

KEEPING YOUR PERSONAL INFO PRIVATE

As the Internet has grown in complexity, many consumers feel they may be disclosing information about themselves and their online travels that they'd rather keep private. This article provides information about tools and techniques to better control how much personal information you share with online stores, Web sites, emailers, chatters and other people who may use your computer.

1. Browsing

Many Web sites record which pages your browser explores while you are within their Web site, using small files called cookies. Examples of how cookies are used includes keeping a "shopping cart" of items you are buying or remembering your address or other key information so you don't have to reenter it each time you visit. Depending on your privacy concerns, you have the option to limit or prohibit cookies on your computer.

Other cookies, used mostly by advertisers, are called third-party cookies, because they are maintained by Web sites other than the one you're visiting. Some people choose to limit only these third-party cookies.

1.1 Change your Web browser's cookie settings- Before you decide to change your browser's cookie setting, first learn a little more about cookies.

What Are Cookies?

Cookies are small coded files that Web sites write onto your hard drive to keep track of the pages you've visited. They can only be read by the site that sent them to you, and they cannot search anything else on your computer. They also don't give away your name or other personally identifiable information (PII).

So, why are some people worried about cookies? Where you search and what you enter online can be very personal, sensitive information. If you've ever filled out a form or entered your name or password at the site, your personal information can be linked to your browsing habits there. So you'll want to read the privacy policy of the Web site you're visiting to see how cookies are handles. You may also change your browser settings to restrict cookies on your computer.

1.2. Purge from your home computer traces of your Web travels - Prevent people with whom they share their computer from viewing traces of their web travels.

1.3. Always read privacy policies of the sites you frequent- Many Web sites will provide information about whether -- and for what purpose -- they use cookies. Just as it's important to read a privacy policy when shopping, you should also read a privacy policy to determine how a site uses information gathered from your cookies. The privacy policy may also tell you whether they merge that cookie information with your name and contact information (assuming you provided it to them).

How to Read a Privacy Policy

The cornerstone of good privacy protection is a Web site's privacy policy -- a statement of how and why a company collects information, what it does with it, what choices you have about how it is used, whether you can access the information, and what the site does to assure that the information is secure.

A website's privacy policy tells you how information the site collects about you is used, shared and protected. On the basis of the information in the privacy policy, you should be able to decide whether or not to give information about yourself to the site.

- **Where to Find the Privacy Policy**

If you don't immediately see privacy policy when you visit a website, there are several places you may want to look.

- Check the bottom, side, or top of the sites home page -- often there will be a button, icon, or simply the words "Our Privacy Policy." Clicking on these should bring you to the sites privacy policy page.
- Look for the policy at the point where information is being collected. You may see the policy, or a place to click through to it, when you are asked to fill out a form with information that allows you to take part in an online activity or submit an order for a product or service. If the policy itself is not posted, there, the site may post a link to the privacy policy.
- Links that refer to "policies," "about us," or "terms of service" may also bring you to the privacy policy.
- If all else fails, use the sites search function and insert the words "privacy policy."

Websites are not required by law to post a privacy policy, and not all sites do so. If you do not find a privacy policy, you may wish to reconsider whether to give your information to the site.

- **Checklist for Reading a Privacy Policy**

When reading a privacy policy, there are questions you should ask:

- What information does the company collect about me?
- Is the information necessary for the online activity I am engaging in?
- How does the site collect information about me? Am I giving the information directly (as in an online form)? Does the site use cookies?
- How does the site use personal information once it is collected?
- Do I have a choice about the way information about me is used or shared? How can I make that choice?
- What assurances do I have that the information is protected?
- Can I access the information collected about me?
- Does the Web site provide a place where I can take my complaints about the use of my information or have my questions about privacy and information use answered?

1.4. Opt-out of profiling by Network Advertisers - Since Network Advertising Companies serve up many of the Web page advertisements you see on Web sites across the Internet, they are in a unique position to view your browsing patterns. You can prevent them from creating a profile from your browsing patterns by visiting their Web site at NetworkAdvertising.org.

Opt Out of Profiling by Network Advertisers

Network Advertising Companies serve up many of the Web page advertisements you see on Web sites across the Internet. While displaying these advertisements, the Network Advertisers place cookies on your browser. Since a single Network Advertiser serves up advertisements to many unrelated Web sites that you may visit, they can track your browser's movements across those sites and build a profile of your browsing pattern and preferences. The major Network Advertisers have established a Web site that allows users to opt-out of this type of profiling or online preference marketing. Just visit <http://www.NetworkAdvertising.org> to opt-out.

