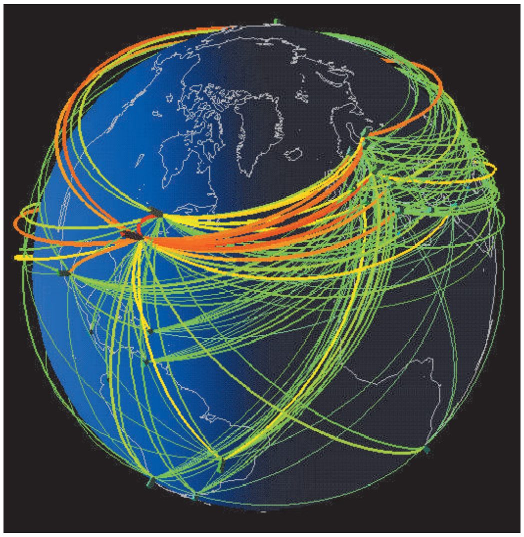
INTERNET AND WEB BASICS

◗ **What is the Internet?** The Internet is the largest computer network in the world, carrying information from one continent to another in the blink of an eye (Figure 15). The computers connected to this network offer many types of resources, such as e-mail, instant messaging, social networking, popular music downloads, and online shopping.

FIGURE 15

The Internet communications network stretches around the globe.



Courtesy of Stephen G. Eick

◗ **What is the Web?** Although some people use the terms *Internet* and *Web* interchangeably, the two are not the same. The Internet refers to a communications network that connects computers all around the globe. The Web—short for World Wide Web—is just one of the many resources available over this communications network.

The Web is a collection of linked and cross-referenced information available for public access. This information is accessible from Web sites located on millions of computers. The information is displayed as a series of screens called Web pages. You'll use the Web for general research and for specific activities designed to accompany this textbook. To use the Web, your computer must have access to the Internet.

◗ **How do I access the Internet?** Most digital devices can be configured to connect to the Internet over telephone, cell phone, satellite, or cable television systems. Internet access can be obtained from school computer labs, local service providers such as your cable television company, and national Internet service providers such as AOL, AT&T, Comcast, Verizon, and EarthLink.

To expedite your orientation, it is assumed that your computer has Internet access. If it does not, consult your instructor, or ask an experienced computer user to help you get set up.

◗ **How do I know if my computer has Internet access?** The easiest way to find out if your computer can access the Internet is to try it. You can quickly find out if you have Internet access by starting software called a browser that's designed to display Web pages.

Browser software called Internet Explorer is supplied with Microsoft Windows. Mac OS X includes a browser called Safari. Other browsers, such as Firefox and Chrome, are also available. Follow the steps in the TRY IT! box to start your browser.

HOW TO USE A WEB BROWSER AND SEARCH ENGINE

◗ **How do I use a browser?** A browser lets you enter a unique Web page address called a URL, such as *www.google.com*. You can also jump from one Web page to another by using links. Links are usually underlined; and when you position the arrow-shaped mouse pointer over a link, it changes to a hand shape.

TRY IT!

Start your browser

1. Click the icon for your browser. It is usually located on the Start screen, near the Start button, or on the dock.

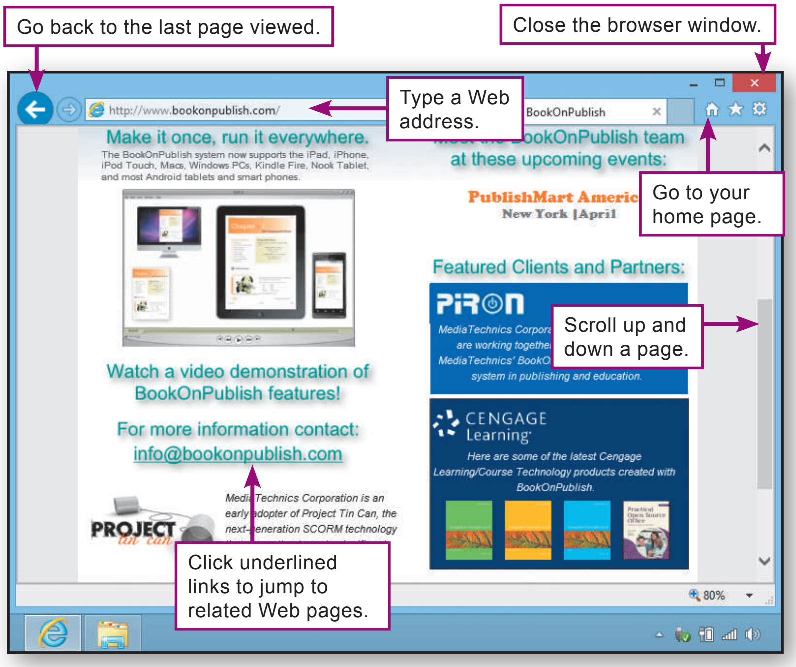
2. Your computer should soon display the browser window.

If your computer displays a *Connect to* box, click the **Dial** button to establish a dial-up connection over your telephone line.

You'll need to cancel the browser command and consult an experienced computer user if:

- Your computer displays a "working off line" message.
- Your computer displays an Internet Connection Wizard box.

Although browsers offer many features, you can get along quite well using the basic controls shown in Figure 16.



Go back to the last page viewed.

Close the browser window.

Type a Web address.

Go to your home page.

Scroll up and down a page.

Click underlined links to jump to related Web pages.

http://www.bookonpublish.com/
BookOnPublish
Make it once, run it everywhere.
Watch a video demonstration of BookOnPublish features!
For more information contact:
info@bookonpublish.com
Featured Clients and Partners:
CENGAGE Learning
80%

Web site © MediaTechnics

FIGURE 16

Using a Browser

A full Web address might look like this: http://www.mediatechnicscorp.com

It is not necessary to type the *http://*. So to access the MediaTechnics Corporation page shown here, you would type: **www.mediatechnicscorp.com**

When typing a Web address, do not use any spaces, and copy uppercase and lowercase letters exactly.

Orientation

◗ How do I find specific information on the Web?

If you're looking for information and don't know the Web site where it might be located, you can use a search engine to find it. Follow the steps in the TRY IT! box to "google it" by using the Google search engine.

TRY IT!

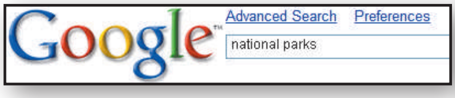
Use a search engine

1. Make sure the browser window is open.

2. Click the Address box and type:

3. Press the **Enter** key. Your browser displays the Web page for the Google search engine.

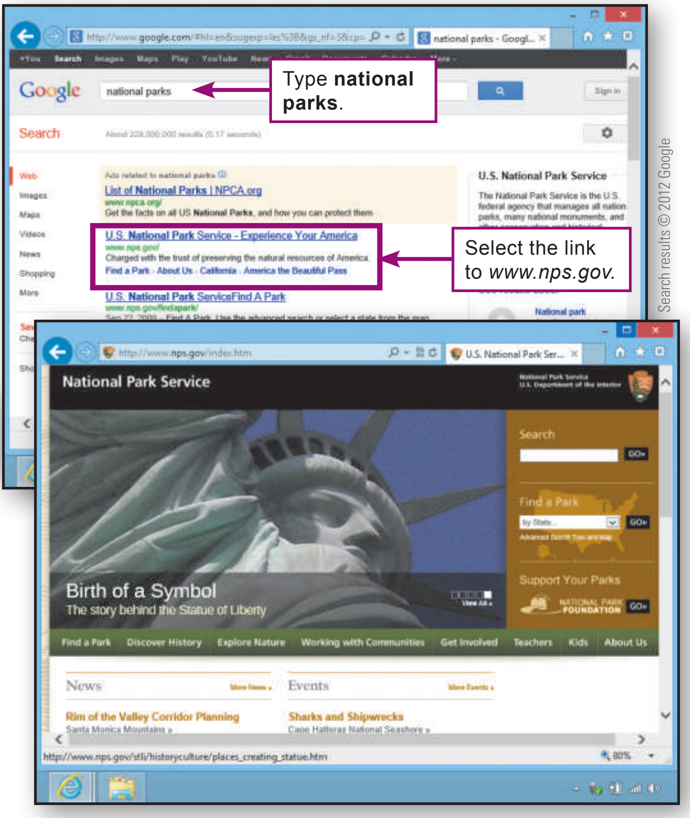
4. Click the blank search box and then type **national parks**.



