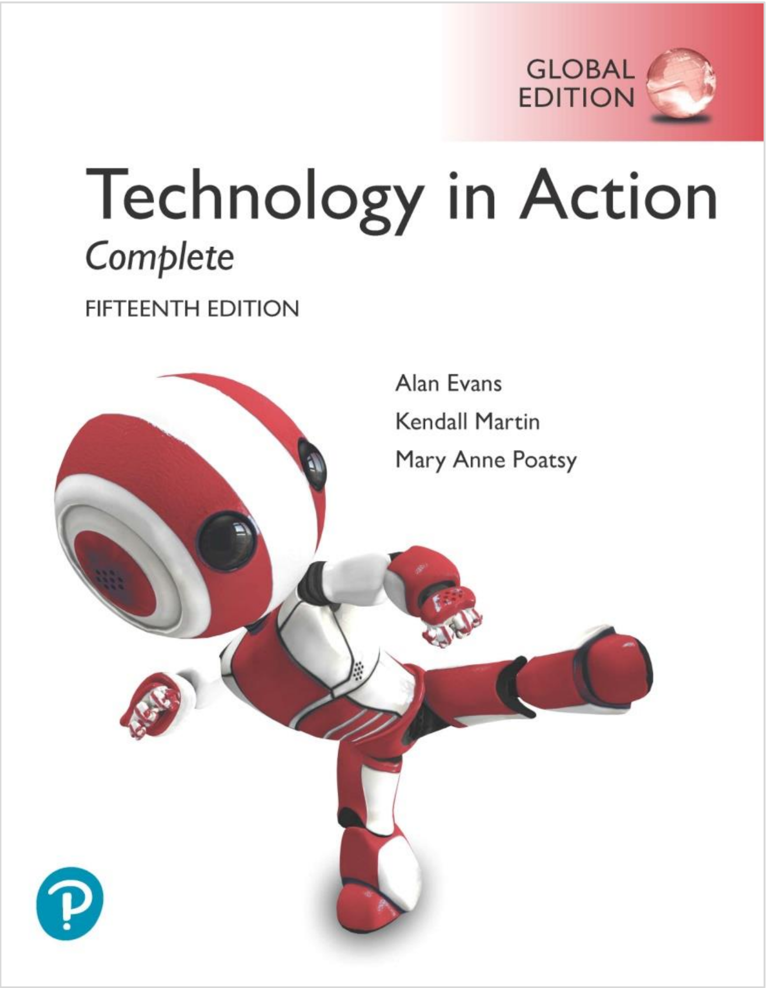
Technology in Action

15th Edition, Global Edition



Chapter 9

Securing Your System: Protecting Your Digital Data and Devices

Learning Objectives (1 of 3)

9.1 Describe how identity theft is committed and the types of scams identity thieves perpetrate.

9.2 Describe the different types of hackers and the tools they use.

9.3 Explain what a computer virus is, why it is a threat to your security, how a computing device catches a virus, and the symptoms it may display.

9.4 List the different categories of computer viruses, and describe their behaviors.

9.5 Explain what malware, spam, and cookies are and how they impact your security.

Learning Objectives (2 of 3)

9.6 Describe social engineering techniques, and explain strategies to avoid falling prey to them.

9.7 Explain what a firewall is and how a firewall protects your computer from hackers.

9.8 Explain how to protect your computer from virus infection.

9.9 Describe how passwords and biometric characteristics can be used for user authentication.

9.10 Describe ways to surf the web anonymously.

Learning Objectives (3 of 3)

