Online Safety

Worksheet 4 Reading Material

Before you start, read the following directions.

1. Read the questions in "Online Privacy" section of the other handout so you know what to look for.
2. YOU MUST read ALL the information and then answer the questions. If you just "skim" to find the answers, I will NOT accept your assignment and you will get a 0%.
3. Repeat these steps for each section of questions.
4. This worksheet should take 45-60 minutes to complete.

Online Privacy

Although the Internet is rapidly becoming the dominant medium for business and global communication, it still remains something of a frontier, because there is little regulation. Most efforts have relied on the Internet industry to police itself. While self-policing has had some success, continued abuses have increased calls for government intervention.

Some aspects of the Internet could undoubtedly use regulation, but it's not as simple as it may seem. The very nature of the Internet--a loose constellation of networks comprising tens of million s of computers and mobile devices ringing the globe--makes it extremely difficult, if not impossible to regulate. At the same time, the absence of regulations means that everyone who uses this essentially public network can be a target for anyone who has the technical know-how and the desire to invade their privacy.

Protecting Personal Information

While the threat from hackers is low for individuals, a more serious threat to personal privacy comes from companies that operate websites. Many sites require you to register before you can use their services. Often you have to provide personal information, such as your name, street address, and e-mail address. Then as you browse the site, data is collected as to which pages you visit, how long you remain on each page, the links you click, which terms you search, and so on. After a number of visits to the site, a personal profile emerges. The question is, what do site operators do with this information?

Most claim that they use it to personalize your experience on the site. For instance, if a gardening site "learns" that you're interested in heirloom vegetables, the next time you visit the site, you might be presented with an article or advertisements for rare tomatoes. But some websites sell this information to marketers, which means that you may find yourself receiving unwanted e-mail from garden suppliers.

Junk mail is more of an annoyance than a serious problem. But what if you read articles about cancer on a health site? Would you want this information revealed to insurance companies? Or what if the gift you bought your boyfriend appeared on your Facebook page? Most people consider that an invasion of privacy.

Control Who Sees Your Information

Social networking sites like Facebook, have at their core the sharing of personal information, whether it's your favorite band or your employment history. Before you post personal information, think about whether you want the world to see it. If not, you can set levels of permission that restrict who can see it.

Many sites now post their privacy policies online. Before you reveal any personal information, read the policy to make sure you agree with it. Some sites specifically seek your permission to share your personal data with third parties or to receive e-mail announcements. This is known as "opting in". To avoid this, opt out by checking the "No" box. For more information about consumer privacy, visit TRUSTe.

Cookies

If you don't want your web surfing behavior to be tracked without your consent, configure your web browser to reject cookies. A cookie is a small file created and installed on your computer's hard drive by a website that wants to collect information about your interaction with the site. As you browse through the content, information is stored in the cookie. The next time you return to the site, that data is transmitted to the site.

Only the site that created the cookie can read it, and it can't access other files on your computer. Cookies can be useful for things like storing a password so you don't have to enter it each time you access the site. But cookies are invasive because they are normally set without your consent.

Encryption

Protect the privacy of your electronic communications by using encryption, a form of cryptography. Encryption requires special software to encode your e-mail or any other files you want to send securely over the Internet. The person receiving these files must use the same software to decode them.

Netiquette

We expect other drivers to observe the rules of the road. The same is true as we travel through cyberspace. That's where netiquette, a term allegedly coined from either network etiquette or Internet etiquette comes in handy. To guide you through your online communications, keep these pointers in mind:

1. Avoid writing e-mail or posting messages in blogs, newsgroups, forums, chat rooms and other online venues using all capital letters. IT LOOKS LIKE YOU'RE SHOUTING! Not only that, it's difficult to read.

2. When you talk with someone, the tone and inflections of your voice convey great meaning. To add personality and humor to your messages, use smileys, also known as emoticons, expressions you create using the characters on your keyboard. Below are some of the more popular smileys. Can you guess what they mean? Roll your cursor over each one to find out.

3. Keep your written communications focused. This is true whether sending e-mail or posting messages online. Few people like reading lengthy text on a computer screen. Many people now receive e-mail on mobile phones and other portable devices. Tiny screens make reading e-mail challenging.

