Internet Safety

[1] Introduction

We all know we need to stay safe while using the internet, but we may not know just how to do that. In the past, internet safety was mostly about protecting your computer from **viruses**. But today, the internet's vast reach, constantly changing technologies and growing social nature have made users more vulnerable to **identity theft, privacy violations** and even **harassment**.

This lesson will introduce you to the types of **threats** you may encounter while online. It will teach you basic strategies like how to **Google yourself** and create **strong passwords**, in addition to encouraging you to adopt a **safer mindset** toward using the internet.

>Adopting a Safer Mindset

When it comes to the internet, people generally think they are safer than they actually are. Why? Well, often the impersonal nature of technology can give us a **false sense of security**. After all, no one can physically attack us through a computer screen. We tend to have an **it-won't-happen-to-me attitude**. We may even believe that our computer programs and the "powers that be" are automatically taking care of all that internet security stuff for us. Sometimes we just avoid it all together because, to be frank, we just don't get it. **Does this sound like you?** Consider the following the questions:

> Have you ever Googled yourself to see what information can be found on you?
> Have you set your computer's security program to make sure you are getting regular updates?
> Do you have an external back-up source for your computer?
> Are you enticed by emails or advertisements with special discount offers?
> When shopping online, do you check a website's security status before entering your billing information?
> Have you customized your privacy settings for your social networking accounts like Facebook, MySpace, Skype, etc.?

Do these questions make you nervous? Don't worry, this tutorial is not meant to scold or scare you, but to make you realize that **there are precautions we should all be taking on a regular basis** to maintain our **personal safety** and **protect our computer** while using the internet.

>Think of the Internet as You Would a Shopping Mall

Generally a mall is not considered a dangerous place. We go there to shop, run errands and meet people, but we also take precautions while there. We wouldn't leave our car unlocked in the parking lot or walk around with our wallet hanging out of our purse. We wouldn't tell a sales clerk our social security number or give our address to a stranger we just met.

The same applies when we are on the internet. We need not fear our every mouse click, but we should take precautions to ensure our safety.

>Understanding Internet Threats

Before we can learn how to protect ourselves, we need to understand what the threats are on the internet.

<Pharming>

Pharming is a technique used to redirect a legitimate website's traffic to another illegitimate website in order to gain access to a user's personal information.

<Phishing>

Phishing is mail or instant message scams that are disguised to look like official communications from a legitimate website. They fool users into providing sensitive information like passwords, credit card details, etc.

<Spyware>

Spyware is a type of malware that collects information about users without their knowledge, often to track browsing habits and to create pop-up advertisements. Along with invading your privacy, it can sometimes interfere with a computer's functions.

Spyware is sometimes bundled with other software. Before downloading software, it's a good idea to read the reviews to see if it has a good reputation.

\<Browser Hijacking\>

Browser hijacking occurs when malware or spyware replaces your browser's home page with its own in order to force more hits to a particular website.

\<Clickjacking\>

Clickjacking is a technique that tricks users into clicking on a malicious link by adding the link to a transparent layer over what appears to be a legitimate web page.

Users think they are clicking on buttons or links in the legitimate page, when in reality they are clicking on the concealed links in the hidden page and often providing access to confidential information in the process.

\<Hoax\>

A hoax is an email chain letter that warns of impending viruses and tries to scare users into forwarding and continuing the hoax email.

\<Mousertrapping\>

Mousetrapping keeps visitors from leaving a website by locking them into a window, opening multiple windows on the desktop, or relaunching their website in a window that can't be closed.

\>Internet Safety and Privacy

In the past, internet safety generally referred to threats to our computer hardware or identity theft, but now with the internet becoming more and more social, **privacy** has become a significant safety concern. Privacy violations can especially affect our **mental and physical well-being**, thus creating distress or harm from the following:

> Undesired advertisements that can be annoying
> Embarrassing or humiliating photos or videos
> Legal entanglements from libelous posts
> Cyber-harassment or cyber-stalking
> Identity theft
> Offline or "real world" crimes

<Sockpuppet>

A sockpuppet is a fake identify that someone creates and uses to deceive others for some kind of personal gain. On most websites it is possible to have more than one account, so it is easy to create sockpuppets.

For example, John could have a few online identities for the same chat service: John45, Sarah03, and HarmonicasRock12. When he is HarmonicasRock12, he might pretend to be a 30-year-old music enthusiast to find out what music stores you go to. And when he is Sarah03, he might pretend to be a 20-year old college student to find out where you went to college.

<Avatar>

An avatar is a virtual representation of yourself. The term usually refers to a virtual image. Instead of using your picture on a social networking profile, you might use an avatar to protect your privacy.

<Dooced>

If someone loses their job because of something they posted on a blog or social networking site, they have been dooced.

<Troll>

A troll is a person who posts comments just to get a rise out of people and cause a distraction. Trolls might say something rude, assert incorrect information, or ask questions unrelated to the topic at hand. People who respond to obvious trolling posts are said to be feeding the trolls, which often causes the trolls to return and continue disrupting the discussion.

<Flame war>

A flame war is a heated argument in a social media outlet such as a web forum, mailing list or chat room, in which intentionally insulting comments and personal attacks become a focus of conversation.

<Screen name>

A screen name, sometimes called a user name, is a virtual name that is used to identify users of a website where social media is a component. Your screen name can be your real name or a pseudonym.

On sites where you regularly interact with strangers, it is a good idea to choose a pseudonym. When choosing a descriptive pseudonym such as tennis247 or partyboy18, keep in mind the image it might protray and the response it will solicit.

<Flamebait>

A comment posted by someone trying to provoke a flame, or an angry response, is called flamebait. If anyone responds to the comment, they are said to have taken the bait.

<Meme>

Meme is something that has gone viral, or spread rapidly around the internet, such as a catchphrase, hoax, topic, concept or piece of media.

Memes are often cute, funny or curious and make you want to pass them on! If you are forwarding an email, just remember that everyone who gets that email in the future could have access to your email address.

<Posts>

Content that people publish on websites involving social media, such as blogs, newsgroups, and forums are called posts. Twitter calls the posts that users make to Twitter sites tweets.

Posts are available to everyone who has access to the site. You do not always have the option to change or delete your post once it is posted. It is an instantly public representation of you or your online identify. Think before you post!

>Googling Yourself

Do you know how much **anyone can quickly find out about you** and your background just by doing a simple web search? Most people don't know that **personal records** such as their **address, phone number**, and sometimes even **pictures** can be easily accessible to anyone online. While this information may not be harmful, in some situations you could put yourself at risk by not knowing what is out there. For instance, someone only needs to find out your home phone number, and they can find your address and directions to

your house just by doing a simple online search. Google yourself regularly to find out which websites and public databases share information about you.

