Introduction to Computer Privacy

Objectives

In this chapter you will:

1. Discuss how to keep the information on your computer private
2. Understand how to prevent other people from accessing your files.
3. Discuss how to be safe while using the Internet
4. Identify a secure website
5. Delete your browsing history
6. Discuss how to be safe while using email
7. Delete your junk mail

Computer Privacy Basics

**Pre-Reading**

## Discussion

1. What can you do to make sure that nobody can access the files on your computer without your permission?
2. Is it okay to give out personal information on the Internet (address, phone, social security number, etc.)?
3. Have you ever purchased anything on the Internet? Or know someone who has? If so, did you/they use a secure website?
4. Is it okay to open emails from senders that you do not know? What about attachments from unknown senders?
5. Have you ever seen advertisements in your email inbox?

Read the email message below. Does anything seem strange about it?

From: Internal Revenue Service (admin@irs.us.gov)

Sent: Thursday, October 08, 2009

To: [your email address]

Subject: IRS Notification—Claim Your Refund

Dear IRS customer,

As of our last review of your tax returns we have determined that you are eligible for a tax refund in the amount of $374.60!

In order to claim your refund, you must submit verification of your identity, your social security number, and mailing address today. If you do not respond by the deadline, your refund will be delayed

As we are committed to your ongoing satisfaction and protection, we will keep all information you provide completely confidential.

thank you

IRS accounts manager

# Vocabulary

Discuss the words that you recognize below with your partner. What do you think they mean?

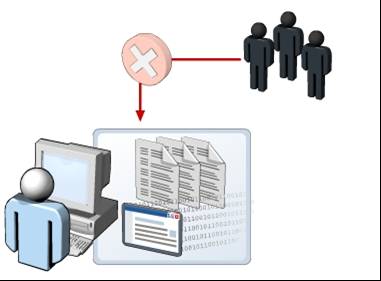
As you read this chapter, find each of these words and write the definitions for the words below.

|  |  |
| --- | --- |
| **Word** | **Definition** |
| 1. Virus |  |
| 1. Hacker |  |
| 1. Spyware |  |
| 1. Firewall |  |
| 1. Cookies |  |
| 1. Malicious |  |
| 1. Scam |  |
| 1. Phishing |  |
| 1. Spam |  |
| 1. Junk Mail |  |

An Introduction to Computer Privacy

In this chapter you will learn about computer privacy. You save your personal files and documents on your computer and don’t want anyone to read them without your permission. Computer privacy includes two main concepts:

1. Making sure that nobody can access your files without your permission.
2. Being careful while using the Internet

When you go to the bank, you have to provide identification and a personal code in order to access your accounts. The same is true for your data on a computer. You can take steps to improve the privacy of your data on your computer! This lesson introduces you to some steps that will help you to protect your computer, your software, and the data on your computer.

# A. Computer Privacy: Privacy from Other Users

C:\Documents and Settings\htatton\Local Settings\Temporary Internet Files\Content.IE5\S6Z6S0PC\MCj04114880000[1].wmfImagine that you finished a very important report on your computer. You have been working for weeks to prepare this document and now you want to share it with your supervisor. You have only one copy of this report on your computer and it is important that nobody can open it, change it, or delete it!

However, this is a sad story! Another employee uses your computer while you are out to lunch and accidentally deletes the document report from your computer! Oh No!!!