9.11 Describe the types of information you should never share online.

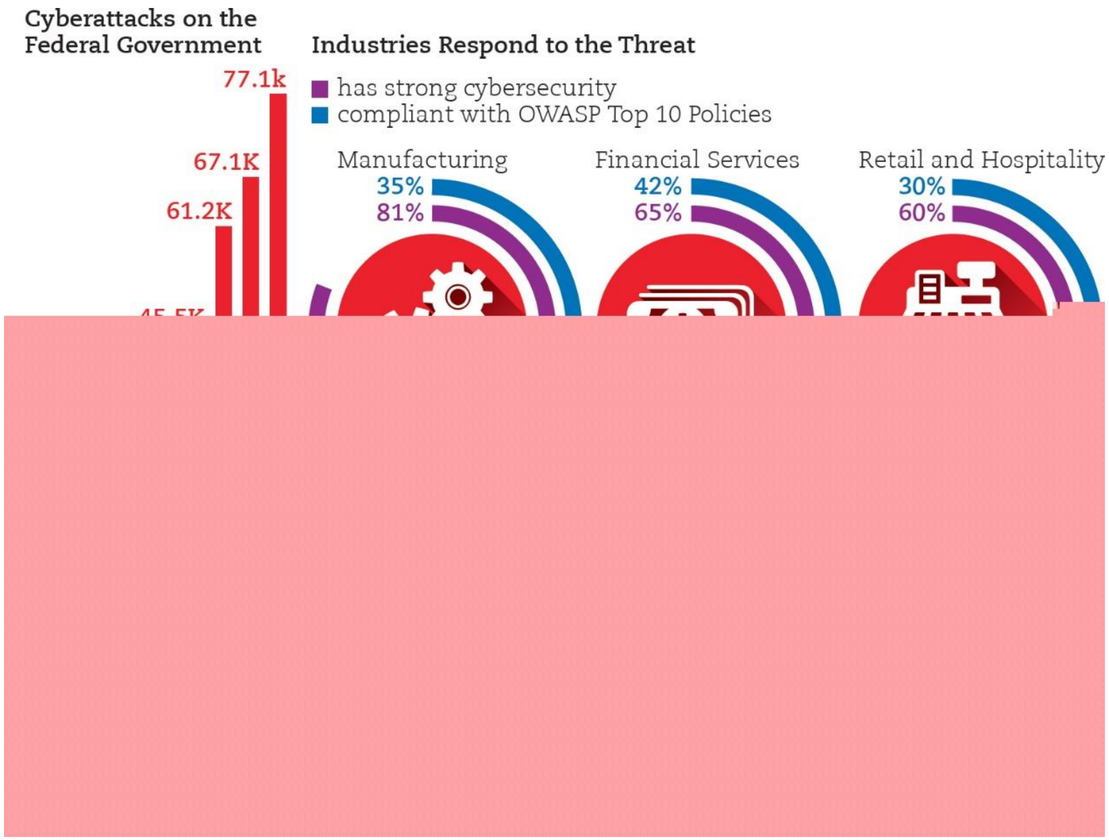
9.12 List the various types of backups you can perform on your computing devices, and explain the various places you can store backup files.

9.13 Explain the negative effects environment and power surges can have on computing devices.

9.14 Describe the major concerns when a device is stolen and strategies for solving the problems.

Identity Theft and Hackers

- Cybercrime
- Cybercriminals
- Common types of cybercrimes



Identity Theft

- Identity theft involves the stealing of someone’s personal information for financial gain.
  - Other complaints received involve equally serious matters such as computer intrusions (hacking), extortion, and blackmail.

Identity Theft and Hackers
Identity Theft
(Objective 9.1)

- Occurs when a thief steals personal information and poses as you
  - Most financially damaging cybercrime for individuals
- Types of scams
  - Counterfeiting credit and debit cards
  - Requesting changes of address
  - Opening new credit cards
  - Obtaining medical services
  - Buying a home

Identity Theft

- Many people believe that the only way your identity can be stolen is by using a computer, but you need to protect your information away from the computer as well. Remember to:

  - Keep purses and wallets safe to protect credit cards.
  - Protect bank statements and credit card bills, shredding
  - Never reveal sensitive information over the phone
  - Be vigilant at ATM machines so that account numbers and passcodes are secure

Pearson

Identity Theft and Hackers
Hacking (1 of 4)
(Objective 9.2)

- Defined as anyone who unlawfully breaks into a computer system
- Types of hackers
  - White-hat (ethical hackers)
  - Black-hat hackers
  - Grey-hat hackers
- Packet analyzer (sniffer)
- Keylogger

Pearson

packet analyzer (sniffer)