>Make the Most out of Your Search

Enter search terms such as your name, email address, home and work address, and phone numbers in a variety of ways to get the most accurate and complete results. Also, putting quotes around your search terms tells the search engine to find a specific phrase just how you wrote it. This will make your search more efficient

> **First** name and **last** name: "Will Bolding"
> **First, middle,** and **last** name: "Will Edward Bolding"
> **Last** name followed by a **comma** and then your **first** name: "Bolding, Will"
> **Last** name followed by a **comma,** your **first** name and **middle** name: "Bolding, Will Edward"
> **Street address**: "2521 Street Address Lane"
> **Phone number** (using no spaces or hyphens searches all instances of your number): "9195554444"
> **Email address**: "boldingsoccer@email.com"

>Removing Your Information from Websites

You can ask a website to remove your information. Keep in mind that they are not always obligated to comply with your request. If the information posted about you is a direct threat to your safety and you need help negotiating with a website to remove the content, you can contact WiredSafety.org. They will be able to advise you on your specific case.

You can also pay an outside service like Reputation.com to remove your personal information online. For most people, this kind of service is unnecessary, but keep in mind that it is an option.

[2] Passwords: The First Step to Safety

>Passwords: The First Step to Safety

Most people don't put a lot of thought into **creating a password**. It's usually easiest just to create a short, easy-to-remember password, or even just to use the same password for every account you have. After all, the average person probably won't be able to guess your password.

However, **hackers** often use password-cracking software that can keep testing many different passwords until they find the correct one, and they **can easily crack weak passwords**. By creating strong passwords, you can greatly reduce the chance that your personal or financial information will be stolen.

>Common Password Mistakes

Many people create passwords based on their **spouse's name**, a **hobby**, or a **simple pattern**, since those types of passwords are easy to remember. Unfortunately, they are also very easy for hackers to guess. To create a strong password, you will need to avoid these types of common mistakes.

>Tips For Creating Strong Passwords:

>>Never use personal information such as your name, birthday, or spouse's name. Personal information is often publicly available, which makes it much easier for someone to guess your password.

>>Use a longer password. Your password should be at least six characters long, and for extra security it should ideally be at least twelve characters (if the site allows it). If you need to write down your passwords, **keep them in a secure place**. It's even better if you "encrypt" your passwords or just write down hints for them that others won't be able to understand.

>>Don't use the same password for each account. If someone does discover your password for one account, all of your other accounts will be vulnerable. Try to include **numbers, symbols** and both **uppercase and lowercase letters** (if the site allows it). Avoid using words that can be found in the **dictionary**. For example, "swimming1" would be a very weak password.

>>Random passwords are the strongest. Use a password generator instead of trying to think of your own. Random passwords are harder to remember, so **create a mnemonic**

device. For example, "H=jNp2#" can be remembered as "HARRY = jessica NOKIA paris 2 #." This may still seem random, but with a bit of practice it becomes relatively easy to memorize.

>Using Password Managers

Instead of writing your passwords on paper where others can easily see them, you can use a **password manager** to encrypt and store them online. Some password managers can also generate random passwords, making your information even more secure. Examples of password managers include LastPass, KeePass, Firefox's password manager, and Google Chrome's password manager.

[3] Protecting Your Computer from Internet Threats

Viruses, Trojan horses, worms and spyware are all threats that can damage our computer systems. We know we need to protect our computer, but with so many antivirus programs on the market, how do we know what's best for our specific needs?

In this lesson, we will review what kind of **antivirus protection** you might need and how you can determine **which product is best for you**. In addition, we will discuss how to **back up your system** and **get the most out of your security programs**.

>What Protection Do You Need?

The best defense against internet threats is good **antivirus software**, or **anti-malware** as it is sometimes known. Antivirus software can protect you from infected email attachments, corrupt websites, internet worms, spyware and more. There are a ton of antivirus products on the market, so figuring out what you need can be quite confusing and overwhelming. Therefore, we will outline the things you need to consider to give you a better idea of what you should be looking for in an antivirus program.

>Multiple Protections

The protection you obtain should include the following three components:

> **Antivirus** – specifically protects against viruses
> **Anti-spyware** – protects against malicious software that may be gathering your information without your knowledge
> **Firewall** – screens out threats that try to reach your computer over the internet Some security suites offer a lot of additional protections, but these are the three main components that you will need.

>Security Suites

Most antivirus companies offer both a stand-alone product that only scans for viruses, and a packaged security suite that offers additional protections like firewalls, spam filtering, anti-spyware tools and more.

>>Security Suites

Security suites are generally easier to manage and offer a wide range of protection which can be useful if you are a beginner. However, in some cases the extra functions of a suite are not as good as the standalone products for that function. In addition, some suites have a tendency to slow down a computer.

>>Stand-Alone Products

More advanced users sometimes prefer to take a pick-and-mix approach, researching and selecting the best products for each component and building their own security

system.

>Things to Consider Before You Buy

>>Investigate Your Computer

If you are purchasing a new computer, you should ask the sales representative about what types of protections are already provided. Some computers come with **security software**, but you may need to subscribe to it after a trial period. Windows 7 and Mac OS X already have **built-in firewalls**. However, they cannot help you unless you make sure they are turned on.

In addition, your **web browser has security settings** that you should review. Before you choose a new antivirus software, it would be a good idea to fully investigate what protections you already have on your computer.

>>Free vs. Paid Premium Software

There are a number of **free antivirus programs** available that can offer an adequate amount of protection. However, many free antiviruses are scaled-back versions of paid software programs that companies hope you will eventually upgrade to. The disadvantage of free antiviruses is that they often do not include technical support and may have limited functions and updating capabilities. It should be noted that most paid software is based on a **yearly subscription** that will need to be renewed in order to receive the latest software and updates.

>>Mac Users

Traditionally, there have been fewer Mac viruses, and as a result many Mac users do not use antivirus software. However, Mac viruses have become **more common** recently. Many experts now recommend using antivirus software, as well as turning on the **OS X Firewall**.

>>Scareware

Malicious links disguised as **security warnings** have become a popular tactic with **cybercriminals**. These official-looking notices warn you that your computer has a virus, and claim that you need to click a link or download a program to fix it. They are trying to scare you into clicking the link, but in reality the link leads to malware.

The word for this type of scam is **scareware**. Scareware also shows up in a lot of advertisements for antivirus software, so as you begin browsing for this software make sure you are checking the address domains and going to legitimate websites for your research. Just note that any virus warnings that show up through your web browser or email are bogus.

>How to Choose an Antivirus Software

Now that you have assessed your needs and determined whether you want a **stand-alone product** or a **security suite**, you can begin the process of choosing an antivirus software. Review the interactive below to learn about what you should focus on in your research.

