# Holiday Shopping On The Internet

## Tips for Safe Online Shopping this Holiday Season

(NAPSA)—If you've been thinking about shopping online this holiday season, you're not alone. Consumers spent $26 billion online last year according to the U.S. Department of Commerce.

Many, however, are worried about the effects of holiday shopping in their e-mail inboxes and the possibility of fraud. A staggering 72 percent said they are concerned that shopping online will result in a flood of unwanted e-mail spam and with 51 unique phishing attacks (a form of e-mail/online fraud) currently taking place per day in 2004, the concern regarding forms of e-mail spam is a valid one.

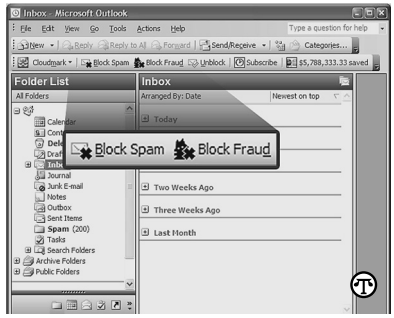
Expert Karl Jacob, CEO of Cloudmark and visionary in the e-mail security space, is working to help educate consumers about ways to protect themselves as they shop online, and has identified five critical tips to avoid being a victim of online identify theft, phishing and unwanted e-mail spam this holiday season.

1. Don't e-mail personal or financial information.

Avoid filling out forms in e-mail messages that ask for personal financial information. Legitimate companies will not ask for this information via e-mail.

2. Be aware of "phishing" and make sure you are protected

Phishing is a high-tech scam that uses spam, pop-up messages or counterfeit Web sites to deceive you into disclosing your credit card numbers, bank account information, social security number, passwords, or other sensitive information. The message may pop up while you are online or take the form of an e-mail notification that says you need to "update" or "validate" your account information. These attempts can often be recognized through grammar errors and general language that is improper for corporation to customer communications.




**If an e-mail seems fishy, it could be the fraud known as "phishing." Don't fall for it.**

3. Don't use the links in an e-mail to get to any Web page, if you suspect the message might not be authentic.

As Web site and e-mail sender addresses are frequently faked it is always safer to log directly onto the Web site address in your browser, or even call the company by phone. For example, a phishing e-mail may open a near replica of a bank Web site and a pop up message will appear that directs the consumer to "please confirm financial information."

If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like checking the beginning of the Web address URL for a Web site that begins "https:" (the "s" stands for "secure"). In addition there are solutions available that will automatically ensure Web site links are legitimate, so that you don't have to worry.

4. Choose e-mail security software that protects you from unwanted e-mail spam

If you use e-mail, you are likely receiving a growing amount of "junk" e-mail (otherwise known as spam) on a daily basis. Researchers estimate that spam represents anywhere from 30 to 70 percent of all e-mail traffic. There are, however, solutions such as Cloudmark SpamNet that stop over 98 percent of spam, protecting you from unwanted junk mail, fraud and all dangerous e-mail threats. Products such as this, can save you time and money avoiding the annoyance of unwanted e-mails and helping to ensure your safety this holiday season.

5. Regularly log into your online accounts

Keep abreast of transactions and look out for any obscure amounts or purchases you don't recognize. If anything looks suspicious, contact your bank or credit card company immediately.

To buy your holiday gifts safely and securely this holiday season it is important to chose an e-mail security software solution that addresses all forms of e-mail spam, including online fraud and phishing, such as the solutions available from Cloudmark, which protect from all e-mail threats—e-mail-born viruses, worms, spam and even the most devious fraud messages.

For more information, visit http://www.cloudmark.com/.