Chapter 12
Privacy and Digital Security
Learning Objectives

• Explain the meaning of privacy; discuss the issues surrounding privacy of information

• List and explain the meaning of the OECD Fair Information Practices

• Discuss the issues concerning U.S. privacy: Opt-in/Opt-out, compliance/enforcement, coverage

• List the ways a computer can be compromised

• Explain the security methods used in public key cryptosystems (PKCs)

• Perform simple encryption from cleartext to cipher text and perform the reverse decryption
Privacy: Whose Information Is It?

• Buying a product at a store generates a transaction, which produces information.
  – The date and time of the purchase
  – The product, the cost, and information about other products in the same “market basket.”
  – Is this information connected to a specific customer?
Privacy: Whose Information Is It?

• Buying a product at a store generates a transaction, which produces information.
  – Paying with cash generally ensures anonymity
  – Paying by check, credit card, or debit card
  – Purchasing through mail order or on the Internet
  – Providing a “preferred customer” number
  – Buying a product that must be registered for a service agreement or warranty
How Can the Information Be Used?

• Transaction information is a normal part of conducting business (keeping a record until our check clears)
  – The information belongs, then, to the store
• If the store decides, based on your previous purchases, to send you ads for other items, the store is using the information for the standard business practice of generating more business
How Can the Information Be Used?

• If the store sells your name to others has the information been misused?
  – Those other businesses are only trying to generate more business.
  – Is it misused if the information gets to the newspaper and is published?
  – Has the store broken the law?
Modern Devices and Privacy

• In the past, it was hard for people’s privacy to be violated without their knowledge
• With modern technological devices, people’s privacy can be violated without their knowing it
• Your image and your information deserves “sufficient safeguards against improper circulation”
Controlling the Use of Information

- Who controls the use, if any, of the transaction information?

- There are four main possibilities:
  1. **No Uses.** The information ought to be deleted when the store is finished with it.
  2. **Approval or Opt-in.** The store can use it for other purposes, but only if you approve.
  3. **Objection or Opt-out.** The store can use it for other purposes, but not if you object.
  4. **No Limits.** The information can be used any way the store chooses.
Controlling the Use of Information

• There is also a fifth possibility, *Internal Use*:
  – The store can use the information to conduct business with you (keeping your address, for example), but for no other use
  – It would not include giving or selling your information to another person or business, but it may not require your approval either
Controlling the Use of Information

• If the transaction took place outside the US, the law and standards would place it between (1) and (2) on the spectrum, but very close to (1).

• If the transaction occurred in the US, the law and standards would place it between (3) and (4) on the spectrum, but very close to (4)
Controlling the Use of Information

• Many Americans assume that there is a privacy law that is close to the fifth case, internal use
A Privacy Definition

• Privacy: The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.

• Privacy is difficult to define

• Generally, privacy concerns four aspects of our lives: our bodies, territory, personal information, and communication
A Privacy Definition

• This definition emphasizes first that it is the person who decides the circumstances and the extent to which information is revealed, not anyone else

• Second, it emphasizes that the range of features over which the person controls the information embodies every aspect of the person—themselves, their attitudes, and their behaviors
Enjoying the Benefits of Privacy

• Sometimes we want publicity, sometimes we don’t
• Strong privacy laws insure that we control the dissemination of our information
• The benefits to us personally are obvious
Threats to Privacy

• What are the threats to privacy?
• There are only two basic threats:
  – Government
  – Business
  – (Snooping or gossiping private parties, will be handled by security)
Threats to Privacy

• Historically, the governmental threat of spying on its citizens, worries people the most

• The business threat is a more recent worry

• There are two types of business threats:
  – Surveillance of employees
  – The use of business-related information for other purposes.
Voluntary Disclosure

- In principle, a person can enjoy perfect privacy by simply deciding not to reveal anything to anyone
- It may be in our interest to reveal private information, freely in exchange for real benefits
Benefits of Voluntary Disclosure

- Doctors receive our personal information so they can help us stay healthy.
- Credit card companies get our personal information to check our credit record in exchange for the convenience of paying with a card.
- Employers read our email at work, because we are using the employer’s computer for a job
Benefits of Voluntary Disclosure

• The government may have information on us regarding our parents’ names and birthplaces, our race and ethnicity, etc. for the purpose of enjoying the rights of citizenship.

