



IDENTITY THEFT: Online Shopping Tips

Co-authored: Utility Consumers' Action Network (UCAN), Privacy Rights Clearinghouse (PRC), Identity Theft Resource Center, Inc. (ITRC)

Resource Material of: www.idtheftcenter.org and www.privacyrights.org

Email: itrc@idtheftcenter.org or prc@privacyrights.org

Copyright: UCAN, PRC, ITRC. All rights reserved. Released December 2000. Revised 9/2002, 2/2003.

This copyrighted document is a joint publication of the Privacy Rights Clearinghouse and its affiliate, the Identity Theft Resource Center. It may be copied and distributed for nonprofit, educational purposes only. The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse. This fact sheet should be used as an information source and not as legal advice.

With just a click of the mouse, shoppers can buy nearly any product online - from groceries to cars, from insurance policies to home loans. The world of electronic commerce, also known as e-commerce, enables consumers to shop at thousands of online stores and pay for their purchases without leaving the comfort of home. For many, the Internet has taken the place of Saturday afternoon window shopping at the mall. The same things can go wrong shopping in cyberspace as in the real world. Sometimes it is simply a case of a computer glitch or poor customer service. Other times, shoppers are cheated by clever cybercrooks. This guide offers advice on how to make your online shopping experiences enjoyable and safe.

1. Shop at Secure Web Sites

How can you tell if a web site is secure? It uses encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en route. The only people who can unscramble the code are those with legitimate access privileges. You can tell when you are dealing with a secure web site in several ways.

- First, if you look at the top of your screen where the web site address is displayed, you should see https://. The "s" that is displayed after "http" indicates that web site is secure. Often, you do not see the "s" until you actually move to the order page on the web site.
- Another way to determine if a web site is secure is to look for a closed padlock displayed at the bottom of your screen. If that lock is open, you should assume it is not a secure site.
- The third symbol that indicates you are on a secure site is an unbroken key.

Of course, transmitting your data over secure channels is of little value to you if the merchant stores the data unscrambled. You should try to find out if the merchant stores the data in encrypted form. If a hacker is able to intrude, it cannot obtain your credit data and other personal information. Be sure to read the merchant's privacy and security policies to learn how it safeguards your personal data on its computers. (See tip 3 below.)

2. Research the Web Site before You Order

Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy. Reliable companies should advertise their physical business address and at least one phone number, either customer service or an order line. Call the phone number and ask questions to determine if the business is legitimate. Even if you call after hours, many companies have a "live" answering service, especially if they don't want to miss orders. Ask how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.

You can also research a company in Internet yellow pages, through the Better Business Bureau (see listing below), or a government consumer protection agency like the district attorney's office or the Attorney General. Perhaps friends or family members who live in the city listed can verify the validity of the company. Remember, anyone can create a web site.

3. Read the Web Site's Privacy and Security Policies

Every reputable e-commerce web site offers information about how it processes your order. It is usually listed in the section entitled Privacy Policy. You can find out if they intend to share your information with a third party or affiliate company. Do they require these companies to refrain from marketing to their customers? If not, you can expect to receive "spam" (unsolicited e-mail) and even mail or phone solicitations from these companies.

You can also learn what type of information is gathered by the web site, and how it is, or is not, shared with others. The online merchant's data security practices are also often explained in the Privacy Policy, or perhaps a separate Security Policy. Look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related practices. TRUSTe (www.truste.org) and BBBOnline (www.bbbonline.org) are two such programs.

Be aware that a strong privacy policy and membership in a web seal program do not guarantee that the web merchant will protect your privacy for all of time. Policies can change. The company can file for bankruptcy and sell its customer database. The web merchant might be



purchased by another company with a weaker privacy policy. And the company's data can be subpoenaed for law enforcement investigations or civil cases. You have little control over the use of your customer data in such matters.

Given all of these uncertainties, you will want to think about the sensitivity of the data that is being compiled about you when you shop online. We cannot prescribe the best approach to take. Each consumer has a different interpretation of what is considered "sensitive."

4. What's Safest: Credit Cards, Debit Cards, Cash, or Checks?

The safest way to shop on the Internet is with a credit card. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. When it has been determined that your credit was used without authorization, you are only responsible for the first \$50 in charges. You are rarely asked to pay this charge. We recommend that you obtain one credit card that you use only for online payments to make it easier to detect wrongful credit charges.

E-commerce shopping by check leaves you vulnerable to bank fraud. And sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase. Make sure your credit card is a true credit card and not a debit card, a check card, or an ATM card. As with checks, a debit card exposes your bank account to thieves. Your checking account could be wiped out in minutes. Further, debit and ATM cards are not protected by federal law to the extent that credit cards are.

5. Never Give Out Your Social Security Number

Providing your Social Security number is not a requirement for placing an order at an e-commerce web site. There is no need for the merchant to ask for it. Giving out your Social Security number could lead to having your identity stolen. (See PRC Fact Sheet 17, "Coping with Identity Theft," www.privacyrights.org/fs/fs17-it.htm.)

6. Disclose Only the Bare Facts When You Order

When placing an order, there is certain information that you must provide to the web merchant such as your name and address. Often, a merchant will try to obtain more information about you. They may ask questions about your leisure lifestyle or annual income. This information is used to target you for marketing purposes. It can lead to "spam" or even direct mail and telephone solicitations.