4. To shorten messages, use common abbreviations:
   - < BTW > means By the Way.
   - A < G > enclosed in brackets indicates grinning.
   - A good one to keep handy in case you're worried about offending someone is < IMHO > -- In My Humble Opinion.
   - One of our favorites is < ROTFL >, which stands for Rolling on the Floor Laughing. A shortened version is < LOL >--Laughing Out Loud. And if you get called away while chatting online, try < BRB >--Be Right Back.

5. Remember that comments you post to a blog, newsgroup, forum or website and write during a public chat session is a publicly available. You never know who's reading it or who may copy and spread it around. It could come back to haunt you.

Adapted from an old website called Learn the Net

6. Stick to the topic when posting a message. Don't indiscriminately post unrelated comments, or worse--advertisements. This practice, known as spamming, will quickly lead to another unpleasant Internet practice, flaming. What is flaming? Sometimes you might offend someone unintentionally. Be prepared to read some angry responses or be treated rudely in a public discussion. This is called being flamed. If you retaliate, you may spark a flame war. To contain the heat, the best response usually is no response at all--or a heartfelt apology.

7. When sending e-mail, make sure that the subject line accurately describes what the message is about. If the topic changes during a string of messages, alter the subject line.

8. If you post a commercial message or send it as an e-mail, clearly identify it in the subject line. That way people who aren't interested can quickly delete it.

9. FAQs (Frequently Asked Questions) are handy documents to read before asking questions. Always consult them whenever available.

10. Electronic communications may seem ephemeral, but when you hit the Delete key, they don't go away. In all likelihood, your missives are stored on a mail server and can be retrieved. Think twice before you send e-mail. Consider all your electronic communications to be public and act accordingly. The same holds true for comments you post. They usually can't be retracted and live on and on.

Netiquette isn't something you learn overnight, so don't let your fear of not knowing online protocol hold you back. For more tips, visit Wikipedia's netiquette article.

Responsibility in a Virtual World

The Internet has made it possible for people all around the world to connect with each other in meaningful ways. Whether for research, education, business, or just fun, the Internet has changed how we live, work and play in ways we may not even be fully aware of.

As the Internet continues to evolve, so do the issues that influence the way we use it. From privacy and freedom of speech, to honesty and consideration in the way we interact with others, we all have a responsibility to preserve and protect its unique character. That means recognizing that while the medium in many ways is a reflection of the physical world, in other ways it is fundamentally different--manifesting unique customs and practices.

Controlling your Clickstream

True or false: are your online activities private and anonymous? False. Almost everything thing you do online--whether it's searching for information, reading a news article, shopping for a gift or downloading music--is recorded. As you move through cyberspace you leave a trail of digital data in your wake. This trail, often referred to as a clickstream, contains a revealing record of your online activities.

How It Works Clients and Servers

When you're online, your computer, known as a client, requests information from a remote computer, known as a server. To do this, you click a link. This instructs the server to send you the information you requested. Think of all the clicking you do as you surf the Web. Although it may seem insignificant, to some people, your clickstream has great value.

Most websites, including Learn the Net, store data about visitors to the site. For instance, we know what site you came from, which pages you visited, how long you stayed on the site, which files you downloaded, and many other related bits of information about your activities. If you register with a website, the site can identify who you are each time you visit. (But even if you didn't register, it's still possible to discover who you are by matching records from your Internet Service Provider or ISP.)

All this information is stored in log files that the site operator can analyze. The information is typically used to improve the website and deliver personalized and more relevant content. For instance, we know that many Learn the Net visitors read articles about e-mail, so we try to publish more information on this topic. Understanding readers' preferences also helps publishers attract advertisers of interest to its audience. While web publishers only have user data from their own sites, your ISP has a complete record of every click you make online. In the wrong hands, this clickstream data poses a serious threat to your privacy.

Risky Business

Let's say you play online poker. Would you want your spouse to know about it? Or suppose you use Yahoo! or Google to search for information about cancer treatments. Would you want your health insurer to learn about it? Maybe not.