• How private can we be when we reveal so much about ourselves, our attitudes, and our behavior?
Fair Information Practices

• If people or organizations are free to give or sell the information to anyone else, they are also revealing information about us.

• Our privacy is compromised.

• There must be clear guidelines adopted for handling private information:
OECD Fair Information Practices

• In 1980 the Organization for Economic Cooperation and Development (OECD) developed an eight-point list of privacy principles that became known as the Fair Information Practices

• They have become a widely accepted standard
OECD Fair Information Practices

- The public has an interest in these principles becoming law
- The principles also give a standard that businesses and governments can meet as a “due diligence test” for protecting citizens’ rights of privacy, thereby protecting themselves from criticism or legal action
OECD Fair Information Practices

• An important aspect of the OECD principles is the concept that the data controller (the person or office setting the policies) must interact with individuals about their information, if any, and must be accountable for those policies and actions!
OECD’s Fair Information Practices

• The standard eight-point list of privacy principles.
  – Limited Collection Principle
  – Quality Principle
  – Purpose Principle
  – Use Limitation Principle
  – Security Principle
  – Openness Principle
  – Participation Principle
  – Accountability Principle
<table>
<thead>
<tr>
<th><strong>Limited Collection</strong></th>
<th>There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.</td>
</tr>
<tr>
<td><strong>Quality</strong></td>
<td>The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td><strong>Use Limitation</strong></td>
<td>Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.</td>
</tr>
<tr>
<td><strong>Openness</strong></td>
<td>There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.</td>
</tr>
<tr>
<td><strong>Participation</strong></td>
<td>An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>The data controller should be accountable for complying with these principles.</td>
</tr>
</tbody>
</table>

Table 12.1  
A brief explanation of the OECD’s Fair Information Practices Guidelines
Privacy Worldwide

• Privacy is not enjoyed in much of the world at the OECD standard

• Privacy often comes in conflict with private or governmental interests:
  – Example, the United States has not adopted the OECD principles, possible because many U.S. companies profit by buying and using information in ways that are inconsistent with the OECD principles
Privacy Worldwide

• The Chinese government isn’t going to protect the right to privacy when it denies other basic human rights

• Many non-EU countries have also adopted laws based on OECD principles
  – One provision in the EU Directive requires that data about EU citizens be protected by the standards of the law even when it leaves their country
U.S. Privacy Laws

• The Privacy Act of 1974 limiting the government’s ability to invade people’s privacy
• The U.S. Patriot Act of 2002 (and its reauthorization in 2005) have seriously weakened its protections.
• The US failed to meet the requirements of the EU Directive concerns information stored by businesses
U.S. Privacy Laws

- US Sectoral Laws and Privacy:
  - Electronic Communication Privacy Act of 1986
  - Telephone Consumer Protection Act of 1991
  - Driver’s Privacy Protection Act of 1994
  - Health Insurance Privacy and Accountability Act of 1996

- The sectoral approach provides very strong privacy protections in specific cases
Privacy Principles: Abroad

• There are three weaknesses in the US privacy laws:
  1. Opt-in/Opt-out,
  2. Enforcement,
  3. Coverage
1. Opt-in/Opt-out

- Refers to the approval and objection aspects of privacy
- "Opt-in" means the business cannot use it unless the person opts-in or explicitly allows the new use
- "Opt-out" means the business can use it unless the person explicitly opts-out or denies the new use
- The US the default is opt-out
1. Opt-in/Opt-out

- Privacy principles as far back as 1972 have consistently required opt-in for all changes in use otherwise the person does not control the use of private information. (Opt-in is actually a longer-standing principle than stated)
2. Compliance/ Enforcement