- Data travels through the Internet in small pieces called packets. The packets are identified with an Internet protocol (IP) address, in part to help identify the computer to which they are being sent. Once the packets reach their destination, they're reassembled into cohesive messages.
- A packet analyzer (sniffer) is a program deployed by hackers that examines each packet and can read its contents. A packet analyzer can grab all packets coming across a particular network—not just those addressed to a particular computer.
- Wireless networks can be set to use encryption to protect against this

Identity Theft and Hackers

Hacking (2 of 4)

- A Trojan horse is a program that appears to be something useful or desirable, like a game or a screen saver, but while it runs it does something malicious in the background without your knowledge

Identity Theft and Hackers

Hacking (2 of 4)

(Objective 9.2)

- Trojan horses appear to be useful but run malicious code
- Backdoor programs and rootkits allow hackers to gain access to your computer
- Zombies are computers that a hacker controls

Identity Theft and Hackers
Hacking (2 of 4)

- the malicious activity perpetrated by a Trojan horse program is the installation of a backdoor program or a rootkit. Backdoor programs and rootkits are programs that allow hackers to gain access to your computer and take almost complete control of it without your knowledge. Using a backdoor program, hackers can access and delete all the files on your computer, send e-mail, run programs, and do just about anything else you can do with your computer.
- A rootkit is a program that gives an outsider remote control over a computer. A computer that a hacker controls in this manner is referred to as a zombie.
- Zombies are often used to launch denial-of-service attacks on other computers.

Identity Theft and Hackers

Hacking (3 of 4)

(Objective 9.2)

- Denial-of-Service
  - Legitimate users are denied access to a computer system
  - System shuts down
- DDoS
- Botnet (large group of software running on zombie computers)

Identity Theft and Hackers
Hacking (3 of 4)

- In a denial-of-service (DoS) attack, legitimate users are denied access to a computer system because hackers are repeatedly making requests of that computer system through a computer they have taken over as a zombie. A computer system can handle only a certain number of requests for information at one time. When it’s flooded with requests in a DoS attack, it shuts down and refuses to answer any requests, even if the requests are from a legitimate user

Identity Theft and Hackers

Hacking (3 of 4)

- Often, the attacks are coordinated automatically by botnets. A botnet is a large group of devices that have been infected by software programs (called robots or bots) that runs autonomously. Some botnets have been known to span millions of computers

Identity Theft and Hackers

Hacking (4 of 4)

- Hackers can gain access to computers directly or indirectly. Direct access involves sitting down at a computer and installing hacking software. It’s unlikely that such an attack would occur in your home, but it’s always a wise precaution to set up your computer so that it requires a password for a user to gain access.

Pearson

Identity Theft and Hackers
Hacking (4 of 4)

- Indirect access involves subtler methods. Many professional hackers use exploit kits. Exploit kits are software programs that run on servers and search for vulnerabilities of computers that visit the server. Exploit kits look for security holes in browsers and operating systems that haven’t yet been patched by the users. When they detect a vulnerability
- Hackers also can access a computer indirectly through its Internet connection. Many people forget that their Internet connection is a two-way street. Not only can you access the Internet, but also people on the Internet can access your computer

Pearson

Identity Theft and Hackers

Hacking (4 of 4)

(Objective 9.2)

- Exploit kits–software that runs on servers searching for vulnerabilities
- Logical ports are virtual, not physical, communications paths

Pearson

Identity Theft and Hackers
Hacking (4 of 4)

- Logical ports are virtual—that is, not physical—communications paths. Unlike physical ports, you can’t see or touch a logical port; it’s part of a computer’s internal organization. Logical ports allow a computer to organize requests for information. So all information arriving from another computer or network that’s related to e-mail will be sent to the logical port associated with e-mail.
- Logical ports are numbered and assigned to specific services. For instance, logical port 80 is designated for hypertext transfer protocol (HTTP), the main communications protocol for the Web. Thus, all requests for information from your browser to the Web flow through logical port 80

Computer Viruses

Virus Basics

(Objective 9.3)

- Program that attaches to a computer program to spread to other computers
- Main purpose–replicate itself and copy its code into as many other host files as possible. a virus normally can’t infect your computer until the infected file is opened or executed
- Secondary objectives can be destructive
- Smartphones, tablets, and other devices can be infected with viruses