5. Press the **Enter** key. Google displays a list of Web pages that relate to national parks.

6. Click the underlined **U.S. National Park Service** link. Your browser displays the Park Service's home page.

7. Leave your browser open for the next TRY IT!.



Type **national parks**.

Select the link to *www.nps.gov.*

national parks
U.S. National Park Service - Experience Your America
www.nps.gov/
National Park Service
Birth of a Symbol
The story behind the Statue of Liberty

Search results © 2012 Google

Courtesy of the U.S. Park Service

◗ What are the best sources of information on the Web?

The best sources of information are easy to access, dependable, and preferably free. Sites such as Wikipedia, Answers.com, WhatIs.com, and HowStuffWorks are great sources for general information and researching topics for computer courses.

When you're looking for information on the Web, remember that virtually anyone can post anything. Consequently, some information you encounter might not be accurate.

To check the quality of information provided by a Web site, you can cross-check facts with other sites. Be sure to check when the material was posted or updated to determine if it is current. You might also consider the information source. Blogs, tweets, Facebook posts, and YouTube videos often express opinions rather than facts.

◗ How does Wikipedia work? Wikipedia is an encyclopedia that is written and maintained by the people who use it. More than 23 million articles on a vast range of topics have been submitted and updated by users, many of them experts. Wikipedia information tends to be accurate because users are continually reading the articles and correcting inaccurate or biased information. However, some vandalism occurs and from time to time a few articles contain false or misleading information.

Most Wikipedia articles include a View history tab that tracks changes. Check the date of the last change to determine if the information is current. Articles also include a Discussion tab that can help you spot controversial aspects of the information. Use the TRY IT! below to see how Wikipedia works.

TRY IT!

Check out Wikipedia

1. In the Address bar of your browser, type **www.wikipedia.org** and then press the **Enter** key.

2. When the Wikipedia window appears, enter **cyberspace** in the search box and then press **Enter**.

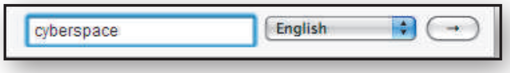
3. Read a bit of the article to get an idea of its scope and detail. Do you detect any bias in the article?

4. Click the **View history** tab. Look at the last few updates. Does this article seem up to date?

5. Click the **Discussion** tab. What is the status of the article? Does it contain controversial statements? Can you envision how you might use Google or other Web resources to explore specific controversies?

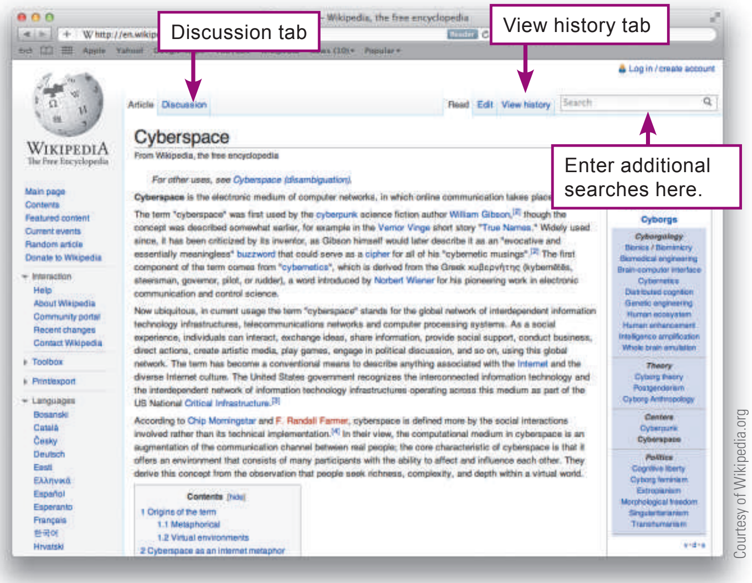
6. Click the **Article** tab to return to the Cyberspace article.

7. You can leave your browser open for the next TRY IT!.



cyberspace

English



Cyberspace

From Wikipedia, the free encyclopedia

For other uses, see Cyberspace (disambiguation).

Cyberspace is the electronic medium of computer networks, in which online communication takes place

The term "cyberspace" was first used by the cyberpunk science fiction author William Gibson,[2] though the concept was described somewhat earlier, for example in the Vernor Vinge short story "True Names." Widely used since, it has been criticized by its inventor, as Gibson himself would later describe it as an "evocative and essentially meaningless" buzzword that could serve as a cipher for all of his "cybernetic musings".[2] The first component of the term comes from "cybernetics", which is derived from the Greek κυβερνήτης (kybernētēs, steersman, governor, pilot, or rudder), a word introduced by Norbert Wiener for his pioneering work in electronic communication and control science.

Now ubiquitous, in current usage the term "cyberspace" stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. As a social experience, individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on, using this global network. The term has become a conventional means to describe anything associated with the Internet and the diverse Internet culture. The United States government recognizes the interconnected information technology and the interdependent network of information technology infrastructures operating across this medium as part of the US National Critical Infrastructure.[3]

According to Chip Morningstar and F. Randall Farmer, cyberspace is defined more by the social interactions involved rather than its technical implementation.[4] In their view, the computational medium in cyberspace is an augmentation of the communication channel between real people; the core characteristic of cyberspace is that it offers an environment that consists of many participants with the ability to affect and influence each other. They derive this concept from the observation that people seek richness, complexity, and depth within a virtual world.

Contents [hide]

1 Origins of the term

1.1 Metaphorical

1.2 Virtual environments

2 Cyberspace as an internet metaphor

Courtesy of Wikipedia.org

WORKING WITH E-MAIL

◗ **What is e-mail?** E-mail is a form of communication that relies on computer networks, such as the Internet, to transmit messages from one computer to another. Like regular mail, e-mail messages are sent to a mailbox where they are kept until the recipient retrieves them. Messages might arrive at their destination within seconds, or might not arrive for a few hours. Once sent, e-mail messages cannot be recalled.

◗ **What do I need to use e-mail?** To send and receive e-mail, you need an Internet connection, an e-mail account, and software that enables you to compose, read, and delete e-mail messages. An e-mail account consists of an e-mail address (Figure 17), a password, and a mailbox. You can usually obtain an e-mail account from your Internet service provider, your school, or a Webmail provider, such as Hotmail, Yahoo! Mail, or Gmail.

Webmail providers store your mail online. To access your mail, simply use your browser. In contrast, local mail, such as Microsoft Outlook, transfers mail to your computer and requires you to use special e-mail software instead of a browser.

◗ **How do I get a Webmail account?** Registering for a Webmail account is easy and many online e-mail providers offer free basic service. Work with the TRY IT! below to see how.

FIGURE 17

E-mail Addresses

An e-mail address consists of a user ID followed by an @ symbol and the name of a computer that handles e-mail accounts. Ask your instructor for his or her e-mail address. It is likely similar to the following:

instructor@school.edu

When typing an e-mail address, use all lowercase letters and do not use any spaces.

TRY IT!

Get a Web-based e-mail account

1. In the Address bar of your browser, enter **www.gmail.com**.

2. When the Gmail window appears, click the button labeled **CREATE AN ACCOUNT**.

3. Follow the directions to enter your first name, last name, and username.

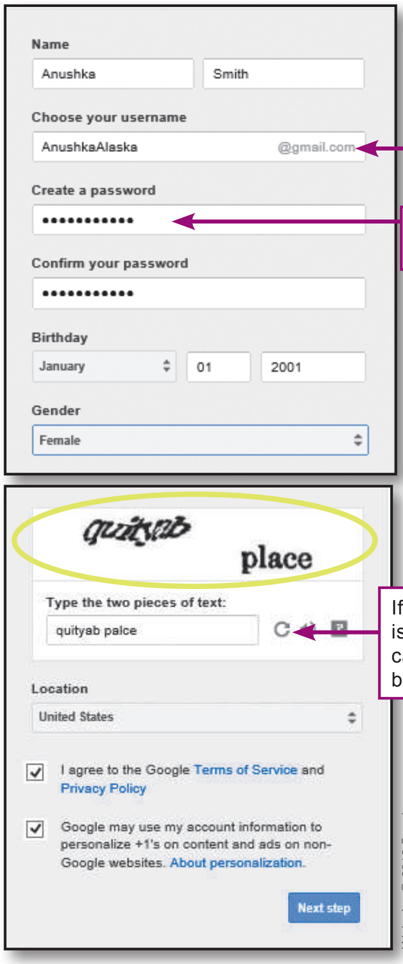
4. The login name you select is checked for uniqueness. If it is already in use, you'll have to try a different one.