2. Shopping

The realities of shopping online are that you have to provide some personal information about yourself to the online store if you make a purchase. Usually, you provide your postal address for shipping and you provide financial information (credit card info) for payment. Reputable merchants will tell you how they will use this information in their posted privacy policies. Because information is being transmitted more and more online, fraud is an ever-present concern. It is important to observe certain precautions in order to ensure that the information you give out while shopping online is not used fraudulently.

2.1 Know who you're buying from - When shopping online deal only with reputable companies and give them only enough information to make the purchase. Learn how to identify reputable companies and to read a privacy policy.

Know Your Merchant

When shopping online deal only with reputable merchants and only give out enough information to make the purchase. Use these tips to learn how to identify reputable companies and how to read a privacy policy.

- Deal with **reputable companies** (companies you already know from their retail stores, mail order catalogs or other services).
 - At a minimum be sure that you have the company's physical address (preferably not a PO Box) and a telephone number so that you can contact them offline.
 - See if the site is a member of a privacy seal program, for example [BBBOnline](#), [CPAWebTrust](#) or [TRUSTe](#).
 - Check with your state Attorney General for any adverse reports of the company you are dealing with. (Be aware that information on some companies that may be fraudulent is not always available if they are new.)
- Read the **Web Site Privacy Policy**
 - Although sometimes very lengthy, the privacy policy provides important information about the **information that the business collects about you**, how it is used and whether they have taken **reasonable security precautions** to protect you from credit card fraud. (Reasonable security precautions include: encrypting your credit card and other personal information during your transaction, the merchant keeping your personal information in its computers encrypted, allowing you to block personal information from being shared with other people or companies).
- Only give out information that is **necessary for the transaction**.
 - If you are unsure of the **credibility and security** of the Web site or why the information is needed, don't divulge any personal information such as your credit card number, Social Security number, phone number or address.
 - To clarify any uncertainties you may have about Web site's security or privacy policy, contact the company by phone and ask questions about these issues.
- Make sure you are on the Web site of the company that you want to do business with. Online crooks can create Web site names (URL's) very similar to those of legitimate companies.

1.2. Make sure your purchases and information are secure- Use credit cards to limit your financial exposure, look to see if the web transaction is securely encrypted, and be careful with your passwords. [More information](#).

Shop Securely

1. **Never use cash** - Credit cards are a good way to limit your financial exposure online if you are scammed. If your credit card information is used to make unauthorized purchases, you are only responsible to pay a maximum of \$50 under federal law. But, you must act [responsibly](#).
2. **Look for security** - Before you type in your credit card or sensitive information, be sure the site is encrypted. This is shown by either:
 - o A closed lock on the bottom of your screen.
 - o An unbroken key on the bottom of your screen.
 - o The prefix **https://** instead of **http://** in the URL -- look for the "s".
3. **Create unique passwords** - don't use your date of birth, social security number or recognizable words. Try to use a password with a combination of letters, numbers and symbols and make the password as meaningless as you can remember. One strategy for creating and remembering passwords is to come up with a phrase that only you would remember. For example, the phrase "I was married on June 24 in Finland," would result in the password "iwmoj24if" by using the first letter of each word in the phrase. This password includes both letters and numbers and will be more difficult to guess. Another easy way to remember a combination of these is to take the first letter of a favorite song or phrase, for example "Old McDonald Had a Farm" could be "omhaf." And remember to keep your passwords to yourself and to use different passwords for different things. If someone guesses a password for one, you don't want him to have access to all those services. Never give out your password to anyone -- including someone claiming to be a customer service representative.

1.3. Learn to spot unscrupulous marketers and fraudsters before you shop - Learn to spot a scam before you fall for it. Also, find out where to look to see if marketers will misuse your personal information. [More information](#).

Signs of Online Fraud

There are many signs that point to online fraud and scams. By learning and paying attention to these signs you can avoid becoming a victim. To protect your personal information, always [read a Web site's privacy policy](#).