Computer Viruses
Virus Basics

Sometimes it can be difficult to definitively tell whether your computer is infected with a virus. Some signs include:

- Existing program icons or files suddenly disappear. Viruses often delete specific file types or programs.
- You start your browser and it takes you to a home page you didn’t set or it has new toolbars.
- Odd messages, pop-ups, or images are displayed on the screen or strange music or sounds play.
- Data files become corrupt. (However, note that files can become corrupt for reasons other than a virus infection.)
- Programs stop working properly, which could be caused by either a corrupted file or a virus. Your system shuts down unexpectedly, slows down, or takes a long time to boot up

Computer Viruses

Types of Viruses (1 of 2)

(Objective 9.4)

- Boot sector viruses
- Logic Bombs and Time Bombs
- Worms
- Script and macro viruses
- Email viruses
- Encryption viruses

Pearson

Computer Viruses
Types of Viruses (1 of 2)

- A boot-sector virus replicates itself onto a hard drive’s master boot record. The master boot record is a program that executes whenever a computer boots up, ensuring that the virus will be loaded into memory immediately, even before virus protection programs can load.
- A logic bomb is a virus that is triggered when certain logical conditions are met, such as opening a file or starting a program a certain number of times. A time bomb is a virus that is triggered by the passage of time or on a certain date.
- Viruses require human interaction to spread, whereas worms take advantage of file transport methods, such as e-mail or network connections, to spread on their own. A virus infects a host file and waits until that file is executed. A worm works independently of host file execution and is much more active in spreading itself

Computer Viruses
Types of Viruses (1 of 2)

- Some viruses are hidden on websites in the form of scripts. A script is a series of commands, a miniprogram—that is executed without your knowledge. Scripts are often used to perform useful, legitimate functions on websites, such as collecting name and address information from customers. However, some scripts are malicious. A macro virus is a virus that attaches itself to a document that uses macros. A macro is a short series of commands that usually automates repetitive tasks. The Melissa virus became the first major macro virus to cause problems worldwide
- E-mail viruses use the address book in the victim’s e-mail system to distribute the virus.

Computer Viruses
Types of Viruses (1 of 2)

- When encryption viruses (also called ransomware) infect your computer, they run a program that searches for common types of data files, such as Microsoft Word files, and compresses them using a complex encryption key that renders your files unusable. You then receive a message that asks you to send payment to an account if you want to receive the program to decrypt your files

Computer Viruses
Types of Viruses (2 of 2)
(Objective 9.4)

- Classified by methods used to avoid detection
  - Polymorphic viruses changes their code or periodically rewrites themselves to avoid detection
  - Multipartite viruses are designed to infect multiple file types
  - Stealth viruses temporarily erase their code from the files where they reside and hide in active memory

Pearson

Online Annoyances and Social Engineering
Online Annoyances (1 of 3)

Malware is software that has a malicious intent (hence the prefix mal). There are three primary forms of malware: adware, spyware, and viruses. Adware and spyware are not physically destructive like viruses and worms, which can destroy data. Known collectively as grayware, most malware consists of intrusive, annoying, or objectionable online programs that are downloaded to your computer when you install or use other online content such as a free program, game, or utility.

Online Annoyances and Social Engineering
Online Annoyances (1 of 3)
(Objective 9.5)

- Malware has malicious intent
  - Adware displays sponsored advertisements
  - Spyware is an unwanted piggy-back program
    - Transmits information
    - Tracking cookies
    - Keystroke logger
- Many anti-spyware packages are available

Online Annoyances and Social Engineering
Online Annoyances (1 of 3)

- Adware is software that displays sponsored advertisements in a section of your browser window or as a pop-up box. It’s considered a legitimate, though sometimes annoying, means of generating revenue for those developers who don’t charge for their software or information. Web browsers such as Safari, Chrome, and Edge have built-in pop-up blockers, the occurrence of annoying pop-ups has been greatly reduced.