>>Strategies for Using an Antivirus Software

The most important thing to remember is that new viruses are being introduced on a constant basis; therefore, your antivirus software is only as good as the **latest update**. Follow these strategies to make sure you are using your antivirus software effectively:

· Make sure the **automatic update** function is turned on.
· Don't ignore your **renewal notices**. Once your subscription expires, you will stop receiving updates.
· There may be times when you need to disable your antivirus to allow certain programs, upgrades or downloads. Just make sure you don't forget to **re-enable your program** when finished.
· Your antivirus should give you specific instructions for dealing with difficult problems, but if you are having trouble with an issue, **contact technical support**.
· If you are unhappy with an antivirus program, make sure you **uninstall it** before installing a new product.

>>Additional Computer Safety Practices to Consider

Below are some additional tips that you can use to keep your computer healthy.
· **Restart Your Computer Regularly**
Some of us leave our computers on all the time, but it is a good practice to turn it off and **restart it at least once a week**. This gives your computer a chance to perform regular diagnostic checks, and fix minor issues before they become a problem.

· **Install Software Updates**
When your operating system informs you of a **software update**, download and install it. Software updates are designed to fix security vulnerabilities and other bugs in your operating system. This will help protect your computer against some of the latest threats.

· **Use System Restore**
If you have a download that is causing problems, then try your operating system's **system restore** function. This feature allows you to restore your computer to a time and place before it started to have issues.

>Back Up Your Computer

With antivirus protection, your chances of losing your files to damaging malware are greatly reduced. However, **no product offers 100% security**; therefore, it is a good idea to **back up your files on an external source**. Windows 7 and Mac Operating Systems do come with an internal backup system, but this will not help you if your computer is **lost, damaged** or **stolen**. For externally backing up your files, there are two basic options for home users: external hard drives or online backup services.

>External Hard Drives

You can purchase an **external hard drive** and copy the contents of your computer to it. The **initial backup could take several hours**, so you will need to select a period of time where you do not need access to your computer. Running the backup overnight usually works best. Follow-up backups should be conducted on a regular basis, but will not take as long because the drive will only need to copy your most recent files.

Western Digital, **Iomega** and **Seagate** produce popular external hard drives. Conduct some research on which product best suits your storage needs, or ask a computer sales representative for recommendations.

One drawback, compared to online backup services, is that your external hard drive can be lost, damaged or stolen just as your computer might be. Therefore, it is important to keep your drive in a **secure location** when not in use.

>Online Backup Services and the Cloud

You can also back up your files online—in other words, **in the cloud**. When you store something in the cloud, it's your computer is lost, damaged or stolen.

Popular **online backup services** that utilize this technology include Mozy, Carbonite and Box. The amount of storage space provided by these sites varies and you may have to pay a monthly or yearly fee for adequate storage. Again, do your research as these services are constantly changing and offer varying features.

One drawback to online backup services is that the **initial backup can be slow** and may even take days to upload if you have a large amount of files. However, subsequent backups should not take as long.

[4] Email Tips for Scams and Spam

Email has become an essential tool for communicating, which is why it is so popular with scammers, cybercriminals and advertising companies. In order toprotect ourselves from phishing scams and malware, it is essential that we learn how to safely manage our mail.

In this lesson, you will learn tips for **managing spam and email attachments**.

In addition, you will learn how to **identify and avoid phishing scams**.

>Spam

Spam is another term for **junk email** or **unwanted email advertisements**. Today, the majority of emails are spam. That's because it's very easy and inexpensive for a spammer to send an email to thousands of people at the same time, and they can do it anonymously, making anti-spam laws difficult to enforce. **Phishing scams** and **malware** are often included in spam, so it is important to be able to effectively manage the spam we receive in our inbox.

>Tips For Dealing With Spam:

· **Use a Spam Blocker.** A spam blocker can greatly reduce the amount of spam that ends up in your inbox. Most online email services like Yahoo or Gmail have a built-in spam blocker. You can also use a separate anti-spam program such as MailWasher, which can be used with Outlook or any other email program. Unfortunately, even with a spam blocker, some spam may still get through.

· **Don't Reply to Spam.** You may be tempted to reply to a spam email or click on a link within the email to unsubscribe. This may work with legitimate emails that you have subscribed to; however, spammers will rarely honor these requests. In fact, by replying or clicking on a link, you are confirming to the spammer that your email address works, and you may end up getting more spam.

· **Turn Off Images.** An email may contain images that the spammer can track. When you open the email, the images will load, and the spammer will be able to tell that your email address works, possibly resulting in even more spam.

· **Turn Off Your Preview Pane** (if your email service has one). You cannot avoid viewing spam when your email automatically displays it in your preview pane. Once you view a spam message it may actually lead to receiving more spam. Therefore, you will need to weigh the convenience of using your preview pane withyour desire to avoid spam.

· **Regularly Check Your Spam Folder.** Sometimes, spam blockers block legitimate emails. It's a good idea to regularly check your spam folder to make sure you are not missing important emails. Check your email program for settings that will "allow" legitimate emails that are being blocked.

>Email Scams

Many spam emails aren't trying to sell you something—they're trying to steal your money or personal information. **Email scams** come in many different forms, but generally they work by promising you something that's too good to be true or by making you think something bad will happen if you do not act. Popular email scams include **work-at-home offers, weight-loss claims, debt-relief programs** and **cure-all products**.

>Advance-Fee Fraud

Have you ever seen an email or classified ad (for example, on Craigslist) promising you something if you advance them a certain amount of money? The word for this is **advance-fee fraud**. It's different from other email scams because it involves corresponding with an actual person—someone who is trying to trick or mislead you by sharing their "personal story," which is almost always false.

One of the most notorious examples of advance-fee fraud is the **Nigerian letter scam**.

>Phishing

Phishing is a type of scam where an email pretends to be from a bank or another trusted source in order to trick you into handing over your personal information. Scammers can use this information to withdraw money fromyour bank account or steal your identity. A phishing email will often have a **sense of urgency**. For example, it may claim that "unauthorized charges" were made on your credit card and that you need to immediately verify your information.

>Additional Tips and Resources

· **Don't follow the link.** It's easy for an email to use the logo from a legitimate company in order to look "official," but any link you click could take you to a shady site. Always type in the web address or click on one of your own bookmarks to go to your bank or other trusted websites.

· **Report scams and spam.** Some email service providers have a "This is Spam" button or another method for reporting spam. You can also contact the company being misrepresented and report the spam. Another option is to email a report of the spam to the Federal Trade Commission at spam@uce.gov.

· **Get more information** and learn about **specific scams** by visiting New Email Scams & Warnings from FBI.gov and Phishing from OnGuardOnline.gov.

>Dealing with Email Attachments

Email attachments are especially dangerous because they can contain viruses and

other malware. When you open the attachment, the malware can be automatically installed on your computer, and you may not even realize that anything has happened. Malware may damage files on your computer, steal your passwords, or spy on you, so it's important to be extra careful when you receive attachments.