- How do organizations meet their obligations under the principles?
- OECD-subscribing countries have introduced offices to perform the duties of the data controller
- There is no such person/office in the US
- The FTC proposes that U.S. companies “comply voluntarily” as a result of “market pressure”
3. Coverage

• The OECD rules apply to all stored and transmitted information, though exceptions can be made by law
• Countries adopting the Fair Information Practices have everything covered
• Unless the United States passes an explicit law there are almost no constraints. Most information is unprotected
Privacy Success Story

• The Do-Not-Call List
  – In the 1990s households would receive numerous calls from telemarketers trying to sell products
  – The “industry self-policing” mechanism was a little-known system requiring a person either (a) to write a letter to the industry association or (b) to opt-out online by paying a fee using a credit card. People had to pay to stop being harassed!
Privacy Success Story

• The Do-Not-Call List
  – The US government set up the Do-Not-Call List, a central place where people could simply give their phone number to stop telemarketers.
  – Instant success! Ten million households opted-out on the first day of operation.
  – Today more than 175,000,000 are on it.
  – The telemarketing business has largely collapsed.
Cookies

- Cookies are a standard computer science concept originally used by Netscape engineers to connect the identity of a client across a series of independent client/server events.
Cookies

• Imagine this is your bank’s server, and you are a client
• The server is helping many clients at once, and to know who’s who, the server stores a *cookie* of information that uniquely identifies you.
Cookies

- Cookies are exchanged between the client and the server on each transmission of information, allowing the server to know which of the many clients is sending information.

Figure 12.1 Server’s view of the client/server relationship.
Cookies

- Many sites use cookies, even when the interaction is not intended to be as secure as a bank transaction (National Air and Space Museum sent the above)
- The meaning of the fields is unimportant
- The first is the server and the last is the unique information identifying the session
Cookie Abuse

• There is a loophole called a third-party cookie
• A cookie is exchanged between the client and server making the interaction private
• But, if the Web site includes ads on its page, the server may direct it to link to the ad company to deliver the ad
• This new client/server relationship place a cookie on your computer
Cookie Abuse

• All browsers allow users to control how cookies are processed
• You could turn them off, forcing the browser to ask you every time whether you will accept a cookie or not
• Turning off cookies prevents you from being able to bank online
• Simply set your browser’s cookie policy to your own comfort level
Privacy

Tracking
- [x] Tell websites I do not want to be tracked

History
- Firefox will: [Use custom settings for history]
- Always use private browsing mode
- [✓] Remember my browsing history
- [✓] Remember download history
- [✓] Remember search and form history
- [✓] Accept cookies from sites
- [✓] Accept third-party cookies
  - Keep until: [they expire]
- [☐] Clear history when Firefox closes

Location Bar
- When using the location bar, suggest: [Bookmarks]
Tracking

• Tracking is the practice of a Web site automatically sending details about a visit to other content providers
• This is an emerging problem of concern to privacy experts
• The consequences of being tracked are not yet fully understood
• HTTP has a tracking flag telling servers what your tracking preferences are
Do Not Track

<table>
<thead>
<tr>
<th>Table 12.2</th>
<th>Finding the “Do Not Track” Setting In Popular Browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Preferences &gt; Privacy</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Tools (⌘) &gt; Safety &gt; Tracking Protection</td>
</tr>
<tr>
<td>Safari (5.1 and later)</td>
<td>Preferences &gt; Advanced &gt; Click “Show Develop menu in menu bar” &gt; Develop</td>
</tr>
</tbody>
</table>

Notice that Google’s Chrome browser does not support user requests not to track.
Cell Phone Location Tracking

- Another tracking issue is unfolding…it is cell phone location tracking
- Cell phone carriers know the locations where cell phones are used based on the proximity to cell phone towers
- What happens to the location data, which allows a person’s movements to be tracked and archived?
Cell Phone Location Tracking

