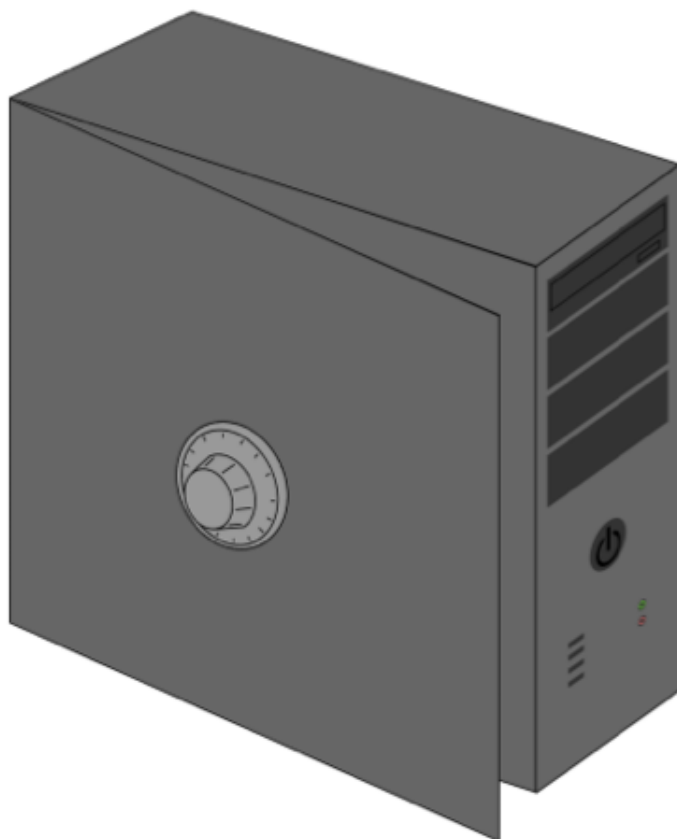


# Demystifying Technology

---



## Learning Outcomes

The Demystifying Technology workshops are designed to promote the following learning outcomes:

- Students will be able to describe the major building blocks of computer hardware, software, and networks in order to develop a basic understanding of how digital technologies work.
- Students will be able to recognize the key similarities and differences between different types of computers in order to more effectively evaluate and select the right digital tool for a task.
- Students will perform essential troubleshooting skills in order to improve their ability to maintain, upgrade, and repair their own digital technologies.
- Students will be able to identify different social influences that become fixed in technical objects in order to guide future selection of digital tools that might more closely align with and support community values and goals.

## International Society for Technology in Education (ISTE) Standards for Students

1. **Creativity and innovation** – Students demonstrate creative thinking, construct knowledge, and develop innovative products and processes using technology.
2. **Communication and collaboration** – Students use digital media and environments to communicate and work collaboratively, including at a distance, to support individual learning and contribute to the learning of others.
3. **Research and information fluency** – Students apply digital tools to gather, evaluate, and use information.
4. **Critical thinking, problem solving, and decision making** – Students use critical thinking skills to plan and conduct research, manage projects, solve problems, and make informed decisions using appropriate digital tools and resources.
5. **Digital citizenship** – Students understand human, cultural, and societal issues related to technology and practice legal and ethical behavior
6. **Technology operations and concepts** – Students demonstrate a sound understanding of technology concepts, systems, and operations

Standards•S © 2007 International Society for Technology in Education.

ISTE® is a registered trademark of the International Society for Technology in Education

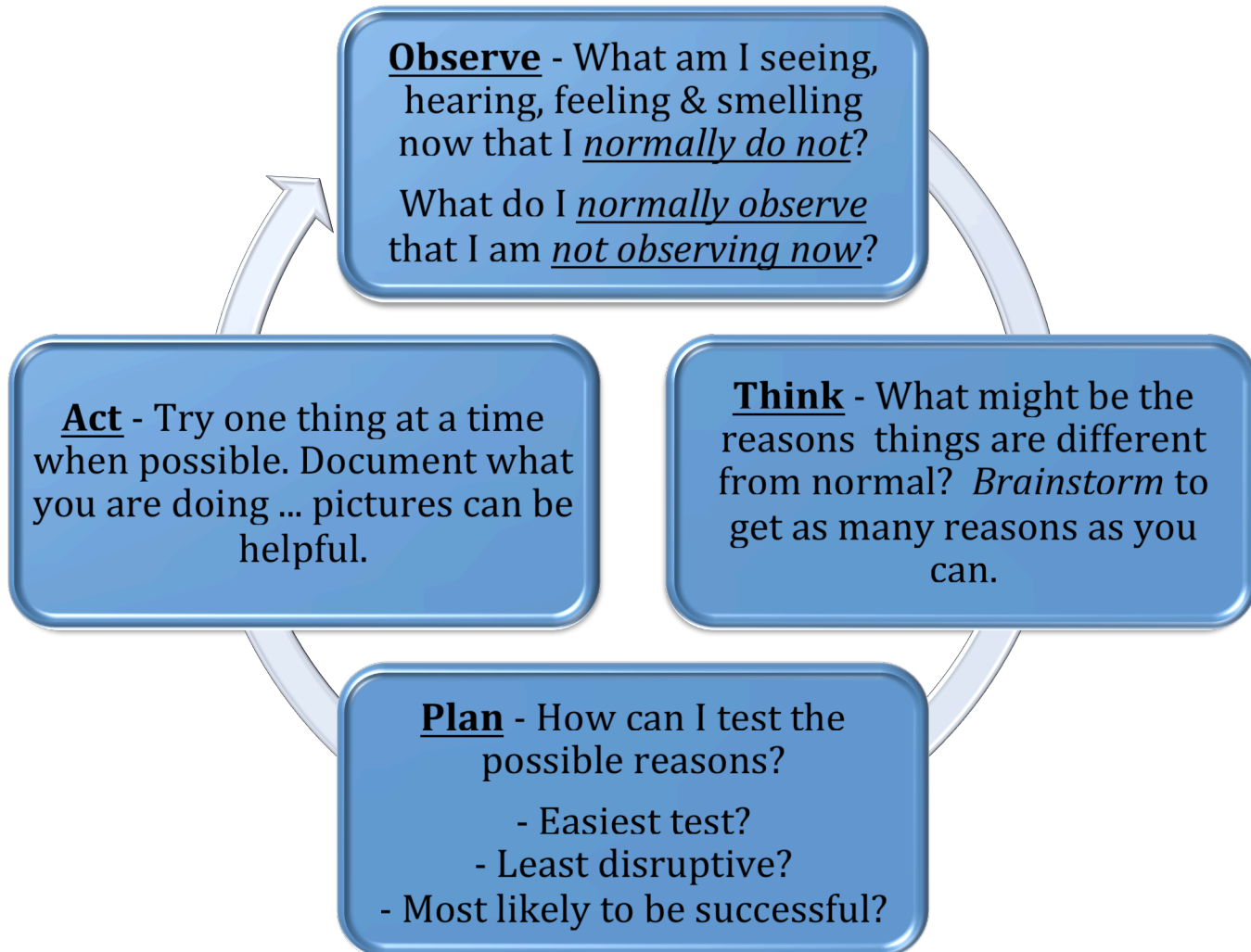
## Computational Thinking = Critical Thinking + Digital Technologies