>Tips For Dealing With Attachments:

· **Don't open any attachment that you weren't expecting.** Even if an email looks like it's from someone you know, it may have been automatically sent to you by a virus. That's how many email viruses spread. If you receive an attachment from a friend, you should call or email them to verify that they meant to send it to you.

· **Keep your antivirus software updated.** Viruses can spread quickly, and if your antivirus software isn't upto-date, it may not be able to block new viruses.

· **Keep your computer's firewall on.** Firewall software helps to prevent people or malware from gaining access to your computer through the internet.

· **Scan attachments for viruses before downloading.** Many online email providers can scan attachments for viruses, and some will not let you download any attachment without scanning it.

[5] Staying Safe While Browsing

Most browsers have very similar security functions, although how you access these functions and what they are called can vary. For the purpose of our tutorial, we will focus on showing you features from Internet Explorer, Mozilla Firefox and Google Chrome. If you use the Safari or Opera internet browsers, many of these concepts will still apply.

¿ Protecting Against Malicious Sites

Every browser has security features that protect you against visiting malicious sites that contain malware or phishing scams. When you visit a malicious site, your browser will display a red warning message. To learn how each browser screens and blocks these types of sites, choose from the following:

>Internet Explorer uses its **SmartScreen Filter** to block malicious websites. Go to our Internet Explorer 8 Security Lesson to learn about the SmartScreen Filter.

>Firefox displays a red warning message and blocks access to malicious websites. Go to Firefox Safe Web Browsing to learn more.

>Chrome uses a warning message, an extra security feature called **sandboxing**, and **auto-updates** to protect against malicious sites. Go to Google Chrome and Browsing Security to learn more

¿ Keeping Your Browser Updated

New malware and phishing threats are constantly being introduced, so it is important to keep your browser updated. **How do you do this?**

1. **Make sure you have the latest version of your browser.** Your browser usually notifies you when it has a new version, but if you want to double-check, visit your browser's website. If your version is not the latest, then download the newer version.

2. **Make sure you have installed all recent updates.** Your browser also notifies you when it has updates. Ifyou think you have missed or ignored these updates, then locate the "Updates" option from your browsertoolbar and install any available updates.

¿ Domain Checking

Malicious sites often use deceptive domains to trick users into believing they are on a legitimate site. Consider the example of www.bankofamerican.com. It should read

www.bankofamerica.com, without the added "n". If you are about to download content, shop with a credit card or access your bank account, then you should carefully check the domain before continuing.

¿ Verifying Secure Sites

Browsers have security features to help you check to make sure a site is secure for

¿ financial transactions.

¿ Downloading Precautions

One of the easiest ways malware, spyware and adware can access our computers is through downloads. Therefore, we all need to take precautions when we download content to our computer, whether it is a software program, the latest pop song or a cool game we found. There are two things that provide the best defense against infected downloads: your computer's security programs and your own judgment. That's why it is important to make sure all your security programs are up-to-date and your firewall is turned on.

In addition, you can help by treating all downloads as suspicious until you determine they are safe. The following interactive offers various tips on how you can download content safely.

¿ Understanding How Your Browsing Activity is Tracked

Did you know that your actions and what you click on may be tracked when you browse the internet?

If you are surprised, then you may be wondering why and how this is happening. Sometimes it is done for website efficiency, other times to collect data, and in some cases for spying or cyber-snooping. Here are a few examples:

>A website places a cookie on your computer to remember certain data, so that it may run smoother when you return to the site.

>Websites, like Amazon, eBay or Netflix, collect data about your preferences so they may make suggestions to you for products or movies they think you might like.

>Google tracks and analyzes activity to provide statistical data to companies. These companies may use this data for marketing, advertising or to analyze the effectiveness of a website.

>Sometimes by downloading a program or signing up for a website, we agree to allow the program or site to collect data that may be provided to third-parties for advertising.

>If we share a computer, other people can spy on our activity by reviewing the browsing

history.

>Most malware or spyware is used to track and obtain sensitive information like credit card numbers and bank account passwords that can be used for identity theft crimes.

It is important to have an awareness of this tracking, in order to practice safe browsing habits based on the levelof privacy that you desire.

¿ How to Keep Your Browsing Private

All browsers have privacy features for cookies, private browsing and deleting browsing history that you can use to manage your privacy based on your needs. For a tour of these features, choose from the following:

>**Internet Explorer** – Go to Videos for Internet Explorer and select the Security video for an overview tour.

>**Firefox** – Go to Firefox Safe Web Browsing for an overview of Firefox's privacy features.

>**Chrome** – Go to Explore the Chrome Browser to learn more about Chrome's security and privacy features.

¿ How to Keep Your Browsing Private

All browsers have privacy features for **cookies, private browsing** and **deleting browsing history** that you can use to manage your privacy based on your needs. For a tour of these features, choose from the following:

>**Internet Explorer** – Go to Videos for Internet Explorer and select the Security video for an overview tour.

>**Firefox** – Go to Firefox Safe Web Browsing for an overview of Firefox's privacy features.

>**Chrome** – Go to Explore the Chrome Browser to learn more about Chrome's security and privacy features

¿ Control Cookies

Many web sites add small text files to your computer called **cookies**. Cookies can help your computer communicate with a web server, but they can also be used to **track your**

browsing activity. Every browser has tools for controlling, blocking and deleting cookies from your computer. By becoming familiar with these tools, you can help protect your information from being accessed. Be aware that completely blocking cookies may negatively impact your experience on certain web pages.

⟩**Internet Explorer** – Go to our Internet Explorer 8 Tutorial to learn how to access the cookie settings in Internet Explorer.

⟩**Firefox** – Go to Cookies to learn how to manage cookie settings in Firefox.

⟩**Chrome** – Go to Manage Cookies to learn how to manage, block and delete cookies in Chrome.

¿ Use Private Browsing

Most browsers have a tool option that allows you to browse in private. When in **private browsing** mode, the following information will not be saved by the browser:

> Pages you visit will not be recorded to your history or address bar
> Cookies will be deleted at the end of the session
> The cache that stores temporary internet files will be emptied at the end of the session
> Forms, search bars and text boxes will not save the data you enter including passwords
> Downloads listed in your download window or folder will be deleted, although the download itself will remain on your computer

It is important to note that private browsing **does not make you anonymous** on the web. Websites can still track your visit and activity through your IP address.

⟩**Internet Explorer** – Go to our Internet Explorer 8 Tutorial to learn how to access private browsing in Internet Explorer.

⟩**Firefox** – Go to Private Browsing to learn how to access private browsing in Firefox.

⟩**Chrome** – Go to Incognito Mode to learn how to access private browsing in Chrome.

