



Intelligence Note

*Prepared by the **Internet Crime Complaint Center (IC3)***

November 21, 2011

HOLIDAY SHOPPING TIPS

In advance of the holiday season, the FBI reminds shoppers to beware of cyber criminals and their aggressive and creative ways to steal money and personal information. Scammers use many techniques to fool potential victims including fraudulent auction sales, reshipping merchandise purchased with a stolen credit card, sale of fraudulent or stolen gift cards through auction sites at discounted prices, and phishing e-mails advertising brand name merchandise for bargain prices or e-mails promoting the sale of merchandise that ends up being a counterfeit product.

Fraudulent Classified Ads or Auction Sales

Internet criminals post classified ads or auctions for products they do not have. If you receive an auction product from a merchant or retail store, rather than directly from the auction seller, the item may have been purchased with someone else's stolen credit card number. Contact the merchant to verify the account used to pay for the item actually belongs to you.

Shoppers should be cautious and not provide credit card numbers, bank account numbers, or other financial information directly to the seller. Fraudulent sellers will use this information to purchase items for their scheme from the provided financial account. Always use a legitimate payment service to protect purchases.

Diligently check each seller's rating and feedback along with their number of sales and the dates on which feedback was posted. Be wary of a seller with 100% positive feedback, if they have a low total number of feedback postings and all feedback was posted around the same date and time.

Gift Card Scam

The safest way to purchase gift cards is directly from the merchant or authorized retail merchant. If the merchant discovers the card you received from another source or auction was initially obtained fraudulently, the merchant will deactivate the gift card number, and it will not be honored to make purchases.

Phishing and Social Networking

Be leery of e-mails or text messages you receive indicating a problem or question regarding your financial accounts. In this scam, you are directed to follow a link or call the number provided in the message to update your account or correct the problem. The link actually directs the individual to a fraudulent Web site or message that appears legitimate; however, any personal information you provide, such as account number and personal identification number (PIN), will be stolen.

Another scam involves victims receiving an e-mail message directing the recipient to a spoofed Web site. A spoofed Web site is a fake site or copy of a real Web site that is designed to mislead the recipient into providing personal information.

Consumers are encouraged to beware of bargain e-mails advertising one day only promotions for recognized brands or Web sites. Fraudsters often use the hot items of the season to lure bargain hunters into providing credit card information. The old adage "if it seems too good to be true" is a good barometer to use to legitimize e-mails.

Black Friday has traditionally been the "biggest shopping day of the year." The Monday following Thanksgiving has more recently (2005) been labeled *Cyber Monday*, meaning the e-commerce industry endorses this special day to offer sales and promotions without interfering with the traditional way to shop. Scammers try to prey on Black Friday or Cyber Monday bargain hunters by advertising "one day only" promotions from recognized brands. Consumers should be on the watch for too good to be true e-mails from unrecognized Web sites.

Along with on-line shopping comes the growth of consumers utilizing social networking sites and mobile phones to satisfy their shopping needs more easily. Again, consumers are encouraged to beware of e-mails, text messages, or postings that may lead to fraudulent sites offering bargains on brand name products.

Tips

Here are some tips you can use to avoid becoming a victim of cyber fraud:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Always run a virus scan on attachment before opening.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the web address link you are directed to and determine if they match.
- Log on directly to the official Web site for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- Contact the actual business that supposedly sent the e-mail to verify that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act impulsively.
- If you receive a request for personal information from a business or financial institution, always look up the main contact information for the requesting company on an independent source (phone book, trusted internet directory, legitimate billing statement, etc.) and use that contact information to verify the legitimacy of the request.
- Remember if it looks too good to be true, it probably is.

To receive the latest information about cyber scams, please go to the FBI Web site and sign up for e-mail alerts by clicking on one of the red envelopes. If you have received a scam e-mail, please notify the IC3 by filing a complaint at www.ic3.gov. For more information on e-scams, please visit the FBI's New E-Scams and Warnings webpage at <http://www.fbi.gov/cyberinvest/escams.htm>.