Computational thinking is a way of problem-solving that takes advantage of opportunities made possible through access to digital technology tools, and includes the following characteristics:

- Formulating problems in a way that enables us to use a computer and other tools to help solve them
- Logically organizing and analyzing data
- Representing data through abstractions such as models and simulations
- Automating solutions through a series of ordered steps (algorithmic thinking)
- Identifying, analyzing, and implementing possible solutions with the goal of achieving the most efficient and effective combination of steps and resources
- Generalizing and transferring this problem-solving process to a wide variety of problems

Computer Science Teachers Association (CSTA) & ISTE, 2011

## Troubleshooting basics



### **Knowing normal:**

1. Try to observe and document normal operations before a problem occurs.
2. Compare your system or network to others that are similar.
3. Use your manual when available on hand or online to determine normal.
4. Experience helps. Each activity is a learning opportunity.

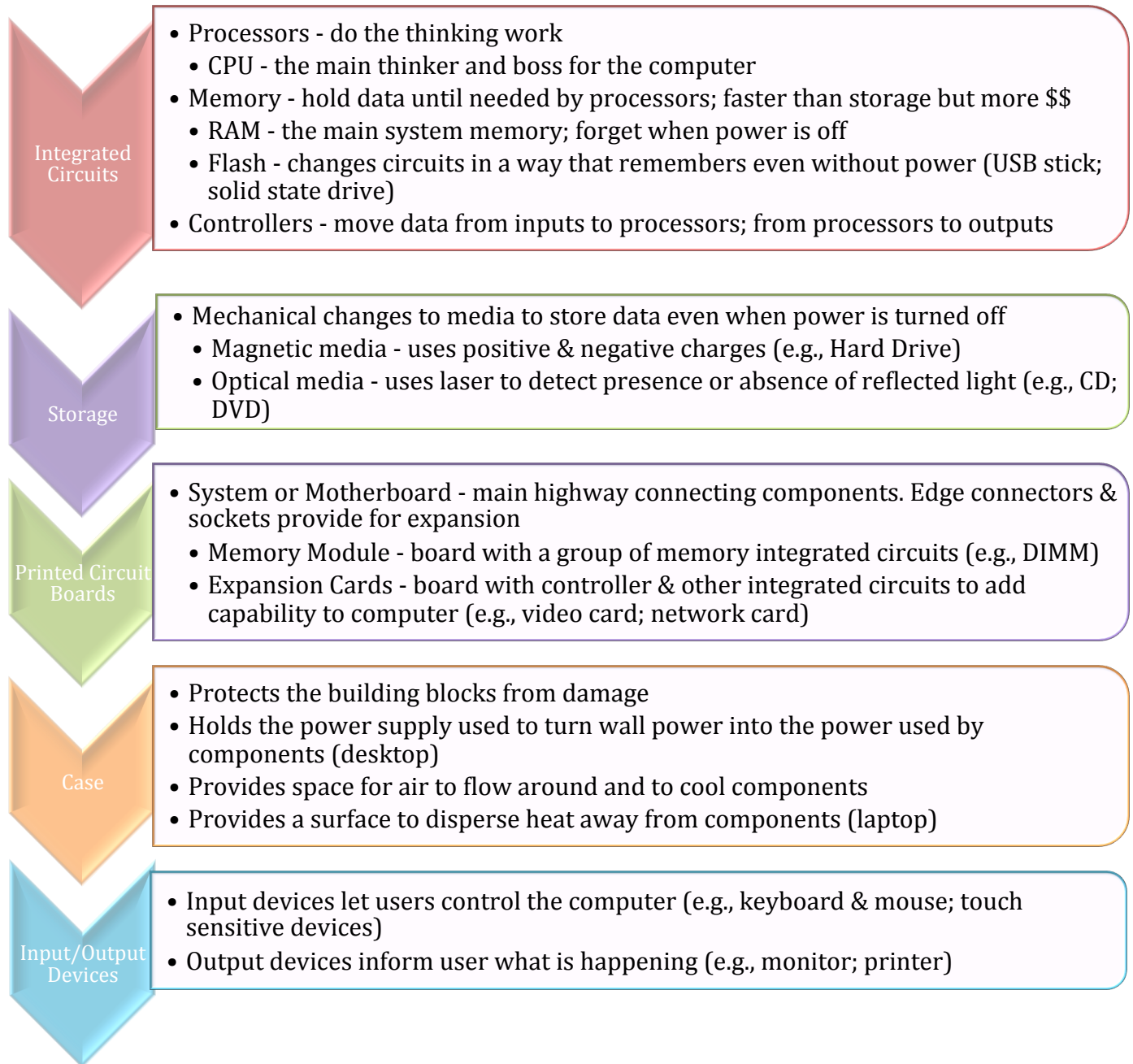
# Collaborative Discussion Framework

Developed by and for use at Kenwood Elementary School, Champaign, IL

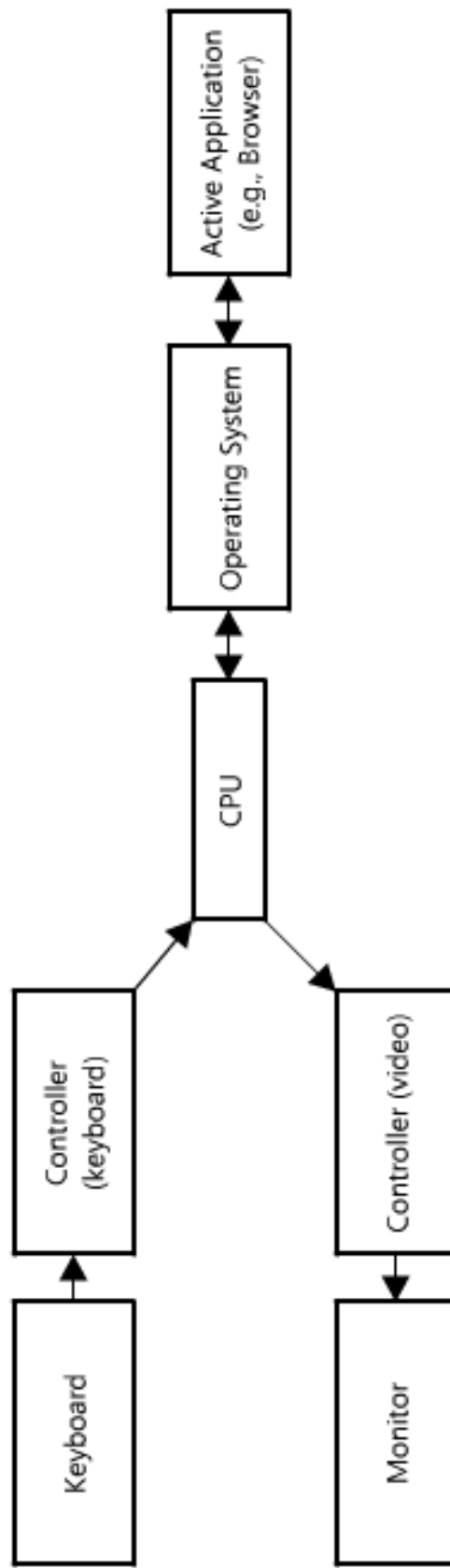
- **What are you trying to do?**  
(Do they have or understand the purpose?)
- **What have you tried already?**  
(Restate in steps what they have already done)
- **What else do you think you can try?**  
(Brainstorm, encourage students to take a chance)
- **What would happen if....?**  
(Come up with some possible solutions and hypothesize the outcomes. Test each hypothesis).

## Hardware Building Blocks

- ✚ All computers are made up of the following basic building blocks.
- ✚ The basic building blocks can be assembled in many different ways
  - How innovators, producers, marketers, etc. see the world influences design
  - Economic, social & political contexts influence how designs are turned into products
- ✚ Different products (different designs & contexts) have different social consequences
- ✚ We influence the social consequences through our choices and our [re]invention of products