¿ Delete Browsing History

Accessing your browsing history is one way a site or person can collect information about your online activity and preferences. The browsing history is a convenient feature that allows you to view and access sites that you have been to before. However, you may want to **delete your browsing history for added privacy**. Most browsers have options for

customizing how much history you delete and if you are concerned about losing a site you like to visit, you can always bookmark the site or save it to your Favorites.

>Internet Explorer – Go to our Internet Explorer 8 Tutorial to learn how to delete browsing history in Internet Explorer.

>Firefox – Go to Clear Recent History to learn how to delete your browsing history in Firefox.

>Chrome – Go to Delete Browsing History to learn how to delete your browsing history in Chrome.

¿ Additional Privacy Options

>Internet Explorer – Go to our Internet Explorer 8 Tutorial to learn about Internet Explorer's **Content Advisor** which allows you to block undesired websites.

>Internet Explorer – Go to our Internet Explorer 8 Tutorial to learn about Internet Explorer's **InPrivate**

¿ Pop-Up Blocker

Pop-ups are small browser windows that automatically pop up when you visit certain sites. Pop-ups usually contain **advertisements** that can be annoying or objectionable. However, some pop-ups may contain **malware**; therefore it is important to make sure your browser's **pop-up blocker** is turned on.

Most browsers are set to block pop-ups by default, but if you want to check your settings to make sure, choose from the following:

>Internet Explorer – Go to our Internet Explorer 8 Tutorial to learn how to check pop-up blocker settings in Internet Explorer.

>Firefox – Go to Pop-up Blocker to learn how to check pop-up blocker settings in Firefox.

>Chrome – Go to Pop-ups to learn how to check pop-up blocker settings in Chrome.

If you do encounter a pop-up that seems suspicious, **do not click "OK", "Cancel" or "Agree"** to try and close the window, as this may access malware. Close the window by clicking the **X** in the upper-right corner or by pressing **ALT+F4** on your keyboard (if you

use Windows).

¿ How to Clear Your Cache

Web browsers store pages, images and downloaded content to the **cache** when you visit sites. The browser can speed up access to sites by loading pages from the cache rather than re-downloading content when you return to a site. However, with high-speed internet connections you may not notice the difference. In addition, the cache can take up space over time causing your browser to slow down. Therefore, it is a good idea to **clear the cache on a regular basis** to help free space on your computer.

Clearing the cache can also **protect your privacy** as it deletes stored content and information from your browsing activity.
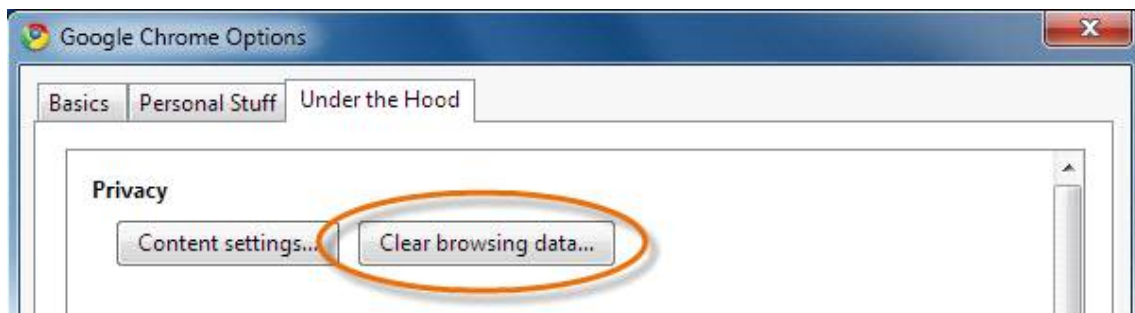
To learn how to clear the cache, choose from the following:

>**Internet Explorer** – To clear the cache in Internet Explorer, go to Delete Browsing History and make sure you select "Temporary Internet Files" (cache) to delete.

>**Firefox** – Go to Clear the Cache to learn how to clear the cache in Firefox which includes using "Clear Recent History" along with more advanced settings.

>**Chrome** – Go to Clear Browsing Data to learn how to clear data including the cache in Chrome.

[6] Protecting Your Financial Transactions

The internet has made banking, shopping and conducting other financial transactions online quite convenient. But when it comes to our money, we definitely want to make sure our transactions are safe.

In this lesson, we will review strategies you should employ when dealing with money and the internet. You will learn how to make sure a **website is secure**, including checking the **SSL Security Certificate**. In addition, we will show you the steps you need to take to make **shopping online** a safe and enjoyable experience.

When is a Website Secure for Financial Transactions?

Before sending any sensitive or financial information online, you want to know that you are communicating with a **secure site**. Secure sites make sure that all information you send is **encrypted**, or protected as it travels across the internet. The **https** address heading and your browser's **security symbol** are two signs that indicate you are on a secure site.

>Https

Web addresses either begin with **http** or **https**. If the address is **https** then the information you send to it is **encrypted** and will look like gibberish if intercepted by cybercriminals.
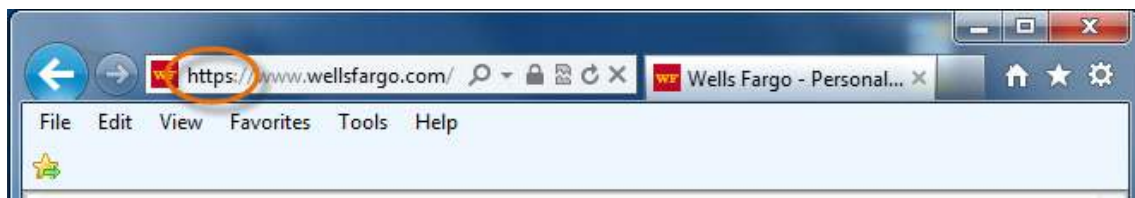
>Security Symbol

Your browser will use a **security symbol** or a **lock** to indicate that the **browser verifies** the website is a **secure site**. As seen in the examples below, the look of each browser's symbol can be slightly different, and it is usually located in the address bar.

Security Alerts and the SSL Certificate

>SSL Certificate

Secure sites have an **SSL certificate**. An **SSL certificate does two things**. First, it acts like a **virtual passport** or **driver's license**. It means, "I am who I say I am." Second, it enables **encryption**. If a site does not have an SSL certificate, the address will begin with http instead of https, and your browser will not show a lock symbol. If it does have an SSL certificate, you can **access it by double clicking on your browser's lock**.

>Security Alerts

Current versions of Internet Explorer, Firefox, and Chrome **verify SSL certificates for you.** They will alert you if the certificate is not up to date, or if it was not issued from a trusted **certificate authority**. To guarantee these alerts, **make sure you are always running the most updated version of your browser**. For more information on these alerts, choose from the following:

>>Internet Explorer 8 uses a four-level color system to alert you about **certificate validation**. Go to our Internet Explorer 8 Security Lesson to learn more.

>>Firefox verifies certification with its **One-Click Site ID**. Go to About One-Click Site ID to learn more.