• Freedom of Information request in 2010
  – Privacy groups launched a request to handle cell phone information
  – For a landline, finding out who a person calls normally requires a warrant
  – The same is currently not true with regard to cell phones
<table>
<thead>
<tr>
<th></th>
<th>Verizon</th>
<th>T-Mobile</th>
<th>AT&amp;T/Cingular</th>
<th>Sprint</th>
<th>Nextel</th>
<th>Virgin Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subscriber Information</strong></td>
<td>Post-paid: 3–5 years</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td><strong>Call detail records</strong></td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Pre-paid: varies</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>2 years</td>
</tr>
<tr>
<td><strong>Cell towers used by phone</strong></td>
<td>1 rolling year</td>
<td>Officially 4–6 months, really a year or more</td>
<td>From July 2008</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>Not retained — obtain through Sprint</td>
</tr>
<tr>
<td><strong>Text message detail</strong></td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Post paid: 5–7 years</td>
<td>18 months (depends on device)</td>
<td>18 months (depends on device)</td>
<td>60–90 days</td>
</tr>
<tr>
<td><strong>Text message content</strong></td>
<td>3–5 days</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>90 days (search warrant required with “text of text” request)</td>
</tr>
<tr>
<td><strong>Pictures</strong></td>
<td>Only if uploaded to Web site (customer can add or delete pictures any time)</td>
<td>Can be stored online and are retained until deleted or service is canceled</td>
<td>Not retained</td>
<td>Contact provider</td>
<td>Contact provider</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>IP session information</strong></td>
<td>1 rolling year</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>IP destination information</strong></td>
<td>90 days</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>Bill copies (post-paid only)</strong></td>
<td>3–5 years, but only last 12 months readily available</td>
<td>Not retained</td>
<td>5–7 years</td>
<td>7 years</td>
<td>7 years</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Payment history (post-paid only)</strong></td>
<td>3–5 years, check copies for 6 months</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Store Surveillance Videos</strong></td>
<td>Typically 30 days</td>
<td>2 weeks</td>
<td>Depends. Most stores carry for 1–2 months</td>
<td>Depends</td>
<td>Depends</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Service Applications</strong></td>
<td>Post-paid: 3–5 years</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Depends</td>
<td>Depends</td>
<td>Not retained</td>
</tr>
</tbody>
</table>
Identity Theft

• The Security Principle of the Fair Information Practices is also important
  – The Security Principle states that those who hold private information are obligated to maintain its privacy against unauthorized access and other hazards

• Americans do not enjoy protection from this principle either
Identity Theft

• How can this private information be used?
• One possibility is identity theft the crime of posing as someone else for fraudulent purposes
• Over 800 identity thefts have been reported from the one instance of private information “viewed” by unauthorized persons!
Managing Your Privacy

• In the United States, protecting your privacy is your job:
  – Adjust your cookie settings in your browser to match your comfort level.
  – Read the privacy statement of any site before you give it information
  – Review the phishing protections given in Chapter 11 to avoid scams
  – Be skeptical. Paranoia isn’t necessary, but skepticism is.
Managing Your Privacy

• In the United States, protecting your privacy is your job:
  – Familiarize yourself with the current assaults on privacy; they’re often announced in the national media, but it’s easy to find them at sites such as EPIC (www.epic.org).
  – Consider writing to your congressperson for U.S. adoption of OECD’s Fair Information Practices.
Digital Security

• Computer security is a topic that is in the news almost daily.
• Remember the long list of “dos and don’ts” for online behavior?
  – Do check with the sender before opening an attachment you’re unsure about
  – Don’t fall for phishing emails
  – And the other’s from Chapter 11?
Koobface…Facebook

• Koobface is a worm that targets social media and the main operating systems
• You receive a message from a “friend” whose computer is infected
• You are directed to a Web site to see a video
• When you reach the Web site the video isn’t streamed, but a message says that first you have to install an updated version of some software
Koobface…Facebook

• Instead, you’re about to get a worm.
• If you take the bait, and install the worm, your machine is infected
• Koobface is gathering your log-in information, like account numbers and passwords
• It also participates with other Koobface-infected computers as part of a botnet to generate income for the “bad” guys
Koobface...Facebook

• In security circles, such compromised, Internet-connected computers are known as **zombies**
Viruses and Worms