Online Annoyances and Social Engineering
Online Annoyances (1 of 3)

- Spyware is an unwanted piggyback program that usually downloads with other software you install from the Internet and that runs in the background of your system. Without your knowledge, spyware transmits information about you, such as your Internet-surfing habits, to the owner of the program so that the information can be used for marketing purposes.
- Many spyware programs use tracking cookies (small text files stored on your computer) to collect information. One type of spyware program known as a keystroke logger (keylogger) monitors keystrokes with the intent of stealing passwords, login IDs, or credit card information

Online Annoyances and Social Engineering

Online Annoyances (2 of 3)

(Objective 9.5)

- Spam (junk e-mail)
- Tactics to minimize spam (spam filter)

Online Annoyances and Social Engineering
Online Annoyances (2 of 3)

- Companies that send out spam—unwanted or junk e-mail— find your e-mail address either from a list they purchase or with software that looks for e-mail addresses on the Internet
- A spam filter is an option you can select in your e-mail account that places known or suspected spam messages into a special folder (called “Spam” or “Junk Mail”). Most e-mail services, such as Gmail and Outlook, offer spam filters

Online Annoyances and Social Engineering

Online Annoyances (3 of 3)

(Objective 9.5)

- Cookies are small text files received when you visit a website
- Help companies determine the effectiveness of their marketing
- Do not search your hard drive for personal information
- May invade your privacy
- Pose no security threat

Pearson

Online Annoyances and Social Engineering

Social Engineering (1 of 3)

(Objective 9.6)

- Social engineering is any technique using social skills to generate human interaction
  - Entices individuals to reveal sensitive information to generate human interaction that entices individuals to reveal sensitive information. Social engineering often doesn’t involve the use of a computer or face-to-face interaction. For example, telephone scams are a common form of social engineering because it’s often easier to manipulate someone when you don’t have to look at them.
- Pretexting involves creating a scenario that sounds legitimate

Online Annoyances and Social Engineering
Social Engineering (1 of 3)

Most social engineering schemes use a pretext to lure their victims. Pretexting involves creating a scenario that sounds legitimate enough that someone will trust you. For example, you might receive a phone call during which the caller says he is from your bank and that someone tried to use your account without authorization. The caller then tells you he needs to confirm a few personal details such as your birth date, Social Security number, bank account number, and whatever other information he can get out of you.

The information he obtains can then be used to empty your bank account or commit some other form of fraud. The most common form of pretexting in cyberspace is phishing.

Online Annoyances and Social Engineering

Social Engineering (2 of 3)

(Objective 9.6)

- Phishing
  - Luring people into revealing information
- Pharming
  - Malicious code planted on your computer to gather information
- Guidelines to avoid schemes

Pearson

Online Annoyances and Social Engineering
Social Engineering (2 of 3)

- Phishing: lures Internet users to reveal personal information that could lead to identity theft. The scammers send e-mail messages that look like they’re from a legitimate business such as a bank. The e-mail usually states that the recipient needs to update or confirm his or her account information. When the recipient clicks on the provided link, they go to a website. The site looks like a legitimate site but is really a fraudulent copy that the scammer has created. Once the e-mail recipient enters his or her personal information, the scammers capture it and can begin using it.

Online Annoyances and Social Engineering
Social Engineering (2 of 3)

- Pharming is much more insidious than phishing. Phishing requires a positive action by the person being scammed, such as going to a website mentioned in an e-mail and typing in personal information. Pharming occurs when malicious code is planted on your computer, either by viruses or by your visiting malicious websites, which then alters your browser’s ability to find web addresses. Users are directed to bogus websites even when they enter the correct address of the real website. You end up at a fake website that looks legitimate but is expressly set up for the purpose of gathering information.