>>Chrome uses basic warning messages and some color-coded domain highlighting to alert you about certificates. Go to Security Settings to learn more.

What About Phishing?

Secure sites can protect your information from being **intercepted** by cybercriminals, but you also need to be aware that cybercriminals can **contact you directly through phishing scams**. Many phishing scams are made to look like official notices from your **bank, credit card company or other financial institutions**.

Cybercriminals can send official looking emails and create official looking websites pretending to be an organization you trust, in order to trick you into giving up credit card numbers and other account information.

Never respond to emails, pop-ups, text messages, or phone calls from your financial institutions asking for personal information. **Always call them** to verify if there is a problem.

Safe Online Shopping

Online shopping is a convenient way to shop and gives you access to products that may not be available to you locally. However, as with any online financial transaction, there is the potential for fraud. When using a shopping site, you should practice the normal safety precautions that include **making sure a site is secure, carefully reading the**

terms of use and utilizing your security programs.

1. Research the Company of Seller
2. Closely Examine the Product
3. Understand the Terms and Costs
4. Pay with a Credit Card
5. Save and Print a Record of the Transaction
6. Enjoy Your Purchased

Additional Tips for Conducting Online Financial Transactions

>Leave No Trace

Consider always doing financial transactions in a **private browsing session** so that your browsing history, passwords and other private data will not be saved or accessible to anyone who uses the computer after you. Make sure to **log off the website** and **close all browser windows** when you are finished. And if possible, do not conduct any financial transactions from a **public or shared computer** or over a **public wireless internet connection.**
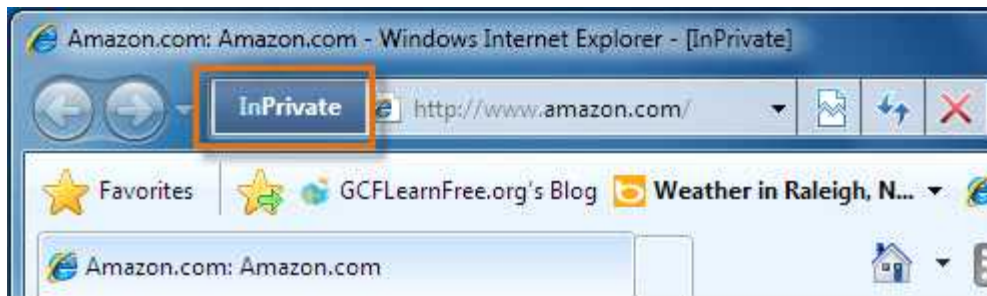
>Be Careful with the Back Button

If you are making a purchase from an online store, the site has to gather and process information about your purchase. If you press the **back button** after you have entered information, it may cause the information to be sent again. Depending on the site, this could result in your credit card being charged twice. A similar thing could happen on a banking site if you press the back button while transferring funds.

If you accidentally press the back button, your browser will often ask you if you want to "send the form again," and you can click **cancel** to prevent it from re-sending.

[7] Smart Social Networking and Communication Tips

Social networking through sites like Facebook, Twitter and LinkedIn is flourishing like never before and many of us have now become comfortable with communicating online. However, before we relax too much into this new way of interacting, we may need to take a closer look at the issues regarding safety and privacy in order to protect ourselves both online and off.

In this lesson, we will introduce current issues regarding **privacy**, in addition to providing strategies and tips for communicating safely and effectively while online. These tips will include how to **set up a profile**, **what to consider before you share**, what to do when you **meet people face-to-face** and how to practice good **netiquette**.

Social Networking and Privacy

Social networking and **sharing on the web** are taking off in ways that we may never have imagined. But along with all of the fun social aspects, come big questions about **privacy**.

Review the interactive to see why everyone should be aware of the consequences social networking may have on privacy.

Additional Resources

Go to Online Privacy & Technology from **PrivacyRights.org** for more information on how privacy is affected by technology.

Go to Can the law keep up with technology? from **CNN.com** to review an article on legal cases regarding online technology.

Setting Up Profiles on Social Networking Sites

Most social networking sites require you to **set up a profile** to join. Some profiles are simple and may only include a **screen name** and **image**, like when you join a website's discussion board. Other profiles, such as those on YouTube or Facebook pages, can give you a lot of freedom to be creative and elaborate. Review the interactive to **learn how to safely represent yourself** in a profile.

Don't forget to create a strong password, so no one can access your accounts.

Review Your Privacy Settings

Social networking sites have settings for privacy, but many people either do not customize them or do not understand how to do so. Facebook is a perfect example of a site with complicated settings that have the potential to expose a user's private

information. **So with all this confusion, how can you make sure your profile is protected?**

>Carefully Review a Site's Privacy Policy

It is best to thoroughly review the privacy policy of any site that you join in order to understand how your information is being displayed and used. If the privacy policy is overwhelming and confusing, then conduct some research and see what kind of advice or tutorials are offered.

>Look for Advice or Tutorials

Conduct a search on how to set up a profile for the site that you are interested in. Often, there will be blogs or how-to tutorials that will uncover the things you really need to know about how to maintain your privacy on certain sites.

>Google Yourself

The best way to see how your profile is being displayed is to enter your name into a search on Google.

Netiquette Tips

In order to avoid awkward or negative experiences while communicating online, it is helpful to know the basics of **netiquette**. Netiquette refers to network etiquette for online communications and can be very helpful for beginners. Listed below are a few basic tips everyone should practice when communicating online.

>Be Respectful

Always treat others as you would like to be treated. A good rule of thumb is not to communicate anything online that you would not be willing to say to a person's face.

>Don't Be Too Quick to Take Offense

In online communication, we usually cannot see facial expressions, judge body language or hear tone of voice. Therefore, it is very easy to misinterpret the meaning of a message or post. Also, the technology itself tends to make us less personable. Before taking the offensive, clarify a message with the sender.

>Use Emoticons and Abbreviations to Convey Meaning

To convey tone, humor and meaning, learn common abbreviations, like "lol" (laugh out loud) or "jk" (just kidding), or use emoticons, such as :) or :(or =0. However, be careful not to overuse these symbols, otherwise your messages might become annoying or hard to read.

>Protect the Privacy of Others

As a courtesy, you should ask permission before posting photos or videos of others online. You should also protect the email addresses of others by deleting them from emails

you forward.

>Check Your Spelling, Grammar and Language

Using incorrect spelling, poor grammar or offensive language is unpleasant to read and can cause people to portray you negatively. Spare a few moments to check your communication before sending it and avoid using foul or inappropriate language.

For a more extensive resource on netiquette, visit Albion.com or NetworkEtiquette.net. Also, keep in mind that the rules may vary for **email, online chats, web forums, online gaming** and other social networking outlets. It may be smart to search for specific rules pertaining to the particular outlet you are using.

Think Before You Share!

