Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Online Shopping Tips [1]

Posted Dec 01 2000
Revised Nov 07 2018

1. Introduction

This guide offers advice on how to make your online shopping experiences safer. Just as shoppers should take measures to protect themselves when shopping in retail stores, online shoppers also need to take sensible precautions while shopping.

2. Look for Secure Websites

How can you tell if a website is secure? Secure sites use 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 others from seeing it while in transit. The only people who can unscramble the code are those with legitimate access privileges. Here's how you can tell when you are dealing with a secure site:

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

3. Do Your Research Before You Order

When doing business with a company that you don't already know, do your research. Remember, anyone can create an app or a website.

- Research the company through the Better Business Bureau or a government consumer protection agency like the district attorney's office or the Attorney General.
- 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.
- Determine how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.
- 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.

4. Read the Privacy Policy

Read the merchant's “Privacy Policy.” You can find out if the business intends to share your information with a third party or an affiliate. Do they require these companies to refrain from marketing to their customers? If not, you can expect to receive “spam”

(unsolicited email) and even mail or phone solicitations from these companies.

You can also learn what type of information is gathered by the website, and how it is — or is not — shared with others.

However, be aware that a strong privacy policy does not guarantee that the merchant will protect your privacy forever. Policies can change. The company can file for bankruptcy and sell its customer data base. The merchant might be purchased by another company with a weaker privacy policy.

5. Be Aware of Behavioral Marketing

Most online merchants watch our shopping and online habits by using cookies and other tracking mechanisms to track which sites you visit online. Persistent cookies remain stored on your computer while session cookies expire when you turn the browser off. Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You can set your browser to disable or refuse cookies but the trade off may limit the functions you can perform online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order.

As more data is compiled about us — sometimes without our knowledge or active consent — it can be combined to create a detailed consumer profile. This data is often collected to market goods and services to us. There are many companies that specialize in targeted online advertising called "behavioral marketing." What if your behavioral marketing profile is shared with others, without your permission? You might not care if a drug company shares your prescription drug information with a coupon service to save you money. But what if that same information were obtained by your insurer, resulting in more expensive insurance coverage?

6. The Safest Way to Pay Online

The safest way to shop [2] online 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.

Make sure your credit card is a true credit card and not a debit 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.

Using only one of your credit cards for online purchases can make it easier to spot fraudulent activity. Likewise, turning on text message or email alerts to notify you about any purchases can be a great way to quickly detect fraud.

Online shopping by personal check leaves you vulnerable to bank fraud. Sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase.

Never pay for online purchases by using a money transfer service. You could be transferring cash to a fraudster. Scammers will ask consumers to send them payment using a money transfer service such as Western Union or MoneyGram because they can get your cash fast and it’s difficult to trace. Legitimate sellers normally do not ask consumers to send payment that way. Money transfer services should only be used to send money to people that you know well, not to unknown sellers of merchandise online.

You can learn more about the benefits and risks of different methods of payment by reading PRC's guide Privacy When You Pay: Debit, Credit, Cash and More [3].

7. 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 direct mail and telephone solicitations.

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

Providing your Social Security number is not a requirement for placing an order at an online shopping 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.

8. Keep Your Password Private

Many online shopping 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. Don't have your computer or device remember your password if a website has your payment information or other personal data.

Never reveal your password to anyone. When selecting a password, do not use commonly known information, such as your birth date, mother's maiden name, or numbers from your driver's license or Social Security number. Do not reuse the same password for other sites, particularly sites associated with sensitive information.

9. Don't Fall for "Phishing" Messages

Identity thieves send massive numbers of emails to Internet users that ask them to update the account information for their banks, credit cards, online payment service, or popular shopping sites. The email may state that your account information has expired, been compromised or lost and that you need to immediately resend it to the company.

Some emails sent as part of such “phishing” expeditions often contain links to official-looking websites. Other times the emails ask the consumer to download and submit an electronic form.

Remember, legitimate businesses don’t ask for sensitive information via email. Don’t respond to any request for financial information that comes to you in an email. Again, don’t click on any link embedded within a suspicious email, and always call the retailer or financial institution to verify your account status before divulging any information.

10. Be Aware of Dynamic Pricing

Some online retailers use dynamic pricing or personalized pricing [4] to engage in price discrimination by charging different prices to different consumers for identical goods or services. When you purchase goods or services online, you may be paying a higher or lower price than another online customer buying the same item from the same site at the same time. While online shopping enables consumers to easily compare prices, it also allows businesses to collect detailed information about a customer's purchasing history and preferences. Online stores can use that information to customize the prices they charge you.

Amazon.com began experimenting with dynamic pricing in 2000. Different customers were offered different prices for the same product. Depending upon a consumer’s purchase history and other information, Amazon might offer different prices matched to a customer’s perceived willingness to pay a higher or lower price than the standard price.

While dynamic pricing has existed for a long time for time-sensitive products such as airline tickets, hotel room reservations, and rental cars, it’s difficult to justify the use of dynamic pricing for goods and services that are not of a time-sensitive nature.

Online merchants can easily implement dynamic pricing by placing cookies on a customer’s computer which will track the user’s past interactions with the site. By using this information, sites can customize their interactions based on your past activities. Online stores can read the cookies on your browser to determine what products or services you searched for and bought and how much you paid for them. This information helps them to predict how much you might be willing to pay for a product or service.

Some online stores may also consider other factors when determining pricing. For example, merchants might charge higher prices to customers who make repeated returns or demand extra service.

There are several ways that you may be able to defeat dynamic pricing. Obviously, do not log in to a site before you obtain a price quote. Be sure to clear the cookies from your browser before you visit a site. Utilize price comparison sites that check prices from multiple vendors. Finally, if you do log in to a site, try leaving items in your shopping cart for a few days, to see if the merchant offers any discounts.

Source URL (modified on November 7, 2018): https://www.privacyrights.org/consumer-guides/online-shopping-tips

Links
[1] https://www.privacyrights.org/consumer-guides/online-shopping-tips
[2] https://www.privacyrights.org/consumer-guides/privacy-when-you-pay-credit-debit-cash-and-more
[3] https://www.privacyrights.org/consumer-guides/paper-or-plastic-what-have-you-got-lose
[4] https://hbr.org/2017/10/how-retailers-use-personalized-prices-to-test-what-youre-willing-to-pay