

Technology in Action

Chapter 9
Securing Your System:
Protecting Your Digital Data and Devices

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 1

Chapter Topics

- Cybercrime
- Computer threats: Computer viruses
- Computer safeguard: Antivirus software and software updates
- Computer threats: Hackers
- Restricting access to your digital assets
- Managing online annoyances
- Protecting yourself ... from yourself!
- Protecting your physical computing assets

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 2

_____ is any criminal action perpetrated primarily through the use of a computer.

1. Identity theft
2. Computer crime
3. Cybercrime
4. Hacking

0% 0% 0% 0%

1 2 3 4

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

What type of Malware appears to be something useful, but actually carries out malicious acts?

1. Trojan Horse
2. Stealth Virus
3. Polymorphic Virus
4. Boot Sector Virus

0% 0% 0% 0%

1 2 3 4

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

A _____ is a section of the virus code that is unique to a particular computer virus.

1. Virus stamp
2. Virus sign
3. Virus signature
4. Virus snip

0% 0% 0% 0%

1 2 3 4

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Cybercrime

- Cybercrime is any criminal action perpetrated primarily through the use of a computer
 - Programs damaging computers
 - Stealing identities online
 - Attacking corporate Web sites
- Cybercriminals are individuals who use computers, networks, and the Internet to perpetrate crime.

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

6

Types of Cybercrime

- Top categories of complaints
 - Non-delivery of payments/merchandise
 - Identity theft
 - Auction fraud
 - Credit card fraud
- Complaints not related to fraud
 - Computer intrusions
 - Extortion and blackmail
 - Child pornography

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

7

Types of Cybercrime (cont.)

- Computer virus is a program that attaches itself to another computer program
- Attempts to spread to other computers when files are exchanged
- One of the most widespread types of cybercrimes

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

8

I have accessed my bank account or other sites containing my personal information on an unsecured wireless connection.

1. Yes
2. No



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

1

2

Computer Threats: Computer Viruses

- Computer viruses are engineered to evade detection
- Viruses hide within code of host program
- Not just limited to computers
- Can also infect smartphones, notebooks, or tablet computers
- Even cars can catch a virus

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

10

What Viruses Do

- Main purpose
 - Replicate themselves and copy code to as many other files as possible
- Secondary objectives
 - Slow down networks
 - Display annoying messages
 - Destroy files or contents of hard drive

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

11

Catching a Virus

- If exposed to an infected file, the virus will try to copy itself and infect a file on your computer
- Sources of virus infection
 - Downloading infected audio and video files
 - Shared flash drives
 - Downloading or executing a file attached to e-mail

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

12

Types of Viruses

- Viruses can be grouped into five categories based on behavior and method of transmission
- Boot-sector viruses
 - Replicates itself into hard drive's master boot record
- Logic bombs and time bombs
 - Logic bomb is triggered when certain logical conditions are met
 - Time bomb is triggered by the passage of time or on a certain date

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

13

Types of Viruses (cont.)

- Worms
 - Use transport methods like e-mail and networks to spread without human interaction
- Script and macro viruses
 - Script is miniprogram hidden on Web sites that is executed without user's knowledge
 - Macro virus attaches itself to a document that uses macros

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

14

Types of Viruses (cont.)

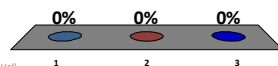
- Encryption viruses
 - Run program that searches for common types of data files
 - Compress files using a complex encryption key that makes files unusable
 - Asks for payment to receive the program to decrypt your files

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

15

Viruses can spread without human interaction.