As we become more comfortable with communicating and sharing online, we still need to keep in mind that what we post has the potential to get us into trouble. Something about the impersonal nature of technology makes us feel safe about writing or posting things that we would likely not say to an individual face-to-face. In some situations, we definitely need to think before we hit send.

Consider the following examples:

>A teacher in North Carolina complained about her students on Facebook and ended up getting suspended and then reassigned to a different position. Think before you hit share, especially when posting comments about your job.

>A job candidate sent a scathing email when he was rejected for a position by a hiring manager. He may have been considered for a second opening, but instead he destroyed his chances. Think before you hit send, especially if you are upset, frustrated or angry.

>A politician in South Carolina used his work email account to send romantic messages to his lover. The messages were retrieved and published in the media causing great

embarrassment. Think! Never post or write personal or inappropriate content in the accounts you use on the job. They are not considered private and any content belongs to the company and can be used against you.

>An administrative assistant takes a sick day and heads out to the beach for a day of fun. Unfortunately, her "tweets" about her great day at the beach get back to her boss. Think! Managers are now using social media more and more to catch employees participating in unprofessional behavior.

We tend to use online sharing for casual communication and socializing; therefore it's easy to become careless. Here's a good rule to keep in mind: Do not write or post anything you would not be comfortable sharing with an entire room full of people.

Precautions to Take When Meeting People Face to Face

As we get to know people online, there may be times when we want to meet them in person in the real world. It is extremely important that we take precautions before meeting face-to-face with someone from online. Criminals and fraudsters can easily fake their identities and pretend to be someone else while online in order to lure victims into meeting with them in person.

1. Protect Your Identity
2. Tell Someone
3. Research the Person
4. Meet in Public
5. Bring a Friend
6. Repeat Until Safe

You can also chat with a person on the phone before meeting them in person, but be careful to block your caller ID or use an anonymous phone service like Skype. Never use your home phone or give out your phone number as this information can be used to identify and locate you.

Warning Signs

Review the following tips to avoid running into trouble with people you meet face to face.

>**Trust your instincts** and pay attention when something doesn't feel right. Watch for **"red flags"** and questionable characteristics. Is the person too controlling? Do they talk badly about others? Do they avoid certain questions? Are they quick to get mad? Your gut instincts are a good measure of whether you should proceed with someone or end

things right away.

>**Take your time and maintain control**. At any time you feel uncomfortable, you have the right to walk away and end communications without any need to explain. Do not allow someone to persuade or badger you into moving forward before you are comfortable with doing so. If a person is genuine, then they will understand your need to take things slow.

>**End things with someone who brings up "sex talk" too soon or asks about money**. These people are almost always insincere and could end up scamming or harming you.

>**Avoid drinking alcohol** before or during your meeting, as this can impair your ability to judge another person and the safety of the circumstances.

Additional Resources

Go to these additional resources for **online dating** and **online buying and selling**:

> Online Dating Safety Tips from **OnlineDatingMagazine.com**
> 11 Safety Tips for Online Dating from **iLookBothWays.com**
> Safety Tips for Selling Things on the Internet from **iLookBothWays.com**

[8] Cyber-Harassment, Stalking and Addiction

Unfortunately, our use of the internet has the potential to turn ugly. As we integrate technology more and more in our lives, we need to be aware of the potential for cyber-harassment, stalking and internet addiction.

In this lesson, we will discuss how to prevent negative communications and how to respond to cyber-harassment and cyber-stalking. In addition, we will explore the aspects of internet addiction and provide resources for assessment and treatment.

The Negative Side to Communicating Online

Social networking can be a great way to communicate on a global level and a fun way to socialize and maintain relationships. However, this form of communication can have its negatives. The anonymous nature and open access of the internet allows for the **potential to be exposed to offensive, derogatory and inappropriate communications**. Usually, you can ignore this type of content or simply leave a page where you are being exposed to it.

However, there may be times when things suddenly escalate into the following:

>**Flame Wars:** heated arguments online where intentionally insulting statements and personal attacks become the focus of conversation

>**Cyber-Harassment:** any kind of harassment that happens online

>**Cyber-Stalking:** cyber-harassment that is ongoing, with the cyberstalker often using multiple online resources to harass the victim, such as emails, instant messages, and posts written on various message boards

Tips to Help Prevent Cyber-Harassment and Cyber-Stalking

Unfortunately, these experiences can create mental and emotional distress and have the potential to become harassment offline or in the "real world." While most sites have policies against such negative content, they are often limited in how they can respond and control it. Therefore, it is important to take the following precautions to prevent these circumstances from occurring in the first place.

>**Avoid Getting Involved in Flame Wars**

It is important to think before you share comments, especially if they are controversial, religious, political or disagreeing in nature. These types of posts have the potential to provoke a negative response and should be considered carefully.

>Avoid Using a Revealing Screen Name

Choose a screen name that is gender and age neutral, and that does not reveal your name, or any personal information about you. If you have a racy or attention-grabbing nickname, be aware that this may cause you to be the target of unwanted attention.

>Avoid Sharing Personal Information

Be extremely cautious about sharing any personal information online. The more someone knows about you, the easier it is to access you online and offline.

>Responding to Cyber-Harassment and Cyber-Stalking

If you do find yourself in a cyber-harassment or cyber-stalking situation, then there are specific steps you should take to respond. Review the interactive to learn the details of these steps.

Internet Addiction

Internet addiction is becoming a growing concern as more and more people are spending larger quantities of time online. Internet addiction is generally defined as a compulsive use of the internet and may include the unhealthy use of the following:

> **Online gambling**
> **Online shopping** including auction sites like eBay
> **Online dating** including online affairs
> **Cyberporn and cybersex** sites
> **Social networking** sites like Facebook and Twitter
> **Online gaming**
> **Compulsive surfing of the web** for entertainment and information

For some of us, spending a lot of time on the internet may seem like a necessity as we integrate technology with our daily work tasks, home life tasks and communications. But how can you tell when your internet use has shifted from normal to unhealthy?

If your use of the internet starts interfering with your life offline then there may be a problem. Signs include neglecting your work, relationships and daily responsibilities in order to spend time on the internet. In addition, if you have an extreme emotional response to the internet, like feeling anxious when you are offline and euphoric when you get back online, then you may need to seek help.

[9] Wireless and Mobile Device Safety

The days when we had to be tied to a desk in order to use the internet are long gone. With devices like the iPad and smartphones, along with the widespread availability of wireless signals, we can now access the internet from just about anywhere at anytime. So what precautions should we take while we are on-thego?

In this lesson, you will learn tips for securing your wireless network and mobile devices from internet threats, especially in Wi-Fi hotspots. You will learn how to practice mobile device courtesy. In addition, we will discuss strategies for using mobile devices while driving.