Online Annoyances and Social Engineering

Social Engineering (3 of 3)

(Objective 9.6)

- Scareware
  - Type of malware
  - Attempts to convince you something is wrong … and to pay money to fix it

Pearson

Online Annoyances and Social Engineering Social Engineering (3 of 3)

- Scareware is a type of malware that downloads onto your computer and tries to convince you that your computer is infected with a virus or other type of malware. Pop-ups, banners, or other annoying types of messages will flash on your screen, saying frightening things like "Your computer is infected with a virus . . . immediate removal is required." You're then directed to a website where you can buy fake removal or antivirus tools that provide little or no value. Some scareware even goes so far as to encrypt your files and then demand that you pay to have them unencrypted, which is essentially extortion.
- Scareware is a social engineering technique because it uses people's fear of computer viruses to convince them to part with their money

Restricting Access to Your Digital Assets Firewalls (1 of 2)

(Objective 9.7)

- Firewall—hardware or software
- Windows and macOS include firewalls
- Security suites include firewall software

Restricting Access to Your Digital Assets Firewalls (1 of 2)

- Firewalls are designed to restrict access to a network and its computers. Firewalls protect you in two major ways: (1) by blocking access to logical ports and (2) by keeping your computer’s network address secure. How do firewalls block access to your logical ports? Recall that logical ports are virtual communications paths that allow a computer to organize requests for information from other networks or computers.

- To block access to logical ports, firewalls examine data packets that your computer sends and receives. Data packets contain the address of the sending and receiving computers and the logical port that the packet will use. Firewalls can be configured so that they filter out packets sent to specific logical ports in a process known as packet filtering. Firewalls can also be configured to completely refuse requests from the Internet asking for access to specific ports. That process is referred to as logical port blocking.

Restricting Access to Your Digital Assets Firewalls (2 of 2)

(Objective 9.7)

- Packet filtering
  - Filter out packets sent to logical ports
- Logical port blocking
  - Completely refuses requests from the Internet asking for access to specific ports
- Network address translation
  - Assign IP addresses on a network

Pearson

Restricting Access to Your Digital Assets Firewalls (2 of 2)

- Every computer connected to the Internet has a unique address called an Internet protocol address (IP address). Data is routed to the correct computer on the Internet based on the IP address. If a hacker finds out the IP address of your computer, they can locate it on the Internet and try to break into it. Your IP address for your home network is assigned to your router by your Internet service provider (ISP). Then each device on your home network has its own IP address. Firewalls use a process called network address translation (NAT) to assign internal IP addresses on a network. The internal IP addresses are used only on the internal network and therefore can’t be detected by hackers. For hackers to access your computer, they must know your computer’s internal IP address.

Restricting Access to Your Digital Assets
Preventing Virus Infections (1 of 3)

- Antivirus software
  - Detects viruses and protects your computer
- Popular programs
  - Symantec
  - Kaspersky
  - Trend Micro
  - Avast

Restricting Access to Your Digital Assets Preventing Virus Infections (2 of 3)

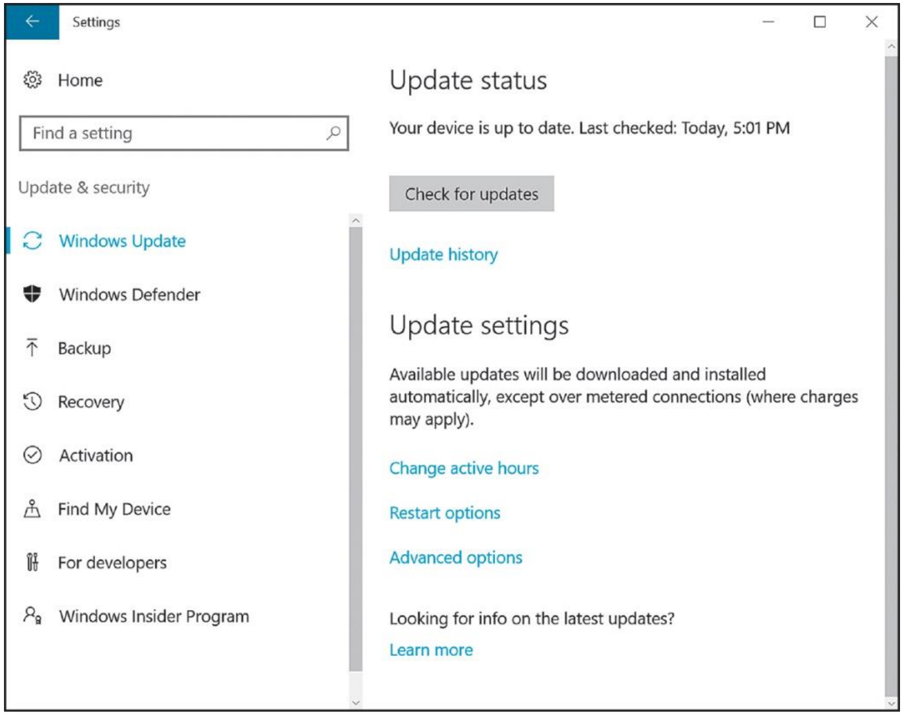
(Objective 9.8)

