November 18, 2010

HOLIDAY SHOPPING TIPS

This holiday season the FBI reminds shoppers that cyber criminals aggressively create new ways to steal money and personal information. Scammers use many techniques to fool potential victims, including conducting fraudulent auction sales, reshipping merchandise purchased with stolen credit cards, and selling fraudulent or stolen gift cards through auction sites at discounted prices.

Fraudulent Classified Ads and Auction Sales

Internet criminals post classified ads and auctions for products they do not have, and make the scam work by using stolen credit cards. Fraudsters receive an order from a victim, charge the victim's credit card for the amount of the order, then use a separate, stolen credit card for the actual purchase. They pocket the purchase price obtained from the victim's credit card and have the merchant ship the item directly to the victim. Consequently, an item purchased from an online auction but received directly from the merchant is a strong indication of fraud. Victims of such a scam not only lose the money paid to the fraudster, but may be liable for receiving stolen goods.

Shoppers may help avoid these scams by using caution and not providing financial information directly to the seller, as fraudulent sellers will use this information to purchase items for their schemes. Always use a legitimate payment service to ensure a safe, legitimate purchase.

As for product delivery, fraudsters posing as legitimate delivery services offer reduced or free shipping to customers through auction sites. They perpetuate this scam by providing fake shipping labels to the victim. The fraudsters do not pay for delivery of the packages; therefore, delivery service providers intercept the packages for nonpayment and the victim loses the money paid for the purchase of the product.

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, with a low total number of feedback postings, or with all feedback posted around the same date and time.

Gift Card Scam

Be careful when purchasing gift cards through auction sites or classified ads. It is safest to purchase gift cards directly from the merchant or retail store. If the gift card merchant discovers that your card is fraudulent, the merchant will deactivate the gift card and refuse to honor it for purchases. Victims of this scam lose the money paid for the gift card purchase.

Phishing and Smishing Schemes

In phishing schemes, a fraudster poses as a legitimate entity and uses emails and scam web sites to obtain victims' personal information, such as account numbers, user names, passwords, etc. Smishing is the act of sending fraudulent text messages to bait a victim into revealing personal information.

Be leery of emails or text messages that indicate a problem or question regarding your financial accounts. In this scam, fraudsters direct victims to

follow a link or call a number to update an account or correct a purported problem. The link directs the victim to a fraudulent web site or message that appears legitimate. Instead, the site allows the fraudster to steal any personal information the victim provides.

Current smishing schemes involve fraudsters calling victims' cell phones offering to lower the interest rates for credit cards the victims do not even possess. If a victim asserts that they do not own the credit card, the caller hangs up. These fraudsters call from TRAC cell phones that do not have voicemail, or the phone provides a constant busy signal when called, rendering these calls virtually untraceable.

Another scam involves fraudsters directing victims, via email, to a spoofed web site. A spoofed web site is a fake site that misleads the victim into providing personal information, which is routed to the scammer's computer.

Phishing schemes related to deliveries are also rampant. Legitimate delivery service providers neither email shippers regarding scheduled deliveries nor state when a package is intercepted or being temporarily held. Consequently, emails informing of such delivery issues are phishing scams that can lead to personal information breaches and financial losses.

Tips

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

- Do not respond to unsolicited (spam) email.
- Do not click on links contained within an unsolicited email.
- Be cautious of email 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 email messages that ask for personal information.
- Always compare the link in the email with the link to which you are directed and determine if they match and will lead you to a legitimate site.
- Log directly onto the official web site for the business identified in the email, instead of "linking" to it from an unsolicited email. If the email 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 email to verify if the email is genuine.
- If you are asked 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, please go to the FBI web site and sign up for email alerts by clicking on one of the red envelopes. If you have received a scam email, 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.