5. When you've selected a valid username, continue down the page to create a password. Try not to use a name, a date, or any dictionary word as your password.

6. Continue down the page to complete the rest of the registration form.

7. Before finalizing your registration, review the information you've entered and jot down your login name and password.

8. Read the Terms of Service. If you agree, click the **Next step** button. That's it! You now have a Gmail account.



Name: Anushka | Smith

Choose your username: AnushkaAlaska @gmail.com

Create a password: ●●●●●●●●●●●

Confirm your password: ●●●●●●●●●●●

Birthday: January | 01 | 2001

Gender: Female

Type the two pieces of text: quityab palce

Location: United States

☑ I agree to the Google Terms of Service and Privacy Policy

☑ Google may use my account information to personalize +1's on content and ads on non-Google websites. About personalization.

You might have to try several usernames to find one that is available.

Try to choose a strong password.

If the CAPTCHA text is too garbled, you can get different text by clicking this icon.

Web site © 2012 Google

▶ Is Webmail better than local e-mail? Both Web-based and local e-mail have their advantages and disadvantages. Webmail accounts are definitely easier to set up and you can use them from any computer with an Internet connection. Webmail accounts are also ideal for "throw-away" accounts.

▶ What is a throw-away e-mail account? Whether you use local mail or Webmail for your regular correspondence, you might consider creating one or two throw-away accounts for occasions when you have to give an e-mail address, but you don't want any continued correspondence from that source. Later in the chapter, you'll learn more about how e-mail scams and online marketing contribute to all the junk e-mail you receive. Your throw-away e-mail address can become the recipient for lots of those messages, and eventually you can simply delete the throw-away account and all the junk it contains.

▶ How do I create and send an e-mail message? Many e-mail systems are available, and each uses slightly different software, making it impossible to cover all options in this short orientation. You might want to enlist the aid of an experienced computer user to help you get started. The steps in the TRY IT! box pertain to Gmail, but other e-mail packages work in a similar way.

E-MAIL PRIVACY

E-mail messages are not necessarily private; their contents might be seen during system maintenance or repair, and commercial e-mail archives are subject to search by government agencies.

Free Web-based mail is typically searched as you write it by digital bots that look for keywords, like *vacation* or *pet*, to display related advertising. If you want more privacy, consider private e-mail providers and local e-mail software.

TRY IT!

Create and send e-mail

1. If Gmail is not open, open your browser and type **www.gmail.com** in the address box. Log in to your Gmail account.

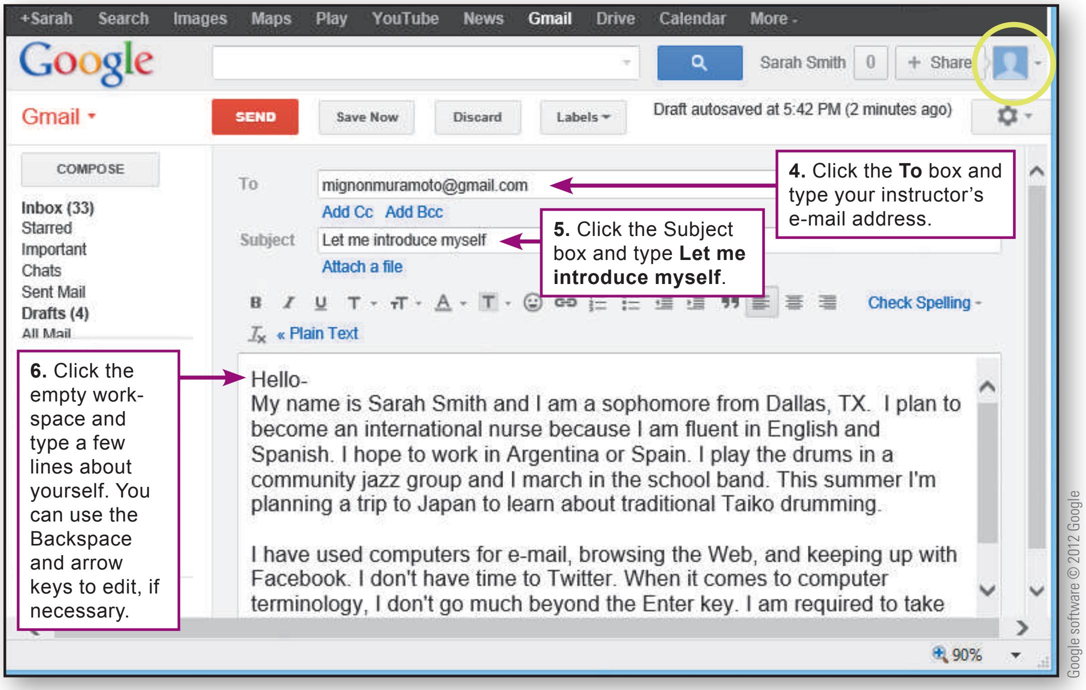
2. Click the **Compose** button to display a form like the one below.

3. Follow steps 4 through 6 as shown below.

7. When your message is complete, click the **SEND** button and Gmail sends the message.

8. You can continue to experiment with e-mail. When done, use the **Sign out** option under the link for your account (circled), then close your browser.

Note: With some local e-mail configurations, the Send button places the e-mail in an Outbox and you have to click the **Send/Receive** button on the toolbar to ship the message out from your computer.



Draft autosaved at 5:42 PM (2 minutes ago)

To: mignonmuramoto@gmail.com

Subject: Let me introduce myself

Hello-
My name is Sarah Smith and I am a sophomore from Dallas, TX. I plan to become an international nurse because I am fluent in English and Spanish. I hope to work in Argentina or Spain. I play the drums in a community jazz group and I march in the school band. This summer I'm planning a trip to Japan to learn about traditional Taiko drumming.

I have used computers for e-mail, browsing the Web, and keeping up with Facebook. I don't have time to Twitter. When it comes to computer terminology, I don't go much beyond the Enter key. I am required to take

4. Click the **To** box and type your instructor's e-mail address.

5. Click the Subject box and type **Let me introduce myself**.

6. Click the empty workspace and type a few lines about yourself. You can use the Backspace and arrow keys to edit, if necessary.

Google software © 2012 Google

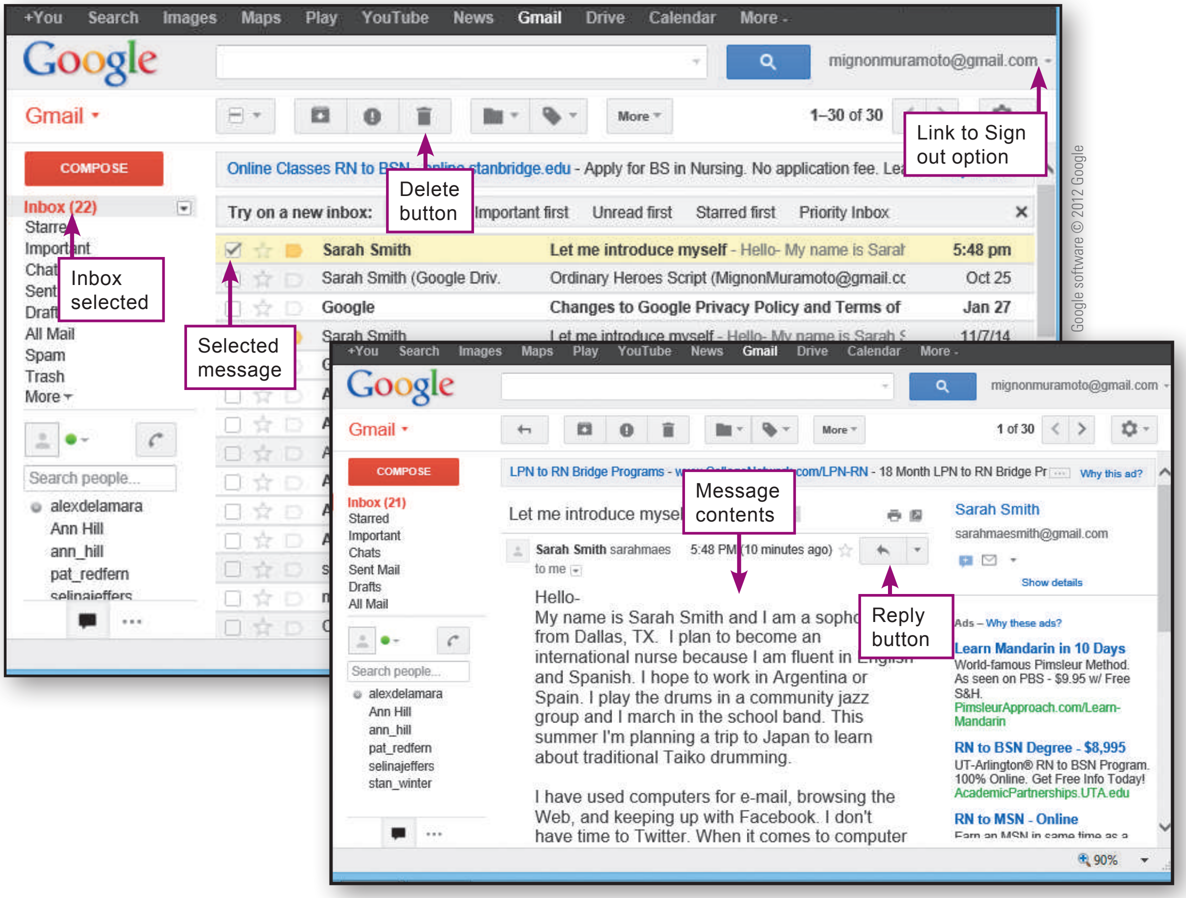
◗ **How do I get my e-mail?** As with sending mail, the way you get mail depends on your e-mail system. In general, clicking the Send/Receive button collects your mail from the network and stores it in your Inbox. Your e-mail software displays a list of your messages. The new ones are usually highlighted or shown in bold type. You can click any message to open it, read it, and reply to it, as shown in Figure 18.