• Software viruses and worms are classified as **malware**, or **malicious software**

• Viruses and worms are programs that can clone themselves

• The difference between these two:
  – Viruses hide in other software, and “fire up” when that software is run
  – Worms find your address book or friends list, and send themselves as email or messages to your contacts
Viruses and Worms

• They can also harm your computer:
  – Maliciously harming the information stored on your
  – Using your computer and Internet connection to send spam, or other practices (zombie)
  – Grabbing secure information from your computer such as your passwords, account numbers, etc
  – Propagate and move on to your friends and family
Vectors of Attack

• There are five methods/vectors of virus or worm attack:
  1. Email Attachments
  2. Spoofed Links
  3. Social Engineering
  4. P2P File Sharing
  5. Bluetooth and MMS File Transfers
1. Email Attachments

- The email attachment is actually a program
- By clicking the attachment, the program runs
- The instructions make a copy of the email (program and all) as well as the code.
- They go to the address book on your computer and send the copied email to everyone listed
1. Email Attachments

• The people who send you worms are people who regularly send you email—they just didn’t know they sent it!

• If you are not sure why you got the attachment, email the sender and ask BEFORE opening it.

• Not all attached files are created equal. Some are riskier than others.
# File Extensions and Malware

File extensions can be used by malware to hide its presence and avoid detection by security software. This table lists some file extensions that are commonly used by malware, primarily for Windows OS.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.386</td>
<td>Virtual Device Driver (Windows 386 enhanced mode)</td>
</tr>
<tr>
<td>.3gr</td>
<td>VGA Graphics Driver/configuration files</td>
</tr>
<tr>
<td>.add</td>
<td>Adapter Driver file</td>
</tr>
<tr>
<td>.ade</td>
<td>Microsoft Access project extension</td>
</tr>
<tr>
<td>.asp</td>
<td>Active Server Page</td>
</tr>
<tr>
<td>.bas</td>
<td>Microsoft Visual Basic class module</td>
</tr>
<tr>
<td>.bat</td>
<td>Batch file</td>
</tr>
<tr>
<td>.chm</td>
<td>Compiled HTML Help file</td>
</tr>
<tr>
<td>.cmd</td>
<td>Microsoft Windows NT command script</td>
</tr>
<tr>
<td>.com</td>
<td>Microsoft MS-DOS program</td>
</tr>
<tr>
<td>.cpl</td>
<td>Control Panel extension</td>
</tr>
<tr>
<td>.crt</td>
<td>Security certificate</td>
</tr>
<tr>
<td>.dbx</td>
<td>Database Index</td>
</tr>
<tr>
<td>.dll</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>.exe</td>
<td>Program file</td>
</tr>
<tr>
<td>.fon</td>
<td>Font file</td>
</tr>
<tr>
<td>.hlp</td>
<td>Help file</td>
</tr>
<tr>
<td>.hta</td>
<td>HTML program</td>
</tr>
<tr>
<td>.inf</td>
<td>Setup information</td>
</tr>
<tr>
<td>.ins</td>
<td>Internet Naming Service</td>
</tr>
<tr>
<td>.isp</td>
<td>Internet communication settings</td>
</tr>
<tr>
<td>.js</td>
<td>JavaScript file</td>
</tr>
<tr>
<td>.jse</td>
<td>JavaScript encoded-script file</td>
</tr>
<tr>
<td>.lnk</td>
<td>Shortcut</td>
</tr>
<tr>
<td>.mdb</td>
<td>Microsoft Access program</td>
</tr>
<tr>
<td>.mde</td>
<td>Microsoft Access MDE database</td>
</tr>
<tr>
<td>.msc</td>
<td>Microsoft Common Console document</td>
</tr>
<tr>
<td>.msi</td>
<td>Microsoft Windows Installer package</td>
</tr>
<tr>
<td>.msp</td>
<td>Microsoft Windows Installer patch</td>
</tr>
<tr>
<td>.mst</td>
<td>Microsoft Windows Installer transform</td>
</tr>
<tr>
<td>.ocx</td>
<td>Microsoft Object Linking</td>
</tr>
<tr>
<td>.pcd</td>
<td>Corel Adaptec CD Creator image file</td>
</tr>
<tr>
<td>.pif</td>
<td>Shortcut to MS-DOS program</td>
</tr>
<tr>
<td>.reg</td>
<td>Registration entries</td>
</tr>
<tr>
<td>.scr</td>
<td>Screen saver</td>
</tr>
<tr>
<td>.sct</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.shb</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.shs</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.url</td>
<td>Internet shortcut</td>
</tr>
<tr>
<td>.vb</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vbe</td>
<td>Visual Basic Script-encoded file</td>
</tr>
<tr>
<td>.vbs</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vxd</td>
<td>Microsoft Windows Virtual Device Driver</td>
</tr>
<tr>
<td>.wsc</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.wsf</td>
<td>Windows Script File</td>
</tr>
<tr>
<td>.wsh</td>
<td>Windows Script Host Settings file</td>
</tr>
</tbody>
</table>
2. Spoofed Links

