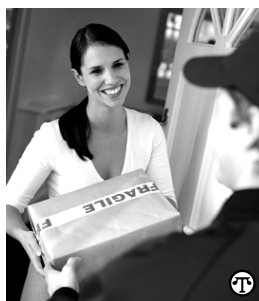
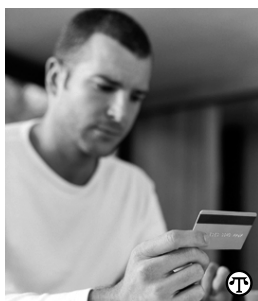


Visa Urges Consumers To Be Safe When Holiday Shopping Online

Online Sales Expected To Reach \$26 Billion This Season



(NAPSA)—Online shopping has come a long way in just a few years. A dazzling array of gifts is only a mouse click away—minus the holiday angst of crowds, parking squabbles and endless odes to reindeer.

According to eMarketer's Online Holiday Shopping Preview report, online sales are projected to reach \$26.2 billion this holiday season, a 21.9 percent jump over 2004.

But before you don your Santa hat and fire up your browser, Mike Yakel, vice president of Authentication and Security Solutions, Visa USA, reminds shoppers to stay safe.

"With online shopping heating up for the holidays and millions of new households venturing into online shopping, Visa is seeing strong consumer interest in the added layer of security provided by services such as Verified by Visa, an anti-fraud password program, which ensures only you can use your Visa card online," Yakel said.

"Online merchants that offer Verified by Visa have a distinct advantage in consumer confidence as increasingly informed shoppers choose sites that show a real commitment to customer protection."

So keep these tips in mind when piling gifts into your eSleigh.

What's Hot

- At checkout, sharing only your address, phone number and credit/debit card information.

- Creating passwords that are a combination of random letters, numbers and symbols.

- Enrolling your credit or debit card in an anti-fraud password program such as Verified by Visa that ensures only you can use your card for online purchases. Thousands of merchants offer the service including online retailers such as Liz Claiborne, Wal-Mart, Blue Nile, Comp USA and PlayStation.

- Never sharing passwords with anyone and using different

passwords for different Web sites.

- Shopping with a Visa credit card or check card, both of which offer Zero Liability for unauthorized transactions.

- Shopping only at Internet merchants you know and trust; checking with the Better Business Bureau, which has given its BBBOnline Reliability Seal to almost 25,000 Web sites.

- Setting your browser to the highest level of security notification and monitoring.

- Printing and saving the confirmation page when completing an online purchase.

- Always closing your browser window after you've finished your online shopping.

- Not waiting for paper statements each month; checking your card and bank statements periodically online or by phone for signs of fraud.

What's Not

- Sharing your birth date, your social security information or your bank account number.

- Using easy-to-remember passwords such as your mother's maiden name, your phone number or any personal information.

- Experimenting with new payment methods that require the sharing of sensitive personal information.

- Writing down passwords on Post-Its, in PDAs or on bulletin boards.

- Shopping with less secure payment methods such as checks.

- Shopping wherever your browser takes you.

- Assuming computer safety options are activated automatically.

- Assuming the merchant will archive a copy of your transaction.

- Leaving your computer on when sensitive information is still displayed.

- Assuming all statements are correct.