Savvy online shopping

Tips for trouble-free transactions

The popularity of online shopping has grown every year for good reason. The internet offers a far greater selection of goods than we could find at our local stores (often at better prices), enables us to shop from virtually anywhere at any time, and delivers our purchases right to our door.

This doesn't mean online shopping is without risks: the potential for order errors, lost or stolen deliveries, breached payment information, dissatisfaction with products or merchant policies, or even outright fraud. But you **can** enjoy all the advantages of shopping online and reduce the likelihood of hassles if you know how to protect your personal information, make wise choices about where you shop and how you pay, and take steps to avoid disputes.

Start with security

While there are risks anytime you're connected to the internet, technology offers many ways to make sure your personal and payment information is as protected as possible when shopping online.

Start by locking your computer and/or mobile device (smartphone or tablet) so that a passcode (or fingerprint on some devices) is needed to log on. That way, if your computer or device were to be lost or stolen, nobody else could use it. Along those same lines, make sure that your apps and online accounts are secured by a strong password. When offered the option, don't choose to save your login or payment information—it's safer to enter it yourself at checkout.

When shopping, do so on your home network or your mobile service carrier's network. Avoid conducting financial transactions in public Wi-Fi or on a shared (public) computer.

Visit retailers directly from your browser or the company's downloaded app rather than through a link in an email that might have been sent by a scammer. "Phishing" emails are designed to look like they are from a legitimate company, but they lead you to a spoofed (copycat) website that the scammer has designed to fool people. If you click on a spoofed internet link, a scammer can steal any confidential information you provide. Logging in to a spoofed site may infect your computer with malware (malicious software) that causes damage, or spyware that steals your information. Keep your browser and apps updated—new versions often include patches that fix security weaknesses.

Once you are at a legitimate retailer's site, confirm that the connection is secure before you hand over your personal and payment information. You can do this by looking for the HTTP**S**:// (rather than just HTTP://) in the address bar. A closed padlock icon might also appear, or you might see the address bar go green, depending on your browser. All these signs mean that the site uses encryption, which "scrambles" your personal and payment information to protect you from hackers. Never send your payment information by email.

Vet the merchant

There are millions of merchants on the internet, yet not all of them merit your business. Where you make purchases has a huge bearing on how trouble-free your shopping experience is likely to be, so make sure that you patronize retailers who are legitimate, honest, equipped to protect your personal information and committed to customer satisfaction.

When possible, deal only with businesses you are familiar with. When that's not possible, vet the merchant. In other words, read online customer reviews and ratings at a variety of sites, check the Better Business Bureau's complaint history and verify information on the merchant's site. For example, call the phone number provided, check the address in an online search, and/or send an email to customer service to see how responsive the company is. Check the merchant's Facebook page, Twitter account and other social media accounts for customer feedback.

Always check the merchant's privacy policy. Ideally, it should say that the company won't share your information with third parties or that you can "opt out" of such sharing.

Don't be lured in by prices that are too good to be true—there's probably a catch. Some scammers create websites offering popular products at very low prices specifically to trick people. Then they steal buyers' personal and payment information and never fill the order.

Pay wisely

When shopping online, you might have a number of payment options. Choosing the right one can add another layer of protection.

Never pay by cash or a cash equivalent, such as a wire transfer, personal check, money order or debit card. If you do, it can be impossible to get your money back if there's a problem with your order.

The safest payment option is a credit card. By law, you have the right to dispute charges and withhold payment if something goes wrong with your order. And your liability for fraudulent transactions is limited to $50. (This amount is waived by many card issuers under their zero-liability policy.) So whether you use your credit card directly on the merchant's site or use a secure payment service like PayPal or Google Checkout, as long as the purchase is on your credit card, you're protected against unauthorized transactions, billing errors, undelivered merchandise and other issues under the Fair Credit Billing Act (FCBA). (Your liability for unauthorized use of a debit card can be much higher, depending upon when you report the loss. And the fact that a debit card is linked to your bank account means a thief could wipe you out, at least temporarily.)

Another tool you might want to make use of is the disposable credit card number. Many major banks and card issuers let you create a unique, single-use number for use online. Although that number is linked to your credit card, if your account with the merchant were ever breached, your actual credit card number would not be compromised.

If you don't have a credit card, you can get a prepaid Visa, MasterCard or American Express card. These usually have the same zero-liability policies as credit cards—check with the issuer. But prepaid cards carry fees that credit cards don't, so be sure to shop around for the most user-friendly card with the lowest costs.

