



**Who's
Watching?**

Online Commerce Tipsheet

from "Who's Watching Charlottesville?"

October 1, 2008

Some Tips for Safer Online Shopping

Quick Tips

- When shopping online, always check for the [https](#) in the top website address bar so you know you're entering your account information into a secure website. And if the URL changes suddenly during checkout, you should be very concerned.
- Use a credit, not a debit, card when shopping online for the most protection.
- If you had a bad online shopping experience and are not satisfied the merchant resolved it, report it to the Better Business Bureau!

Learn More

Online Shopping
[whoswatchingcharlottesville.com/onlineshopping.html](#)

Phishing Scams
[whoswatchingcharlottesville.com/phishing.html](#)

Mobile Security
[whoswatchingcharlottesville.com/mobile.html](#)

- **Be skeptical.** If a deal sounds too good to be true—say, \$20 for that new iPod—it probably is. It's probably an attempt to trick you into divulging personal information.
- **Read between the lines.** Pay close attention to the look of the merchant's site. Is it amateurish? Are there spelling or grammatical errors? Do the prices seem unusually low? Read the seller's description of the product closely, especially the fine print.
- **When in doubt, check 'em out.** If you are shopping with a merchant you've never heard of, or on a little-known Web site, look around the site before you make a purchase. Do they have clearly posted information about shipping rates, return policies, warranties, and privacy protection? Can you find contact information easily? Beware if the site doesn't list phone numbers and only includes an email address -- or worse, just a post office box.
- **Know what to look for.** A recent study revealed that 67 percent of people can't identify a secure Website. How do you tell? Always check for the following three things on the checkout or order page:
 - 1). **The "plural URL:"** Look for [https](#) in the Website address bar;
 - 2). **A closed padlock or unbroken key:** A small image of a closed padlock or an unbroken key should appear in the bottom or top window frame of your browser, letting you know your personal information will be encrypted; and
 - 3). **The URL in general:** Always make sure the Web address is what you'd expect. Avoid strange-looking Web addresses. *If you don't see [all three of these](#), or you notice that the URL changes from what you expect in the course of your transaction, log out immediately and shop elsewhere!*
- **Sharing can be a bad thing.** Save your online shopping expedition (and checking your bank account balance) for your own computer. Conducting your private business on shared computers, such as the ones available at Internet cafés, libraries, hotels, and other public places, can be very dangerous since it exposes your credit card or bank account number to possibly unsecured computers.
- **Say "no" to public, unsecured wireless.** Avoid conducting your private business on wireless networks that are available to the public in places like airports, bookstores, and coffee shops.
- **Pay with a credit card.** In the event that a criminal *does* get hold of your card number when you shop online, you're safer if you've been using a credit card than if you used a debit card. Many companies won't hold you responsible for *any* use by imposters. If you are reluctant to give out your credit card number over the Internet, you can use a third-party escrow service such as PayPal.
- **Suspect the suspicious.** If you're on a checkout page and the site asks for your date of birth and Social Security number, be very careful. These shouldn't be required for most types of shopping transactions.
- **Keep a paper trail.** Print and save records of your online transactions, including the product description and price, the online receipt, and copies of any email you exchange with the seller. and receipts.
- **Review your credit card statements frequently.** Read your statements as you receive them, particularly if you shop often online.