◗ **How do I log off?** When working with a Webmail account, it is important to use the Log out or Sign out link before you close your browser. Taking this extra step makes your e-mail less vulnerable to hackers.

FIGURE 18

When e-mail software displays your Inbox, you can:

- Open a message and read it.
- Reply to a message.
- Delete unwanted messages (a good idea to minimize the size of your mailbox).
- Forward a message to someone else.



Online Classes RN to BSN - online.stanbridge.edu - Apply for BS in Nursing. No application fee. Lea

Try on a new inbox: Important first Unread first Starred first Priority Inbox

☑ Sarah Smith	**Let me introduce myself** - Hello- My name is Sarah	5:48 pm
Sarah Smith (Google Driv.	Ordinary Heroes Script (MignonMuramoto@gmail.cc	Oct 25
Google	**Changes to Google Privacy Policy and Terms of**	Jan 27
Sarah Smith	Let me introduce myself - Hello- My name is Sarah S	11/7/14

Link to Sign out option

Delete button

Inbox selected

Selected message

LPN to RN Bridge Programs - www.CollegeNetwork.com/LPN-RN - 18 Month LPN to RN Bridge Pr ... Why this ad?

Let me introduce myself

Sarah Smith sarahmaes 5:48 PM (10 minutes ago)
to me

Hello-
My name is Sarah Smith and I am a sophomore from Dallas, TX. I plan to become an international nurse because I am fluent in English and Spanish. I hope to work in Argentina or Spain. I play the drums in a community jazz group and I march in the school band. This summer I'm planning a trip to Japan to learn about traditional Taiko drumming.

I have used computers for e-mail, browsing the Web, and keeping up with Facebook. I don't have time to Twitter. When it comes to computer

Sarah Smith
sarahmaesmith@gmail.com

Ads – Why these ads?

Learn Mandarin in 10 Days
World-famous Pimsleur Method. As seen on PBS - $9.95 w/ Free S&H.
PimsleurApproach.com/Learn-Mandarin

RN to BSN Degree - $8,995
UT-Arlington® RN to BSN Program. 100% Online. Get Free Info Today!
AcademicPartnerships.UTA.edu

RN to MSN - Online
Earn an MSN in same time as a

Message contents

Reply button

Google software © 2012 Google

QuickCheck

SECTION B

1. Documents that you send along with e-mail messages are referred to as □ .

2. Popular □ software includes Internet Explorer, Chrome, and Firefox.

3. When looking for information on the Web, you can use a(n) □ engine to produce a list of links to Web pages that might contain the information you seek.

4. An e-mail □ looks something like student@school.edu.

5. To access Webmail, you use a browser; but to access □ e-mail, you use e-mail software such as Microsoft Outlook.

▶ CHECK ANSWERS

Security and Privacy

SECTION C

AS WITH MOST OTHER facets of modern life, the digital world has its share of troublemakers, scam artists, and identity thieves. Section C offers some tips on navigating through the sometimes rough neighborhoods of cyberspace, while keeping your data safe and your identity private.

SECURING YOUR DIGITAL DEVICES AND DATA

What's at risk if my computer or phone is stolen? The value of a stolen computer or phone is not so much in the hardware as in the data it contains. With stolen data such as your bank account numbers and PINs, a thief can wipe out your checking and savings accounts. With your credit card numbers, a thief can go on a spending spree. Even worse, a criminal can use stolen data to assume your identity, run up debts, get into legal difficulties, ruin your credit rating, and cause you no end of trouble.

How can I protect my data from theft? Never leave your devices unattended. If a thief steals your computer or phone, you can make it difficult to access your data by setting up a password. Until the password is entered, your data is off limits. Thieves will not be able to get beyond the login screen and should not be able to easily access your data.

Use security tools to protect your phone. Keep it locked while not in use and consider subscribing to a tracking service that allows you to use a Web site to find your phone, lock it, or erase it.

Many new computers are shipped with a standard administrator password that everyone knows. If you are the only person using your computer, you can use the administrator account for your day-to-day computing, but create a secure password (Figure 19) for this account as soon as you can.

Your computer might also include a preset guest account with a nonsecure password such as *guest*. You should disable this guest account or assign it a secure password.

FIGURE 19

To create a secure password:

- Use at least eight characters, mixing numbers with letters, as in *2by4lumber*.
- Do not use your name, the name of a family member, or your pet's name.
- Do not use a word that can be found in the dictionary.
- Do not forget your password!

TRY IT!

Check the accounts on your computer

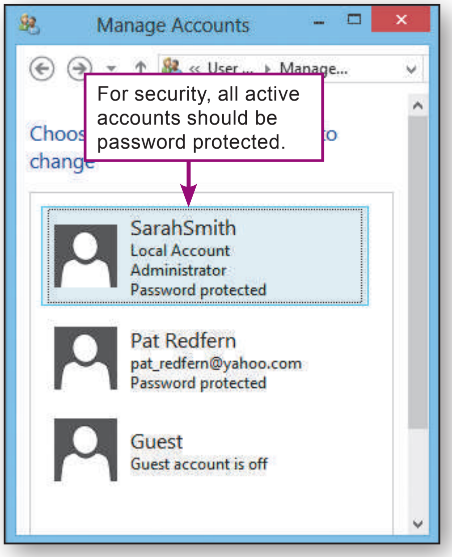
1. Access user accounts.

Windows 8: From the Start screen, type **c** and then select **Control Panel**. Select **User Accounts** and then select **Manage another account**.

Windows 7: Click the **Start** button, and then select **Control Panel**. Select **User Accounts and Family Safety**, select **User Accounts**, and then select **Manage another account**. (You might be required to enter an administrator password.)

Mac: Click the **Apple** icon, select **System Preferences**, and then select **Accounts**.

2. Check the password protection on all accounts. If you are working on a school lab computer, do not make changes to the account settings. If you are using your own computer, click the Administrator account and make sure it has a secure password.



Manage Accounts

« User ... › Manage...

Choos... to change

For security, all active accounts should be password protected.

SarahSmith
Local Account
Administrator
Password protected

Pat Redfern
pat_redfern@yahoo.com
Password protected

Guest
Guest account is off

AVOIDING VIRUSES

◗ What's so bad about viruses? The term *virus* has a technical meaning, but is loosely used when referring to malicious programs that circulate on infected downloads, in e-mail attachments, and on the Internet. This malware, as it is sometimes called, can steal your data, destroy files, or create network traffic jams. It might display an irritating message to announce its presence, or it might surreptitiously spread itself to various files or mail itself out to everyone in your e-mail address book.