1. True
2. False
3. I don't know



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Virus Classifications

- Viruses can also be classified by methods they take to avoid detection
 - Polymorphic viruses
 - Periodically rewrite themselves to avoid detection
 - Multipartite viruses
 - Infect multiple file types
 - Stealth viruses
 - Erase their code from the hard drive and reside in the active memory

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

17

Computer Safeguard: Antivirus Software and Software Updates

- Antivirus software is designed to detect viruses and protect your computer
- Popular antivirus software companies
 - Symantec
 - Kaspersky
 - AVG
 - McAfee
- Comprehensive Internet security packages protect you from other threats

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

18

Antivirus Software

- Designed to detect suspicious activity
 - Scan files for virus signatures (unique code)
 - Identifies infected files and type of virus
 - Provides choice of deleting or repairing infected file
 - Places virus in secure area (quarantining)
 - Records key attributes about file and rechecks these statistics during scan (inoculating)

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

19

Software Updates

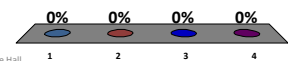
- Make sure antivirus software and your operating system are up to date and contain latest security patches
 - Windows operating system has automatic update utility called *Windows Update*
 - Mac OS X has similar utility

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

20

Which type of hacker breaks into systems for illegal gain or to destroy information?

1. White Hat
2. Black Hat
3. Grey Hat
4. Script Kiddies



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Computer Threats: Hackers

- Anyone who unlawfully breaks into a computer system
- Types of hackers
 - White-hat or ethical hackers
 - Black-hat hackers
 - Grey-hat hackers

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

22

Problems Hackers Cause

- Steal credit and debit cards information from hard drives
- Break into sites that contain credit card information
- Capture login ID and password using packet analyzer or keylogger
- Use information to purchase items illegally
- Sell credit card numbers and information

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

23

Trojan Horses and Rootkits

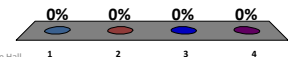
- Trojan horse appears to be useful but while it runs it does something malicious in background
- Rootkits are programs (or sets of programs) that allow hackers to gain access to your computer and take control without your knowledge
- Zombie is computer controlled by hacker

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

24

Hackers use zombies to perform what type of attack?

1. Stealth
2. Trojan
3. Distributed denial-of-service
4. Zombie Invasion



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Denial-of-Service Attacks

- In a denial-of-service (DoS) attack, users are denied access to computer system because hacker is making repeated requests
- When flooded with requests, the system shuts down
- Distributed denial-of-service (DDoS) attack launches attacks from more than one zombie computer

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

26

How Hackers Gain Access

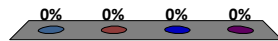
- Direct access
 - Installing hacking software
- Indirect access
 - Through Internet connection
 - Logical ports

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

27

Computers that are controlled by hackers are referred to as:

1. Machines
2. Zombies
3. Robots
4. Droids



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

1 2 3 4

Restricting Access to Your Digital Assets

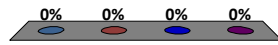
- Keep hackers out
 - Prevent them from accessing computer
 - Protect your digital information
 - Use passwords
 - Hide activities from prying eyes

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

29

A firewall is:

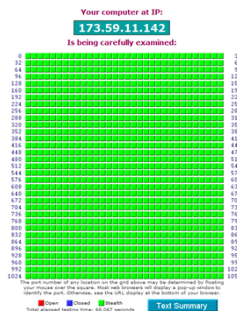
1. A software program
2. A hardware device
3. Both 1 & 2
4. Neither 1 nor 2



Firewalls

- Software program or hardware designed to protect computers from hackers
 - Consider installing both for maximum protection
- Software firewalls
 - Most operating systems include firewall
 - Many security suites include firewall software
- Hardware firewall devices
 - Routers
 - Keep unused logical ports closed

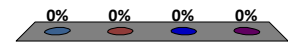
Knowing Your Computer is Secure



- Web sites test computer
 - Gibson Research
 - ShieldsUp
 - LeakTest
- Closed ports are safe
- Open ports are subject to exploitation

Which of the following is *NOT* a strong password?

