14 Tips for Safe Online Shopping

By Eric Griffith | PC Mag | November 13, 2018

Billions of dollars will be spent online in the next month and while most transactions will be uneventful, online shopping security is not a given. These tips can help.

There's every reason in the world to shop online. The bargains are there. The selection is mind-boggling. The shopping is secure. Shipping is fast. Even returns are easy, with the right e-tailers. Shopping has never been easier or more convenient for consumers. But what about the bad guys who lay in wait? It happens. The FBI's own Internet Crime Complaint Center says the number one cybercrime of 2017 was related to online shopping: non-payment for or non-deliver of goods purchased. Phishing was third, but it was at an all-time high during Q2 2018, according to the APWG's Phishing Activity Trends Report.

A recent PCMag survey asked if people had experienced a cyber attack like malware, credit card fraud, or ransomware—a full 25 percent said they had. Stay calm. While somewhat alarming, these stats should *not* keep you from shopping online. You simply need to use some common sense and follow practical advice. Here are basic guidelines; use them and you can shop with confidence as you check off items on that holiday shopping list.

1 Use Familiar Websites

Start at a trusted site. Search results can be rigged to lead you astray, especially when you drift past the first few pages of links. If you know the site, chances are it's less likely to be a rip-off.

We all know Amazon.com carries everything under the sun; likewise, just about every major retail outlet has an online store, from Target to Best Buy to Home Depot. Beware of misspellings or sites using a different top-level domain (.net instead of .com, for example)—those are the oldest tricks in the book. Yes, sales on these sites might look enticing, but that's how they trick you into giving up your info.

2 Look for the Lock

Never ever, ever buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed—at the very least. You'll know if the site has SSL because the URL for the site will start with HTTP**S**—instead of just HTTP. An icon of a locked padlock (🔒) will appear, typically to the left of the URL in the address bar or the status bar down below; it depends on your browser.

HTTPS is pretty standard now even on non-shopping sites, enough that Google Chrome flags any page without the extra S as "not secure." So a site without it should stand out even more.

3 Don't Overshare

No online shopping e-tailer needs your Social Security number or your birthday to do business. However, if crooks get them *and* your credit card number, they can do a lot of damage. The more scammers know, the easier it is to steal your identity. When possible, default to giving up as little personal data as possible. Even major sites get breached.

4 Check Statements Regularly

Don't wait for your bill to come at the end of the month. Go online regularly during the holiday season and look at electronic statements for your credit card, debit card, and checking accounts. Look for any fraudulent charges, even originating from payment sites like PayPal and Venmo. (After all, there's more than one way to get to your money.)

Speaking of, you should definitely only buy online with a credit card. If your debit card is compromised, scammers have direct access to your bank funds. Any seller that wants a different kind of payment, like wired money, is a big red flag.

The Fair Credit Billing Act ensures that if you get scammed, you are only responsible for up to $50 of charges you didn't authorize. There are protections even if you're not happy with a purchase you did make.

If you see something wrong, pick up the phone to address the matter quickly. In the case of credit cards, pay the bill only when you know all your charges are accurate. You have 30 days to notify the bank or card issuer of problems, however; after that, you might be liable for the charges anyway.

5 Inoculate Your Computer

Swindlers don't sit around waiting for you to give them data; sometimes they give you a little something extra to help things along. You need to protect against malware with regular updates to your anti-virus program.

Better yet, pay for a full-blown security suite, which will have antivirus software, but also will fight spam, spear-phishing emails, and phishing attacks from websites (the latter two try and still your personal info by mimicking a message or site that looks legit). We're happy to report that 53 percent of respondents in a PCMag survey this past summer say they're using antivirus software.
Remember, it's not enough to just have it installed. Make sure your anti-malware tools are always up to date. Otherwise, they can let in any new threats—and there are always new threats.

6 Privatize Your Wi-Fi
If you're shopping via a public hotspot, stick to known networks, even if they're free, like those found at Starbucks or Barnes & Noble stores. Any of the providers in our roundup of the Fastest Free Nationwide Wi-Fi can generally be trusted, but you should probably also use a virtual private network to be safe.
In a survey by PCMag, 48 percent of the respondents said they'd never used a VPN service. Only 26 percent knew they should have a VPN for safely using public Wi-Fi. That's not enough. It should be 100 and 100 percent on both of those.