- Virus signature
  - Portion of the virus code that’s unique to a particular computer virus
- Quarantining
  - Placing virus in a secure area so it won’t spread to other files
- Inoculation
  - Records key attributes about your computer files and keep stats in secure place

Restricting Access to Your Digital Assets Preventing Virus Infections (3 of 3)

(Objective 9.8)

- Drive-by download
  - Exploit weaknesses in operating systems



Update status

Your device is up to date. Last checked: Today, 5:01 PM

Check for updates

Update history

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

Change active hours

Restart options

Advanced options

Looking for info on the latest updates?

Learn more

Windows 10, Microsoft Corporation

Restricting Access to Your Digital Assets

Authentication: Passwords and Biometrics (1 of 2)

(Objective 9.9)

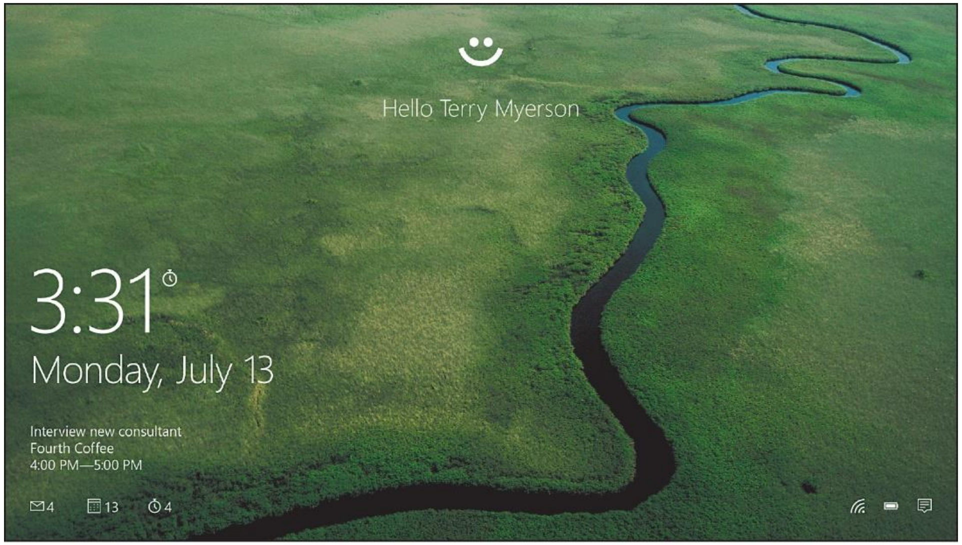
- Need strong passwords
- Password strength tests
- Operating systems have built-in password protection
- Managing passwords

Pearson

Restricting Access to Your Digital Assets Authentication: Passwords and Biometrics (2 of 2)

(Objective 9.9)

- Biometric Authentication Devices
  - Fingerprint
  - Iris pattern in eye
  - Voice authentication
  - Face pattern recognition
  - Provide a high level of security