Signs of Online Fraud

1. **Flashy Advertising** -- this type of advertising is typically seen in emails and pop up banner ads and attempts to blind consumers to the scam.
2. **High Pressure Sales** -- companies who claim they have limited availability or pressure you for an immediate response is a good indication of online fraud.
3. **Requests for Cash Payments via Courier or Overnight Delivery** - typically a sign that the seller wished to bypass postal fraud laws.
4. *****!!!Free!!!***** -- Nothing is Ever FREE! These companies typically request money later or for you to pay an up front fee.
5. **Get Rich Quick** -- The Internet has provided another venue for con artists to pitch get rich quick schemes at a large audience, pitching that large sums of money can be made with little time and no effort through Internet related businesses. The only winner in these situations is the con artist.

1.4. Check company policies and keep records of your purchases - Before you buy, make sure you're aware of the company's policies on returns, warranties, etc. After you buy, keep good records of your purchases and keep an eye on your credit card statements. [More information](#)

Check Policies and Keep Records

1. **Check company policies.**
 - o Before you purchase online check the return and cancellation policy, delivery time, warranty information and check the final cost, including the shipping. Print out this information in case you need it later.
2. **Print and keep information for your records.**
 - o Print out the order form with your purchases and confirmation numbers in case there is a dispute later or the products are not delivered.
 - o Online purchases are protected under the federal Mail/Telephone Order Merchandise Rule (unless the site says otherwise merchandise should be delivered to you within 30 days.)
3. **Look out for unauthorized charges** - Regularly check your checking and credit card accounts to ensure that there are no errors or unauthorized charges.
4. [Understand your responsibilities if your credit card information is used fraudulently.](#)

3.Communicating

The most common way to communicate online with friends and family is through email. Using a combination of technology tools and common sense, you can quickly and easily make your online communications more secure. Follow the below **Tips**, use the **Tools** and, when necessary, **Take Action** to help preserve your privacy while communicating online.

2.1 Understand the concerns associated with e-mail- First you should understand some of the privacy concerns that may be associated when communicating online via e-mail. [More Information](#).

Risks

1. Email can be easily forwarded with a click of the mouse to others Pthus exposing your personal email to others.
2. Several copies of your email message are created every time you send a message (one on your computer in the "sent folder," one on your Internet service provider's computer, one on your friend's Internet service provider's computer and one on your friend's computer).
3. When friends and family communicate by letter, things like penmanship, letterhead used and the signature allowed you to be pretty sure that the letter was truly from the person who claimed to send it. When using e-mail it is easier for a message to be forged.
4. **Review the [tips](#)** to help ensure your privacy while communicating online.

1.2. Know the recipient - Make sure that your e-mail recipient is a trustworthy person and will not forward your e-mail on to others without your consent.

1.3. Use a password - If you share your computer with others - such as family members or roommates - use an e-mail application that can be password protected.

1.4. Use Web-based applications - Using Web-based e-mail (like Hotmail or Yahoo) may be a good approach if you're concerned about people who have access to your computer reading your locally stored e-mail.

1.3. Delete local copies of messages - You can also delete the local copy of your sent e-mail message by opening the "sent" or "out" folder in your e-mail program and deleting the message. You will also need to then open the "deleted" or "trash" folder in your email program and delete the message one more time to make sure that it is removed from your email application.

1.4. Learn more about unwanted e-mails- You can learn more about unwanted e-mails

4. Sharing

Since many of us use our computers for everyday, personal tasks, we'd prefer to keep much of the information stored on our computer private. If you share your computer with others such as roommates or family members or use a public computer (ex: library or school computer), you may want to take steps to ensure your information stays private. Here is a list of things you may not want to share with others and tips on how to keep them private. *If you are looking for privacy tips on sharing your computer in the workplace please check this [editor's caveat](#).*

2.1 Learn how to erase traces of your Web travels- Make sure others cannot access your history and cache files. [More Information](#).

Risks

5. Email can be easily forwarded with a click of the mouse to others Pthus exposing your personal email to others.
6. Several copies of your email message are created every time you send a message (one on your computer in the "sent folder," one on your Internet service provider's computer, one on your friend's Internet service provider's computer and one on your friend's computer).
7. When friends and family communicate by letter, things like penmanship, letterhead used and the signature allowed you to be pretty sure that the letter was truly from the person who claimed to send it. When using e-mail it is easier for a message to be forged.
8. **Review the [tips](#)** to help ensure your privacy while communicating online.

1.2. [Keep files and data on your computer hidden from others](#) - If you share a computer, you may want to keep certain sensitive files private. Whether they are word processing documents or photos, there are many ways to keep others from viewing them while using your computer.

