Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 20, 2012

HOLIDAY SHOPPING TIPS

The FBI continues to remind shoppers to be wary of Internet fraud during the holiday shopping season. Scammers use many techniques to deceive potential victims, including creating fraudulent auction sales, reshipping merchandise purchased with a stolen credit card, selling fraudulent or stolen gift cards through auction sites at a discounted price and using phishing e-mails to advertise brand-name merchandise for bargain prices or e-mails to promote the sale of merchandise that is counterfeit.

In advance of the holiday season, the FBI, in partnership with the Merchant Risk Council (MRC), would like shoppers to be informed of the common scams that affect consumers and E-commerce. The MRC is an organization that works to increase networking and information sharing among merchants to better enable members to successfully fight online fraud.

Purchasing any new product or gift card on an auction or classified advertisement site where the price is significantly lower than any sale prices in retail outlets

Many of these sellers, especially for gift cards and tickets, have purchased these items with a stolen credit card. Most likely, the gift card or ticket will be deactivated by the time the recipient uses the card or ticket.

Never provide credit card numbers, bank account information, personally identifiable information or wire money to a person who advertises items on these sites at a too good to be true price. Many times, fraudsters will post a popular item to obtain this information, and the goods will never be mailed, but your card or identity will be used fraudulently later. If you make a purchase from these sites, we encourage you to check a seller's ratings and feedback to ensure he or she is reputable.

Phishing and scam e-mails, text messages or phone calls

Many times, e-mails, texts or phone calls will look or sound like they are coming from a well-known retailer, stating a need to "verify" the full credit card number you used for a purchase or ask you to click a link to update personal account information. If you receive an e-mail that asks you to click a link to verify information, delete it. Type the retailer's or financial institution's website into a browser to log into your account. If the fraudster is insistent, ask him or her to read you the card number first or ask to call back. If it is a legitimate call, the company representative will have no problem with your calling back through the customer service line.

"One Day Only" websites featuring the sale of a "hot item"

During the holiday season, there will be an increase in websites created to sell specific items in high demand. Typically, the cardholders never receive the product, but the credit card information they entered is used for fraudulent purchases. It is important to only make purchases with companies and sellers who have a history and can be identified when searching reviews and ratings.

Postings of popular items for free or drastically reduced prices

There are many gift card offers on social media sites claiming to be from major retailers. These offers are typically used to gain access to consumers' social media accounts either to log in to other accounts you may have tied to this account or to post illegitimate offers on your behalf. Purchasing an item at a reduced rate based on a posting from someone you do not know can often lead to a credit card compromise or the purchase of a counterfeit item.

"Work from home" offers, to act as a private reshipper, often fronting the shipping costs on behalf of the fraudster

Offers to work from home to reship items to another country or another person often means the goods were purchased with stolen credit cards. Having these goods shipped to your home and sending them to another person could have legal implications. Also, many times the money promised for completing this service is never paid. These scams can sound legitimate at first, so be leery of anyone offering a lot of money for a simple task.

Remember, if an offer seems too good to be true, it probably is. Consumers are urged to be very skeptical of people offering a great deal outside of any established retail business.

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. Scan the attachments for viruses 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 website 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.
- 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 quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
- Remember if it looks too good to be true, it probably is.

To receive the latest information about cyber scams, go to the FBI website and sign up for e-mail alerts by clicking on the red envelope labeled "get FBI updates." 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, visit the FBI's New E-Scams and Warnings webpage at http://www.fbi.gov/scams-safety/e-scams.