1. gR3@t!6k3S
2. Skipper2009
3. sK!ppe200R9
4. techn0I9G&y



Password Protection and Password Management

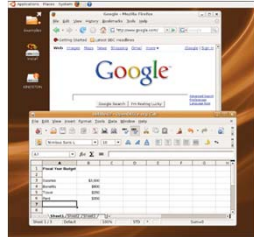
- Strong passwords are difficult to guess
 - At least 14 characters, including numbers, symbols, and upper- and lowercase letters
 - Not a single word or a word from a dictionary
 - Not easily associated with you (birth date, name of pet, nickname)
 - Use different passwords for different Web sites
 - Never tell anyone or write down password
 - Change password regularly (every month)

Managing Your Passwords

- Well-constructed passwords can be hard to remember
- Password-management software remembers passwords for you
- Most security suites and Web browsers provide password-management tools

Anonymous Web Surfing: Hiding from Prying Eyes

- Shared computers
 - Libraries
 - Coffee shops
 - Colleges
- Privacy tools
 - Google Chrome
 - Firefox
 - Internet Explorer



Google Chrome's Incognito feature

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

36

Biometric Authentication Devices

- Read unique personal characteristics
 - Fingerprint
 - Iris pattern in eye
 - Voice authentication
 - Face pattern-recognition
- Provide high level of security
 - Eliminate human error

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

37

Managing Online Annoyances

- Using the Web has become a common part of most of our lives
- Web has become fertile ground for:
 - Advertising products
 - Tracking our Web browsing behaviors
 - Conning people into revealing personal information

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

38

Malware, Adware, and Spyware

- Malware
 - Software that has malicious intent
- Adware
 - Displays sponsored advertisements
 - Pop-up windows
- Spyware
 - Unwanted piggyback programs that download with other software you install from Internet that transmit information about you

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

39

Spam

- Unwanted or junk e-mail
- Avoid spam in primary e-mail account
 - Create free Web-based e-mail account
 - Use spam filter
 - Read privacy policy
 - Don't reply to spam to remove yourself from list
 - Subscribe to e-mail forwarding service

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

40

Cookies

- Small text files that Web sites automatically store on hard drive to make return visit more efficient and better geared to your interests
- Web site assigns ID number to computer
- Provide Web sites with information about browsing habits
- Some sites sell information cookies collect
- Not a security threat

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

41

Protecting Yourself ... from Yourself!

- Keep your data safe from damage
 - Accidental
 - Intentional
- Keep unscrupulous individuals from tricking you into revealing sensitive information

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

42

Protecting Your Personal Information

- Never share:
 - Social Security number
 - Phone number
 - Date of birth
 - Street address
- Social networks ask for potentially sensitive information
 - Use privacy settings

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

43

Backing Up Your Data

- Data faces three major threats:
 - Unauthorized access
 - Tampering
 - Destruction
- Backups are copies of files that can replace originals
- Store backups away from computer in at least two different places

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

44

Backing Up Your Data (cont.)

- Types of files to back up
 - Program files without media
 - Data files you create
- Types of backups
 - Incremental backup (partial backup)
 - Image backup (system backup)
- Backup data files frequently

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

45

Backing Up Your Data (cont.)

- Location of backup files
 - Online sites
 - Local drives
 - Network-attached storage devices and home servers
- Performing file backups
 - Windows Backup and Restore utility
 - Mac OS X Time Machine feature

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

46

Social Engineering: Fooling the Unwary

- Any technique that entices individuals to reveal sensitive information
- Pretexting creates a scenario that sounds legitimate
 - Bank calling to confirm personal details
 - Information can then be used to commit fraud
- Most common form of pretexting is phishing

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

47


Phishing and Pharming

- Phishing lures users to reveal personal information that could lead to identity theft
 - E-mail messages look legitimate
- Pharming is when malicious code is planted on your computer
 - Alters browser's ability to find Web addresses
 - Directed to bogus Web sites that gather personal information

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 48

Scareware

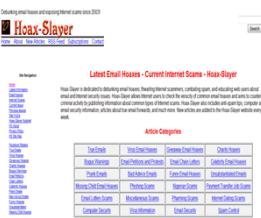
- Type of malware downloaded onto computer that tries to convince you that computer is infected with virus
- Then directed to site to buy fake removal tools



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 49

Hoaxes


- Attempt to make someone believe something that is untrue
 - Target large audiences
 - Practical joke, agents of social change, or time wasters
 - Mostly by e-mail



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 50

I know how to check emails to determine if the message is a hoax.

