**」一種程式或是程式中一些指令集讓使用者能通過安全管理而直接存取電腦資源
- 後門程式通常係指「**不明的遠端人士**未經系統管理員之允許，且利用不正當的手法」進入電腦系統中，並且可能偷 走個人資料、機密資訊等，甚至可以隨心所欲地操控您的電腦，通常不明的遠端人士會透過電子郵件、IRC 或其他方式將後門程式植入使用者電腦中。
  - 目前Windows上常見的後門程式有Netbus、Netspy、Netbuster、BirdSpy等等。
- 後門程式通常無法自行散播。

Pages 217

Internet **R**elay **Ch**at ：Computer conferencing on the Internet.

Internet and Network Attacks

- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate
  網路欺騙(假冒)是一種技術，入侵者讓使用者的網路或網際網路傳輸的技術顯示合法
- Two common types of spoofing schemes
  - IP spoofing
  - E-mail spoofing

spoofing中文意指欺騙，是一種技術用以取得非經授權的存取電腦，其手法主要以**偽裝發送訊息、郵件的位址或偽裝成為已被授權的使用者**，在未經許可下進入安全的電腦系統，以進行任何不法的行為。
Spoofing多為垃圾郵件發送者、駭客或網路詐騙者所使用，藉以達到犯罪行為而不被發現。

全民資訊網

Pages 217

Internet and Network Attacks

- IP spoofing
  - 入侵者的電腦會讓網路相信它是來自可信的網路位址
  - IP 位址偽裝 **(IP 詐騙)**

是駭客用來隱藏身份與位置，藉以進行後續攻擊的技術。

由於路由器或防火牆所採用的封包過濾（Packet Filtering）規則是依據該封包的來源位址而定，經由 IP Spoofing 來改變封包的來源位址，佯裝入侵者是來自於被信任的網路，因此可以達到入侵的目的。

新一代的路由器或防火牆已可提供IP Spoofing 的保護機制。

IP 詐騙也是一種攻擊方法，該方法使用偽造的來源位址來傳送 IP 封包，此類封包可能會採用受信任來源的 IP 位址來嘗試規避防火牆。

這將使防火牆誤以為來自駭客的封包確實是來自受信任來源的。

IP 詐騙也可以僅用於隱藏攻擊的真實來源。

IP 詐騙是入侵者使用其他電腦的 IP 位址來取得資訊或存取權限的程序。

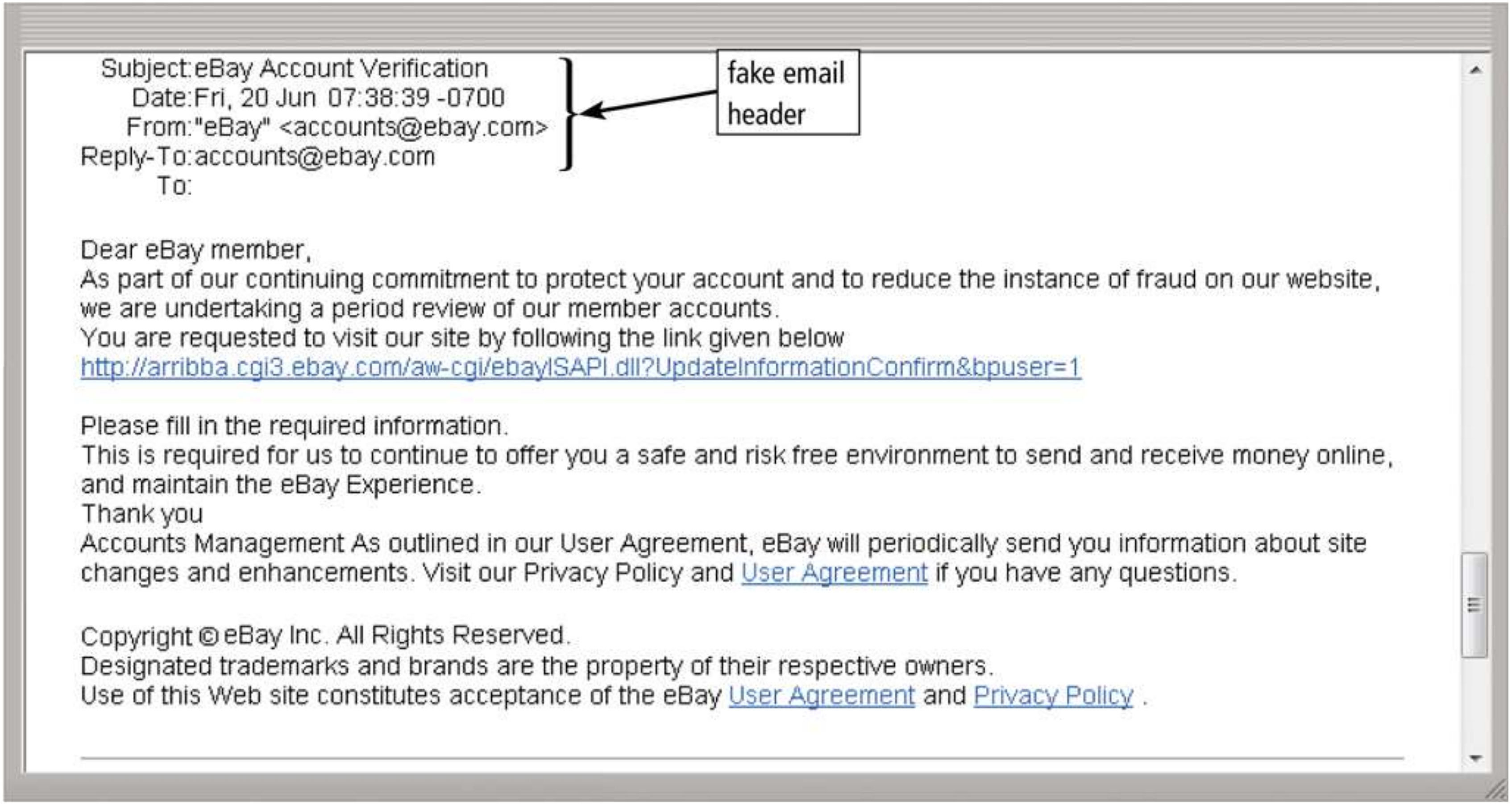
由於入侵者偽裝成他人出現，因此如果傳送回覆，該回覆將發往入侵者所偽造的位址，而非其入侵者的位址。

