Avoid cyber Grinches, scams and schemes

November 18 2005

As consumers go online in record numbers this holiday to shop and make travel plans, security experts advise that they take a few basic precautions to keep from getting ripped off or have their identity stolen.

Analysts are expecting strong online spending this holiday. Marketing firm Retail Forward said Thursday that 2005 online holiday sales will go up 16 percent from last year to $27.3 billion.

Last year holiday-season shopping jumped by 25 percent year-over-year, with shoppers spending a record $23.2 billion online, excluding travel, according to Harris Interactive.

The National Consumers League, Better Business Bureau and the National Cyber Security Alliance are offering 12 tips for online shoppers to protect against the "Cyber Grinches, Scams and Schemes."

The group cautioned in a release Thursday that the "Internet can make your shopping faster and easier, but there can also be pitfalls if you're not careful," adding that with a few precautions online shoppers can have a "safe online shopping experience" that won't provide an "an opportunity for cyber thieves."

The 12 tips the group suggest are:

-- Know who you're dealing with. Check out unfamiliar sellers with the Better Business Bureau and your state or local consumer protection agency.

-- Get all the details. Get the name and physical address of the seller; how much the product or service costs; what is included for that price; whether there are shipping charges; the delivery time, if any; the seller's privacy policy; and the cancellation and return policy.

-- Look for signs that online purchases are secure. At the point that you are providing your payment information, the beginning of the Web site address should change from http to shttp or https, indicating that the information is being encrypted.

-- Pay the safest way. It's best to use a credit card because under federal law you can dispute the charges if you don't get what you were promised. You also have dispute rights if there are unauthorized charges on your credit card.

-- Never enter your personal information in a pop-up screen. When you visit a company's Web site, an unauthorized pop-up screen created by an identity thief could appear with blanks for you to provide your personal information.

-- Keep documentation of your order.

-- Know your rights. Federal law requires orders made by mail, phone or online to be shipped by the date promised or, if no delivery time was stated, within 30 days. If the goods aren't shipped on time, you can cancel and demand a refund.

-- Be suspicious if someone contacts you unexpectedly and asks for your personal information. Identity thieves send out bogus e-mails about problems with consumers' accounts to lure them into providing their personal information.

-- Check your credit card and bank statements carefully. Notify the bank

immediately if there are unauthorized charges or debits.

-- Keep your computer secure for safe shopping and other online activities. Protect your computer with spam filters, anti-virus and anti-spyware software, and a firewall.

-- Beware of e-mails offering loans or credit, even if you have credit problems. Con artists take advantage of cash-strapped consumers during the holidays to offer personal loans or credit cards for a fee upfront.

-- Contact the seller promptly about any problems with your order. Check with the company's Web site for a customer service page, "contact us" link, e-mail address, or phone number to get your complaint addressed or questions answered. If you can't resolve the problem, contact the Better Business Bureau.

According to iBAHN, a provider of secure high-speed Internet access to more than 2,200 hotels and 285,000 hotel rooms worldwide, it can be a "dangerous misconception," that hotel Net connections are always safe.

"There are still thousands of hotels with poorly protected Internet connections. Moreover, many travelers are completely unaware how easy it is for a hacker sitting in a room just down the hall, or in a hotel lobby, to view personal information, credit card and bank account numbers stored on their computer's hard drive," the company warned in a release.

iBAHN offers the following tips to travelers who want to safeguard their personal information while on the road:

-- When making a reservation, check whether the hotel uses a secure Internet provider.

-- Disable the file-sharing option on your computer to prevent hackers

from accessing your hard drive.

-- Disable the peer-to-peer or ad hoc capabilities on your computer.

-- Watch your use of WiFi. iBAHN suggest not using WiFi in "hot spots" such as airports, hotel lobbies and other public places, unless it's protected by WPA encryption. (Your computer will indicate whether this is the case when you attempt to logon.)

iBAHN notes that data from the Federal Trade Commission indicates that 27.3 million Americans have been victims of identity theft in the last five years. It is estimated that this year more than 10 million Americans will lose an average of $5,000 from identity theft.