As part of USC's efforts to increase awareness, ITS is providing this booklet to increase awareness of the dangers that exist when online while shopping and just generally browsing through the Internet.

So much of our daily life, at work and in our personal lives, relies on the use of computers. We should understand that we are transmitting information through our computers into a cyber world of intertwined public highways where many other people are traveling and to which many other people have access.

There are risks, some more serious than others. You may already be aware of viruses, worms, malicious software and malware, phishing, email spam, social engineering, identity theft, and other cyber hacking activities through various news media reports, USC's ITS Security Blog, and newsletters. You may also have learned of ways to protect yourself against these risks, such as using strong passwords, anti-virus software, and encryption through USC's ITS Security website. These are all steps taken to minimize the chances of the misuse of information or other fraudulent activity.

In our personal lives, we need to develop a similar mindset. We need to be aware of the risks. We need to understand the situation, know the countermeasures, and avail ourselves of the resources to help us increase our chances of staying safe online. The same types of risks that apply at work also apply at home.

Additional Reading

The information contained within this booklet is derived from the following websites:

- http://www.staysafeonline.org
- http://www.us-cert.gov

We encourage you to read this booklet as an introduction to cyber security issues. To continue expanding your awareness of these and other issues, visit the websites above.

As in most situations in life, you will need to use your best judgment in any given situation. Be sure to seek the advice of law enforcement officials and other professionals as warranted. This content should not be used as a substitute for professional advice.
Staying Safe Online

Why do online shoppers have to take special precautions?

The Internet offers a convenience that is not available from any other shopping outlet. From the comfort of your home, you can search for items from countless vendors, compare prices with a few simple mouse clicks, and make purchases without waiting in line. However, the Internet is also convenient for attackers, giving them multiple ways to access the personal and financial information of unsuspecting shoppers. Attackers who are able to obtain this information may use it for their own financial gain, either by making purchases themselves or by selling the information to someone else.

There are three common ways that attackers take advantage of online shoppers:

1. Targeting vulnerable computers - If you do not take steps to protect your computer from viruses or other malicious code, an attacker may be able to gain access to your computer and all of the information on it. It is also important for vendors to protect their computers to prevent attackers from accessing customer databases.

2. Creating fraudulent sites and email messages - Unlike traditional shopping, where you know that a store is actually the store it claims to be, attackers can create malicious websites that appear to be legitimate or email messages that appear to have been sent from a legitimate source. Charities may also be misrepresented in this way, especially after natural disasters or during holiday seasons. Attackers create these malicious sites and email messages to try to convince you to supply personal and financial information.

3. Intercepting insecure transactions - If a vendor does not use encryption, an attacker may be able to intercept your information as it is being transmitted.

When visiting a website, a certain amount of information is automatically sent to the site. This may include:

- Your computer’s specific IP (Internet Protocol) address, which uniquely identifies your computer.
- The domain name associated with your user account; for example, the .edu at the end of an email address indicates an educational institution, .gov indicates a US government agency, .org refers to organization, .com is for commercial use.
- Software details about your browser, including the version, as well as the operating system your computer is running.
- Web pages you visited, the duration of visits, and the search engine used to get there.

If a website uses cookies, even more information, such as your browsing patterns and other sites you've visited, may be collected. If the website you're visiting is malicious, files on your computer, as well as passwords stored in the temporary memory, may be at risk. Malicious users maintaining those sites may be able to steal your identity, using and abusing your personal information for financial gain. The attackers may be able to alter the security settings on your computer so that they can access and use your computer for other malicious activity.

Cookies can be disabled. Refer to your browser Internet options and/or ask your Internet service provider for more information.
By representing a malicious site as a legitimate one, websites may be able to convince you to give them your address, credit card information, social security number, or other personal data.

Be careful supplying personal information. Unless you trust a site, don't give your address, password, or credit card information. Look for indications, such as the “https” in the address line of your browser, that the site uses SSL (secure socket layer) to encrypt your information. Although some sites require you to supply your social security number, for example sites associated with financial transactions such as loans, be especially wary of providing this information online.

Be careful which websites you visit. If a site seems suspicious, leave. Also make sure to take precautions by increasing your browser security settings (refer to the US-CERT Security Tip ST05-001 – “Evaluating Your Web Browser’s Security Settings”), keeping your virus definitions up to date (refer to the US-CERT Security Tip ST04-005 – “Understanding Anti-Virus Software”), and scanning your computer for malware (refer to US-CERT Security Tip ST04-016 – “Recognizing and Avoiding Spyware”).

As we approach the season for holiday shopping and surf the web for those “perfect gifts” and bargains, we should consider add-on software that will facilitate a safer experience when browsing. Additionally, you may wish to know who is tracking you as you browse the web. Here are options to assist you in this regard.

