Computer Security and Safety, Ethics, and Privacy

System Failure

- A *system failure* is the prolonged malfunction of a computer.
- It can cause loss of hardware, software, data, or information.
- One of the most common causes is electrical power variation, including noise, undervoltage, and overvoltage.

System Failure

- **Noise** is any unwanted signal, usually varying quickly, that is mixed with the normal voltage entering the computer.
- An **undervoltage** occurs when the electrical supply drops (usually more than 5%)
  - A *brownout* is a prolonged (>1 minute) undervoltage.
  - A *blackout* is a complete power failure.
- An **overvoltage**, or **power surge**, occurs when the incoming electrical power increases (usually more than 5%)
  - A *spike* is an increase in power for less than one millisecond.

Safeguards against System Failure

- A **surge protector**, also called a *surge suppressor*, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment.
- An **uninterruptible power supply (UPS)** is a device that contains surge protection circuits and one or more batteries that can provide power during a temporary or permanent loss of power.

Safeguards against System Failure

- A *standby UPS*, sometimes called an *offline UPS*, switches to battery power when a problem occurs in the power line.
  - This gives users from 10 to 50 minutes of use, enough to save work and properly shut down.
- An *online UPS* always runs off of battery for continuous protection, and is more expensive.

Safeguards against System Failure

- A *fault-tolerant computer* has duplicate components so that it can continue to operate when one of its main components fail.
  - Ex. Airline reservation systems and communications networks.

Backing Up – The Ultimate Safeguard

- To prevent against data loss caused by system failure or hardware/software/information theft, users should back up files regularly.
- A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed.
- To **back up** a file means to make a copy of it.
- In the case of system failure or corrupted files, you **restore** the files by copying the backed up files to their original location.

Backing Up – The Ultimate Safeguard

- Keep backup copies in a fireproof and heatproof safe or vault, or *offsite*, which means in a location separate from the computer site.
- A *full backup* copies all of the files in the computer.
- With a *selective backup* users choose which folders and files to include.

Backing Up – The Ultimate Safeguard

- Some users implement a *three-generation backup* policy for a full backup and selective backup.
- The *grandparent* is the oldest copy of the file.
- The *parent* is the second oldest copy of the file.
- The *child* is the most recent copy of the file.

Wireless Security

- Wireless networks are more common than ever, at homes, schools, and businesses.
- However, along with the conveniences, it also poses additional security risks.
  - About 80% of wireless networks have no security protection.
- *War driving*, or *access point mapping*, is where individuals attempt to detect wireless networks through their mobile devices while driving through areas expected to have wireless networks.
- *War flying* uses airplanes instead of vehicles to detect unsecured wireless networks.

Wireless Security

- In addition to firewalls, some safeguards that improve the security of wireless networks are:
  - A wireless access point (WAP) should not broadcast its *SSID* (service set identifier), which is the network's name.
  - *Wi-Fi Protected Access (WPA)* is a security standard that authenticates network users and provides advanced encryption.
  - An *802.11i* network, sometimes called WPA2, is the most recent security standard and uses even more encryption.

Health Concerns of Computer Use

- Users, being the key component of information systems, must be protected.

Computers and Health Risks

- A **repetitive strain injury (RSI)** is an injury or disorder of the muscles, nerves, tendons, ligaments, and joints.
- Computer-related RSIs include
  - *Tendonitis*: an inflammation of a tendon due to repeated motion or stress on that tendon.
  - *Carpal tunnel syndrome (CTS)*: an inflammation of the nerve that connects the forearm to the palm of the wrist.

Computers and Health Risks

- Precautions can be taken to prevent these types of injuries.
  - Take frequent breaks.
  - Proper keyboard and mouse usage.
  - Minimize the amount of times you switch between the mouse and keyboard.