The following table explains the steps that you can take to make the data on your computer private.

| **STEP** | **DESCRIPTION** |
| --- | --- |
| User identification | An effective way to keep your files (documents, pictures, etc.) safe is to prevent other people from seeing those files. One way to do this is to set up separate accounts for each user. This way, each user can save and delete files, but ONLY his/her files.  This is how the Carlos Rosario computers are set up. When you log into a computer, you have a user account. You use your user name (your ID) and your password to access your account (your files)! |
| Keep IDs and passwords secure | Your ID and password are like a key to your computer. Anyone who knows your ID and password can access your computer and use your data/files. You must keep your ID and password a secret.  Do not share your password with others. Do not write the password and leave it on your computer or desk. If you think that someone knows your ID or password, change it immediately. |
| Back up data | You can also help protect your files from loss or damage by making copies of important files and storing them on a different storage media, such as CDs, external drives, or flash drives. This process is known as backing up data. You should keep the backups in secure locations, so that you can use the backup data in case the original data is damaged or deleted. |

# B. Computer Privacy: Privacy on the Internet

Connecting your computer to the Internet introduces it to a world of information and entertainment. However, it also leaves your computer open to many online threats. For example, it becomes easier for **viruses** to transfer from an infected computer to your computer. *Viruses* are computer programs that can damage the documents, files and software on your computer. They can also slow your computer down and take over functions of your computer. These viruses can reach your computer, without your knowledge, through the Internet if you are using unsafe websites.

You can protect yourself when you use the Internet by using a combination of steps such as creating strong passwords and using antivirus software. The following table explains the various steps that you can take to make online transactions more private and secure.

*With your partner, decide who will be reader A and who will be reader B. Only read your assigned parts. Afterwards, share what you learned.*

| **STEP** | **DESCRIPTION** |  | |
| --- | --- | --- | --- |
| Use strong passwords (A) | A strong password is a password that cannot be guessed easily.  A strong password is your first defense against security and privacy threats. | | |
| Protect against hacking and spyware (A) | While you are browsing the Internet, it is possible that a software program installed on your computer is sending your personal information to a **hacker** in another country. Such software programs are examples of **spyware**. How does spyware get installed on your computer? Usually, it gets installed when you click on a pop-up window and agree to download something.  Make use of Internet service provider (ISP) support for online security. The support can be in the form of **antivirus** and **anti-spyware** software. | | |
| Install and update protective software (A) | You need to protect your computer against threats such as viruses. You can protect your computer from viruses by installing antivirus software. These protective software programs help you find and remove viruses that are in your computer. They also prevent new ones from infecting your computer.  It is a good practice to use a **firewall**. A firewall is software that filters out and blocks certain websites or webpages from getting to your computer. Your Operating System has firewall software. You just have to turn it on! Installing a firewall also protects against hackers by restricting access by other online users. | |
| Perform online transactions only on secure sites (A) | While shopping online, you usually need to provide sensitive information such as your bank account number or credit card details. Therefore, it is important to make sure that you make online transactions only on secure websites.  A website is secure if its web address starts with *https*. If the address starts with http:// it is NOT secure. If it starts with https:// it IS secure – the “s” means “secure” and tells you that the website uses security in order to protect your data. It also certifies that the website is genuine and ensures that the data you provide to the site is not misused.  When you enter a secure website, you will see the locked padlock icon that appears in the Address bar. You can also check the security certificate of a website before performing any online transaction on that site. | | |
| Clear browsing history periodically (B) | The websites that you visit while browsing the Internet are saved in your browser’s *History*. Also, while you browse the Internet, information is stored in a special internet temporary memory. This temporary memory is known as *cache memory* or *temporary internet files*. The files stored in the memory record information about the web pages you visit.  Some of these temporary Internet files might contain your personal information, such as your username and password, which can be accessed by hackers. To prevent hackers from getting your personal information, delete your browsing history.  While visiting a website, you might notice that it displays your name! This is possible through the use of **cookies**. *Cookies* are small files that are created on your computer to identify and record your preferences. Their purpose is to provide a more personal experience while visiting a website. However, cookies can also be a threat to computer privacy because they contain your personal information. For example, the cookies might contain your credit card details that you have used while shopping online. For these reasons, it is a good idea to delete cookies in order to prevent your personal information from being misused. | | |
| Avoid sharing personal information (B) | Some websites require you to fill out forms containing personal information such as your name, gender, and age. But, remember that hackers can access and misuse this information. Some companies may also use this information to send you advertisements through email. So, before you share any personal information on a website, make sure that there is a specific need to provide the information! | | |