**Safer Web Browsing**

When browsing the Internet, it’s not always possible to tell where a link will take you before you click it. You may land on a page with the latest current events or a site filled with ads for questionable products and services — or, worse yet, malware. Safe web browsing add-ons can help give you an idea of what to expect when you follow a link. These add-ons collect information about thousands of websites and rank their “trustworthiness,” allowing you to make better-informed decisions about whether to visit them.

For example, the Web Of Trust (WOT) add-on rates sites from green (excellent) to red (very poor) based on crowd-sourced information from users and information taken from databases maintained by well-known, trusted sources. These sources collect lists of websites that are known for adult content, malware, fraudulent pharmaceutical sales, phishing, and spam, among other categories. WOT is available for Firefox, Chrome, Internet Explorer, Safari, and Opera browsers on the Windows, Mac, and Linux operating systems. For more information, visit [https://www.mywot.com](https://www.mywot.com).

Other safe-web-browsing add-ons you may want to consider include:


**Know Who Is Tracking You as You Browse the Web**

Many of today’s websites include mechanisms that monitor your online activities. These can include anything from cookies that maintain your site preferences to embedded tracking programs that send
your browsing information to online marketing companies. However, it is possible to limit or block these mechanisms with browser add-on software.

For example, Ghostery (https://www.ghostery.com) provides a discreet popup window at the corner of your browser, which details any ad networks, behavioral data providers, web publishers, or other companies that may have embedded code in the web pages you visit. To learn more about how Ghostery can block these tracking mechanisms and help you choose how much information you are willing to share, visit https://www.ghostery.com/en/faq.

Ghostery is free, easy to use, and available for most of the popular web browsers including Firefox, Google, Chrome, Opera, and Safari. Mobile versions are available for iOS and Android devices. Similar browser add-on software includes:

- NoScript: http://noscript.net
- DoNotTrackMe: https://www.abine.com/donottrackme.html
- Adblock Plus: http://adblockplus.org

Additional Tips for Online Consumers

- When shopping on the Internet, paying with a credit card is preferable over paying by check, money order, or wire transfer because a credit card gives you “charge back” rights allowing you to challenge the charges with your credit card issuer.

- Know the terms of the transaction. Who pays for shipping and delivery? What is the timeframe for delivery? What if the delivery does not arrive? Who is responsible? What recourse is there? What is the seller’s return policy? Does the item come with a warranty?

- Shop through known, reputable merchants. Conduct your own research of unfamiliar merchants by looking for the merchant’s phone number and physical address in case there is a problem with your purchase or bill, verifying the merchant through the online Better Business Bureau, and searching for online reviews of the merchant.

- Ensure the website is legitimate by looking for the closed padlock on the web browser’s address bar or a URL address that begins with https. This indicates that your purchase is encrypted or secured.

- Never use unsecured wireless networks to make an online purchase. Refer to details at http://security.getnetwise.org/tips/secure-web.php

- Be alert to the information you are asked to provide. Give only the minimum necessary information to complete the transaction. Review the privacy policy and understand how your information will be used and stored.

- If shopping through an online auction, before bidding, obtain information of the seller’s and buyer’s obligations by carefully reading all the fine print.
Staying Safe Online

• Be wary of online contests. They can use the contest to get your phone number, enroll you for a calling card (or some similar service), and bill you on your phone bill.

• Be cautious of offers that promise a “free” vacation. There are hidden charges that add up quickly and accommodations are often nowhere near as luxurious as advertised. Sometimes after paying an initial deposit, consumers find out there is actually no trip at all. Obtain all the details of the vacation offer in writing before paying any deposit or giving out credit card information.

• Capture the payment confirmation window. Print a hardcopy, or take a screenshot and paste it into a word processing document that can be saved electronically or printed.

• Compare evidence of your online receipt to your monthly statement. Report any differences immediately.

• Close your browser session after a purchase is made.

• Turn your computer off when you are finished shopping and/or when it is not in use so as to not allow attackers to access your computer.

• Contact the merchant directly if you are alerted to a problem. Use contact information found on your account statement, not in the email.

• Keep your computer updated with the latest browser and operating system updates/patches.

• Make passwords long and strong; adding complexity (upper and lowercase letters, numbers and special characters) is even better.

• Use unique login/passwords across different accounts.

• Avoid using public wireless for financial transactions. It is preferable to use your own Hotspot/Jetpack and equip it with VPN that encrypts your data. Make sure your personal hotspot is using the strongest possible encryption settings. Choose WPA2 (aka 802.11i) if available, as it offers the highest level of security. If at home shopping be sure you are on a WPA2-protected network with enabled encryption settings.

• Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.