



The worldwide bazaar is always open

Shopping Safely Online

Now that Halloween's over, the real horror of the holiday shopping season has begun. You can bundle up, fight traffic, struggle for a distant parking space at the mall, compete with huge mobs of other unhappy consumers shambling about like zombies, maybe find a gift, compare prices by memory, pay up, and wrestle your goodies home. Or you can fix a nice hot cup of cocoa, put on your bunny slippers, and snuggle up on the couch to do it all effortlessly online.

The latter option sounds so much more pleasant. But with convenience comes nagging worries about how safe online shopping really is. Happily, there are ways to avoid pickpockets and scams online just as there are at the mall, and this issue will list some of them.

Digital dollars

The Internet was invented to share data between nuclear scientists; the Web for their results. It wasn't intended to exchange tweets, lolcats, or to stream videos, but has been adapted to do so. Likewise, the system also handles financial transactions, but this is a rather tricky thing, because the Net was designed to be open, trusting, and transparent throughout.

Buying something online is complicated. To do so involves more parties – not just you and the seller, but your bank, their bank, the credit card provider and an online payment service provider. And all these negotiations have to be conducted properly and above all, securely and privately, in real time.

The rules which govern these interactions are called the **Payment Card Industry Data Security Standard** (PCIDSS), grown out of Visa's and Mastercard's attempts to fight credit card fraud. Since it is not mandatory for anyone else, critics claim it provides a bare minimum level of protection, but supporters claim that in major attacks, the affected entity was not actually in full compliance at the time.

Online commerce has been around a long time. The **first online sale** was a marijuana deal arranged between students at MIT and Stanford in 1971 or 72. Many such activities have now moved to the **Dark Web** and sites such as **Silk Road**, aided by

electronic currencies like **bitcoin**. But it wasn't until **Amazon** was founded in 1995 that online commerce became a normal part of life for millions of ordinary people. Now with smartphones and token systems, Apple, Google, and Paypal are combining online paying convenience for brick and mortar stores, too.

Online shopping is here to stay, but it's blending in with the real world. While it's far easier to comparison shop online, you might pay different prices for items than your neighbor, depending on your browsing and buying history. For example, Home Depot buyers were charged more when ordering from cellphones than from desktops. Even listings generated by search engines using identical terms are affected. And don't be surprised if the price online is *not* the same as the one offered in the physical marketplace.

It may be difficult or futile to try to get around this. **Money magazine** suggests deleting cookies and using a private browsing window, but that could backfire depending on the site because retailers all use their own criteria. But products online are often cheaper, even with shipping charges and despite the uneven collection of sales taxes.

You can now be alerted to nearby deals and offers on your phone just because of your physical location. But it works both ways: the same Wi-fi seeking behavior of your cell also allows merchants to indi-



Continued on back

Continued from front

vidually **track** you and your activity in their shops in much the same way Amazon does on its website.

10 tips for safe cybershopping

Like going to a bazaar or flea market, shopping online requires certain preparations and precautions. You need to know what to look out for and keep cash tightly in hand until the deal is done. As in the physical world, if a deal seems too good to be true, it probably is. "Let the buyer beware," still applies.

1. Prep your computer. Make sure your browser and antivirus programs are updated and current and various **passwords** are as strong as you can make them. If using Wi-Fi at home, make sure the connection is secured and do *not* shop in public. The dangers of both unsecured terminals in Internet cafes and free public Wi-fi are simply too great. Plus at home you can shop in your pajamas at midnight. Sweet!

2. Stick to what's tried and true. If using your smartphone, only use apps you trust, downloaded from reputable sources like the **Apple App Store** or **Google Play**. For shopping in stores, not many merchants accept Apple Pay yet, and Google Wallet is not as easy to use, but they may be safer than credit cards.

3. Avoid email and search pitfalls. The holidays are a prime time for **scammers**. *Never* open e-cards, attachments from retailers, or coupons. Watch out for emails claiming "wrong transactions" have taken place, undelivered packages, and websites with fabulous deals on hot or expensive items. *Never* click on a link in an email. Visit the site from a bookmark if possible or check search results carefully to avoid frauds. More at security firm McAfee's **list of holiday scams**.

4. Note the details. Anybody can set up shop using a bogus name or flog shoddy merchandise. Get the address and phone in case of problems. Read the product descriptions carefully. Terms like "refurbished", "vintage", and "close out" could indicate less than perfect goods. Checking out customer reviews and comparison shopping sites is a good idea, too.

5. Shop only at trusted sites. Amazon has a huge inventory and lots of associated merchants, but they don't have everything. For sites unknown to you, customer reviews may be helpful along with googling for complaints. Look at their return and refund policies to avoid hidden restocking fees and so on. Also watch out for sites who resell personal information. Opt out from having info shared with third parties. You can also check on merchant ratings at **Google Shopping** and the **Better Business Bureau**.

6. Look out for the lock. When ready to order, make sure the order page uses **SSL** to encrypt data. There should be an icon of a locked padlock visible and the


address should begin with "**https**" not just "**http**". If you don't see that, do *not* enter any information. Visa also suggests shopping only at sites online or over the phone which require the **3-digit security code** on the back of the card for identity authentication.

7. Credit is best. The **American Bar Association** strongly recommends using credit cards rather than debit cards or checks due to **limited liability** in cases of online fraud and for other reasons. Gift cards, other limited-value type cards, and PayPal are also good. Plus, Visa and American Express now offer **disposable credit cards**, which are like gift cards but are refillable. If criminals steal a limited-value card, they can empty it, but they cannot clean out your bank account or plunder your personal information.

8. Give out as little data as possible. Most retail sites, especially big ones, are more than happy to keep your account details to make online shopping even easier. But it might prove more convenient for cybercrooks than for you if the merchant is hacked. It's best to take the time to enter your information at each site, even if you plan on returning.

9. Save on shipping. Getting the purchase sent to you or your intended recipient can easily eat up any savings gained by careful shopping. Doing it early can make a big difference. You can avoid higher priced methods, group items together to save, and some retailers even offer free shipping if done before the rush. Look over their terms and options carefully.

10. Check accounts often. Don't wait until January to look over your bank and credit card statements. Most banks and card issuers grant just a 30-day window after a fraudulent purchase to make claims, so it's best to check your accounts frequently and report any suspicious activity at once.

Despite all precautions, things can still go wrong through no fault of your own. If that happens, don't panic, but don't ignore it. The ABA has a **list** of steps you can take if there's a problem. But relax; the ease, convenience, savings, and built-in safeguards of online shopping outweigh the risk of cyber-crime, even of being hacked by the Grinch. 



Southwest Cyberport

New Mexico's Expert Internet Service Provider since 1994

505-243-SWCP (7927) • SWCP.com • Help@swcp.com

5021 Indian School NE, Suite 600, Albuquerque, NM 87110

Portal editor/chief writer, Jay Nelson jnelson@swcp.com
Click on **blue terms** in PDF file to open links.