Once all these bits of data are pieced together, a picture of you emerges, one that you may not want to share with the rest of the world. Even though you may be a law abiding citizen, some details of your online activity can be embarrassing. Worse, it may be misinterpreted. For instance, what if you are doing research about alcoholism? How might your employer interpret this? What if you are researching a report on terrorist organizations? Would you want law enforcement agencies to know about it?

As you can see, in a perfect world, you should be the master of your clickstream. Your trail of digital data should be as private as your telephone conversations, mail and other communications. Unfortunately, there has been a steady erosion of the privacy of online activities. The U.S. government has subpoenaed search records from AOL, Google MSN, and Yahoo! A number of data-mining companies now trade in personal information. The purpose of this article is not to make you paranoid, only to make you aware of the current situation and its implications.

Concealing Your Clickstream

If you have privacy concerns, you can limit the amount of information collected about you. Here are some resources that we recommend:

According to "How to Foil Search Engine Snoops", an article from Wired News, the most important step you can take is to manage the cookies placed on your computer.

Two software programs claim to keep your identity private by erasing your tracks as you surf the Web: GhostSurf, Anonymizer, You can also use The Cloak to surf a website anonymously.

Finally, if you use Internet Explorer, Chrome, and Safari’s feature called InPrivate Browsing, which "...helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data." Note that it doesn't prevent sites you visit from gathering data. You'll find this feature under the Safety menu on the toolbar.

How Private is Your E-mail

Every day, tens of millions of people use electronic mail to conduct business and to communicate with friends and family. But if you think your e-mail is private, guess again.

E-mail is no more private than a postcard. Unlike other forms of communication, such as telephone calls, which are protected in the United States under laws like the Electronic Communications Privacy Act of 1986 and by similar laws in other countries, e-mail has little similar protection. The situation becomes even murkier for messages sent or received at your place of business.

For Your Eyes Only?

An electronic message typically makes numerous stops at computers along the route to its final destination. At each stop, it can be intercepted and read by snoops. Why would someone want to do this? For hackers, there's the challenge of eavesdropping in cyberspace; for business competitors, confidential data may have strategic value. After all, information is power.

Where Has All the E-mail Gone?

Even after you've received a message and deleted it, the message doesn't vanish. Many Internet service providers and e-mail services archive e-mail for some period of time. These archives can be accessed and even subpoenaed in the event of an investigation or lawsuit. The same holds true for messages received at work. Although you hit the Delete key, the message still exists in the company system. Those inappropriate comments you wrote may come back to haunt you!

Writer Beware

While U.S. law offers limited privacy protection for communication over the Internet, almost none exists for electronic messages sent within the workplace. In fact many companies take the position that they not only have a right, but the responsibility to review employees' e-mail. They argue that e-mail is no different than writing letters and memos on company letterhead. Because electronic communication represents the company and is conducted using company equipment over the company network, businesses contend that they have a right to monitor e-mail. Many employees take the opposite position, claiming their right to privacy unless informed otherwise.

Adapted from an old website called Learn the Net

While most companies routinely use e-mail, many don't have an official e-mail policy. In the absence of a policy, employees often feel a false sense of security, particularly because their e-mail accounts are password protected. Passwords do offer some protection, but not from system administrators, who can access almost anyone's e-mail. This comes as news to many employees who mistakenly believe that communication with colleagues is private. In fact in a number of cases, casual e-mail messages that criticized the company have landed on the boss's desk. The result? The employees were fired. In the ensuing lawsuit, U.S. courts have upheld company actions.

To avoid legal skirmishes, businesses, even small ones, should establish an Acceptable Use Policy for e-mail that clearly sets out permissible workplace uses, prohibited uses, and penalties for violation of the policy.

An Ounce of Prevention

You can protect yourself from prying eyes. First of all, regard e-mail as you would a postcard. Would you send confidential information this way? Obviously not. Second, to transmit sensitive data, use encryption software to encode your message so no one but the recipient can read it. Try TrueCrypt, a free open-source encryption program.

Passwords

As you surf the Web, you've undoubtedly noticed that many websites require a user name and password to access services like e-mail, to read premium content and to shop online.

Typically, you get a password by registering with the site, usually by filling out an online form. With most sites registration is free; with others you may have to pay a fee, such as sites with proprietary research and financial information.