After a virus takes up residence in a computer or phone, it is often difficult to disinfect all your files. Rather than wait for a virus attack, you can take steps to keep your digital devices virus free.

◗ How can I steer clear of malware? It helps to avoid risky behaviors, such as downloading pirated software, opening e-mail attachments from unknown senders, installing random social networking plug-ins, installing non-approved apps, and participating in illegal file sharing.

Antivirus software protects digital devices from malware (Figure 20). Because fewer viruses target Macs, OS X users who don't engage in risky online activities sometimes opt to work without antivirus software.

If you use antivirus software, configure it to run continuously whenever your computer is on. You should make sure your antivirus software is set to scan for viruses in incoming files and e-mail messages. At least once a week, your antivirus software should run a full system check to make sure every file on your computer is virus free.

As new viruses emerge, your antivirus software needs to update its virus definition file. It gets this update as a Web download. If you've selected the auto update option, your computer should automatically receive updates as they become available.

FIGURE 20

Popular Antivirus Software

Windows Defender
Norton AntiVirus
McAfee AntiVirus Plus
Kaspersky Anti-Virus
F-Secure Anti-virus
Panda Antivirus
Trend Micro Antivirus+
AVG AntiVirus FREE
Avast! Free Antivirus

TRY IT!

Get familiar with your antivirus software

1. Look for antivirus software (refer to Figure 20 for a list). In Windows 7, click the **Start** button, and then select **All Programs**. In Windows 8, scroll through the tiles on the Start screen. On the Mac, use **Finder** to access the Applications folder.

Can't find any? If you are using your own computer and it doesn't seem to have antivirus software, you can connect to an antivirus supplier's Web site and download it.

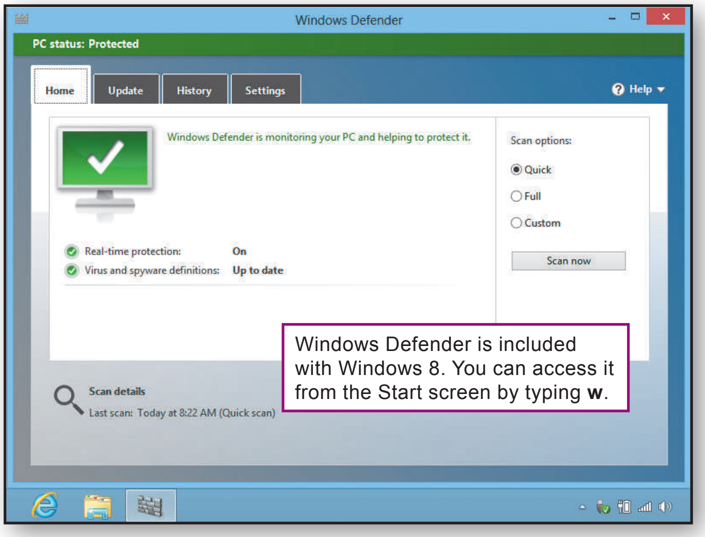
2. Open your antivirus software. Each antivirus program has unique features.

3. Explore your antivirus software to find out if it offers options to:

- Scan incoming e-mail.
- Run continuously in the background—a feature sometimes called Auto Protect.
- Block malicious scripts.

4. Check the date of your last full system scan. If it was more than one week ago, you should check the settings that schedule antivirus scans.

5. Check the date when your computer last received virus definitions. If it was more than one week ago, you should make sure your antivirus software is configured to receive automatic live updates.



PC status: Protected

Windows Defender is monitoring your PC and helping to protect it.

Scan options:
● Quick
○ Full
○ Custom

Scan now

Real-time protection: On
Virus and spyware definitions: Up to date

Scan details
Last scan: Today at 8:22 AM (Quick scan)

Windows Defender is included with Windows 8. You can access it from the Start screen by typing **w**.

PREVENTING INTRUSIONS

◗ **Is the Internet risky?** The Internet offers lots of cool stuff: music, movies, online shopping and banking, and much more. Most Internet offerings are legitimate, but some downloads contain viruses, and shady characters called hackers control programs that lurk about waiting to infiltrate your digital devices. If a hacker gains access to your phone or computer, he or she can view your files and steal personal information.

An infiltrated computer can be used as a launching platform for viruses and network-jamming attacks, or turned into a server for pornography and other unsavory material. Hackers have even found ways to turn thousands of infiltrated computers into “zombies,” link them together, and carry out coordinated attacks to disrupt online access to Microsoft, Bank of America, and other Internet businesses.

◗ **How do hackers gain access?** Intruders gain access by exploiting security flaws in your device’s operating system, browser, and e-mail software. Companies such as Microsoft, Apple, and HTC constantly produce software updates to fix these flaws. As part of your overall security plan, you should download and install security updates as they become available.

◗ **Do I need a firewall?** Firewall software and Internet security suites, such as those listed in Figure 21, provide a protective barrier between a computer and the Internet. If your computer is directly connected to the Internet, it should have active firewall software. If your computer connects to a local area network for Internet access, the network should have a device called a router to block infiltration attempts.

When a firewall is active, it watches for potentially disruptive incoming data called probes. When a probe is discovered, your firewall displays a warning and asks what to do. If the source looks legitimate, you can let it through; if not, you should block it (Figure 22).

◗ **Where do I get a firewall?** Mac OS X and Windows include built-in firewalls. Third-party Internet security suites also include firewall modules.

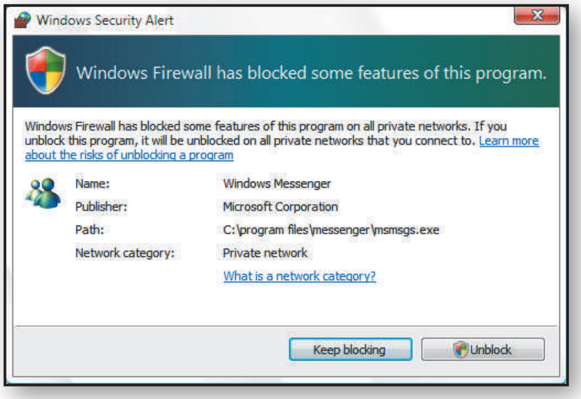
FIGURE 21

Popular Firewall Software and Internet Security Suites

Emsisoft Online Armor
McAfee Internet Security
ZoneAlarm Free Firewall
Norton Internet Security
Mac OS X Firewall
Agnitum Outpost Firewall
Windows Firewall
Comodo Firewall
Kaspersky Internet Security
Trend Micro Internet Security

FIGURE 22

When your firewall software encounters new or unusual activity, it asks you what to do.



Windows Security Alert

Windows Firewall has blocked some features of this program.

Windows Firewall has blocked some features of this program on all private networks. If you unblock this program, it will be unblocked on all private networks that you connect to. Learn more about the risks of unblocking a program

Name: Windows Messenger
Publisher: Microsoft Corporation
Path: C:\program files\messenger\msmsgs.exe
Network category: Private network

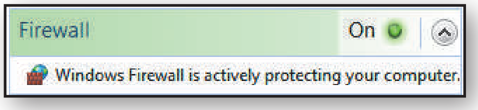
What is a network category?

TRY IT!

Check your Windows computer’s firewall

1. Access the **Control Panel** and then click the **Windows Firewall** link.

2. If the Windows firewall is not active, you should check to see if a third-party firewall is protecting your computer. To do so in Windows 7, click the **Start** button, select **All Programs**, and then look through the program list for firewalls such as those in Figure 21. In Windows 8, scroll through the tiles on the Start screen. If you find a firewall listed, start it and explore to see if it has been activated.



Firewall On

Windows Firewall is actively protecting your computer.

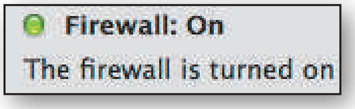
Check your Mac computer’s firewall

1. Click the **Apple** icon, and then select **System Preferences**.

2. Click the **Security** icon, and then click the **Firewall** button.

3. If the firewall is off, click the **Start** button if you want to activate it.

4. If the Start button is grayed out, click the lock at the bottom of the page and then enter an administrator name and password.



