

# 11 Tips for Safe Online Shopping



Copyright (c) 2010 Ziff Davis Inc. All Rights Reserved.

Let's face it, 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 pretty easy, with the right e-tailers. It's a golden age for not going to the store, yet buying more than ever.

You're already a step up in safety by shopping online—there's no way for you to leave behind a credit card or wallet that way—but you could still run into trouble. However, with some common sense and basic guidelines in place, your online shopping should never be troubling. Here are 11 tips for staying safe online while knocking out that holiday shopping list.

## 1. Use Familiar Web Sites

Start at a trusted site rather than shopping with a search engine. Search results can get 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 and that it 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 misspellings or sites using a different top-level [domain](#) (a .net instead of a .com, for example)—those are the oldest tricks in the book. Yes, the sales on these sites might look enticing... that's how they get 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 it has it because the URL for the site will start with HTTPS:// (instead of just HTTP://) and an icon of a locked padlock will appear, typically in the status bar at the bottom of your Web browser. Never give anyone your credit card over e-mail. PayPal, however, is still a good, safe way to make a payment.

## 3. Don't Tell All

No online shopping store is going to need your social security number or your birthday to do [business](#). But if a bad-guy gets them, combined with your credit card number for purchases, they can do a lot of damage. When you can, default to giving up the least amount of information.

## 4. Check Statements

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.

Make sure you don't see any fraudulent charges, even originating from sites like PayPal (after all, there's more than one way to get to your money). If you do see something wrong, jump on the phone to address the matter quickly. In the case of credit cards, don't pay the bill until 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 PC**

Bad-guys don't just 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 such Trojan horse malware with regular updates to your anti-virus program. One good recommendation is Norton EndPoint Protection. A good solid Anti-Malware program is also a must. One good choice is MalwareBytes Anti-Malware software. This program gives extra protection against Malware type attacks in addition to whatever antivirus program you may be using. It is a good idea to use both programs together for a safer online experience.

### **6. Use Strong Passwords**

We like to beat this dead horse about making sure to utilize uncrackable passwords, but it's never more important than when banking and shopping. Our [tips for making a unique password](#) for each site can come in handy during a time of year when shopping around probably means creating new accounts on all sorts of shopping sites.

### **7. Think Mobile**

The NRF did a survey that also predicts that 25 percent of adults will do their online shopping via their smartphones, but mostly as a way of find gifts, not purchase them. You can buck that trend, just follow the advice above. Better yet, download store specific apps like those for Amazon, Target, etc. and use them to find what you want and make the purchase without going to the store or the Web site.

### **8. Stay at Home**

Do we really have to tell you it's a bad idea to use a public computer to make purchases? Hopefully not. If you do, just remember to log out every time you use a public terminal, even if you were just checking e-mail.. But 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 number and expiration date on a Web site 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.

### **9. Privatize Your Wi-Fi**

If you do decide to go out with the laptop to shop, you'll be on a Wi-Fi connection. Only use the wireless if you access the Web over a virtual private network (VPN) connection. By the way, now is not a good time to try out a hotspot you're unfamiliar with. Stick to known networks, even if they're free, like those found at Starbucks or Panera Bread.

### **10. 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 upon arrival.

### **11. Know What's Too Good to Be True**

McAfee compiled a list of scams to look for and one of them is the offer of a free product with purchase, in particular the iPad (a very coveted gadget this holiday) or even holiday job offers. Many of these "offers" will come in via social media. Beware even of your friends, who might innocently forward such a thing. Skepticism in these cases can go a long way toward saving you from a stolen card number.