Wireless Network Security

If you are using a wireless network (also known as Wi-Fi) to access the internet, then you need to make sure it is secure; otherwise, all of your activity and information could be accessible to hackers and cybercriminals. Securing a wireless network can get very technical, so beginners may prefer to get help from their internet service provider (ISP). When setting up your wireless security, consider the following tips:

> **Limit your signal strength** so that it cannot be detected beyond the boundaries of your home.

> **Disable SSID broadcasting** so your network is not visible to other wireless users within its signal range.

> **Use a strong password.** You should choose a password or passphrase that's easy for you to remember, but hard for other people to guess.

> **Enable MAC (Media Access Control) address filtering** to prevent unauthorized wireless clients from breaking into your network.

> Make sure your network utilizes **WPA (Wi-Fi Protected Access)** or **WPA2**.

> If you use the older **WEP (Wired Equivalent Privacy)** instead of WPA, then make sure to maximize the encryption.

Wi-Fi Hotspot Safety Tips

Being able to access the internet through Wi-Fi hotspots in coffee shops, hotels, airports, etc. can be quite convenient. However, these Wi-Fi hotspots are often not as secure as your home network. Review the following interactive to learn how to stay safe when connecting to a public network.

Mobile Device Safety

In recent years, mobile phones have become much more powerful, allowing you to browse the internet, check your email, download programs, and more. But these new abilities also mean there is a greater risk of viruses and other malware, as well as threats to your privacy. When using a mobile device, you should use the same caution that you would use with a computer.

Tips for Avoiding Malware

Some companies, such as Norton and Kaspersky, offer antivirus software that can run on a mobile phone, but do your research as they may potentially slow down your phone's functions. Here are some tips to help you avoid malware on your mobile device.

>**Keep your mobile phone updated.** Check your phone manufacturer's website for instructions on downloading security updates.

>**Be cautious when downloading programs or apps.** A program or app could contain malware, so research it before downloading.

>**Avoid "free offers" and "free ringtones."** An email or instant message that offers software for download, such as a ringtone or security update, may contain malware.

>**If something seems suspicious, trust your instincts.**

Privacy on the Go

If privacy is important to you, you should pay close attention to the apps you install on your device. Always review their terms of service and privacy policy, so you know how they may or may not be using your information. You can also customize your privacy settings if the app gives you that option.

In addition, you should think back to privacy concerns that you've already learned about (for example, geolocation), and how they might affect your experience on a mobile device. This is especially important for social networking apps, and other apps that track your activity.

Wireless and Mobile Device Courtesy

With the new wireless capabilities and advanced mobile devices like the iPad and smartphones, we can communicate and access media almost anywhere and anytime. However, these new technologies are also becoming increasingly intrusive and can sometimes contribute to troublesome behavior. Disruptive ringtones, noisy conversations and

rude texting can disrupt, annoy and anger others, leading to what is now being called Cell Phone Rage.

Mobile Devices and Physical Safety

Distracted Driving

The number of accidents related to driving while talking, surfing and texting on mobile devices is increasing significantly. So why do the majority of us continue to participate in these activities, despite the overwhelming evidence of their dangers? Consider the following:

>We believe we can multi-task.

The brain is capable of engaging in more than one activity at a time if one of the activities is passive, or noninteractive, like driving and listening to music. However, our brains cannot participate in two interactive behaviors that require thinking and responding at the same time, like driving and dialing a phone number.

One activity is always being ignored for the other, thus exposing us to danger.

>We believe we are better drivers than others.

We may get upset with others for driving recklessly while talking on their cell phones, but we believe we are better drivers and can pull it off. In reality, we are not driving well either, but "inattention blindness" prevents us from noticing.

>We believe we have to respond.

In today's world of instant access, we believe we have to be constantly available; therefore, ignoring a phone call or text message may seem unheard of. Also, some of us get a little "rush of excitement" when we hear that ring or bing telling us we are wanted. Unfortunately, these emotional desires seem to overrule the reasonable side of our brain that cautions us to be safe.

For your safety, as well as the safety of others, review the interactive to learn how to stay safe while using mobile devices and driving. Accidents from distracted walking are also on the rise. For many of the same reasons as listed above, walking and engaging with a mobile device can also prove harmful to your health.

Cell Phone Radiation and Cancer

Interest and debate regarding cell phones and their link to cancer, particularly brain cancer, is on the rise due to increasing research. Cell phones, as well as other wireless devices, emit low-frequency "non-thermal" radiation that is considered the cause of the

cancer. At this time, the World Health Organization, American Cancer Society, National Cancer Institute, and Food and Drug Administration have all found that the use of cell phones do not pose a public health risk. However, they do support continued research on the subject, especially in regard to long-term exposure.

[10] Links to Resources for Internet Safety

General Internet safety websites and resources:

>WiredSafety.org, an extensive global resource on Internet safety
>OnGuardOnline.gov, maintained by the Federal Trade Commission (FTC) and includes
   games, videos, and information on various topics
>NetLingo.com, for the latest Internet terms and text and chat acronyms
>Reputation.com, to remove personal information from websites
>StrongPasswordGenerator.com, to create stronger passwords

Independent reviewers of software programs:

>CNET.com
>TopTenReviews

Email scams, spam, and phishing:

>Email Scams from FBI.gov
>Email and Web Scams: How to Protect Yourself from Microsoft.com
>Phishing from OnGuardOnline.gov
>Spam Blocker Software from FireTrust.com

Browsing security

>P2P Security from OnGuardOnline.gov
>Safe Downloads from CNET.com
>Internet Explorer download page, for information on IE's privacy features
>Firefox's Privacy Page, for an overview tour of Firefox's privacy features
>Explore the Chrome Browser, to learn more about Chrome's privacy features

Online banking, shopping, selling, and other financial transactions

>Online Shopping from OnGuardOnline.gov
>SafeShopping.org from the American Bar Association
>Better Business Bureau Online, for researching businesses

>Safety Tips for Selling Things on the Internet from iLookBothWays.com

Online dating

>Online Dating Safety Tips from OnlineDatingMagazine.com
>11 Safety Tips for Online Dating from iLookBothWays.com

Social networking

>Online Privacy & Technology from PrivacyRights.org (how privacy is affected by technology)
>Albion.com and NetworkEtiquette.net, for resources on Netiquette

Internet addiction

>NetAddiction.com
>Internet Addiction Test from NetAddiction.com
>Other Self Tests for Internet-Related Addictions from NetAddiction.com
>Internet Addiction - Signs, Symptoms, Treatment, and Self-Help from HelpGuide.org

Wireless and mobile device safety

>Wireless-Safety.org, for information on securing a wireless network
>MobileBeyond.net, for an article on the cell phone and brain cancer debate
>Hotspot Location Resources from GoDISH.com, for a list of articles about Wi-Fi radiation,
>wireless security, and other wireless hotspot information.

-FIN-