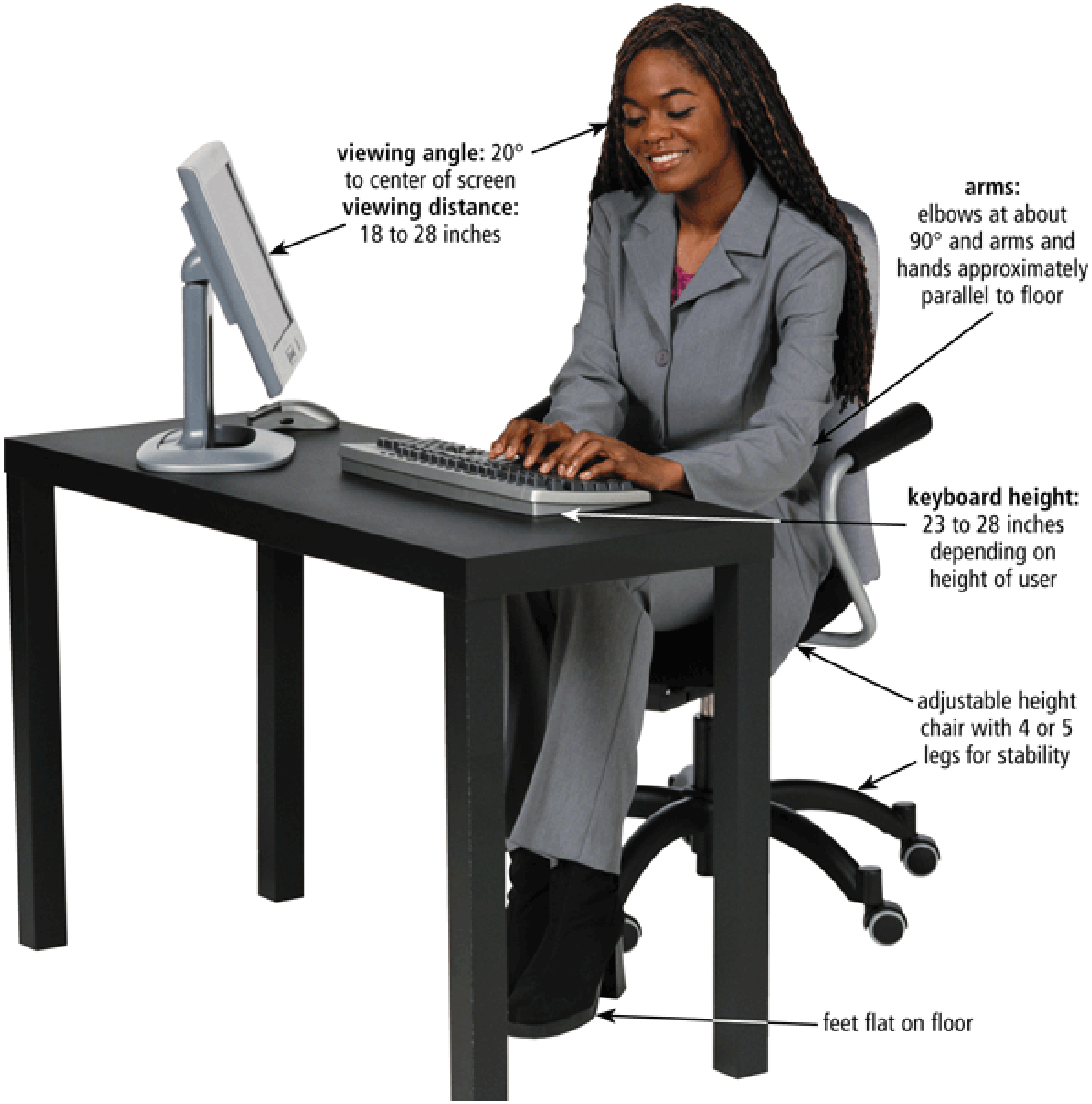
Computers and Health Risks

- Another type of health-related condition is **computer vision syndrome** (CVS), which includes symptoms of sore, tired burning, itching, or dry eyes; blurred or double vision; distance blurred vision; headache or sore neck…

Ergonomics and Workplace Design

- *Ergonomics* is an applied science devoted to incorporating comfort, efficiency, and safety into the design of items in the workplace.

Ergonomics and Workplace Design



Computer Addiction

- **Computer addiction** occurs when the computer consumes someone’s entire social life.
  - Craves computer time
  - Overjoyed when at the computer
  - Unable to stop computer activity
  - Irritable when not at the computer
  - Neglects family and friends
  - Problems at work or school

Ethics and Society

- **Computer ethics** are the moral guidelines that govern the use of computers and information systems.
  - Unauthorized use of computers and networks
  - Software theft (piracy)
  - Information accuracy
  - Intellectual property rights
  - Codes of conduct
  - Information privacy
  - Green computing

Information Accuracy

- Do not assume that because the information is on the Web that it is correct.
- Be aware of the organization providing access to the information may not be the center of information.
- Using graphics equipment and software, users can easily digitize photos and modify them.

