SAFETY

CA, Inc. Offers Safety Tips for Online Holiday Shopping

NewsUSA

(NU) - The allure of Internet deals and the pure convenience of "click and ship" continue to drive shoppers online this holiday season. An estimated $44 billion will be spent online purchasing holiday gifts in 2008, up more than 12 percent over 2007.

Although more money will be spent online this holiday season, consumers are concerned about security risks when making purchases over the Internet. According to a CA-sponsored survey, 72 percent of consumers in North America think retailers do not spend enough on online security and privacy.

To help ease consumer worry, security experts at CA, Inc. offer the following tips to help consumers protect themselves online this holiday season.

- **Secure, then shop.** Before connecting to the Internet, be sure to install anti-virus, a firewall and anti-spyware programs.
- **Update, Update, Update.** The bad guys constantly update their techniques, so consumers need to update their protection. Make sure your firewall, anti-virus, anti-spyware and operating software are up-to-date.
- **Never shop on an open wireless network.** Open networks are easy targets for hackers to break into your computer and capture financial information.
- **Know who you're dealing with.** Get the name and physical address of any online-retailer before submitting personal or financial information. When shopping online auctions, check the track record of the seller before bidding.

When a Web site processes your payment information, make sure the URL changes from HTTP to SHTTP or HTTPS.

- **Never e-mail your personal or financial information.** E-mail is not a secure method of sending information like your credit card, bank account or Social Security number.
- **Look for secure payment processing.** When a Web site processes your payment information, be sure the URL address changes from HTTP to SHTTP or HTTPS. This indicates that the purchase is encrypted or secured.
- **Be alert and be suspicious.** Identity thieves count on the holiday rush to catch consumers off guard with bogus e-mails that seem to be coming from a legitimate organization such as the bank, the IRS or UPS. These "phishing" scams can lure shoppers into divulging personal information. Be suspicious of anyone asking for additional personal information or asking you to click on links in an e-mail.