# TASK 1 – FIND A SECURE WEBSITE

1. Open Internet Explorer
2. Go to [www.chase.com](http://www.chase.com)
3. Notice if the web address becomes http OR https
4. Notice the padlock icon



# TASK 2 – DELETE YOUR BROWSING HISTORY

1. Open Internet Explorer
2. Click on Tools 🡪 Delete Browsing History
3. Write each of the items that is included in your Browsing History below (one is included as a model)

|  |  |
| --- | --- |
| **Browsing History Item** | **Description** |
| *Temporary Internet Files* | *Copies of websites, images, and media that are saved for faster viewing.* |
|  |  |
|  |  |
|  |  |
|  |  |

1. Click on “Delete All” at the bottom of the box.

# C. Computer Privacy: Privacy on Email

E-mail is used for business and personal communication. However, hackers, **scams**, and the people who create viruses use e-mail for **malicious** reasons, which means that they want to cause damage. For example, these people can send e-mail attachments containing harmful software. These people can also use e-mail to ask for sensitive information or to interest you in fake advertisement. It is important for you to take certain steps to ensure e-mail security.

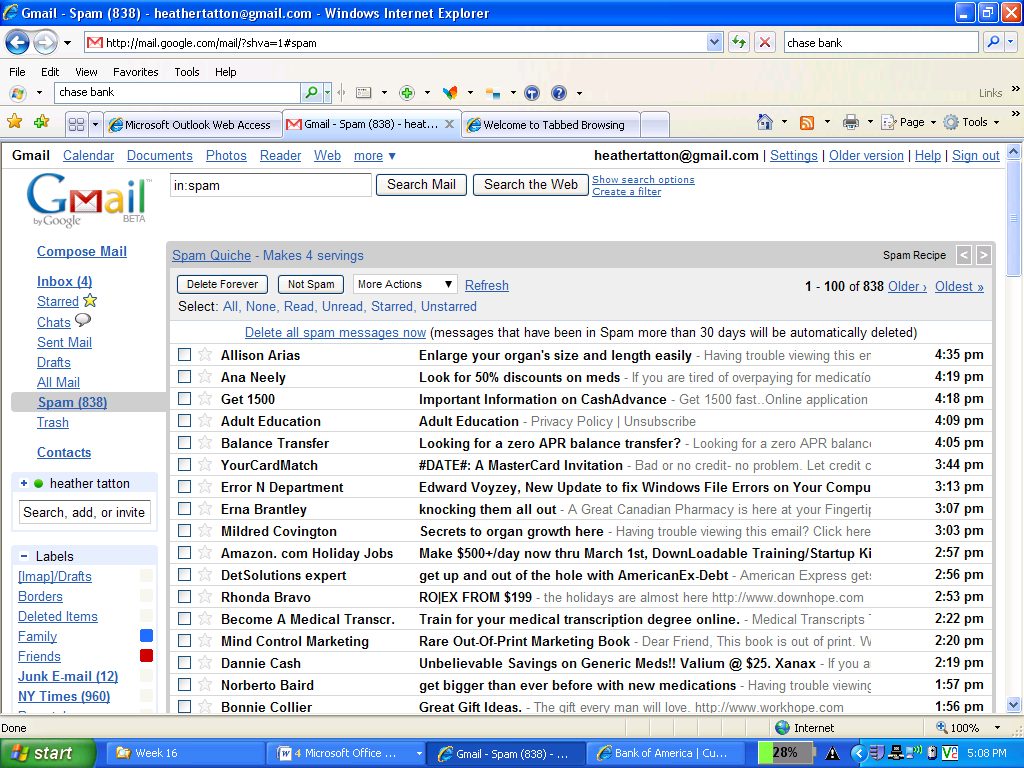
To ensure e-mail security, do not open e-mail with attachments from senders who you do not recognize, do not respond to junk mail (email from advertisements that you do not recognize). The following table explains the steps to ensure e-mail security.