Intellectual Property Rights

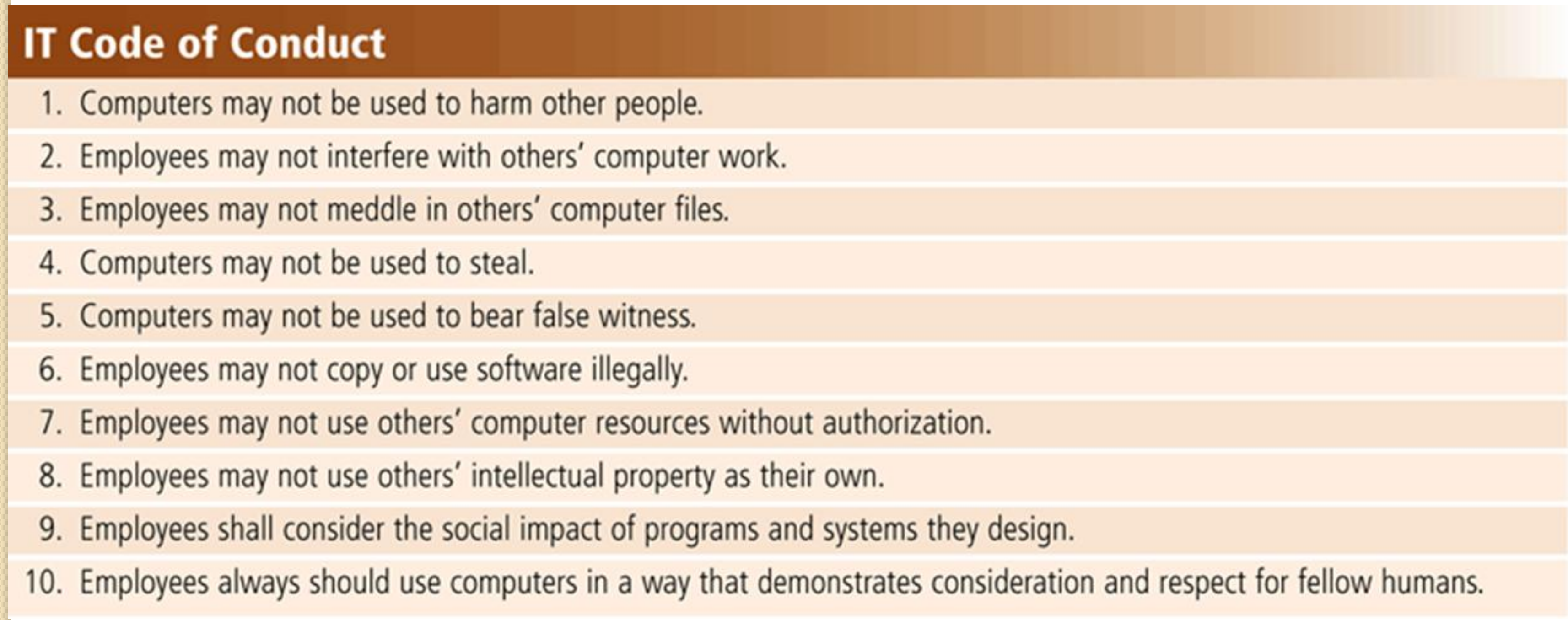
- *Intellectual property* refers to unique and original works such as ideas, inventions, art, writings, processes, company and product names, and logos.
- **Intellectual property rights** are the rights to which creators are entitled for their work.
- A **copyright** gives authors and artists exclusive rights to duplicate, publish, and sell their materials.
  - Piracy is a common infringement.

Intellectual Property Rights

- The vague definition of copyright is subject to widespread interpretation and raises many questions.
- These issues with copyright law led to the development of *digital rights management (DRM)*, a strategy designed to prove illegal distribution of movies, music, and other digital content.

Codes of Conduct

- An IT **code of conduct** is a written guideline that helps determine whether a specific computer action is ethical or unethical.