Your password is your prime defense against unauthorized access to your personal account. Do you want someone reading your e-mail or reviewing your banking records? Of course not, so it's important to choose passwords carefully and just as critical, to safeguard them.

A website's security system can only confirm that a password is legitimate, not whether you're authorized to use the password. Make it tough for potential snoops by following these guidelines:

1. Don't use passwords that consist of easily obtainable personal information, such as your address, phone number or date of birth. Also avoid using common words found in a dictionary.

2. Devise passwords of at least six characters and consisting of upper and lower case letters, numbers, and symbols, for example: 2le@rN.

3. Use a different password for each service you register with.

4. Ideally, a password should be easy to remember. However, the reality is that having multiple passwords becomes confusing; which password is for which site? If you need to record your passwords, store them in a secure location. A piece of paper in the top drawer of your desk is tempting fate. Even worse is a Post-It note on your monitor!

5. Never disclose your password.

6. For sensitive accounts, such as financial services, change your passwords frequently. We recommend every two months.

Adapted from an old website called Learn the Net

Computer Virus

Viruses, worms, Trojan horses, botnets, malware and spyware are human-made software programs created specifically to wreak mischief on personal computers and networks. The chance of contracting one of these malicious programs over the Internet has increased dramatically. Unless you exercise great caution or routinely run anti-virus software, your computer will almost certainly become infected. Typically, you get a virus by opening infected e-mail attachments or downloading and installing infected software.

The Good, the Bad and the Ugly

Some viruses are relatively harmless to individuals. They just attach themselves to outgoing messages and e-mail themselves to all the contacts listed in your address book. The sudden flood of e-mail overwhelms mail servers, causing the system to crash.

Other viruses are more destructive and may lie dormant until a certain date. Then they spring to life to do their dirty deeds. Sometimes a strange message appears on your screen, or data and programs may be modified. In the worst case, all the files on your hard drive may be wiped out. These pernicious programs start on one computer, then replicate quickly, infecting other computers around the world.

In 1988 a student at Cornell University sent out a virus out by accident, infecting more than 6,000 computers in minutes, nearly bringing the Internet to its knees. The "I Love You" virus caused over $1 billion USD in lost productivity as it crippled e-mail systems worldwide in 2000. And a worm called Conficker hobbled 15 million computers in 2008 and continues to do damage.

Inoculate Your Computer

If you download and run software from the Internet or receive e-mail attachments, protect yourself by using anti-virus programs to scan attachments and downloaded programs to alert you of infection. The software also scans your hard drive periodically, searching for rogue viruses and deleting them.

Adapted from an old website called Learn the Net

Prevent Infection

1. Run anti-virus software and configure it to automatically download updates.
2. DO NOT OPEN an e-mail attachment unless you know the sender. To be completely safe, scan the attachment with anti-virus software BEFORE you open it.
3. If you receive a suspicious message, delete it immediately from your Inbox. Next, open the Deleted Mail folder and delete the message again to permanently remove it.
4. Regularly back up your files. If your system becomes infected, you won't lose your valuable data.

Warning Signs of Virus Infection

1. Your computer starts running sluggishly.
2. It shuts down unexpectedly or crashes frequently.
3. It experiences memory problems or runs out of disc space.
4. Unusual files or directories appear on your system.
5. Strange messages appear on your screen.

Secure Transactions

The Internet has become a global marketplace for goods and services. For e-commerce to prosper, you have to feel safe transmitting credit card and other financial information. But data traveling over a network presents an opportunity for someone to intercept this confidential information. How might this affect you?

Let's say you want to buy merchandise from an online store. If you provide your credit card number, how do you know it will travel safely from your computer to its final destination? With the tremendous potential for doing business online, there's a lot of time and money being spent trying to make data protection secure.

How It Works

Sensitive data is protected by a technology called encryption. Encryption software scrambles the data with a secret code so that no one can make sense of it while it's being transmitted. When the data reaches its destination, the same software unscrambles the information. When you see a small lock icon at the bottom of your web browser or next to the address bar, it indicates that your data is encrypted during transmission.