1. Yes
2. No



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

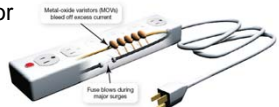
Protecting Your Physical Computing Assets

- Protect your computer from
 - Environmental factors
 - Power surges
 - Power outages
 - Theft

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 52

Environmental Factors

- Computers can be damaged by
 - Sudden movements such as a fall
 - Excessive heat or excessive cold
- Power surges occur when current is in excess of normal voltage
 - Use a surge protector
- Power outages
 - Use a UPS



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall 53

Deterring Theft

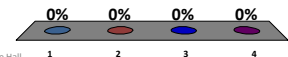
- Portable devices are easy targets for thieves
- Four main security concerns:
 1. Keeping them from being stolen
 2. Keeping data secure in case of theft
 3. Finding the device if it is stolen
 4. Remotely recovering and wiping data of a stolen device

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

54

HTTP, the main protocol used for world wide web communication, uses which logical port?

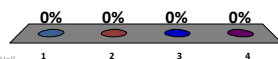
1. 25
2. 443
3. 23
4. 80



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Which type of virus attaches to a Word or Excel file?

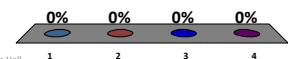
1. Boot sector
2. Script virus
3. Worm
4. Macro



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Which type of virus loads into RAM to avoid detection?

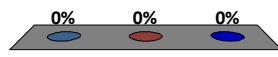
1. Polymorphic
2. Stealth
3. Boot sector
4. RAM Load



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

What are Evil Twins?

1. Programs that appear to be legitimate, but are actually malware
2. Look alike free hotspots
3. Word or Excel files that are embedded with malware



Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

Chapter 9 Summary Questions

1. What is cybercrime and who perpetrates it?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

59

Chapter 9 Summary Questions

2. From which types of viruses do I need to protect my computer?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

60

Chapter 9 Summary Questions

3. What can I do to protect my computer from viruses?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

61

Chapter 9 Summary Questions

4. How can hackers attack my computing devices, and what harm can they cause?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

62

Chapter 9 Summary Questions

5. What is a firewall, and how does it keep my computer safe from hackers?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

63

Chapter 9 Summary Questions

6. How do I create secure passwords and manage all of my passwords?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

64

Chapter 9 Summary Questions

7. How can I surf the Internet anonymously and use biometric authentication devices to protect my data?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

65

Chapter 9 Summary Questions

8. How do I manage online annoyances such as spyware and spam?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

66

Chapter 9 Summary Questions

9. What data do I need to back up, and what are the best methods for doing so?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

67

Chapter 9 Summary Questions

10. What is social engineering, and how do I avoid falling prey to phishing and hoaxes?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

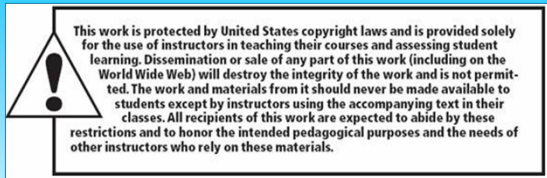
68

Chapter 9 Summary Questions

11. How do I protect my physical computing assets from environmental hazards, power surges, and theft?

Copyright © 2013 Pearson Education, Inc. Publishing as Prentice Hall

69



All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.

Copyright © 2013 Pearson Education, Inc.
Publishing as Prentice Hall