IT Code of Conduct

1. Computers may not be used to harm other people.
2. Employees may not interfere with others' computer work.
3. Employees may not meddle in others' computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' computer resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

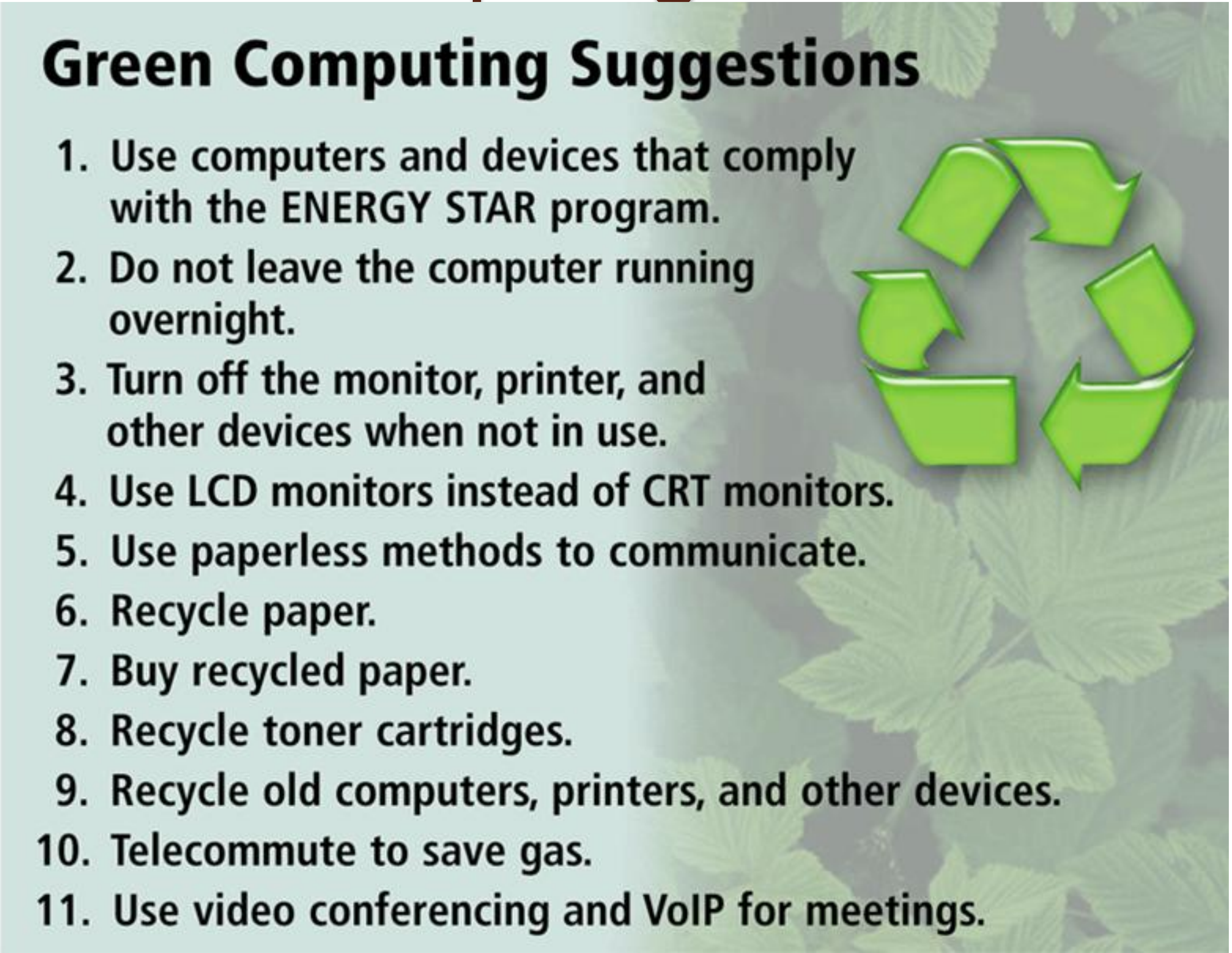
Green Computing

- **Green computing** involves reducing the electricity and environmental waste while using a computer.
- The U.S. Department of Energy and Environmental Protection Agency developed the *ENERGY STAR program* to help reduce the electricity used by computers and related devices/
- It encourages manufacturers to create energy-efficient devices that require little power when they are not in use.

Green Computing

- Some organizations continually review their *power usage effectiveness* (PUE), which is a ratio that measures how much power enters the computer facility against the power required to run the computers.
- Obsolete computers should not be stored since they contain toxic materials and elements such as lead, mercury, and flame retardants.
- Recycling and refurbishing old equipment are much safer alternatives.