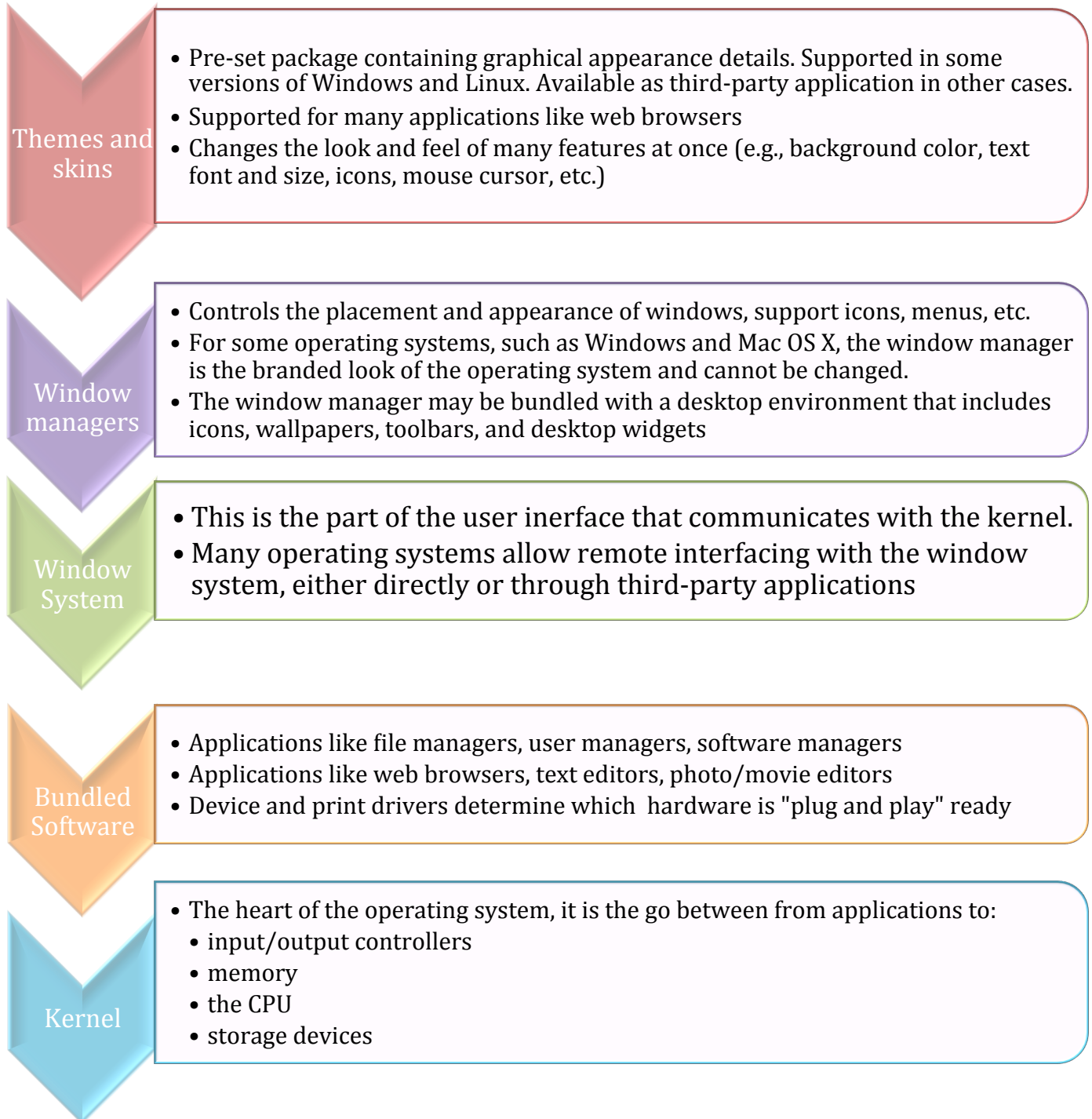


# The Flow of Information Through a Computer



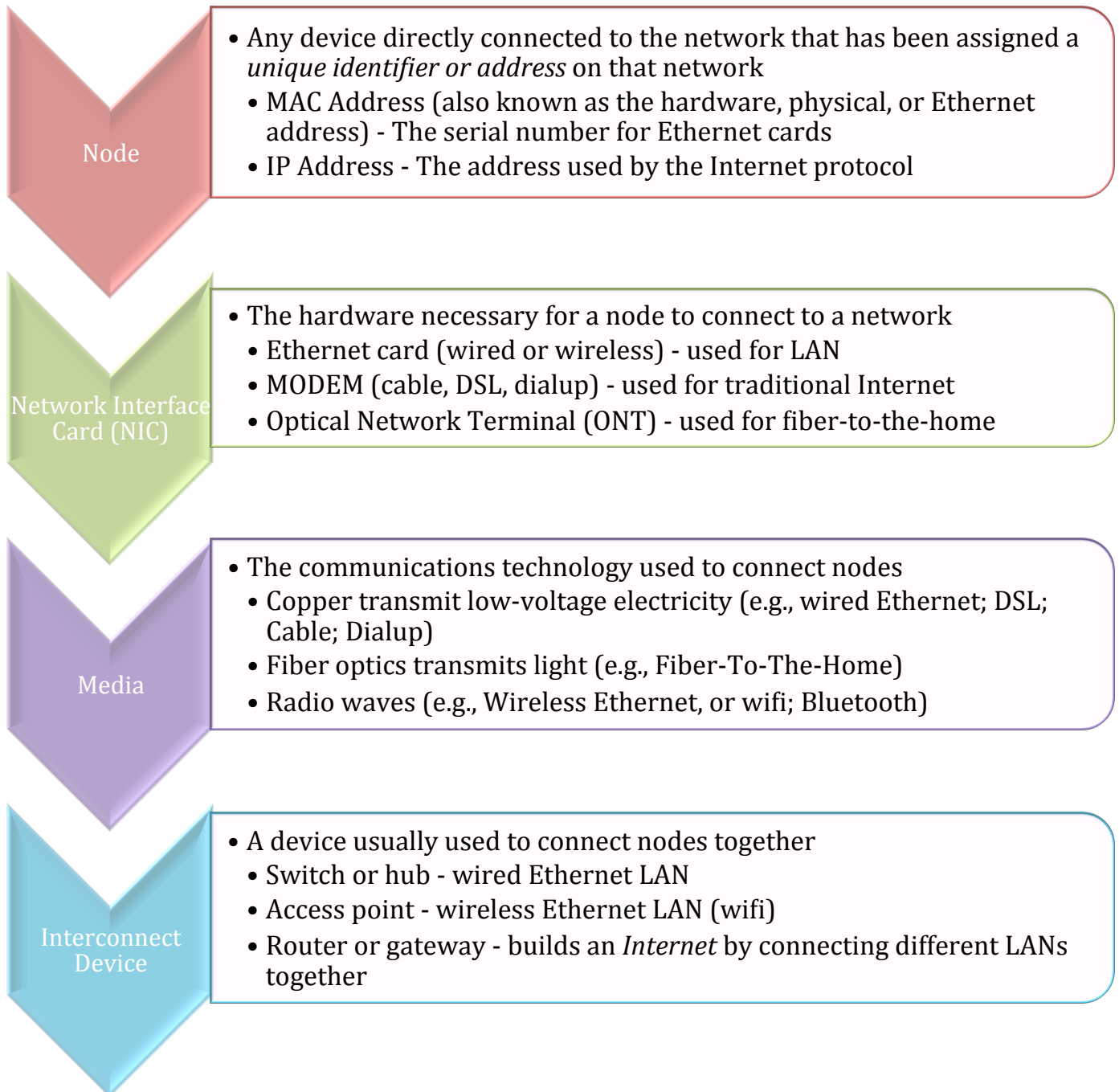
## Operating System Building Blocks

- ✚ Operating systems are comprised of the following basic building blocks
- ✚ The same OS can work on many different hardware platforms (e.g., desktop/laptop and smartphone/tablet) by using the same kernel but different window managers
- ✚ Different editions (e.g., Windows 8, Windows 8 Pro) or distributions (Ubuntu, Edubuntu, Linux Mint) add/remove bundled applications and/or administration features



## Network Building Blocks

- ✚ All computer networks are made up of the same following basic building blocks
- ✚ Networks differ on how far they reach geographically, how many people are meant to use them, and who primarily owns/control them.
  - Local Area Network (LAN) – owned, managed, and used by people in a building
  - Wide Area Network (WAN) – owned and managed by Internet Service Provider
  - Metropolitan Area Network (MAN) – community owned and/or managed WAN





## Essential Network Troubleshooting Tools

### Link Lights

- LED light found on wired Ethernet cards & switches
- When lit, indicates card & switch are on and working properly, and that Ethernet cable is plugged in and working properly

### Network Manager

- Operating system utility that shows network configuration
- An IP address of 0.0.0.0 or one that starts with 169.254 indicates you are connected to the media but aren't getting a proper IP address from the address server (usually the gateway router)

### Ping

- Run from the command line or terminal application to test if you can communicate with another node
- ping *IP\_ADDR* or ping *IP\_NAME* (e.g., ping google.com)
- Times of 1ms or less are good on a local network; 10-50ms or less are good on the Internet
- HINT: ping different nodes to track down faulty component



### Traceroute

- Run from the command line or terminal application to test the performance of each router between nodes
- Windows: tracert *IP\_NAME*; Linux: tracepath *IP\_NAME*; Mac OS X: traceroute *IP\_NAME*; Smartphone apps available
- Astericks (i.e., \*) indicate failure or firewall
- HINT: usually hop 1 is your router; hop 2 is your ISP's

### Speed Test

- Web-based Internet connection speed test
  - <http://www.speedtest.net>
  - <http://www.speakeasy.net/speedtest/>

NOTE: To access the command line:

- **Windows** – click on the Start button, choose run, type in *cmd* in the open bar & hit the enter key