- Hyperlinks are specified on Web pages by the following form:
  \(<a href="http://site.com/puter/goes2">Site U C Underlined In Blue</a>\)

- There are two parts:
  - One is the part the computer uses (the actual site)
  - The other part is the text you see
2. Spoofed Links

• To be clear: It’s fine to click links as follows:
  – When the site containing the link can be trusted
  – When the site containing the link was found in a Google or Bing search
  – When you typed the URL yourself
• Those cases are always safe. Other situations can be riskier.
3. Social Engineering

- This is the Koobface case.
- It induces you to see a video, which you could recognize as a trick when you’re asked to upgrade Flash
- There are other ways in which the site can do harm, and just visiting is enough.
4. P2P File Sharing

- Peer-to-peer (P2P) file sharing is a popular way to share files.
- While it can be convenient, it can also be quite risky.

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Files are transferred containing infected software or spyware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior to Avoid</td>
<td>Installing software from unreliable sites</td>
</tr>
<tr>
<td>Result</td>
<td>Computer is seriously compromised, and often personal information such as passwords and account numbers is lost</td>
</tr>
<tr>
<td>Protect Yourself</td>
<td>Avoid P2P file sharing from unreliable sites; protect your computer with an up-to-date firewall and virus protection software</td>
</tr>
</tbody>
</table>
4. P2P File Sharing

• P2P refers to the relationship between computers that are communicating over the Internet

• Each of the computers—yours and someone else’s—is a “file server” for the other

• Predators can set up “bait” such as pirated music to attract users, and then to become a peer, you install their (infected) software
5. Bluetooth & MMS File Transfers

- Smart phones and other hand-held devices are now as susceptible to malware as laptops and desktops.
- An attack sends infected files with extensions like .jpg or .mp3, which should be fine. When “played” they ask to install software.
Plan of Action

- As more technology is created, more ways to abuse it will be developed
- So, what to do?
- Here’s a brief plan of action:
  1. Installing protective systems
  2. Tuning the installed protections
  3. Behaving to avoid difficulties
1. Installing Protective Systems

• The first rule of security is to set up a barrier:
  – **Firewall.** A firewall is a barrier between two networks, or in the “personal” firewall case, between the Internet and your computer.
  – Generally, firewalls filter network traffic that is trying to cross the barrier.
  – It allows through only those messages with a destination in the protected area.
1. Installing Protective Systems

• The first rule of security is to set up a barrier:
  – Virus Protection. Anti-virus software must be operating at all
  – Install virus protection software
  – Keep it current!
1. Installing Protective Systems

- The first rule of security is to set up a barrier:
  - **Anti-Spyware.** Spyware is software that snoops on your private information, causes advertising pop-ups, and monitors your Internet behavior for advertising purposes.
  - Anti-spyware protection is often bundled with anti-virus software.
  - Find a package that includes both!
1. Installing Protective Systems

• The first rule of security is to set up a barrier:

  – **Rootkit Detection.** A rootkit is malware that directly manipulates the operating system data structures to hide its presence.