Firewall: On

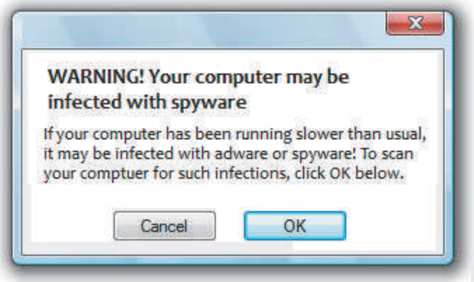
The firewall is turned on

SAFE BROWSING

◗ **Are some Web sites dangerous?** When you access Web sites, data is transferred to your device and displayed by your browser. Most of this data is harmless, but Web-based malware and spyware have the potential to search your device for passwords and credit card numbers, monitor your Web-browsing habits for marketing purposes, block your access to legitimate Web sites, or surreptitiously use your device as a staging area for illicit activities.

FIGURE 23

Some pop-up ads contain fake warnings about viruses, spyware, and intrusion attempts.



WARNING! Your computer may be infected with spyware

If your computer has been running slower than usual, it may be infected with adware or spyware! To scan your comptuer for such infections, click OK below.

Cancel OK

◗ **How can I block spyware?** The first line of defense is to never click pop-up ads—especially those with dire warnings, such as the ad in Figure 23, about your computer being infected by a virus or spyware! To close an ad, right-click its button on the taskbar at the bottom of your screen, and then select the Close option from the menu that appears.

Most browsers can be configured to block spyware and pop-up ads. Your antivirus software might offer similar options.

◗ **What other steps can I take to browse the Web safely?** Browsers include security features. You should take some time to become familiar with them. For example, Internet Explorer allows you to specify how you want it to deal with potentially dangerous ActiveX components, HTML scripts, spyware, and cookies. If you don't want to be bothered by these details, however, Internet Explorer offers several predefined configurations for Medium, Medium-High, and High security. Most Internet Explorer users set security and privacy options to Medium-High.

Your browser might also offer features such as private browsing, do not track, and delete browser history that can make your Web experience safer and more private.

TRY IT!

Check Internet security and privacy options

1. Start your browser and look for its security settings.

Internet Explorer: Click **Tools**, and then select **Internet Options**. Click the **Security** tab. Normally, your security setting should be Medium High. Click the **Privacy** tab. Your privacy setting should be Medium. If your version of IE offers a Pop-up Blocker, make sure its box contains a check mark so that it is activated.

Firefox: Click the **Firefox** tab or menu, select **Options** or **Preferences**, and then click **Content**. Make sure there is a check mark in the box for **Block pop-up windows**.

Safari: Click **Safari** on the menu bar. Make sure there is a check mark next to **Block Pop-Up Windows**.

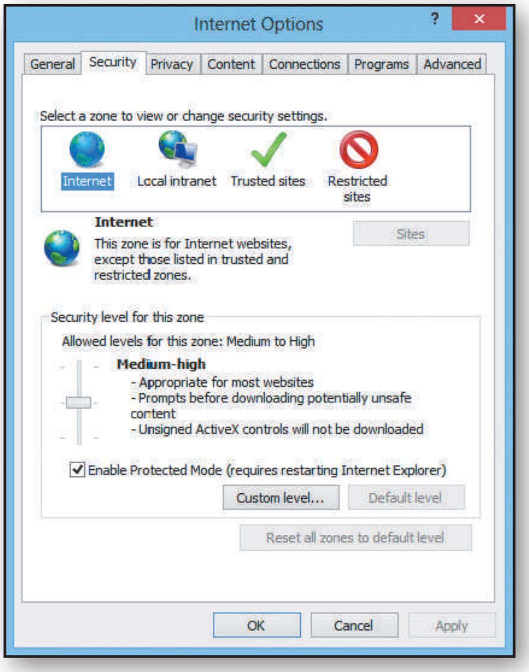
Chrome: Click the **Chrome menu** icon, select **Settings**, and then click **Show advanced settings**. Click the **Content settings** button. Under Pop-ups, make sure that the **Do not allow** option is selected.

2. Use your browser's Help to find out if the following features are available:

Private browsing

Do not track

Delete browser history



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Allowed levels for this zone: Medium to High

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

PROTECTING E-COMMERCE TRANSACTIONS

◗ **Is online shopping safe?** Online shopping is generally safe. From time to time, shoppers encounter fake storefronts designed to look like legitimate merchants but that are actually set up to steal credit card information. You can avoid these fakes by making sure you enter correctly spelled URLs when connecting to your favorite shopping sites.

◗ **How safe is my credit card information when I'm shopping online?** Online shopping has about the same level of risk as using your credit card for a telephone order or giving it to a server when you've finished eating in a restaurant.

That's not to say that credit cards are risk free. Credit cards are surprisingly vulnerable both online and off. Anyone who handles your card can copy the card number, jot down the expiration date, and try to make unauthorized charges. Thieves can break in to merchant computers that store order information. Thieves might even pick up your credit card information from discarded order forms. Despite these risks, we continue to use credit cards.

Many people are concerned about their credit card data getting intercepted as it travels over the Internet. As you wrap up an online purchase and submit your credit card information, it is transmitted from your computer to the merchant's computer. Software called a packet sniffer, designed for legitimately monitoring network traffic, can be used by unscrupulous hackers to intercept credit card numbers and other data traveling over the Internet.

◗ **How can I keep my credit card number confidential?** When you submit credit card information, make sure the merchant provides a secure connection for transporting data. Normally, a secure connection is activated when you're in the final phases of checking out—as you enter your shipping and credit card information into a form and click a Submit button to send it.

A secure connection encrypts your data. Even if your credit card number is intercepted, it cannot be deciphered and used. To make sure you have a secure connection, look for the lock icon. The Address box should also display a URL that begins with *https://*.

TRY IT!

Identify a secure connection

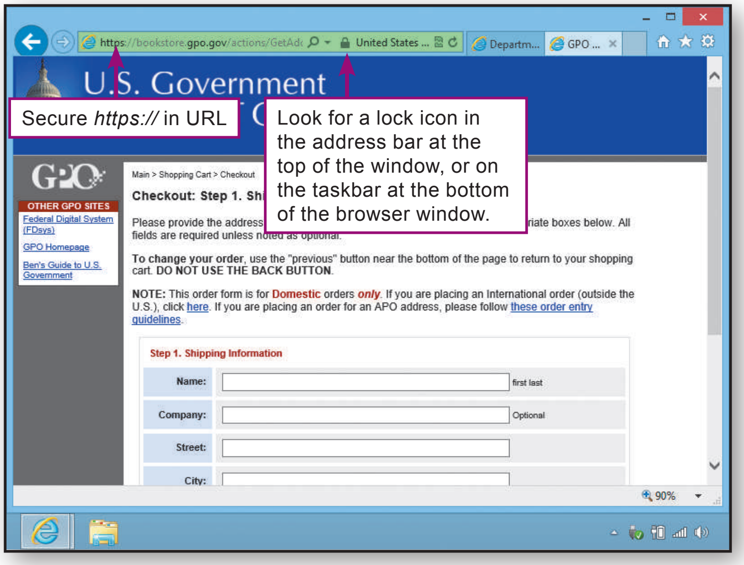
1. Start your browser and connect to the site **bookstore.gpo.gov**.

2. Select any book and place it in your online shopping cart.

3. Click the **Go to Checkout** button to reach step 1 of the checkout process.

4. At the checkout screen, do you see any evidence that you're using a secure connection?

5. Close your browser so that you don't complete the transaction.


https://bookstore.gpo.gov/actions/GetAdc
United States ...
Departm...
GPO ...
U.S. Government
GPO
OTHER GPO SITES
Federal Digital System (FDsys)
GPO Homepage
Ben's Guide to U.S. Government
Main > Shopping Cart > Checkout
90%

Secure *https://* in URL

Look for a lock icon in the address bar at the top of the window, or on the taskbar at the bottom of the browser window.

Checkout: Step 1. Shi

Please provide the address ... riate boxes below. All fields are required unless noted as optional.

To change your order, use the "previous" button near the bottom of the page to return to your shopping cart. **DO NOT USE THE BACK BUTTON**.

NOTE: This order form is for **Domestic** orders ***only***. If you are placing an International order (outside the U.S.), click here. If you are placing an order for an APO address, please follow these order entry guidelines.