- **Mac OS X** – click on the spotlight , type in *terminal* & choose Terminal under Applications
- **Linux** – click on the Start button , choose Terminal under Accessories

## Broadband Choices

### Key differences

- ✚ Do others in your neighborhood split the bandwidth on the media with you (*bus topology*), or do you get a dedicated line to your house (*hub and spoke topology*)?
- ✚ Can the media send a packet of data at the same time it is receiving one (*full duplex*), or can it only do one thing at a time (*half duplex*)?
- ✚ Is the upload speed the same as the download speed (*synchronous*), or is it slower (*asynchronous*)?
- ✚ Are there limits in what you can do with your connection, such as a limited amount of bandwidth each month (*data caps* – cell data plans, *fair use* – satellite data plans), limits based on file size (e.g., Comcast *TurboBoost* only transfers the first part of a large file at the advertised speed), or limits based on contracts with the ISP (for instance, a streaming video company could have a contract to pay Comcast more so that their videos are on a “fast lane” to Comcast homes but not to AT&T homes, contradicting the historic policy of *net neutrality*)

### Digital Subscriber Line (DSL)

- Adds 2 channels to standard phone line for Internet
- Hub and spoke (dedicated line) topology; full duplex
- In the US DSL prioritizes download speeds

### Cable Internet

- Redirects a cable channel to be used for Internet
- Neighborhood shares bus topology; full duplex
- In the US, Cable Internet prioritizes download speeds

### Cell-based Internet

- 3G adds the EV-DO (Verizon, Sprint/Nextel) or HSDPA (AT&T, T-Mobile) protocol to cell's voice protocol
- 4G adds the WiMax (Sprint) or LTE (Verizon, AT&T) standard to cell's voice protocol
- Equivalent to bus (shared) topology; half duplex
- Prioritizes download speeds

### Community Wireless

- Uses standard wireless Ethernet (wifi) outdoors; anyone can use off-the-shelf equipment to create
- Equivalent to bus (shared) topology; typically half duplex
- Synchronous upload and download speeds

### Fiber Optics

- Ultra high speed communications technology with one or more channels for Internet
- Hub and spoke (dedicated) topology; full duplex
- Synchronous upload and download speeds

# Basic System Maintenance

The following maintenance schedule will help you keep your computer up-to-date, and keep your files backed up.