  – Rootkits have become a much more serious problem in recent years for those visiting certain sites

  – Install a rootkit detector
2. Tuning the installed protections

• Stay Up-to-Date
  – Recent versions of Windows have automatic OS updates for fixing or delivering security “patches”
  – This process must be allowed; browsers also depend for their effectiveness on automatic updates.
2. Tuning the installed protections

- Browser Sense.
  - The browser is the main entry point for external information
  - Its security is critical
  - Get one that is sound and responsive in the face of new security threats
  - Do not use the security-plagued older versions
2. Tuning the installed protections

• **Emailer Sense**
  – Use an email program, such as Thunderbird, that is responsive to security issues

• **Spam Filter**
  – Periodically check your spam quarantine to be sure that you are not missing emails
  – Adjust the threshold if spam is still getting through
2. Tuning the installed protections

• Wi-Fi Protection
  – A computer is using a wireless connection to the Internet, is receiving and sending all of its information by radio broadcast
  – Any computer can listen to it!
  – Use encrypted networks!
  – When setting up a wireless network, use Wi-Fi Protected Access (WPA or WPA2) encryption
2. Tuning the installed protections

• Disable File Sharing
  – Though convenient, it is a risky to leave it running in large wireless network situations
  – Leave it turned off until you absolutely need it,
  – Turn it off as soon as you’re done
3. Behaving to Avoid Difficulties

• Download Cautions
  – The greatest security risk to your computer is installing compromised software
  – Install only good software
  – For shareware trust sites like SourceForge and ZDNet,V3
3. Behaving to Avoid Difficulties

- Careful with Attachments
  - Only open email attachments when you are expecting them
  - Contact the sender to find out what the attachment is about
3. Behaving to Avoid Difficulties

• Password Protection
  – Adopt a set of passwords
  – Use strong passwords for sensitive uses
  – Password-protect your computer
Encryption

• Information that is recoded to hide its true meaning uses *encryption*

• A major component of encryption is the *key*

• They come in two forms:
  – Private
  – Public
Encryption

• The key is a “magic number” used to transform text into gibberish (cipher text)
• Both the sender and receiver must agree on the key
• The process of sending an encrypted message is a five-step algorithm
Encryption

• 5-Step Encryption algorithm:
  1. The sender breaks the message into groups of letters
  2. “Multiply” each group of letters times the key
  3. Send the “products”/results from the “multiplications” to the receiver
  4. The receiver “divides” the “products” by the key to recreate the groups
  5. Assemble the groups into the message
Encryption

- This works because the math works
- The “reversibility” of encryption makes them 2-way ciphers
  - Only the sender and receiver know the key, making the products useless numbers
- This is a secure communication
- The technique just explained is called private key encryption, or symmetric-key cryptography
Encryption Example

1. Break into groups, say, ME ET b@ b9. (The blank is a letter, too; I have coded as b.) These letters are, when the ASCII is converted to decimal: 7769 6984 3264 3257.
2. “Multiply” each group by the key, 13:
   7769 × 13 = 100997
   6984 × 13 = 090792
   3264 × 13 = 042432
   3257 × 13 = 042341
   (The “first zeroes” make all number six digits.)
3. Send the “products” 100997 090792 042432 042341 to the receiver.
4. The receiver “divides” by the key, 13:
   100997/13 = 7769
   090792/13 = 6984
   042432/13 = 3264
   042341/13 = 3257
   producing numbers mapped by ASCII: ME ET b@ b9
5. Reassembling the message, MEET @ 9.
Cryptosystem Schematic Diagram

**Figure 12.4** Schematic diagram of a cryptosystem. Using a key $K_{SR}$ known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext. In the middle, where the content is exposed and can be snooped, it is unintelligible.
Private Key Encryption

- Real encryption systems use much longer blocks (hundreds of letters) and larger keys
- Multiplication, division are not the only operations that can be used for encryption
- All that is needed is for an operation to have an inverse (divide is the inverse of multiply)
Private Key Encryption