How Encryption Works

Hackers thrive on outsmarting computer security systems. Some regard breaking into computers as a harmless hobby, but others want to steal data for illegal purposes. Should you worry about this? If you access the Internet through a dial-up account, the chances of someone hacking your computer are slim. If you use a broadband or wireless Internet connection, your chances increase greatly.

The real targets of most hackers, however, are corporate and government computers systems. They protect their systems by erecting firewalls, an extra layer of software security placed between their internal computers and the Internet. These days, almost all personal computers also use firewalls. For instance, Windows XP, Vista, Windows 7 and Mac operating systems have built-in firewalls. If your computer doesn't have one, install one immediately. You can download ZoneAlarm for free.

Adapted from an old website called Learn the Net

Online Shopping

When dealing with online merchants, the best security is common sense. Anyone can establish a professional looking online store these days, so make sure you deal with reputable companies. How can you tell? The answers to these questions provide clues:

- Is this the website of an established retailer?
- Does the site list a street address, not just a post office box?
- Is there a way to call customer service?
- Is a return and refund policy posted?
- Does the merchant belong to organizations such as the Better Business Bureau Online and Truste?

All online financial transactions should be secure. Many online stores have what's known as a secure check-out page. You may see a notice to that effect posted on the site. Alternately, you may see a lock icon on your web browser, indicating that the site uses security technology. Also, check the address of the web page in the address bar of your browser; it should begin with https. The letter "s" indicates that the page is secure.

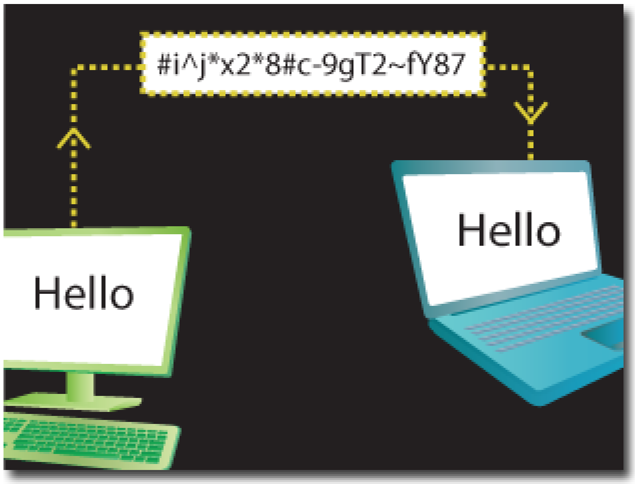
If you are uncomfortable transmitting sensitive information, many sites provide a phone number you can call to give your credit card number, although there is no guarantee that's secure either. According to the National Consumers League, most Internet fraud involves sending checks or money orders to merchants. The organization recommends paying by credit card, because fraudulent charges can be disputed with your bank.

The risks involved in transacting business on the Internet are no greater than those in any other arena in which we do business. While it is relatively safe to conduct business online, many companies are working to improve the technology required to make the Web more secure

Public-Key Cryptography

A technique called symmetric key cryptography was once used to secure information being transmitted across public networks. This method involves encrypting and decrypting a message using the same key, which must be known to both parties in order to keep it private. The key is passed from one party to the other in a separate transmission, making it vulnerable to being stolen as it was passed along.

With public-key cryptography, separate keys are used to encrypt and decrypt a message, so that nothing but the encrypted message needs to be passed along. Each party in a transaction has a "key pair" which consists of two keys with a particular relationship that allows one to encrypt a message that the other can decrypt. One of these keys is made publicly available and the other is a private key. A message encrypted with a person's public key can't be decrypted with that same key, but can be decrypted with the private key that corresponds to it. If you sign a transaction with your bank using your private key, the bank can read it with your corresponding public key and know that only you could have sent it. This is the equivalent of a digital signature.



Public-key cryptography lessens the risk of private information being intercepted, allowing parties to positively identify each other through digital signatures.

