Shop Online Safely

Buying presents through the Internet is fast, easy and just a little scary. Here's how to protect your personal information (and wallet) from thieves this holiday season.

Think Credit, Not Debit

If you must shop through the Internet, try to use your credit card. Debit cards pull money from your account immediately, and if you're scammed, it's your responsibility to resolve the matter, say representatives from Access Smart, an online protection service. With credit cards, if somebody rips you off, your credit card company won't hold you responsible, and your credit rating won't be damaged (Good Housekeeping's Quick & Simple, December 11, 2007 issue).

Shop at Secure Sites

When you enter the site's "checkout" page, glance at the URL. It should contain an "s" after "http," which indicates that your personal information is in a safe and secure zone. Sometimes a closed padlock icon or key will also appear on the screen; it means that your credit card number will be "encrypted" (scrambled) in the transaction. Note: Some legitimate companies don't take this security measure, but it doesn't necessarily mean the site is suspect. To be positive your transaction is safe, ask about the company's privacy policy.

Go With Who You Know

As a general rule, always shop at major, well-known companies. Run the site by buySAFE, the only company that puts online merchants through an extensive screening process to verify their identity, sales experience and ability to deliver on their promises. If the merchant passes the test and still don't come through, buySAFE guarantees your refund, says Scott Morgan, Senior Marketing Director of buySAFE. Look for the buySafe seal wherever you do your online shopping.

Try a Virtual Account

Check with your credit card company to see if it offers a "secure online account number" service. Discover gives you a onetime or permanent account number so you never have to type in your card information online.

Get Protection

Install a firewall like NETGEAR, which prevents people from seeing where you go online; anti-spyware software like Windows Defender, which prevents people from recording what you type; and a virus-protection program like Virex.

If you are asked for your driver's license number or social security number, log out immediately. Someone is trying to steal your information.

For more information, contact the Fraud Section at 310/412-5240.