- o Use Removable Disks or External Drives to Save Data. [More Information](#).
- o Use the "Hide" Feature to Mask Sensitive Files and Folders in Your PC. [More Information](#).
- o Delete and Double Delete Erased Data. [More Information](#).

Why Should I Use Removable Disks and External Drives?

If your files are not stored on the computer you share then others cannot access them. You can store your most sensitive files on removable disks such as floppy disks or other disks that hold more data. The advantage is that you can take your most sensitive files with you and keep them with your other personal belongings. If your files exceed the space provided by a floppy drive then consider using other drives that store more data. Zip Disks can hold up to 250MB of data and are quite easy to work with. Many new computers come with CD burners that allow users to write files and, often, rewrite files onto the same CD disk. They are called CD-RW drives. Some manufacturers make external hard drives that can be connected to your computer using a USB or 1394 connection. These connectors can be easily attached and removed from most computers. If you use removable media for the computer documents you've been working on, make sure you move or [completely delete](#) the original file(s).

How To "Hide" Files and Folders in PCs

Most recent PC operating systems such as Windows Me, Windows 2002 and Windows XP allow users to "hide" certain folders and files. With this feature you can make any folder or file on your computer hard drive "invisible". When you hide files and folders this way others who share your computer will not be able to see the file or folder. Also, words in the file or folder name will not appear in a search of the hard drive. However, there are several cautions to keep in mind. First, this technique is not secure. Anyone who shares your computer can reveal "hidden" files with a few clicks of the mouse. It is the same as hiding your belongings in the bushes. If someone is looking for it, they probably can find it. Second, since the files will be hidden, be sure to remember where you "hid" them.

How to Prevent Others From Retrieving Deleted Computer Data

Sometimes information you delete may remain accessible to others using your computer. First, when you delete data or send it to the Recycling Bin or Trash, go into the recycling or trash bin and make sure it has been purged. If it is still visible, select the file and delete it one more time. Digital files can sometimes be recovered even after they have been deleted using special recovery tools. This may be a concern if you are selling your computer or throwing it in the trash. There may be sensitive files, such as financial and medical information, that you may want to be sure are never recovered. Here is a search that will provide information on tools you use can absolutely delete computer files:

1.3. Use a password - If you share your computer with others - such as family members or roommates - use an e-mail application that can be password protected.

1.4. Thoroughly delete your email files - If you use an email program like Outlook or Eudora chances are all your email, sent and received, can be accessed by anyone you share a computer with. If you want to keep those emails private, there are several things you can do. [More Information](#).

How to Prevent Others From Accessing Your Emails

If you use an email program like Outlook or Eudora chances are all your email, sent and received, can be accessed by anyone you share a computer with. If you want to keep those emails private, there are several things you can do.

Double Delete Sensitive Emails: You can delete certain emails in your "in box" or "sent" email folder but that does not mean they've been deleted from your computer. Often, they are simply placed in your "deleted items" folder until deleted later. Make sure that you double delete sensitive emails by going into your deleted items folder and deleting the sensitive emails once again.

Use Web-Based Email Services: A good way to keep others who you share a computer with from accessing your email is to use Web-based email services. Web-based email stores your email on a computer server like a Web page and not on your own computer. To prevent others from accessing your Web-based email [keep your password](#) to yourself.

1.5. Keep your passwords to yourself. - And make them hard to guess. [More Information.](#)

Keep Your Passwords to Yourself

If you use a password to access any computer or Internet services, make sure that they are hard to guess and keep them to yourself. Also, use different passwords for different things. If someone guesses a password for one, you don't want him to have access to all those services. Never give out your password to anyone, use a combination of letters and numbers in your password and make the password as meaningless as you can remember.

Create unique passwords - don't use your date of birth, social security number or recognizable words. Try to use one with a combination of letters, numbers and symbols and make the password as meaningless as you can remember.

One strategy for creating and remembering passwords is to come up with a phrase that only you would remember. For example, the phrase "I was married on June 24 in Finland," would result in the password "**iwmoj24if**" by using the first letter of each word in the phrase. This password includes both letters and numbers and will be more difficult to guess. Another easy way to remember a combination of these is to take the first letter of a favorite song or phrase, for example "Old McDonald Had a Farm" could be "**omhaf**."

Compiled by: Ezmir Mr (ezmir@mmu.edu.my) with referenced to <http://www.getnetwise.org/>