ESET's Guide to Safer Cyber-Shopping 2012

12 Tips for Happier Holidays

Digital devices are sure to play a bigger role in the holiday shopping process this year than ever before, from pre-purchase research on the home or office computer, to in-store price checking on the smartphone. And of course, online holiday shopping is now available 7x24, from before Black Friday, through Cyber Monday, all the way to end-of-year clearances and New Year Sales.

Sadly, that means criminals will be keener than ever 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.

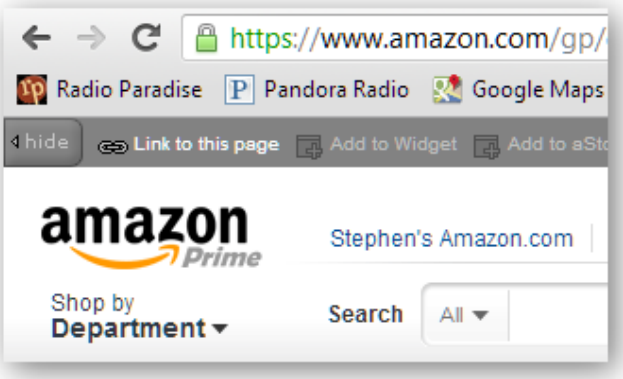
Here are some tips that ESET security researchers have put together to help savvy cyber-shoppers avoid getting scammed while hunting for the best holiday deals.

1. **Tune your shopping machine**: Like the tune-up your car gets before a long drive to deliver holiday gifts to relatives, your laptop may need 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 smoothly throughout the season, and it's free. (You can run a free antivirus scan of your Windows PC at www.eset.com/online-scanner.)

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.

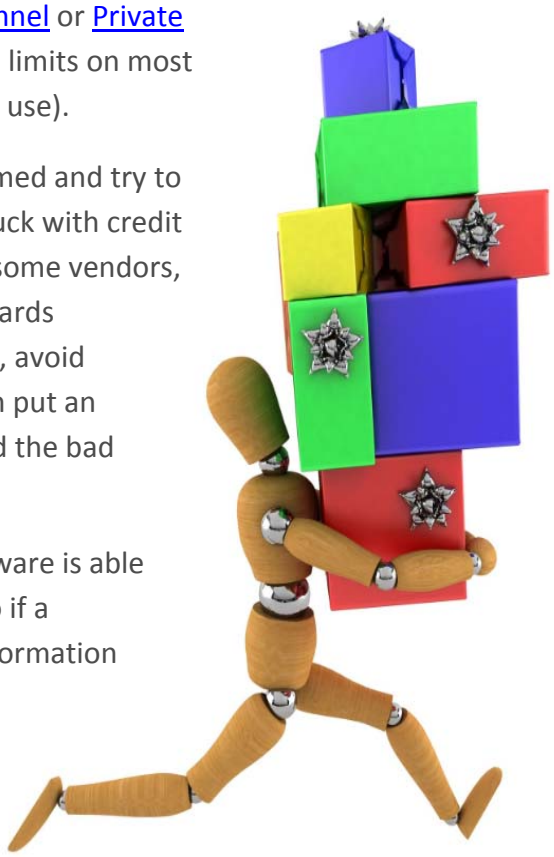
3. **Be wary of AMAZING deals:** If a deal looks too good to be true, it probably is, particularly if it's an amazing offer on one of the hottest products of the season. Such deals can be very tempting, but it really is safer to avoid following links that offer goods, services, or gift cards at impossibly 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** 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 (like an unexpected email from a delivery service with an attachment). 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 (there is a thriving black market in stolen identity data which crooks purchase to commit credit card fraught, tax fraud, and other crimes).

6. **Don’t shop at a leaky hotspot**: If you need to do any shopping over Wi-Fi, at home or at a hotspot, make sure it is secure (look for the lock symbol in the Wi-Fi connection dialog). The last thing you want is someone snatching your personal and financial details out of thin air as you transmit them from your laptop (or smartphone or tablet). When using Wi-Fi outside your home consider using a VPN or virtual private network such as PrivateTunnel or Private WiFi (bear in mind that there are bandwidth limits on most free VPNs so you may need to pay for heavy use).



7. **Use credit instead of debit**: If you get scammed and try to get your money back you may have better luck with credit card transactions versus debit cards. While some 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 **T**oo **M**uch **I**nformation 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 survey questions**: There are many legitimate website satisfaction surveys, but when a window pops up promising you cash or gift cards just for answering a simple survey question like “Do you use the Internet?” close it and move on. And do NOT enter your cell phone number to claim the $1,000 gift card that a website is promising you, 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 you're 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 folks who live on the outskirts of Moscow, it's a safe bet that any wire transfers to that region are fraudulent, and the sooner you act, the more likely you are to recover your money.

11. **Lock up your devices**: Password protect your laptop, tablet, and smartphone so that, if lost or stolen, your data will be harder for strangers to access. Each of these devices should have a settings menu from which the security options should be readily accessible. Choose a password or code that is easy for you to remember but hard for other people to guess. Set the timing so that the device locks after a short period of inactivity. You are now better protected against multiple scary holiday scenarios, such as leaving your device in a taxi or on the plane, someone stealing your device, or a friend "borrowing" your device and then using it inappropriately.

12. **Backup your data**: If you have to face a worst-case scenario this holiday season, like a laptop going missing or a smartphone being stolen, the situation will be much less upsetting if you have your device backed up, that is, copies of your files safely stored somewhere else. Your smartphone is probably backed up to your computer already—now is the time to check—and your computer can be backed up to an external hard drive, or online backup such as BackBlaze, but preferably both.

Follow these tips and you should sleep a little better during the holiday shopping season. Remember, as in life, there are online deals that can seem too good to be true, and probably more of them during the holiday shopping season. A cautious and skeptical approach 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 deal with fraudulent charges, flaky deals, or stolen data.

For more advice on safe web-surfing and cybersecurity be sure to visit the ESET Threat Blog at blog.eset.com.