Secure Servers

Netscape Corporation (now owned by AOL) created the best known secure server technologies. It uses a security protocol called Secure Sockets Layer (SSL) that provides data encryption, server authentication, message integrity and optional client authentication for a TCP/IP connection. When a client program connects with a secure server, they exchange a "handshake" which initiates a secure session. With this protocol, the same server system can run both secure and unsecured web servers simultaneously. This means an organization or company can provide some information to all users using no security, and other information that is secured. For example, a business that sells products online can have its storefront (merchandise catalog) unsecured, but ordering and payment forms can be secure.

Why are these developments important? As the Internet becomes a way to buy and sell products and services, financial transactions become essential. Right now, most transactions involve the exchange of credit card information, either directly over the network, or by phone, to complete a transaction initiated online. Eventually, you will be able to use cash as well as credit, directly over the network.

There are two basic kinds of digital cash, anonymous cash and identified cash. Anonymous cash is just like paying for something with paper cash -- it carries no information about the person making the transaction, and leaves no transaction trail. You create it by using numbered bank accounts and blind signatures. Identified cash, on the other hand, contains information revealing the identity of the person who withdrew it from the bank. Like credit card transactions, identified cash can be tracked as it moves through the system and involves fully identified accounts and non-blind signatures.

For more information about online payments, visit VeriSign (now owned by PayPal)

Safety Tips for Parents

You may have heard stories about children and teenagers being exploited online, whether through unwanted overtures by adults or exposure to sexually oriented or violent material. Considering the tens of millions of kids who use the Net daily, the frequency with which these incidents occur is small. Yet they do happen.

Online Predators

Sites like Facebook that appeal to teenagers are a magnet for sexual predators who try to befriend them, then arrange to meet. Instant Messaging is another way that adults foster online contact with kids.

While it's true that material of a sexual nature can be readily accessed over the Internet, this kind of content represents only a fraction of the vast collection of information online. The chances of a child accidentally stumbling across inappropriate material are slim, as most sites now clearly post warnings. Before permitting access, many adult-oriented sites require visitors to register and provide a credit card number to verify their age. Unfortunately, a few high profile incidents obscure the fact that cyberspace teems with extraordinary resources for both adults and children--one reason why Internet access is a top priority for schools around the world.

Parental Supervision

Just like in the real world however, parents must exercise supervision. Of course this is easier said then done, particularly when children may be more comfortable with computers than their parents. If this sounds like you, don't be intimidated by the technology. After all, you don't have to understand how an internal combustion engine works to drive a car. Obviously if a six-year-old can use a computer, you can too. Many libraries, community centers and colleges offer hands-on training, so take the time to familiarize yourself with the technology. Or ask your kids for help!

Adapted from an old website called Learn the Net

To prevent children from becoming victims, consider these guidelines:

1. Use common sense - Don't just get an Internet account and turn them loose.
2. .Monitor their activity. Ask them which sites they visit and why. Set up the computer in a common area so you can keep an eye on things. Check the web browser's History file to see which sites they access and how often.

