

The ESET Guide to Safer Cyber-Shopping

10 Tips for Happier Holidays



Even more holiday shopping will happen online this year, and that means more scammers will be looking to do some shopping of their own, possibly at your expense. This might involve using **your** credit card and bank account to fund **their** gift-buying, or perhaps capturing and selling your personal information so they have some extra holiday cash. Here are some tips that Cameron Camp and other ESET researchers have put together to help savvy cyber-shoppers avoid getting scammed while hunting for the best holiday deals online.

1. **Tune your shopping machine:** Like the tune-up your car might be getting before a long drive to deliver holiday gifts to relatives, your laptop may need a little attention before going online for some power shopping. Give it some love, and improved protection, by updating and patching your browser, operating system, and anti-malware suite. Patching will help you avoid malware infections and scams, and keep you running smooth throughout the season, and it's free.
2. **Stick with familiar faces:** Buy from websites that have established a reputation for doing what they say, providing accurate descriptions of merchandise and delivering it in good shape and on time. When you're getting down to the wire with shipping deadlines, the last thing you need is friends and relatives getting the wrong gifts, which could be worse than no gifts at all.
3. **Be wary of AMAZING deals:** If it looks too good to be true, it probably is, particularly if it's an amazing offer on one of the hottest products of the season. Such deals can be very tempting, but it really is safer to avoid following links that offer goods, services, or gift cards at impossibly cheap prices, they are just too risky. Not all discount vendors are scammers, but ask yourself if the promised savings are worth the gamble (or Google the offer and/or vendor to see what others are saying).

4. **Insist on secure transactions:** When you are in the ordering process on a website check to make sure it is using SSL, the standard in secure transactions that shows up in several ways. You should be able to see **https** or **shttp** in front of the web address instead of http. There may also be a lock or key symbol in the browser window as well. Using SSL encrypts the exchange of information, such as your credit card, so eavesdroppers cannot read it. When in doubt, a quick search in Google for the word “scam” or “fraud” along with the site name should tell you if that site has a history of problems.

5. **Think before you act:** Watch out for URGENT deals that arrive in unsolicited email or purport to be from friends on social networking sites. Exercise extra caution if the message uses broken English (or whatever your native



language might be) or if it doesn't seem quite right for some reason. If you think the deal is real, open a browser and type the name of the website directly into the address bar. This will keep you from getting swept away by scam links to fake websites built by cyber crooks that harvest your information and spirit it off to the underworld (the black market in stolen identity data).

6. **Don't shop at a leaky hotspot:** If you need to do any shopping over WiFi, at home or at a hotspot, make sure it is secure (look for the lock symbol in the WiFi connection dialog). The last thing you want is someone snatching your personal details out of thin air as you transmit them from your laptop (or smartphone or tablet).

7. **Use a credit card:** If you get scammed and try to get your money back you may have better luck with credit card transactions versus debit cards. Many vendors, whether at the mall or online, prefer debit cards because the transaction is cheaper for them. Avoid this when holiday shopping. Credit cards can put an extra layer of protection in between you and the bad guys.

8. **Question detailed info requests:** Some malware is able to add questions to forms you use online, so if a shopping website is asking for Too Much Information relative to your purchase, like wanting your Social Security Number to complete a simple order for flowers, abandon the transaction and run an anti-malware scan right away.
9. **Don't expect money for answering questions:** There are legitimate website satisfaction surveys, but when a window pops up promising you cash or gift cards just for answering a question like "Coke or Pepsi?" close it and move on (and do NOT enter your cellphone number, unless you are prepared to pay for premium services you never ordered).
10. **Stay awake after the holidays:** When New Year lull sets in, there's a tendency to avoid looking at the credit card statements arriving by mail (or email). Maybe your hoping you didn't spend as much as you THINK you may have. But if you got scammed, that statement may be the first sign, so at least skim the statement to see if there are any transactions you don't recognize. For example, if you have never been to Russia and don't know anyone who lives on the outskirts of Moscow, it's a safe bet that any wire transfers to the region are fraudulent, and the sooner you act, the more likely you are to recover your money.

Follow these simple tips and you should sleep a little better during the holiday shopping season. Remember, as in life, there are things on your computer that can seem too good to be true, and holiday shopping on the internet is no different. Caution may sound boring, but it can pay off. After all, if you feel you don't have enough time to get your shopping done, you certainly don't have time to start shopping all over if you do get scammed.



For more advice on safe web-surfing and get news of the latest malware threats be sure to visit the ESET Threat Blog at blog.eset.com.