---

## Regularly: Empty the Trash

Items placed in the trash are still on your computer and can be taken out, just like documents in your actual kitchen trash can, for example, can be taken out and recovered. Emptying the trash (by right-clicking on it and selecting “Empty Trash”) is like taking the trash out to the curb – any documents can still be recovered before the garbage truck comes, but this is a dirtier job and you might not be able to recover the whole document.

---

## Every Week: Check for updates using the terminal

Go to “Accessories” to open the “Terminal” application. This will open a terminal window where you can enter commands. The command `sudo` is short for “super do,” which means the command is a “super-command.” The following terminal commands will ask you for your password.

**Terminal command:** `sudo app-get update`

*Checks for updates of available applications. You have to do this before using the `app-get dist-upgrade` command, otherwise the computer won't know what's new.*

**Terminal command:** `sudo app-get dist-upgrade`

*Updates all applications and system files to the newest version. LINUX takes the list of new updates it got from `app-get update` and then upgrades all of the software on your computer.*

---

## Every Month: Check that backups are working properly

It's important to back up your files, because hard drives can fail. This is like copying important documents and putting them in a second file box, in case the first one is lost, stolen, or damaged for any reason. Use the “Backups” application under “Accessories” menu to make sure your settings are still what you want them to be.

*Check “Folders to save” and “Storage location” to make sure the files you want to back up are being backed up at the correct place. Schedule automatic backups under “Scheduling,” if desired. Make sure the “switch” at top right is set to “On.”*

---

## As Needed: Basic physical maintenance

Check cable connections to make sure they are tight, and that cords are intact.

*Tighten any loose connections, replace any damaged cables.*

Unplug all cables from the computer. Use compressed air designed for cleaning computers to blow out dust from the keyboard. Use a cloth dabbed in rubbing alcohol to clean the tops of keys. Clean the monitor with a dry microfiber cloth (paper towels and many household cloths are abrasive). If the computer is located in an especially dusty area, open the case and use the compressed air to blow dust from the inside of desktop computer.

Never spray liquids directly on computer parts. Never use furniture cleaners or strong solvents. Reconnect everything once dry.

---

## Yearly: Account and Software Management

Change passwords on local computer and remote systems. Consider using groups of passwords (one for online banking, one for online credit cards, one for email services, one for social media sites, etc. (do not share passwords unless you trust someone with every thing you have and are)

Delete unused applications, consider updating to the newest versions of remaining applications and your operating system, especially if updates are no longer available for existing version.

---

## Security Building Blocks

### Firewall

- Software that chooses which types of services to allow through (for instance, allow web access but not remote login access)
  - On router to stop outsiders from getting in
  - On each computer to stop attacks from a compromised computer

### Encryption

- A big time improvement on the old-fashioned decoder ring
  - On the wireless access point, enable **WPA2** encryption
  - In your web browser, never enter private data unless you see **https**
  - Make sure other applications transferring private data use **SSL** or another encryption
  - Consider encrypting a folder on your storage devices

### Software

- Always run software updates
- Always run antivirus software in Windows
- Create and regularly use a non-administrative account
- Enable second-level access codes when applications store or access in the cloud private data (for instance, a pin to start the dropbox app on a mobile device)

### Passwords

- Use secure passwords that include non-letters; HINT: use phrases
- Use different passwords, or at least different groups of passwords, with different devices and servers
- Never share your password unless you trust that person with all you have & all you are
- Consider using a password manager to keep track of passwords securely

### Physical

- Don't leave your computer (laptop, smartphone, tablet) laying around
- Logoff or lock your screen when leaving your computer or people can easily become you
- Don't leave your external storage devices laying around, including your backup device
- Consider installing/enabling tracking and remote lock/erase software if you store highly private data
- Be careful of over-the-shoulder data snatchers

### Weakest Links

- Social Engineering
  - Using seemingly harmless information to get more private information
  - "Phishing" to trick you into believing you are on a legitimate site
- Server security - only provide/store private data on the most trusted servers
- An insecure computer or user on your local network increases the risk to all other computers and devices

# Common Sense on Online Security

---

## What's the Issue?

Technology makes it very easy for kids to connect and share things with friends and family no matter where they are. But these connections can come with a huge cost if kids aren't careful. Learning to protect personal identity information, creating strong passwords, and being cautious when downloading programs and files are crucial to kids' safety as well as the security of the information stored on their digital devices. Otherwise, kids can expose themselves and their families to digital threats such as computer viruses, data and identity theft, and hacking.