Don't answer any question you feel is not required to process your order. Often, the web site will mark which questions need to be answered with an asterisk (*). Should a company require information you are not comfortable sharing, leave the site and find a different company for the product you seek.

7. Keep Your Password Private

Most reputable e-commerce web sites require the shopper to log-in before placing or viewing an order. The shopper is usually required to provide a username and a password. Never reveal your password to anyone. When selecting a password, do not use commonly known information, such as your birthdate, mother's maiden name, or numbers from your driver's license or Social Security number. Do not reuse the same password for other sites. The best password has at least eight characters and includes numbers and letters.

8. Check the Web Site Address

Above the web site at the top of your screen is a rectangular window that contains the web site address (also called the URL, or Uniform Resource Locator). By checking that address, you can make sure that you are dealing with the correct company.

Cyber-thieves have created web sites that look convincingly like the web sites of well-known companies. These sites capture the credit card numbers of unwary shoppers. The thieves then use the stolen credit card numbers to make fraudulent purchases in the shopper's name. If these shoppers had checked the URL at the top of the screen, they would have noticed that it was not the same address as the real company.

9. Always Print Copies of Your Orders

After placing an order online, you should receive a confirmation page that reviews your entire order. It should include the costs of the order, your customer information, product information, and the confirmation number. We recommend you print out at least one copy of the web page(s) describing the item you ordered as well as the page showing company name, postal address, phone number, and legal terms, including return policy. Keep it for your own records for at least the period covered by the return/warranty policy. Often you will also receive a confirmation message that is e-mailed to you by the merchant. Be sure to save and/or print this message as well as any other e-mail correspondence with the company.

10. Shop with Companies Located in the United States

When you shop within the U.S., you are protected by state and federal consumer laws. You might not get the same protection if you place an order with a company located in another country.



11. Pay Attention to Shipping Facts

Under the law, a company must ship your order within the time stated in its ad. If no time frame is stated, the merchant must ship the product in 30 days or give you an "Option Notice." This gives you an opportunity to cancel the order and receive a prompt refund, or agree to the delay.

Here are key shipping questions to ask:

- Does the site tell you if there are geographic or other restrictions for delivery?
- Are there choices for shipping?
- Who pays the shipping cost?
- What does the site say about shipping insurance?
- What are the shipping and handling fees, and are they reasonable?

12. Learn the Merchant's Cancellation, Return and Complaint-Handling Policies

Even under the best of circumstances, shoppers sometimes need to return merchandise. Check the web site for cancellation and return policies.

- Who pays for shipping?
- Is there a time limit or other restrictions to the return or cancellation?
- Is there a restocking charge if you need to cancel or return the order?
- Do you get a store credit, or will the company fully refund your charges to your credit card? If the merchant only offers store credits, find out the time restriction for using this credit.

Don't expect less customer service just because a company operates over the Internet. This is especially important if you are buying something that may need to be cleaned or serviced on occasion.

- Does the merchant post a phone number and/or e-mail address for complaints?
- How long has the company been in business?
- Will they still be around when you need them?
- Is there an easy, local way for you to get repairs or service?
- Is there a warranty on the product, and who honors that guarantee?
- What are the limits, and under what circumstances can you exercise your warranty rights?

13. Use Shopper's Intuition

Look at the site with a critical eye. And heed the old adage, "If it looks too good to be true, it probably is."

- Are there extraordinary claims that you question?
- Do the company's prices seem unusually low?
- Does it look like the merchant is an amateur?
- Are there a lot of spelling or grammar errors?
- Does the company's phone go unanswered?

The use of a post office box might not send up a red flag, but a merchant who does not also provide the company's physical address might be cause for concern. If any of these questions trigger a warning bell in your head, you will be wise to find another online merchant.

14. Be Wary of Identity Theft

As e-commerce becomes more common, there will be more cases of identity theft committed over the Internet. Imposters are likely to obtain their victims' identifying information using low-tech means like dumpster diving, mail theft, or workplace access to SSNs. But they are increasingly using the web to apply for new credit cards and to purchase goods and services in their victims' names.

The same advice for avoiding low-tech identity theft applies to shopping on the Internet. Many are mentioned in the above tips. Most important: Be aware of who you are buying from. And use true credit cards for purchases, not debit cards. We recommend that you check your credit card bills carefully for several months after purchasing on the Internet. Look for purchases you did not make. If you find some, immediately contact the credit card company and file a dispute claim. Order your credit reports at least once a year and check for accounts



that have been opened without your permission. (See PRC Fact Sheet 17a , "Identity Theft: What to Do if It Happens to You," www.privacyrights.org/fs/fs17a.htm .)

15. Be Cautious with "Electronic Signatures"

A recent federal law enables shoppers to verify online purchases with merchants using an "electronic signature." Usually, this process is nothing more than clicking on a box that says you accept the terms of the order. The Electronic Signatures in Global and National Commerce Act, also known as the E-Sign Act, is a complex law. It states that electronic signatures and electronic records used in interstate and foreign commerce will not be denied validity just because they are in electronic form. Further, the law says that online purchases do not need to be accompanied by the more traditional handwritten signature on a paper document.

Consumer advocates opposed the law because it lacks important safeguard against fraud. For example, the law does not require online merchants to comply with such standards as message integrity (security and accuracy in transmission), privacy of customer data, and authentication of sender.

The faults of the E-Sign Act require you the customer to shop cautiously on the Internet. The tips offered in this guide will help you make sure the online companies you choose are secure and honest.