http://www.synnex.com.tw/asp/newsdetail.asp?seqno=17678&page=&csfilter=

Internet and Network Attacks

– E-mail spoofing

通當用在惡作劇的病毒,垃圾信,



Subject:eBay Account Verification
Date:Fri, 20 Jun 07:38:39 -0700
From:"eBay" <accounts@ebay.com>
Reply-To:accounts@ebay.com
To:

Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy .

Pages 217-218

Safeguards against internet and Network Attacks

- A **firewall** is hardware and/or software that protects a network’s resources from intrusion
  防火牆是保護網路資源避免侵害的硬體/軟體

guard against unauthorized access to an internal network
防止未經授權存取內部網路

program that filters information between a private network and the rest of the Internet
負責篩選私有網路與Internet之間流通資訊的過濾程式

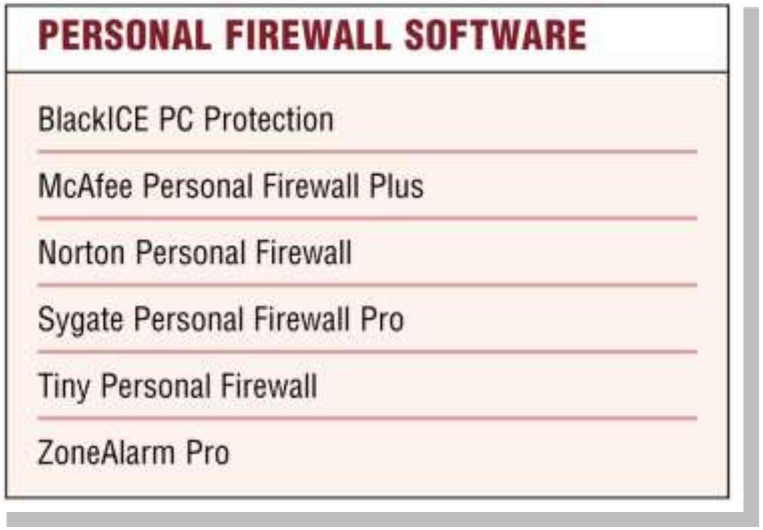
Pages 219

Proxy server

- A **proxy server** is a server outside the company's network that controls which communications pass into the company's network.
- Proxy server screens all incoming and outgoing messages.
- Proxy servers use a variety of screening techniques.
  - Some check the **domain name** or **IP address** of the message for legitimacy.
  - Others require that the messages have **digital signatures**.