To understand digital safety and security, you'll need to learn perhaps some unfamiliar words: *phishing*, *malware*, *spyware*, *spam*, and yes, even *junk*. These refer to greedy little programs that attach themselves to respectable-looking software – for example, a downloadable game that looks really cool – and then wreak havoc once installed on your computer. Security programs can help block them, but one of the most important defenses against these threats is teaching kids to treat their devices and information as the truly valuable things they are.

## Why Does It Matter?

If kids don't protect their personal information, there are many potential risks: damage to the hardware, identity theft, and financial loss. But children may not realize they are putting their information in jeopardy, because the warning signs aren't always obvious. For instance, another child might ask for your child's computer password to play a game, and then access your child's private email account. Or your child might use a file-sharing program that passes along a virus to your computer. Older elementary kids might be asked to provide personal identity information, such as a home phone number, address, date of birth, or your Social Security number, by a thief posing as someone else, all of which opens up the family to the risk of identity theft. Just like in real life, kids online have to know who to trust with information.

## common sense says

**Help your child master the fine art of password creation.** Teach them:

- **Not to use passwords that are easy to guess, such as their nickname or their pet's name.**
- **Not to use any private identity information in their password.** Identity thieves can use this information to pretend to be them.
- **Not to use a word in the dictionary as a password.** Hackers use programs that will try every word in the dictionary to guess passwords.
- **To use combinations of letters, numbers, and symbols.** These are harder to crack than regular words because there are more combinations to try.

**Teach your kids to be careful with what they download.** Let them know not to download free games or videos to their computer. These programs often come with spyware and viruses that will land the computer in the shop – and them in hot water. In the end, what seemed like free software often comes at a cost.

**Let your kids know how to identify and deal with spam.** Teach them that spam is Internet junk mail. This mail should not be opened, because if they do, they will just receive more of it. The best strategy is not to open email from addresses they don't recognize.

# Common Sense on Talking Safely Online

---

## What's the Issue?

Kids love connecting with others online. Most young people talk online only with their friends and family. But as a parent, you might be concerned that a stranger with bad intent (predator) could contact your child.

Predatory behavior is when people contact your child on the Internet (mostly through instant messaging, chat rooms, or social networking sites) and attempt to “groom” your child for a relationship. These people try to win children’s trust by hiding their true identities. They may try to get kids into creepy or dangerous situations by pretending to have similar interests, giving them compliments, and letting them talk about anything they want. They typically tell children to keep the friendship secret, and they may even threaten kids if they tell anybody. As the relationship develops, the predator may send pictures, ask a child to send them pictures, and then ask to meet face to face.

## Why Does It Matter?

Teaching your child to be alert about how predators groom their targets is crucial to keeping your child safe. With very small kids, it is best if you are present when they are online. At this age, you may choose to block your kids from talking online, or create strict rules for them to follow about who they can talk to. For older elementary school children, you may choose to give them more freedom after first discussing how to stay safe online.

## common sense says

**Discuss responsible online behavior.** Establish rules for appropriate instant messaging and chatting online, and explain that you’re enforcing those rules because you care about their safety. You may want to involve an older sibling who can model good online behavior and can stay involved in their younger siblings’ online lives.

**Establish rules for who’s okay to talk to.** Online talk should generally be with people your children know, like family and friends.

**Set boundaries for what topics are okay to discuss.** Kids shouldn’t answer questions online that make them feel uncomfortable. They also shouldn’t talk about adult topics with strangers.

**Make sure your child feels safe telling a trusted adult.** If something creepy or inappropriate happens online, kids need to know they won’t get in trouble if they tell an adult they trust. Also, avoid banning them from the computer. Kids are less likely to tell parents when they experience a problem on the computer if they think as a result they won’t be allowed to use it.

**Remind your kids not to give strangers private information.** Kids should never give out their name, address, school, phone number, email, pictures, or anything that could identify who they are.

**Block, ignore, or leave.** Most kids know to brush off unwanted contact. Encourage this behavior.

**Look for warning signs.** Does your child seem withdrawn, emotionally distant, spend endless hours online, or seem to be hiding something? The kids who get sucked into inappropriate online relationships often show warning signs. They might be hiding an online relationship they don’t want you to know about. If you think this might be happening, ask your child about it!

# Common Sense on Privacy and Digital Footprints

---

## What's the Issue?

Our kids live in a culture of sharing that has forever changed the concept of privacy. In a world where everyone is connected and anything created online can be copied, pasted, and sent to thousands of people in a heartbeat, privacy starts to mean something different than simply guarding personal or private information. In this context, you might think about kids' privacy in three categories: privacy and security, privacy and reputation, and privacy and advertising.

- **Privacy and security:** This is the private information (e.g., Social Security number, first and last name) that could put kids at risk for identity theft if it got into the wrong hands.
- **Privacy and reputation:** The information that could be personally embarrassing or hurtful to them or others if posted publicly.
- **Privacy and advertising:** The information about their habits and behavior online that companies collect in order to target them with ads and other content.

## Why Does It Matter?

For good or bad, everything our kids do online creates digital footprints that migrate and persist. Kids share work with others and, as they get older, receive comments and feedback. This culture of sharing is beneficial in many ways. But if kids aren't careful, their reputations can be harmed, or their information used in ways they never intended. For example, your child may think he or she just sent something to a friend, but that friend can send it to a friend's friend, who can send it to their friends' friends, and so on. Or they may innocently fill out an online form without understanding that this may make them vulnerable to identity theft. And their online behavior will likely be tracked without them knowing by the industry, which has little incentive to be responsible.