Green Computing



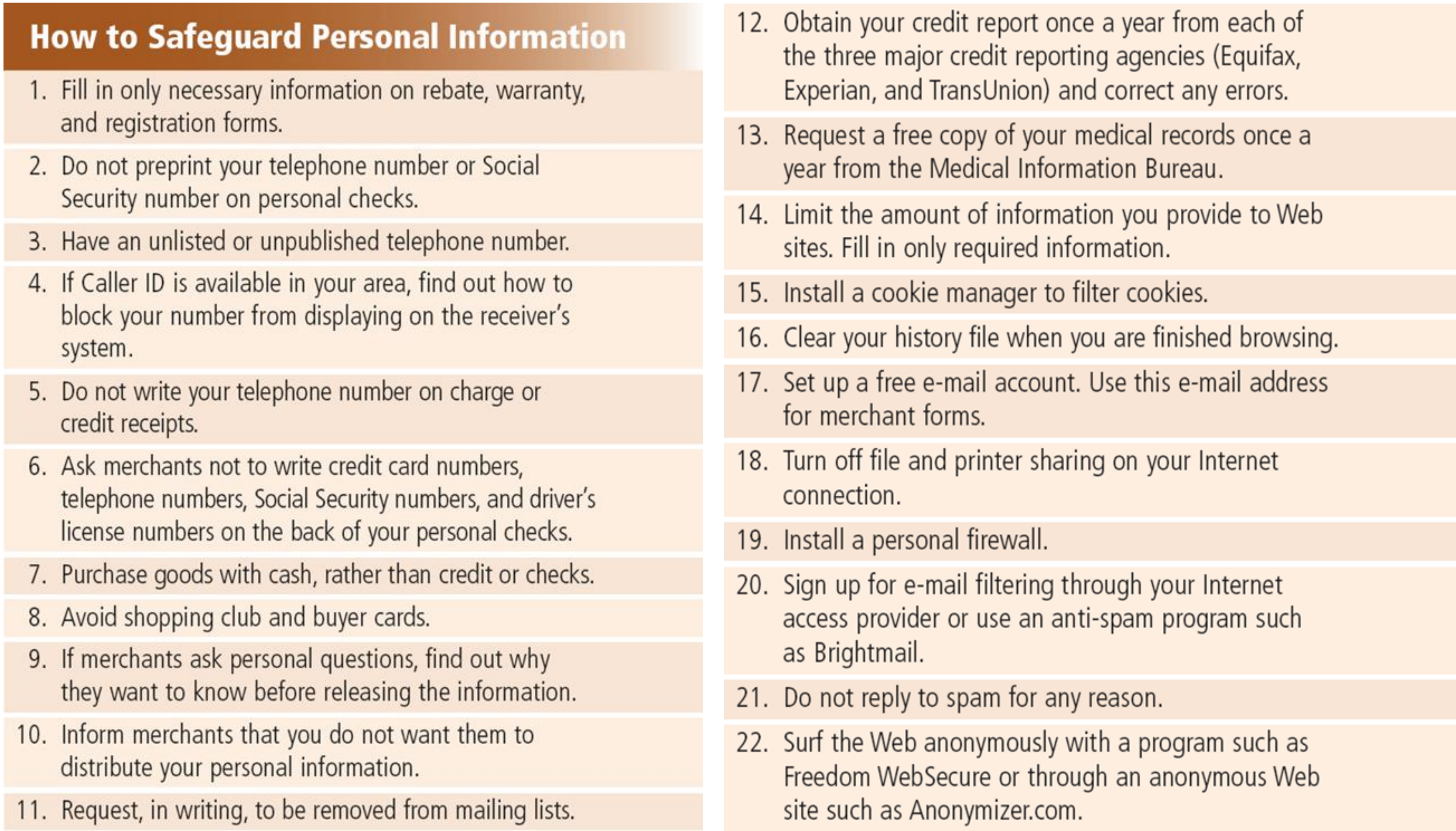
Green Computing Suggestions

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use LCD monitors instead of CRT monitors.
5. Use paperless methods to communicate.
6. Recycle paper.
7. Buy recycled paper.
8. Recycle toner cartridges.
9. Recycle old computers, printers, and other devices.
10. Telecommute to save gas.
11. Use video conferencing and VoIP for meetings.

Information Privacy

- **Information Privacy** refers to the right of individuals and companies to deny or restrict the collection and use of information about them.
- Some companies and individuals collect and use information without your authorization.