Step 1. Shipping Information

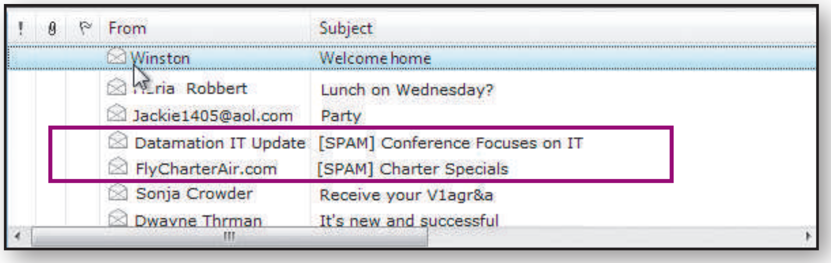
Name:		first last
Company:		Optional
Street:		
City:		

AVOIDING E-MAIL SCAMS

◗ **What are e-mail scams?** From time to time, you hear about con artists who have bilked innocent consumers out of their life savings. The Internet has its share of con artists, too, who run e-mail scams designed to collect money and confidential information from unsuspecting victims. E-mail scams are usually distributed in mass mailings called spam.

◗ **What do I need to know about spam?** The Internet makes it easy and cheap to send out millions of e-mail solicitations. In the United States, the CAN-SPAM Act requires mass-mail messages to be labeled with a valid subject line. Recipients are supposed to be provided with a way to opt out of receiving future messages.

Legitimate merchants and organizations comply with the law when sending product announcements, newsletters, and other messages. Unscrupulous spammers ignore the law and try to disguise their solicitations as messages from your friends, chat room participants, or co-workers (Figure 24).



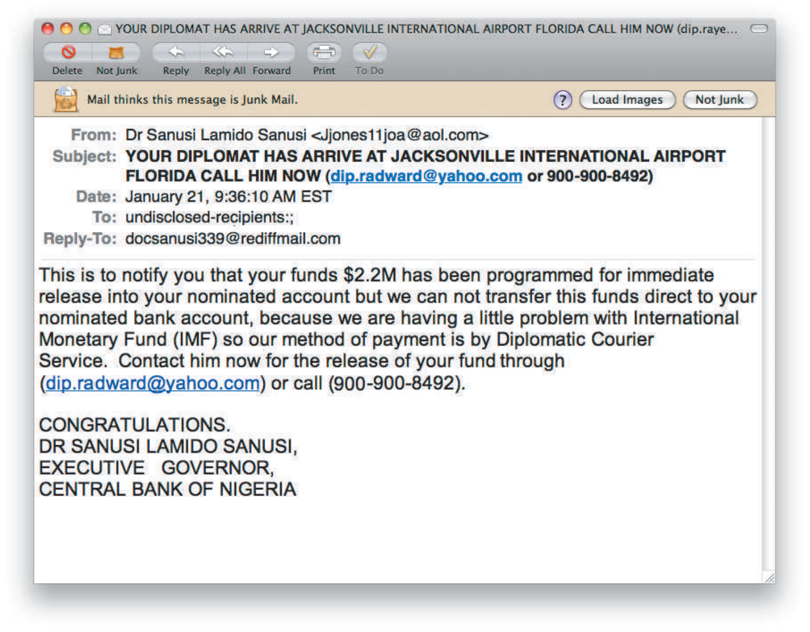
!	🖇	⚑	From	Subject
			Winston	Welcome home
			Maria Robbert	Lunch on Wednesday?
			Jackie1405@aol.com	Party
			Datamation IT Update	[SPAM] Conference Focuses on IT
			FlyCharterAir.com	[SPAM] Charter Specials
			Sonja Crowder	Receive your V1agr&a
			Dwayne Thrman	It's new and successful

FIGURE 24

Some e-mail systems use spam filters to flag suspected spam by adding [SPAM] to the subject line. Spam filters are not perfect, however. Some spam is not flagged and occasionally legitimate mail is mistaken for spam.

◗ **Is spam dangerous?** Some mass mailings contain legitimate information, including daily or weekly newsletters to which you've subscribed. Many mass mailings, however, advertise illegal products. Others are outright scams to get you to download a virus, divulge your bank account numbers, or send in money for products you'll never receive.

Beware of e-mail containing offers that seem just too good to be true. Messages about winning the sweepstakes or pleas for help to transfer money out of Nigeria (Figure 25) are scams to raid your bank account.



YOUR DIPLOMAT HAS ARRIVE AT JACKSONVILLE INTERNATIONAL AIRPORT FLORIDA CALL HIM NOW (dip.raye...
Delete
Not Junk
Reply
Reply All
Forward
Print
To Do
Mail thinks this message is Junk Mail.
?
Load Images
Not Junk

From: Dr Sanusi Lamido Sanusi <Jjones11joa@aol.com>
Subject: **YOUR DIPLOMAT HAS ARRIVE AT JACKSONVILLE INTERNATIONAL AIRPORT FLORIDA CALL HIM NOW (dip.radward@yahoo.com or 900-900-8492)**
Date: January 21, 9:36:10 AM EST
To: undisclosed-recipients:;
Reply-To: docsanusi339@rediffmail.com

This is to notify you that your funds $2.2M has been programmed for immediate release into your nominated account but we can not transfer this funds direct to your nominated bank account, because we are having a little problem with International Monetary Fund (IMF) so our method of payment is by Diplomatic Courier Service. Contact him now for the release of your fund through (dip.radward@yahoo.com) or call (900-900-8492).

CONGRATULATIONS.
DR SANUSI LAMIDO SANUSI,
EXECUTIVE GOVERNOR,
CENTRAL BANK OF NIGERIA

FIGURE 25

Many variations of this African money-transfer fraud—complete with deliberate grammatical errors—have circulated on the Internet for years. Victims who respond to these preposterous e-mails have found their bank accounts raided, their credit ratings destroyed, and their reputations ruined. According to the FBI, some victims have even been kidnapped!

What's phishing? Phishing (pronounced "fishing") is a scam that arrives in your e-mailbox looking like official correspondence from a major company, such as Microsoft, PayPal, eBay, UPS, Yahoo!, or AOL. The e-mail message is actually from an illegitimate source and is designed to trick you into divulging confidential information or downloading a virus.

Links in the e-mail message often lead to a Web site that looks official, where you are asked to enter confidential information such as your credit card number, Social Security number, or bank account number.

The following are examples of phishing scams you should be aware of:

- A message from Microsoft with an attachment that supposedly contains a security update for Microsoft Windows. Downloading the attachment infects your computer with a virus.
- A message that appears to come from PayPal, complete with official-looking logos, that alerts you to a problem with your account. When you click the Billing Center link and enter your account information, it is transmitted to a hacker's computer.
- A message from UPS or the postal service informing you that a package cannot be delivered until you click a link to print or download a mailing label. Clicking the link installs malware on your computer.

How do I avoid e-mail scams? If your e-mail software provides spam filters, you can use them to block some unsolicited mail from your e-mailbox. Spam filters are far from perfect, however, so don't assume everything that gets through is legitimate. Use your judgment before opening any e-mail message or attachment.

Never reply to a message that you suspect to be fraudulent. If you have a question about its legitimacy, check whether it's on a list of known scams. Never click a link provided in an e-mail message to manage any account information. Instead, use your browser to go directly to the company's Web site and access your account as usual. Microsoft never sends updates as attachments. To obtain Microsoft updates, go to the Control Panel and click the Windows Update option.

TRY IT!

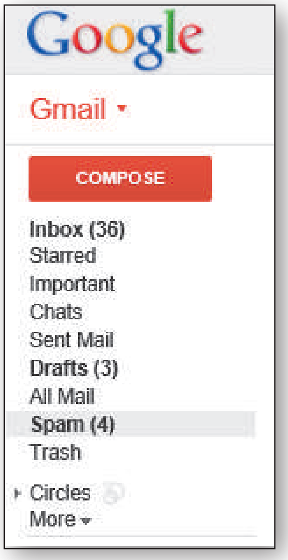
Arm yourself against e-mail scams

1. Start your browser and connect to the site **www.millersmiles.co.uk**. Browse through the list of recent phishing attacks.

2. Open your e-mail software and find out if it includes spam filters. You can usually find this information by clicking **Help** on the menu bar and then typing **spam filter** in the search box.

3. Explore how your e-mail software handles messages that might be spam. Can you create customized spam filters, or does your software have automatic filtering?

4. Spam filters sometimes catch legitimate mail and group it with junk mail. Check your Trash, Spam, or Junk folder. Does it contain any legitimate messages that were automatically labeled as spam and blocked from your Inbox?