7 Avoid Public Terminals
What about using your own laptop to shop while you're out? It's one thing to hand over a credit card to get swiped at the checkout, but when you have to enter the credit card number and expiration date on a website while sitting in a public cafe, you're giving an over-the-shoulder snooper plenty of time to see the goods. At the very least, think like a gangster: Sit in the back, facing the door. And use sites that you trust that already have your credit card stored, so you don't have to pull it out for more than a latte.

8 Create Strong Passwords
We asked PCMag readers in a survey if they frequently changed their passwords. Eleven percent claimed they did it *every day*, but those people are either paranoid, liars, or paranoid liars. The vast majority only change a password to protect privacy a few times a year (27 percent) or more likely, never (35 percent).
If you're going to be like the latter group, we will again beat this dead horse about making sure that you utilize uncrackable passwords. It's never more important than when banking and shopping online. Our old tips for creating a unique password can come in handy during a time of year when shopping around probably means creating new accounts on all sorts of e-commerce sites.
But even your perfect password isn't perfect. The smarter move: use a password manager to create virtually uncrackable passwords for you. It'll also keep track of them and enter them, so you don't have to think about it. About 24 percent of people in a PCMag survey said they use a password manager, but the number should be higher.

9 Blur Yourself Online
Abine's Blur is a browser add-on that acts as a basic password manager and oh so much more. For $36 a year, it'll let you shop without revealing anything about your actual self—no emails, phone numbers, or even credit card numbers. It's one of the most impressive online privacy solutions we've seen this year, and we've named it not only an Editors' Choice, but it'll be featured in our Best Tech Products of 2018.

10 Think Mobile
There's no real need to be any more nervous about shopping on a mobile device than online. Simply use apps provided directly by the retailers, like Amazon and Target. Use the apps to find what you want and then make the purchase directly, without going to the store or the website.

11 Skip the Card, Use the Phone
Paying for items using your smartphone is pretty standard these days in brick-and-mortar stores, and is actually even more secure than using your credit card. Using a mobile payment app like Apple Pay generates a one-use authentication code for the purchase that no one else could ever steal and use. Plus, you're avoiding card skimmers, you don't even need to take your credit card with you if you only go places where you can see this symbol. How does that matter if you're online shopping? Many an online store app will now accept payment using Apple Pay and Google Pay, like Groupon, Airbnb, Staples, Ticketmaster, Starbucks, and many others.

12 Count the Cards

Gift cards are the most requested holiday gift every year, and this year will be no exception. Stick to the source when you buy one; scammers like to auction off gift cards on sites like eBay with little or no funds on them. Plus there are many gift card "exchanges" out there that are a great idea—letting you trade away cards you don't want for the cards that you do—but you can't trust everyone else using such a service. You might get the card—and it's already been used. Make sure the site you're using has a rock-solid and clear-as-crystal guarantee policy in place. Better yet, just go directly to a retail brick-and-mortar store to get the physical card.

13 Check the Seller

If you're wary of a site, perform your due-diligence. The Better Business Bureau has an online directory and a scam tracker. Yelp and Google are full of retailer reviews. Put companies through the ringer before you plunk down your credit card number. There's a reason that non-delivery/non-payment is the most common cyber crime complaint these days: it hurts when that happens, financially and emotionally.

That said—online reviews can also be gamed. If you see nothing but positive feedback and can't tell if the writers are legitimate customers, follow your instincts.

If nothing else, make absolutely sure you've got a concrete address and a working phone number for the seller. If things go bad, you have a place to take your complaint. In fact, call them before you order so you can clarify a return policy and where to go with any issues after the purchase.

14 Complain Loud and Proud

Don't be embarrassed if you get taken for a ride while online shopping. Instead, get very, very mad. Complain to the seller. If you don't get satisfaction, report it to the Federal Trade Commission, your state's attorney general, even the FBI. That's probably going to work best if you buy in the US, rather than with foreign sites. If you're going to get scammed, try to get scammed locally... or at least domestically.