

December 2010 Newsletter Article

Credit Coach Playbook # 4: Avoiding The Blitz When Buying Online

Most of us enjoy Cyber shopping. Some of us do it to avoid crowds, some to save gas, and some for the convenience of shopping at any time of day or night. When you're ready to make an online purchase, pay close attention to the information you need to enter. Should you decide to pay by credit card, make your cyber shopping experience safe. NEVER supply personal information, such as your Social Security number or your mother's maiden name. If you have any doubts, cancel your order immediately. Not even the best game tickets are worth the nightmare of having your credit card compromised!

10 Power Plays for safe on-line shopping:

- **Check out the seller.** If you're thinking about shopping on a site with which you're not familiar, do some independent research before you buy.
- **Read return policies.** A number of retailers offer specific return windows for certain products and some charge "restocking" fees. Find out who covers the shipping cost — the customer or the merchant — on a return.
- **Know what you're getting.** Read the seller's product description closely. Name-brand items at greatly reduced prices could be counterfeit.
- **Don't fall for a false email or pop-up.** Legitimate companies don't send unsolicited email messages asking for your password or login name, or your financial information. But scammers do. In fact, crooks often send emails that look just like they're from legitimate companies — but direct you to click on a link, where they ask for your personal information. Delete these emails. They're an attempt to get your information and to facilitate identity theft or other crimes. In addition, just clicking a link in a fraudulent email could install spyware on your computer.
- **Look for signs a site is safe.** When you're ready to buy something from a seller you trust, look for signs that the site is secure, such as a closed padlock on the browser's status bar, before you enter your personal and financial information. When you're asked to provide payment information, the beginning of the Web site's URL address should change from http to shttp or https, indicating that the purchase is encrypted or secured.
- **Secure your computer.** At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall.
- **Consider how you'll pay.** Credit cards generally are a safe option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Also, if your credit card number is stolen, you generally won't be liable for more than \$50 in charges. Don't send cash or use a money-wiring service because you'll have no recourse if something goes wrong.
- **Know the full price, and check out incentives.** If you're looking for the best deal, compare total costs, including shipping and handling. Some "free" shipping deals may come with strings attached, such as requirements to spend a minimum amount or buy certain products.
- **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. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges.
- **Turn your computer off when you're finished shopping.** Many people leave their computers running 24/7, the dream scenario for scammers who want to install malicious software on your machine and then control it remotely to commit cyber crime. To be extra safe, switch off your computer when you are not using it.