PROTECTING YOUR PRIVACY

◗ **How much information about me has been collected online?** Information about you is stored in many places and has the potential to be consolidated by government agencies, private businesses, and criminals. Some databases are legitimate—those maintained by credit bureaus and medical insurance companies, for example. By law, you have the right to ask for a copy of these records and correct any errors you find. Many other databases, such as those maintained at e-commerce sites and those illegally acquired by hackers, are not accessible, and you have no way of checking the data they contain.

◗ **What's the problem with having my personal information in a few databases?** The problem is that many companies share their databases with third parties. Your personal data might start in a single legitimate database, but that data can be sold to a continuous chain of third parties who use it to generate mass mailings that clog up your Inbox with marketing ploys, unwanted newsletters, and promotions for useless products.

◗ **Can I control who collects information about me?** To some extent, you can limit your exposure to future data collection by supplying personal data only when absolutely necessary. When filling out online forms, consider whether you want to or need to provide your real name and address. Avoid providing merchants with your e-mail address even if you're promised a $5 coupon or preferred customer status. A small reward might not be worth the aggravation of an Inbox brimming with spam and e-mail scams. You should also be careful when using public computers (Figure 26).

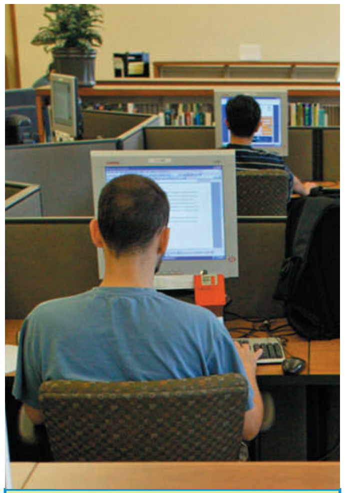
◗ **Can I opt out?** Some mass e-mailings give you a chance to opt out so that you don't receive future messages. Opting out is a controversial practice. On mailings from reputable businesses, clicking an opt-out link might very well discontinue unwanted e-mail messages. However, opting out does not necessarily remove your name from the database, which could be sold to a third party that disregards your opt-out request.

Scammers use opt-out links to look for "live" targets, perhaps in a database that contains lots of fake or outdated e-mail addresses. By clicking one of these opt-out links, you've played right into the hands of unscrupulous hackers—this action lets them know that your e-mail address is valid.

Most experts recommend that you never use opt-out links, but instead go to the sender's Web site and try to opt out from there. If you are tempted to use an opt-out link directly from an e-mail message, carefully examine the link's URL to make sure you'll connect to a legitimate Web site.

FIGURE 26

Using public computers poses security risks from people looking over your shoulder, spyware that collects your keystrokes, and the footprint you leave behind in cookies and temporary Internet pages.



AP Photo/Darren Hauck

To minimize risks when using public computers:

- Be sure to log out from all sites and close all browser windows before quitting.
- Delete cookies and browser history.
- Avoid using public computers for financial transactions such as filing your taxes.
- Reboot the computer before you quit.
- If you're using your own portable apps from a USB drive, make sure your computer is running antivirus software.

TRY IT!

Check your privacy

1. Start your browser and go googling by connecting to **www.google.com**. Enter your name in the Search box. What turns up?

2. Connect to **www.peoplefinders.com**. Enter your name and state of residence. Click the **Search** button. Notice all the information that's offered.

3. Connect to **www.ciadata.com** and scroll down the page to view the kind of information anyone can obtain about you for less than $100.

4. Read about your rights to view credit reports at the Federal Trade Commission site:

www.ftc.gov/bcp/menus/consumer/credit/rights.shtm

SAFE SOCIAL NETWORKING

◗ **What's the risk at sites like Twitter, Facebook, and LinkedIn?** A prolific Twitter user with 650 followers had a nasty surprise one morning. She discovered that private messages she'd sent to specific friends were showing up on her public feed for everyone to see. Although this is an extreme example of how things can go wrong on social networking sites, embarrassing incidents are all too frequent.

The more information you reveal at social networking sites, the more you increase your susceptibility to identity theft, stalking, and other embarrassing moments, such as when a prospective employer happens to see those not-so-flattering photos of you on your spring break.

◗ **How do I stay safe and keep my stuff private when using social networking sites?** The first rule of social networking safety is never share your Social Security number, phone number, or home address. Unfortunately, everyone has access to Web-based tools for finding addresses and phone numbers, so withholding that information provides only a thin security blanket.

Most social networking sites depend on references and friends-of-friends links to establish a trusted circle of contacts. *Trusted* is the key word here. When using social networking sites, make sure you understand what information is being shared with friends, what information is available to strangers on the site, and what data is available publicly to search engines.

Be careful about revealing personal information at social networking sites, blogs, chat rooms, and Twitter. Many online participants are not who they appear to be. Some people are just having fun with fantasy identities, but others are trying to con people by telling hard luck stories and faking illnesses. Resist the temptation to meet face to face with people you've met online without taking precautions, such as taking along a group of friends.

◗ **And what about the site itself?** Social networking sites, like any online business, are always looking for ways to make a profit. Every participant is a valuable commodity in a database that can be used for marketing and research. Before you become a member, read the site's privacy policy to see how your personal data could be used. Remember, however, that privacy policies can change, especially if a site goes out of business and sells its assets.

You should also find out if you can remove your data from a site. Although most sites allow you to deactivate your information, some sites never actually remove your personal information from their databases, leaving it open to misuse in the future.

TRY IT!

Check your social networking sites

1. Log in to any social networking site you use.

2. Locate the site's privacy policy and read it. Are you comfortable with the ways in which the site protects your personal information?

3. If you are not familiar with the site's options for designating who can view your personal data, find out how you can limit its public exposure.

4. Find out if you can delete your data from the site.

ONLINE PRIVACY AND SAFETY GUIDELINES

◗ **What should I do?** Online safety and online privacy are important aspects of computer use today. The average consumer must remain constantly vigilant to detect if his or her personal data has been misused or has fallen into the wrong hands.

Cyberthreats are becoming more troubling. Who would imagine that the webcam at the top of your laptop computer screen could be remotely controlled by hackers to capture video of you without your knowledge?

If you recognize that anything on the Web or in e-mail messages is not necessarily private, you've got the right outlook. You can use the guidelines in Figure 27 to keep track of your personal data and stay safe online.

FIGURE 27

Online Privacy and Safety Guidelines

- Use a password to protect your data in case your computer is stolen.
- Don't leave your digital devices unattended in public places.
- Run antivirus software and keep it updated.
- Install software service packs and security patches as they become available, but make sure they are legitimate.
- Install and activate firewall software, especially if your computer is directly connected to the Internet by an ISDN, DSL, satellite, or cable connection.
- Do not publish or post personal information, such as your physical address, passwords, Social Security number, phone number, or account numbers, on your Web site, in your online resume, in your blog, or in other online documents.
- Be wary of contacts you make in public chat rooms and social networking sites.
- Don't click pop-up ads.
- Install and activate antispyware and ad-blocking software.
- Do not reply to spam.
- Ignore e-mail offers that seem too good to be true.
- Establish a throw-away e-mail account and use it when you have to provide your e-mail address to marketers and other entities whom you don't want to regularly correspond with.
- Make sure you control who has access to the data you post at social networking sites.
- Do not submit data to a social networking site until you've read its privacy policy and have made sure that you can remove your data when you no longer want to participate.
- Avoid using opt-out links in mass mailings unless you are certain the sender is legitimate.
- When using public computers, avoid financial transactions if possible. Make sure you log out from password-protected sites. Delete cookies and Internet history. Reboot the computer at the end of your session.
- Regard e-mail messages as postcards that can be read by anyone, so be careful what you write!
- Cover the webcam on your computer with a sticky note when it is not in use.
- Use the private browsing feature offered by your browser when you don't want to store a record of sites you've visited.
- Activate your browser's Do Not Track feature if you don't want Web sites to collect information about your visit.

QuickCheck

SECTION C

1. Internet security suites usually include antivirus and antispyware tools. True or false? □

2. □ software can block intrusion attempts such as hacker probes.

3. Most Web browsers include settings for blocking pop-up ads. True or false? □

4. E-mail scams are usually distributed in mass mailings called □.

5. Using opt-out links is the most secure and dependable way to reduce the amount of spam you receive. True or false? □

▶ CHECK ANSWERS