

# Online shoppers can take steps against identity theft, online scams

Don't let your guard down during rush of holiday season

As more shoppers turn to their computers and mobile devices to shop, spending smartly this holiday season is about more than knowing how to get a good deal.

Consumers can save money, time and hassle during the Christmas rush by buying online, but they're also targets for identity theft and online scams.

"During the holiday season, you can be in such a rush and let your guard down," said Scott Boding, director of order screening at CyberSource, a Visa company. "Because there's so much more purchasing taking place, it can become easier for a fraudster to blend in and slip through the cracks."

So before you whip out that credit card and power up your laptop or tablet, here are some tips to protect your personal information.

## Keep watch

Update your computer's anti-virus and anti-spyware software and download the latest security updates. If you're using a wireless connection, make sure it's encrypted with a password.

Strengthen your online passwords by making them unique and difficult to steal. Avoid predictable passwords such as pet and spouse names, birthdays and consecutive numbers. Instead, incorporate random numbers, symbols and capitalized letters.

Watch what you post online. Avoid sharing your address and phone numbers on social networking sites, or storing credit card numbers and passwords in your email account.

## How to shop, pay

Use credit cards instead of debit cards. A stolen debit card gives an identity thief a direct line to your bank account; by using a credit card, you'll be better protected from fraud and face less liability in the event your card number is stolen. Review your credit card statements monthly for unauthorized charges.

Shop at trusted brands with secure websites. Before making a purchase, check your browser's status bar for "https://" URLs that indicate secure connections when placing orders. Look for delivery guarantees from online retailers and keep hard copies of order confirmations.

## Scam alert

Be on the lookout for phishing and email scams. One popular scam sends emails, purportedly from UPS or DHL, alerting recipients that a package has been sent and asking them to fill out an attached form with their personal information. Don't open any attachments; instead, delete the emails.

Shoppers should also be wary of fake online stores, California Attorney General Kamala D. Harris said in a consumer alert on safely shopping online for the holidays. Many online scammers steal information by redirecting shoppers to Web pages that look like the checkout pages of legitimate shopping sites.

To avoid those traps, be careful what links you click. Set your browser to block pop-up windows, and make sure you type in the store's Web address into your browser window instead of clicking links from email or other websites.

And finally, use common sense. Beware of suspicious emails that request information such as your social security number or that promise a special deal. If something sounds too good to be true, it probably is.

"If a television that's usually \$2,000 is on sale for \$200, a flag should pop up," said Doron Simovitch, chief executive of shopping search engine SortPrice.com.