How to Safely Shop Online

A TrendLabs Digital Life E-guide

By Paul Oliveria, TrendLabs Security Focus Lead
Convenience, ease, and variety are just some of the reasons why online shopping is growing in popularity. Desktop-based e-commerce boomed to US$49.8B early in 2013. That’s a 16% increase from last year.

And you don’t even need your laptop or desktop computer to shop. Mobile devices are becoming a popular means for e-commerce. In fact, one out of ten US dollars is spent online via mobile devices.

But just like face-to-face financial transactions, you should be careful when making purchases online. Online shopping often requires details like your name, address, email address, and credit card information—all of which are cybercriminal targets. By remembering these few tips, you can help protect both your data and your money.
Think Private, Not Public

Public hotspots and networks might make it tempting to do a little shopping on the go. But are you willing to share your credit card details in a network that anyone, including bad guys, can easily access?

If you’re connected to the same network, cybercriminals can spy on your sessions, steal your information, and hijack your accounts. This isn’t limited to computers. Cybercriminals can also snoop into your smartphone. Bad guys can drop malware into your devices without your knowledge.

Accessing your online accounts using a public computer increases the chance of hacking and having your information stolen. Public computers may also be already infected with malware.

Only shop online when you know you’re connected to a secure network. As long as you keep your device and home network secure, you can enjoy safe, uninterrupted shopping sessions.
Use Bookmarks and Official Apps

If you have regular, go-to shopping sites, create bookmarks for future visits. Cybercriminals often rely on spelling mistakes to lead you to spoofed sites. They can also manipulate your search engine results so that their malicious sites stay on top of the list. You may not know you’re on the wrong website until it’s too late.

As more sites become mobile-friendly, it’s also worth looking into using official apps. Like bookmarks, apps can lessen the risk of accidentally visiting a malicious site, especially since it’s harder to spot spoofed sites on a mobile device’s smaller screen. You just need to make sure that the app you’re downloading is from the site itself, as fake apps are common.
Carefully Check Out Deals

Bargains are a dime a dozen online. You can always count on sales, promo codes, and even freebies when shopping. Unfortunately, you can also count on seeing a lot of bogus deals and scams.

It’s easy to become dazzled and overwhelmed by offers that seem too good to be true. But it’s always best to assume something’s up. Cybercriminals are willing to promise anything to get what they want from you.

Only trust deals offered by reputable shopping sites. Compared to unknown sites, established websites offer more ways of protecting your information. Before trying a new website, check out reviews regarding its safety.

QR codes have also become a popular way to claim promos or shop virtually. However, bad guys can release QR codes that can be used to either download malware into your device or lead you to phishing sites.

Check out QR codes before scanning. Search for details like brand names or descriptions. Location also helps. A QR code printed on a newspaper is more likely to be safe than one printed on a random wall sticker.
Protect Your Wallet

Since you’re dealing with money, checking out is often the most worrisome aspect of online shopping. After all, no one wants to be the victim of a sale gone wrong.

Never use a payment method that doesn’t offer buyer protection. Wire transfers and money orders are not recommended since you have no way of getting your money back once you’ve sent it. This is one of the reasons why scammers prefer these methods.

Opt to use credit cards or reputable payment sites like PayPal. These can offer you better protection in case there’s a problem with your transaction. Make sure you’re logging into the correct site. Financial sites are the most spoofed sites by cybercriminals.

Mobile devices give you other ways of paying. There’s Google Wallet, NFC, and even SMS. But like other methods, there are risks involved. Basic practices like installing a security software and using your device’s locking function can help protect your transactions.
Secure Your Shopping Environment

You don’t shop in a bubble. External factors can have a drastic effect on the safety of your shopping session. For example, an infected computer can do a world of harm, even if you limit your shopping to legitimate sites.

You need to secure each aspect of your digital life:

- **Protect your devices.** Install a security solution that will protect your devices from different kinds of threats. Always lock your devices to prevent strangers from getting into your accounts. You can also install a “device finder” software with remote lock or wipe functions, in case your devices get lost or stolen.

- **Use complex passphrases.** Go for length and complexity when creating passphrases. You can also use a password management tool. Multiple online accounts require thorough management.

- **Read the fine print.** Being aware of policies can help protect you from scams or bad sellers.
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.