Avoid problems

Once you've determined that the merchant is legitimate and has a good customer satisfaction track record, review the business's return/exchange policy. Practices can range from "returns accepted at any time for any reason" to "all sales are final." This is important to know **before** you make the purchase.

Avoid buyer's remorse by doing some research on the item you want to purchase. Make sure it's what you want and that there isn't a model, style or price out there that's better. Also, check differences in the cost of delivery. Shipping can be expensive, so a free shipping offer can make one merchant more attractive than another. But don't sacrifice quality and customer service for savings. A negative shopping experience isn't worth the few extra dollars in your wallet.

Once you've decided to buy, look for a promo code on the merchant's site. If you can't find one, contact the merchant to ask if there are any discounts or free shipping offers you qualify for. Often, merchants are happy to offer something if you ask. If you see the price drop shortly after your purchase, contact the merchant to see if you can get a price adjustment. (Often, you can find the business's price adjustment policy in writing, on its website.)

After you've made the purchase, keep your receipt—typically an email confirmation, and sometimes also a paper receipt inside the package. You may need this if you have to return or exchange the item, whether immediately or in the case of an issue down the road that is covered by warranty or the merchant's return/exchange policy.

Check your credit card bill shortly after you buy something to make sure that the transaction amount is what you expected. Don't wait for your monthly statement to come—go online regularly to check transactions on your real-time account activity record. Experienced online shoppers know that they can greatly improve the odds of being satisfied with their online shopping experience by acting immediately when something goes wrong.

Prevent mystery purchases

It's always alarming to see a charge on your account that you don't recognize. Unrecognized charges aren't always the result of foul play, but sometimes they are. There are ways to avoid mystery charges and, when they appear, to determine whether they're legitimate or resolve the problem if they're not.

First, you can reduce the chances of your account being used by a stranger by practicing safe online shopping practices—vetting the merchant, confirming the site is secure, avoiding public Wi-Fi or unsafe networks, using strong passwords wherever a password is used, and generally being careful with your information.

Before assuming that a transaction on your statement is fraudulent or an error, check with anyone in your household (spouse, child, parent, etc.) who might have used the account. Prevent purchases made by your children without your permission by using parental controls on sites that insist you leave a payment card on record.

Merchants sometimes run transactions under a different name than you might be familiar with (a parent company's name, for example). If there is a phone number on the statement, you can call the merchant for clarification of the business name and what was purchased. Otherwise, you can contact the statement provider (credit card issuer, bank, PayPal, etc.) to see if you can get more information about the merchant. Check the date of the transaction against your activities for around that day to see if that jogs your memory.

Often, uncovering the source of the "mystery" purchase just takes a bit of detective work.

Turn the page for "Information and assistance" resources.

Information and assistance

Privacy Rights Clearinghouse (online shopping tips): https://www.privacyrights.org/online-shopping-tips-e-commerce-and-you

McAfee (hub for articles about safe online shopping): https://home.mcafee.com/advicecenter/?id=ad_sos

ASecureLife.com (how to spot a bogus merchant website): http://www.asecurelife.com/how-to-spot-a-fake-website/

NBC News and Consumerist (how to recognize fake online reviews): http://www.nbcnews.com/business/consumer/fake-online-reviews-here-are-some-tips-detecting-them-n447681

https://consumerist.com/2010/04/14/how-you-spot-fake-online-reviews/

SafeShopping.org (the American Bar Association's website devoted to safe online shopping): http://www.safeshopping.org

StaySafeOnline.org (using parental controls): https://staysafeonline.org/stay-safe-online/for-parents/parental-controls

Consumer Reports (information about choosing a good prepaid card, and a list of prepaid card ratings): www.consumerreports.org/prepaid-cards/prepaid-cards-are-getting-better/

Consumer Action (a library of consumer education materials on a variety of topics, including internet safety): www.consumer-action.org

eConsumerServices.com (the mediation service's blog, which includes posts on a range of online shopping topics): http://econsumerservices.com

Consumer Action

www.consumer-action.org

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy.

Consumer advice and referral hotline

Submit consumer complaints:

Online: English (http://www.consumer-action.org/hotline/complaint_form/) or Spanish (http://www.consumer-action.org/hotline/complaint_form_es/)

Phone: 415-777-9635 (Chinese, English and Spanish spoken)

About this project

Consumer Action created this brochure with funding from eConsumerServices.

A free and comprehensive educational module, including two consumer brochures (available in English and Spanish) and training materials to be used by community educators, is available at http://www.consumer-action.org/modules/module_online_shopping.