## common sense says

**Make sure kids get your permission before filling out forms.** Let kids know that you are the gatekeeper. They should ask your permission before filling out online forms, and they should always keep their Social Security number, birth date, address, and full name private.

**Help kids think long term.** Everything online leaves a digital footprint. Help them think before they post so that they will be proud of their Internet presence down the road.

**Remind kids that the Golden Rule applies online.** Remind kids that they will be treated online as they treat others. Whatever negative things they say can and probably will come back to haunt them, in more ways than they can imagine.

**Help kids see through advertising.** The next time an ad pops up online, or you see that you are being targeted by ads specific to your interests, point it out to your kids. Let them know that some companies advertise to you based on what kinds of things you look at online.

# Common Sense on Digital Life

---

## What's the Issue?

We may think of our kids' online, mobile, and technological activities as "digital life," but to them it's just life. In their world, being able to connect and communicate 24/7 from just about any location is normal – and expected! Between kindergarten and fifth grade, kids go through rapid growth in learning about many topics, including digital media technologies. From playing games on their mom or dad's cell phone, to learning how to point and click a mouse, to navigating online by themselves, kids this age are participating in a connected culture.

## Why Does It Matter?

Young children need to learn early how to make good choices so they can take advantage of the powerful technologies available to them. And to make these good choices, kids need parental guidance.

The stakes are high because our kids' technological abilities can be greater than their maturity and judgment. Having unrestricted access to information and people can result in gaining a wealth of information and experiences. But it can also mean accessing inappropriate content and making inappropriate contact with others. The difference between a great experience and an iffy one lies in the decisions kids make. Just as kids learn to eat properly, swim safely, or drive a car carefully, they need to know how to live in the digital world responsibly and respectfully. Their ultimate success depends on their abilities to use digital media to create, collaborate, and communicate well with others. Those who master these skills in using digital tools will benefit from the digital world's awesome power.

## common sense says

**Use bookmarks and safe search.** Teach your child to bookmark his or her favorite sites. This way, your child is less likely to go somewhere online you don't want. Use safe search options on Web browsers, such as Google or Bing, to make sure your child can search safely.

**Consider using filtering and blocking software.** Some parents find these tools to be useful to help protect younger children from accessing inappropriate content.

**Have older siblings help.** Have your older children help teach your younger children how to be responsible and safe online. Let the older ones know that you want them to help you protect their little brothers or sisters online.

**Share wisdom.** Kids often don't understand the implications of their actions. But we do. So we have to remember to extend our basic parenting wisdom to the digital world. We teach kids to choose their words carefully, play nicely with others, and respect their teachers. Now we have to extend those lessons to a vast, invisible world.

**Pass along your values.** As a parent, you can translate your values into the digital world and help kids understand the implications of their actions. Oftentimes the same rules that apply in the real world apply online, such as "be nice to others," "don't say mean things," and "think critically about information."



**Seek balance.** It's hard to know how much freedom to give kids. We want them to explore, enjoy, communicate, and create. We also want to be sure they are protected. If our kids are going to thrive with digital media, we must balance the negative with the positive, privacy with protection. As our children grow, they need more independence and privacy. But parents have to be sure their kids know how to be safe and responsible before letting them loose.

**Keep an open mind.** We don't see the world the way our kids do. And we don't help our kids when we judge their lives through the lens of a non-digital world. It's important for us to understand that our kids will spend much of their lives in a connected world, where everyone creates and communicates. We need to help them to enjoy it and learn from it.

# Common Sense on Online Research

---

## What's the Issue?

The Internet is bursting with information. Some of it's correct, some of it's questionable, and some of it is just plain wrong. The Internet is typically the first place young people look when they begin researching a report or are just browsing for information on their favorite topic. But as you know, not everything they find on the Web can be trusted. And skills they learn about research and evaluation in elementary school will provide them a foundation they'll continue to use in middle school and beyond.

## Why Does It Matter?

Anyone can publish on the Internet, so not all sites are equally trustworthy. Teens have the ability to be skeptical, but younger children tend to believe what they read and accept it as the truth. When children find sources online that aren't of high quality, they risk using incorrect information, getting only part of the story, and worst of all, denying themselves the opportunity to truly learn as much as possible about a topic.

When children use a website for their research, they should make sure it's worthy of their trust. Fortunately, there are ways to evaluate the trustworthiness of a site. Along with choosing sites with good design and at the right reading level, kids should evaluate the substance and content of the material.

## common sense says

**Ask questions to evaluate the trustworthiness of sites.** You can help your child evaluate the quality of a website with a little detective work.

- *Who wrote this?* Check to make sure the author or organization is credible by looking at their title, expertise, and background.
- *What is the source of the information?* Does the site come from a well-known organization or news source?
- *How does this compare to other information?* When evaluating websites it's important to look at multiple sites so you can compare information.
- *When was this updated?* Has the site been updated recently? If not, move on. What is the site linked to? Was the site linked from another webpage that you trust? If so, that's a good sign.
- *Are advertisers targeting you?* Help your kids notice when advertisers are trying to get their attention as they search. Teach your kids to question what the ads are saying.

Workshop materials funded in part by:

- The Illinois Sustainable Technology Center “Sustainable Electronics Initiative” program; and
- The Illinois Department of Commerce and Economic Opportunity “Eliminate the Digital Divide” program