## Is Online Shopping Safe?

**“Basic safety measures when shopping online.”**

*by Pete Choppin*

I use many online vendors and Web sites for the types of products and services we buy where I work. It has become second nature for me to follow basic safety measures when shopping online.

I am often asked whether online banking is secure, and I generally advise people that doing your online banking and bill paying is generally safe. But it seems that online purchases are decided upon at the drop of a hat, leaving caution to the wind. And why? Because of the allure of shopping from the comfort of your home and receiving your new goods without setting foot in a store.

When you shop online, however, you have to be more aware of thieves and fraudsters who'd like nothing more than to get their hands on your name, credit card information, checking account number or anything else they can use to rip you off.

Fraudsters can get access to your personal information online by setting up fake stores, which can look amazingly similar to the real thing. They may even go so far as to confirm your order and send an e-mail confirmation. However, it's only when you don't receive the merchandise you paid for that you realize you may have been a victim of an online shopping scam.

If you shop online you have to be careful; otherwise, you could find yourself dealing with hundreds of fraudulent charges.

It makes sense that better security often means sacrificing convenience. Open 24 hours a day from anywhere in the world, online shopping sites entice consumers with an array of come-ons, such as free shipping, comparison pricing, bargain deals and extra security features. Saving gas, and being able to shop on your schedule, adds more to the online shopping appeal.

Yet, the question remains: Can online shopping be done safely?

Most experts agree that it can—on the condition that consumers abide by some basic safety tips.

### Tip No. 1: Bigger Names Equal Better Protection

"Go with reputable companies you've heard of," says Jim Stickley, co-founder, CTO and vice president of engineering at TraceSecurity, a company that works with financial institutions to better their network security systems to deter identity thieves.

Stickley, who knows firsthand how easily sensitive information is stolen, says that if a deal sounds too good to be true—say, $20 for an iPod Nano—it probably is. What's worse, it's probably an attempt to trick you into giving out personal information.

Steven Branigan, founder and president of CyanLine and author of *High Tech Crimes*

*Revealed*, agrees and says that it's good to know the site you're going to, such as bigger sites like Amazon.com. "These sites put their name on the line."

On the other hand, the fear factor hurts smaller merchants who might have better deals, which is, of course, immaterial where your security is concerned.

**Tip No. 2: When in Doubt, Check Them Out**

If you go with an unknown merchant or Web site, contact someone there who can verify the company's privacy policy for you before you make a purchase. Ask if they'll send you a catalog. If they don't list phone numbers and only have an e-mail address, that's a huge red flag. Call the phone number and see if it goes to voice mail. Anyone can have voice mail set up.

Bottom line: If you can't get a human being on the phone or don't like what you're hearing, go shopping somewhere else.

**Tip No. 3: Encryption Doesn't Equal Security**

Leah Ingram, author of *Gifts Anytime: How to Find the Perfect Present for any Occasion,* is a certified etiquette and protocol consultant. This expert gift-giver says one of the first things you should do before typing in your credit card information is look for the "plural URL." That is, when you go to the site's checkout page, make sure it is a secured Web site by checking for the "https://" in the URL. The "s" designates a secure site. It isn't a guarantee, so also check for a closed padlock or key that should also be on the page, letting you know your personal information will be encrypted or scrambled.

If you don't see either of these "locked" icons or a change in the URL, log out and shop elsewhere. You can't be sure the site has a secure server, and you shouldn't take that risk.

Here's one tell-tale sign that you've entered a scammer's site: If you ever see numbers at the beginning of the URL, such as http://66.102.7.104@65465.51456%6AD%, it's probably a scam, says Stickley.

Even if you see a proof of encryption, such as the plural URL, you shouldn't equate that with the site's trustworthiness.

"It just means the session is encrypted," says Stickley. He likens the mistaken notion to believing that someone owns a house just because that person can lock the front door. It means nothing. To verify the site's trustworthiness, he advises calling the company to ask about its privacy policy.

**Tip No. 4: When Sharing Is a Bad Thing**

Shared computers, such as the ones available to multiple strangers at computer centers, are a big security risk.

The danger is that hackers can insert a keylogger into the back of the keyboard, a device that looks like a harmless adapter. This monitoring device captures everything you type before it's

encrypted. Sometimes installed as software, the device can be hard to detect. The best thing to do is avoid shared computers when typing sensitive information.

**Tip No. 5: Pay With a Credit Card**

You've found a trustworthy site with a secure checkout page. Now you're ready to pay—with what? Check, money order, debit card, credit card, cash or Monopoly money?

Experts all agree: Credit cards are the safest method for online purchases.

Personally, I hate credit cards. I don't carry any. And although this flies right in the face of expert advice, keep in mind that I am very careful about where I purchase online. I scrutinize every site and I would never hand over a debit card number to a site I didn't know and trust.

However, it is good to know about some of the security protections that credit cards provide.

"The last thing you want to use is a debit card," Stickley says. "Most credit cards have protection on them—if someone rips you off, you can dispute the charge. Debit cards pull money right from your bank account. It can take months to get your money back, if you ever see it again."

The advantage of using a credit card is that it's not just your money on the line—it's the creditor's money, too. If you have a problem with your transaction, the credit card company will go to bat for you to resolve it because, in the end, the creditor has just as much at stake as you do.

Another option is making purchases through a third-party escrow service such as PayPal. PayPal Buyer Protection covers qualifying eBay purchases for up to $1,000 at no additional cost to buyers, helping to guarantee your purchase. After any sale, be sure to print and save all of your receipts and e-mail confirmations in case of a dispute.

Credit shy?

If you are understandably reluctant to give out your credit card number over the Internet, you have alternatives. Some card companies such as Discover Card, Bank of America and Citi, offer a secure online account number service—a virtual credit card or virtual account number.

By providing merchants with a special credit card number instead of your real number, your actual Discover account number is never exposed to scammers. Check with your credit card company to see if it offers this type of security feature.

Another security feature on the horizon is a one-time-use password token. The technology has been developed, but it's not in widespread use yet. To protect yourself, be wise in your choice of passwords. Use a combination of letters and numbers difficult to guess. Don't use a word or number someone else could figure out, such as your birthday or dog's name. Change your password frequently.

**Tip No. 6: Suspect the Suspicious**

If you're at the checkout page and the site asks for your date of birth and Social Security number, be very careful. This kind of information can give people enough to start applying for new credit cards in your name. What's scarier is the ease with which driver's licenses can be purchased overseas. If that scares you, remember a simple rule of thumb: If anything seems suspicious, call the company and ask questions.

Also be wary of sending out credit card information via e-mail or instant messaging—neither is encrypted. Copies can remain on your mail server as well as theirs. Since you can't control who's looking at your information, stick to the site's secure transaction page.

**The Final Word**

The experts offer a silver lining to the cautionary warnings against online identity theft and credit card fraud. People should be aware that as long as they are dealing with reputable companies, online transactions are far more secure than the face-to-face transactions people perform every day.

Online transactions eliminate the middle man, such as the waiter who processes your credit card payment, so there are less people who physically see your private information.

Consumers who research companies before making purchases, watch for warning signs of fraud, use credit cards for purchases and keep receipts should be relatively safe.

"They can be absolutely as confident as physically shopping in a store," says Stickley.