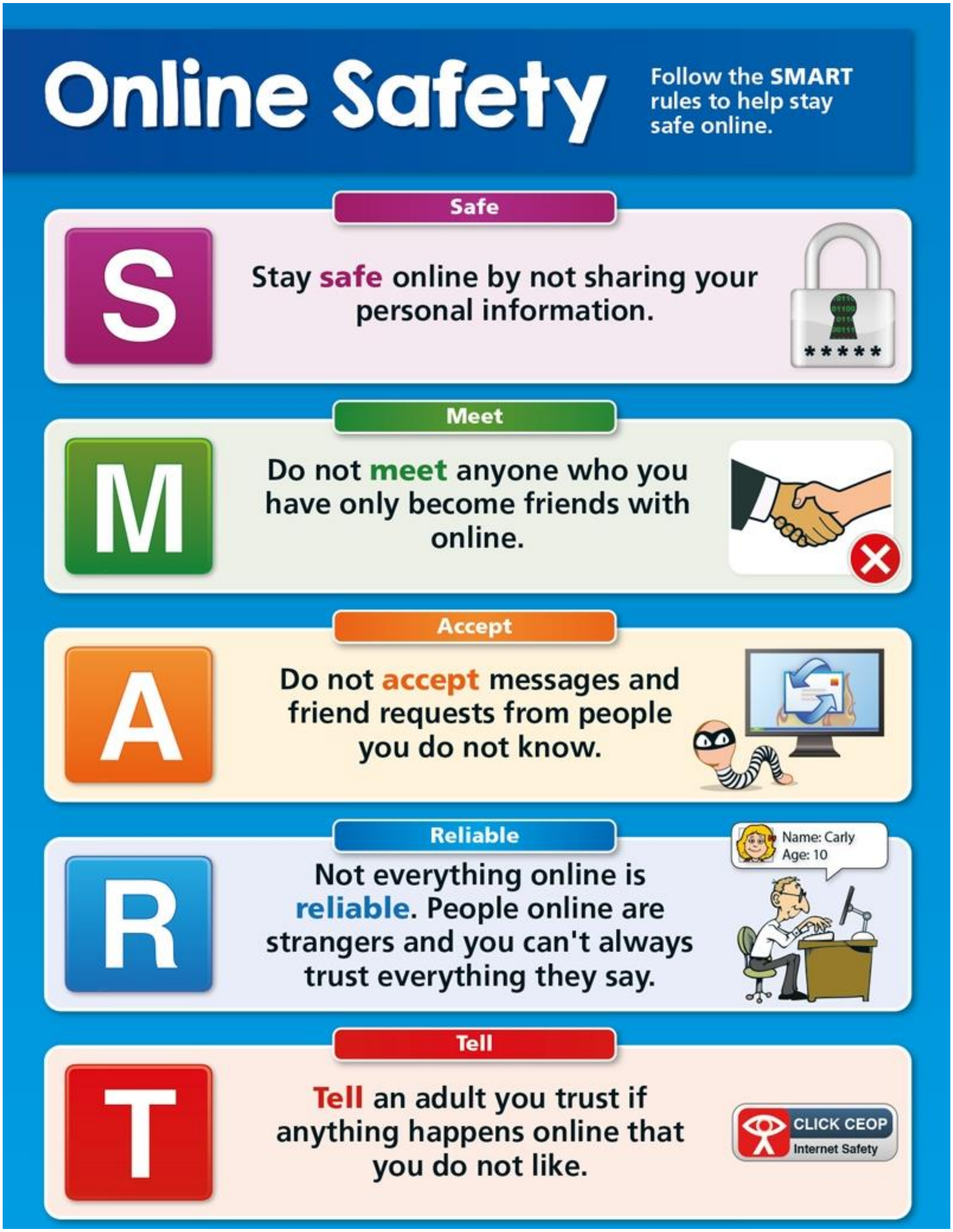
3. Set limits - It's up to you to determine when your kids can go online and how much time they spend.

4. Use filtering software - Although not perfect, you can block selected websites. Here are some products to evaluate:
   - Cyber Patrol
   - CYBERsitter
   - Net Nanny

5. Ask your kids to agree to these rules:
   - Don't give out a credit card number or any other financial information online or via e-mail.
   - Don't divulge personal information without your approval. This includes posting photographs on a web page.
   - Inform you immediately if they encounter any material that makes them feel uncomfortable.
   - Never meet anyone they've communicated with online unless you are present or give your consent.

SafeKids logo Technology expert Larry Magid has an excellent collection of information about child safety on his SafeKids.com website.

Another information-rich site with practical tips is GetNetWise.



Online Safety

Follow the **SMART** rules to help stay safe online.

S — Safe

Stay **safe** online by not sharing your personal information.

M — Meet

Do not **meet** anyone who you have only become friends with online.

A — Accept

Do not **accept** messages and friend requests from people you do not know.

R — Reliable

Not everything online is **reliable**. People online are strangers and you can't always trust everything they say.

T — Tell

Tell an adult you trust if anything happens online that you do not like.

Adapted from an old website called Learn the Net

Staying Safe Online

Lancashire Safeguarding Children Board

Know who online 'friends' are

Understand not everything online is true

Consider using home internet filters

Check security settings are in place

Know how to block unwanted calls & texts

Make sure you have an Anti-Virus program

Check age ratings on games

Be careful what you share

Ask your child to teach you about their online world

Set expectations and time limits

Know how to report problems on Social Media

If in doubt, always ask for help

...useful tips for Parents and Carers