Information Privacy



How to Safeguard Personal Information

1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your telephone number or Social Security number on personal checks.
3. Have an unlisted or unpublished telephone number.
4. If Caller ID is available in your area, find out how to block your number from displaying on the receiver's system.
5. Do not write your telephone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, telephone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.
10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to Web sites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free e-mail account. Use this e-mail address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for e-mail filtering through your Internet access provider or use an anti-spam program such as Brightmail.
21. Do not reply to spam for any reason.
22. Surf the Web anonymously with a program such as Freedom WebSecure or through an anonymous Web site such as Anonymizer.com.

Electronic Profiles

- When you fill out a form (magazine subscription, product warranty registration, etc.) the merchant enters your data into a database.
- Merchants then sell the contents of their databases to national marketing firms and Internet advertising firms.
- Direct marketing supports say that using information in this way lowers overall selling costs, thus product prices.
- Critics contend that the information reveals more about an individual than anyone has a right to know.

Cookies

- A **cookie** is a small text file that a Web server stores on your computer and can contain data about you, such as your user name and viewing preferences.
  - Personalized websites
  - Remember login information
  - Online shopping uses a *session cookie* to keep track of the shopping cart for a limited time.
  - How often users visit a site
  - Targeted advertisements

Spam

- **Spam** is an unsolicited e-mail message or newsgroup posting sent to many recipients or newsgroups at once.
- It is Internet junk mail that ranges from selling a product, promoting a business, and advertising offensive material.
- *Spim* is spam sent over an instant message.
- *Spit* is spam sent over VoIP.

Spam

- Spam can be reduced using:
  - **E-mail filtering**: a service that blocks e-mail messages from designated sources and collects them for viewing at a later time, if desired.
  - **Anti-spam program**: a program that attempts to remove spam before it reaches your inbox.
    - Disadvantage: Sometimes they remove valid e-mails.

Phishing

- **Phishing** is a scam in which a perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information.
- A *phishing filter* is a program that warns or blocks you from potentially fraudulent or suspicious Web sites.
- **Pharming** is a scam, similar to phishing, where a perpetrator attempts to obtain your personal financial information via spoofing.
- *Clickjacking* is another similar scam where a link on a website contains a malicious program.
  - Ex. Getting redirected to a phony Web site.

Spyware and Adware

- *Spyware* is a program placed on a computer without the user's knowledge that secretly collects information about the user.
- *Adware* is a program that displays an online advertisement in a banner or pop-up window on Web pages.
- A *Web bug* is hidden on Web pages or in e-mail message in the form of graphical images, which link to a cookie stored on the hard disk.

Privacy Laws

- Information collected and stored should be limited to what is necessary.
- Provisions should be made to restrict access to the data to those employees within the organization.
- Personal information should be release outside the organization only when the person agrees to its disclosure.
- Individuals should know that the data is being collected and have opportunity to determine the accuracy.

Privacy Laws

- One law with an apparent legal loophole is the 1970 **Fair Credit Reporting Act** which limits the rights of others viewing a credit report to only those with a legitimate business need.
  - The problem is 'legitimate business need' is not defined, causing anyone to claim a legitimate business need to gain access to your credit report.

Social Engineering

- **Social engineering** is defined as gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others.
- Social engineers trick their victims into revealing confidential information, such as usernames and passwords, under false pretenses.
- Social engineers also obtain information from those who do not destroy or conceal information properly.

Employee Monitoring

- **Employee monitoring** involves the use of computers to observe, record, and review an employee's use of a computer, including communications such as e-mail messages, keyboard activity, and Web sites visited.
  - It is legal for employers to use these programs.
- One survey discovered that more than 73% of companies search and/or read employee files, voice mail, e-mail, and Web communication.

Content Filtering

- **Content filtering** is the process of restricting access to certain material on the web.
- Many businesses use content filtering to limit employees' Web access.
- One approach is through a rating system from the *Internet Content Rating Association (ICRA)*, which is similar to those used for movies and videos.

Content Filtering

- Major Web sites use the rating system from the ICRA.
  - If a Web site goes beyond the rating limits set in the browser, a user cannot access the site.
- **Web filtering software** is a program that restricts access to specified Web sites.
  - Some also filter sites that use specific words, and others allow you to filter e-mail messages, chat rooms, and programs.