|  |  |
| --- | --- |
| **Be careful when opening e-mail messages with attachments** |  |
| You can send e-mail attachments to share files with your friends. You might receive a photograph or a music file as an attachment in an e-mail message. However, you need to be careful while opening any mail containing an attachment because it is the most common way to spread viruses. |

|  |  |
| --- | --- |
| **Do not respond to advertisements that you didn’t ask for!** |  |
| You may receive unwanted e-mail messages from unknown senders including individuals and companies that are advertising their products or services. These messages are known as **junk mail** or **spam**.    Junk mail can often include content that is harmful for your computer. Some junk mail is used for “**phishing**” or “**scams**” and is used for stealing identities. A phishing or scam email might ask you for your bank account number or other personal information. Therefore, you should not reply to junk mail! You should delete junk mail whenever you receive it. E-mail programs, like Gmail, include a SPAM or Junk Mail folder. You can delete your spam from this folder at any time. |

# TASK 3: DELETE YOUR SPAM!!

1. Open your Gmail account
2. Click on the Spam Hyperlink – this is your Spam folder
3. Look at the Spam emails. Make sure that there aren’t any messages that are actually from people you know!
4. Click on “Delete All Spam Messages Now”



# Review Case #1

*Directions: Read the story below and write advice to Dwight’s parents below.*

Dwight Lee, a sixth-grader, recently got his very own computer. It was a gift from his parents, who bought it to help him with his studies when he enters middle school next September.

Dwight loves having a computer of his own; he can be online as much as he wants without his little sister or parents complaining or kicking him off. In fact, most days, Dwight goes straight to his room after school, shuts the door, and gets on his computer.

When his parents ask what he spends so much time doing online, Dwight tells them that he spends most of the time doing his homework, and some of the time talking to “friends” he has made through social networking and game sites. His profile, which he has posted on all the popular social networking sites, includes his favorite songs, a list of his hobbies, and information about where he goes to school. There are also personal photos that Dwight’s best friend, Lee, posted using Dwight’s password.

Dwight’s parents have heard of sites such as Facebook and MySpace and Twitter, but they have never visited them themselves.

One of Dwight’s new friends, who he met on a game site, has invited Dwight to meet in person at a local movie theater. He’s a little concerned about meeting his new friend alone, but when he suggested meeting at his home, with his parents present, his friend made him feel bad and pressured him to get together someplace private. They are planning to meet next week.

**Your advice:**

# Review Case #2

*Directions: Read the story below and write advice to Celia below.*

Millie and Jose did not grow up with computers—they used typewriters and sent letters by “snail mail.” They’ve just “inherited” their daughter’s old computer. Celia thinks her parents will enjoy being able to shop and bank from home, send and receive email, and see the latest pictures of the grandkids.

Celia comes home for the weekend to set up the computer for her parents. Before she leaves Sunday, she teaches them the basics. She tells them she’ll be back next weekend to help them with any issues they run into.

Millie and Jose take to the computer like fish to water. In their first week:

* Millie uses the word processing software to type up 27 of her favorite recipes.
* Jose uses his debit card to purchase a fishing rod from a private vendor he came across while “surfing.”
* Millie sets up an online banking account. She doesn’t want to forget the password, so she makes it Willie, the name of their dog.
* Jose responds to an email requesting his name, address, and credit card information in order to verify a transaction with a major online vendor.
* Millie downloads free songs from a site she found by doing an online search for “free music.”
* Millie emails her credit card information to their son so that he can buy a plane ticket home from college for his parents’ 35th wedding anniversary.
* Jose responds to an email from a stranger who says she will share her lottery winnings with him if he will help her claim the jackpot.

When Celia returns the following weekend, she realizes she should have given her parents more information and instruction regarding protecting their computer data and personal information.

**Your advice to Celia:**