Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 30, 2009

HOLIDAY SHOPPING TIPS

This holiday season the Federal Bureau of Investigation (FBI) is reminding people that cyber criminals continue to aggressively create new 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, and sale of fraudulent or stolen gift cards through auction sites at a discounted price.

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 financial information directly to the seller, as 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.

As for product delivery, unfamiliar Web sites or individuals selling reduced or free shipping to customers through auction sites many times are deemed to be fraudulent. In many instances, these Web sites or sellers provide shipping labels to their customers as a service. However, the delivery service providers are ultimately not being paid to deliver the package; therefore, packages shipped by the victims using these labels are intercepted by delivery service providers because they are identified as fraudulent.

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

Be careful about purchasing gift cards from auction sites or through classified ads. If you need a gift card, it is safest to purchase it directly from the merchant or another authorized retail store. If the gift card 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 for purchases.

Phishing and Smishing Schemes

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 individuals to a fraudulent Web site or message that appears legitimate where any personal information you provide, such as account number and 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 and misleads the recipient into providing personal information, which is routed to the scammer's computers.

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. Virus scan the attachments if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they actually match and will lead you to a legitimate site.
- 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 if the e-mail is genuine.

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.