• Private key encryption works very well
• Only one small problem: The sender and receiver have to agree on the key, which means they need to communicate somehow
• Usually, they meet face-to-face (they can’t email, they don’t have a key yet!)
Public Key Encryption

• To avoid that face-to-face meeting, publish the key!
• Use public key encryption
  – Two special prime numbers multiplied together
Public Key Encryption Steps

• After, the receiver publishes the special key, $K$, the following happens:
  1. The sender breaks up the message into blocks as before
  2. The sender cubes each block, and divides by $K$, keeping only the remainders
  3. The remainders are transmitted
Public Key Encryption Steps

- After, the *receiver* publishes the special key, $K$, the following happens:
  4. The receiver raises each remainder to a high power determined by the prime numbers and known only to him.
  5. The receiver divides by $K$, too, and saves only the remainders, which are the original blocks.
  6. The receiver assembles the message.
How Do We Know It Works?

• $K$, the magic public key, is just two prime numbers, $p$ and $q$, multiplied together.
• It is possible to figure out those two numbers from the published key in theory.
• This process, called factoring, is tough if the numbers $p$ and $q$ are large (60 digits apiece).
• It is impractical to factor them no matter how powerful the computer!
Redundancy Is Very, Very, Very Good

• Take precautions with your technology!
• Businesses archive files daily and store these backups off-site
• They have a system recovery team to clean up after a disaster strikes
• They also have system redundancy—multiple computers performing the same work, so that when one fails, another is up and running
Fault Recovery Program

• Full backup
  – A complete copy of everything written on the system as of a date and time

• Partial backup
  – Changes since the last full (or partial) backup are saved
  – “Changes” means to keep a copy of any files or folders that have been created or modified
Fault Recovery Program

- After a disaster, recover by installing the last full backup copy
- Then make the changes saved in the partial backups in order
- Continue with each partial backup until the most recent
- That’s as close to “full recovery” as possible
Backing Up a Personal Computer

• First, you need a place to keep the copy, and you need software to make the copy.
• The two easiest “places” to keep the copy are on an external hard disk or “in the cloud”
• The “cloud” company’s computers store the information for you and they take responsibility of keeping it available to you
Backups

• You don’t have to back up the following:
  – Information that can be recreated from some permanent source
  – Information that was saved but that has not changed
  – Information that you don’t care about
Recovering Deleted Information

• If you accidentally delete important files, file restoration (that backup copy!) is great!
• Backups can save evidence of crimes or inappropriate behavior (digital copies of files are easy to create and store)
• Two copies of email are produced immediately when the **Send button is clicked**—one in the sent mail directory, and one somewhere else
Summary

• Revealing personal information can be beneficial, so the people and organizations that receive the information must keep it private. The guidelines for keeping data private have been created by several organizations, including the Organization for Economic Cooperation and Development (OECD).
Summary

• Guidelines often conflict with the interests of business and government, so some countries like the United States have not adopted them. Because the United States takes a sectoral approach to privacy, adopting laws only for specific business sectors or practices, much of the information collected on its citizens is not protected by OECD standards.
Summary

• The shortcomings for privacy conditions in the United States are Opt-in/Opt-out, compliance/enforcement, and coverage.

• The “third-party cookie” loophole allows companies to gather information; identity theft is an unresolved problem. The best way to manage privacy in the Information Age is to have OECD-grade privacy laws.
Summary

• Public key cryptography (PKC) is a straightforward idea built on familiar concepts.

• Computer scientists have not yet proved the invincibility of the RSA scheme, but it can be “made more secure” simply by increasing the size of the key.
Summary

• Viruses and worms cause damage. We can reduce the chance of infection by installing and running anti-virus software. We must be aware of hoaxes and phishing scams.

• We can implement a plan of action to ensure that our personal computers remain private and secure.
Summary

• There are two key features of encryption: private key and public key techniques.
• Backing up computer files is an essential safeguard. It ensures that your files will survive for a long time, even if you don’t want them to.