Internet and Network Attacks

- Personal firewall utility
  - Program that protects personal computer and its data from unauthorized intrusions
  - Monitors transmissions to and from computer
  - Informs you of attempted intrusion



PERSONAL FIREWALL SOFTWARE
BlackICE PC Protection
McAfee Personal Firewall Plus
Norton Personal Firewall
Sygate Personal Firewall Pro
Tiny Personal Firewall
ZoneAlarm Pro

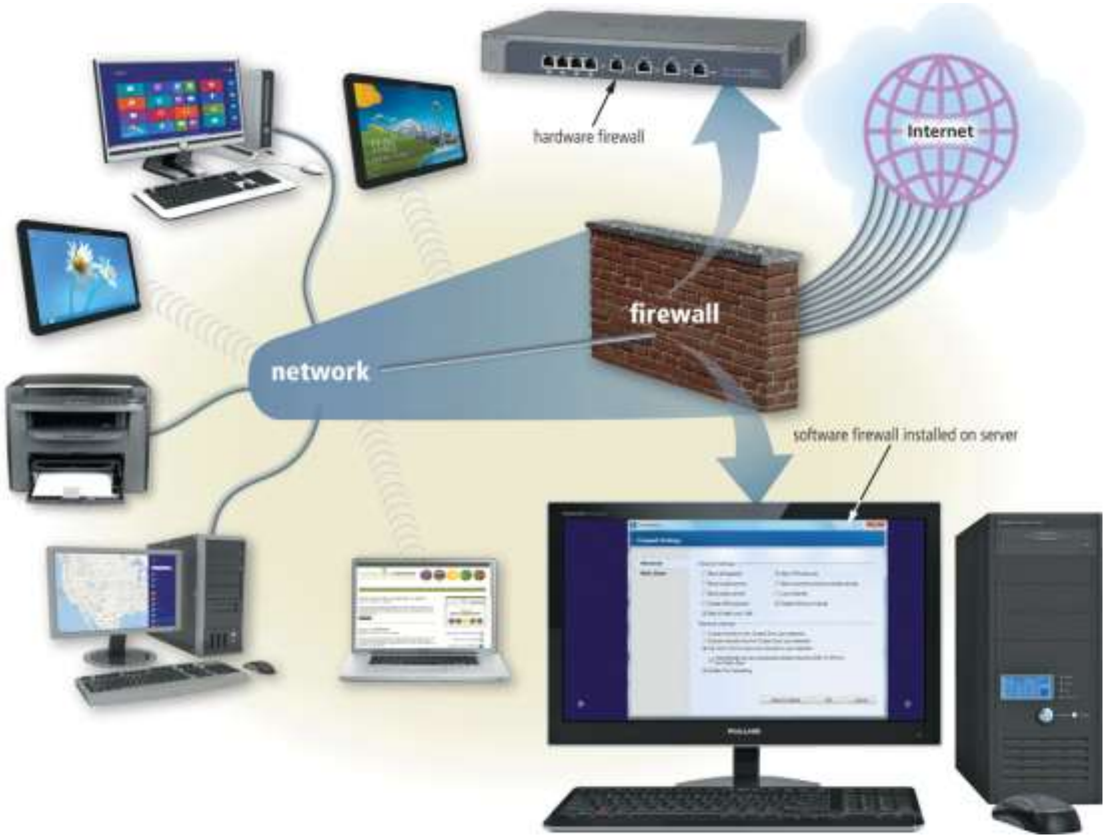
P220

AVG, McAfee, and Symantec

Safeguards against internet and Network Attacks

- Some small/home office users purchase a hardware firewall, such as a router or other device that has a built-in firewall, in addition to or instead of a personal firewall.

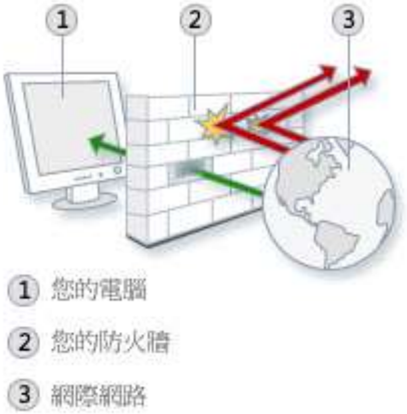
  - Hardware firewalls stop intrusions before they attempt to affect your computer or network maliciously.



Pages 220
Figure 5-4

什麼是防火牆

- 防火牆是可以檢查來自網際網路或網路上資訊的軟體或硬體，檢查後可根據防火牆的設定，決定是否封鎖或允許資訊下載到電腦上。
- 防火牆可協助防止駭客或惡意軟體 (例如：蠕蟲) 透過網路或網際網路來存取您的電腦。 防火牆也可協助阻止您的電腦傳送惡意軟體至其他電腦。
- 就像磚牆可建立物理屏障，
  防火牆能建立網際網路和電腦之間的屏障。



- 防火牆和防毒程式所代表的涵義並不相同。
  若要協助保護您的電腦，
  您需要同時使用防火牆和防毒軟體及防惡意程式。

補充