Hello Terry Myerson

3:31

Monday, July 13

Interview new consultant
Fourth Coffee
4:00 PM—5:00 PM

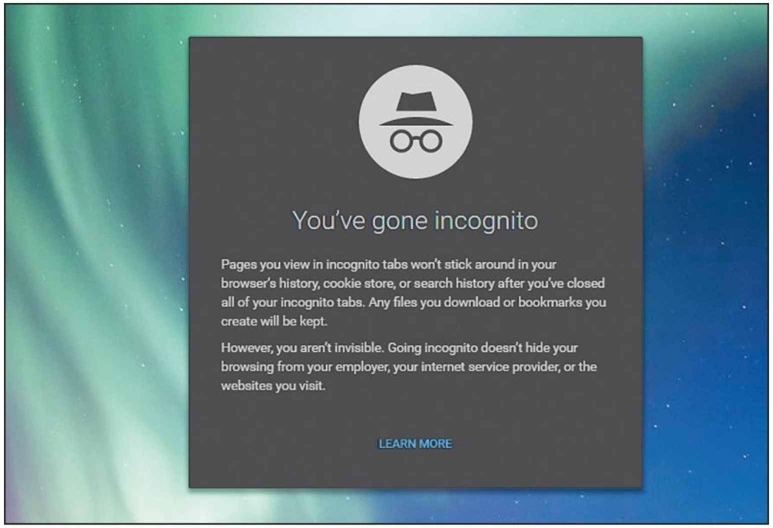
Windows 10, Microsoft Corporation

Restricting Access to Your Digital Assets

Anonymous Web Surfing: Hiding from Prying Eyes

(Objective 9.10)

- Privacy tools
  - Private Browsing
  - InPrivate
  - Incognito
- Portable privacy devices
  - Kingston Personal Flash Drives
- Virtual private networks (VPNs)
  - Secure networks that are established using the public Internet infrastructure



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

© 2015 Google Inc, used with permission. Google and the Google logo are registered trademarks of Google Inc.

Keeping Your Data Safe

Protecting Your Personal Information

(Objective 9.11)

- Reveal as little information as possible
- In Facebook, change your privacy settings

Keeping Your Data Safe

Backing Up Your Data (1 of 2)

(Objective 9.12)

- Backups are copies of files used to replace the originals if they’re lost or damaged
- Files to backup
  - –Data files
  - –Program files
- Types of backups
  - –Full
  - –Incremental
  - –Image

Types of backups

- 1. A full backup means that you create a copy of all your application and data files. This is followed by a schedule of incremental backups (or partial backups). These involve only backing up files that have changed or have been created since the last backup was performed.
- 2. An image backup (or system backup) means that all system files are backed up, not just the application and data files. An image backup ensures you capture a complete snapshot of everything that makes your computer run—the operating system, the applications, and the data. The idea of imaging is to make an exact copy of the setup of your computer so that in the event of a total hard drive failure, you can copy the image to a new hard drive and have your computer configured exactly the way it was before the crash.

Keeping Your Data Safe
Backing Up Your Data (1 of 2)

- Where should I store my backups?
- 1. Online (in the cloud). To be truly secure, backups should be stored online. Because the information is stored online, it’s in a secure, remote location, so data isn’t vulnerable to the disasters that could harm data stored in your home. Image backups may not fit within the storage limits offered for free by cloud providers. Look for a service that specifically provides mirror-image backups, which will include a copy of your full operating system. For example, Carbonite (carbonite.com) offers certain plans that include online storage of a full system backup.

Keeping Your Data Safe
Backing Up Your Data (1 of 2)

- 2. External hard drives. External hard drives, or even large-capacity flash drives, are popular backup options. Although convenient and inexpensive, using external hard drives for backups still presents the dilemma of keeping the hard drive in a safe location. Also, external hard drives can fail, possibly leading to loss of your backed-up data. Therefore, using an external hard drive for backups is best done in conjunction with an online backup strategy for added safety.
- 3. Network-attached storage (NAS) devices and home servers. NAS devices are essentially large hard drives connected to a network of computers instead of to just one computer, and they can be used to back up multiple computers simultaneously. Home servers also act as high-capacity NAS devices for automatically backing up data and sharing files.

Protecting Your Physical Computing Assets Environmental Factors and Power Surges

(Objective 9.13)

- Power surges
  - Old or faulty wiring
  - Downed power lines
  - Lightning strikes
  - Malfunctions at electric company substations
- Surge protector / Whole-house surge protector
  - Replace every 2–3 years
  - Use with all devices that have solid-state components

Protecting Your Physical Computing Assets Preventing and Handling Theft

(Objective 9.14)

- Three main security concerns with mobile devices:
  - Keeping them from being stolen
  - Keeping data secure in case they are stolen
  - Finding a device if it is stolen

Questions

Copyright

Pearson