Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 24, 2014

Alert Number
I-112414-PSA

FBI REMINDS SHOPPERS TO BE AWARE OF CYBER CRIMINALS OFFERING SCAMS THIS HOLIDAY SEASON

IF THE DEAL SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.

The FBI reminds shoppers in advance of the holiday shopping season to beware of cyber criminals and their aggressive and creative ways to steal money and personal information. Scammers use many techniques to defraud consumers by offering too good to be true deals via phishing e-mails advertising brand name merchandise, quick money making offers, or gift cards as an incentive to purchase a product. Remember, if the deal looks too good to be true, it probably is and never provide your personal information to an unknown party or untrusted website.

Scammers often use e-mail to advertise hot-ticket items of the year that may become hard to find during the holidays to lure unsuspecting consumers to click on links. Steer clear of untrusted sites or ads offering items at unrealistic discounts or with special coupons. You may end up paying for an item, giving away personal information and credit card details, and then receive nothing in return, along with your identity compromised. These sites may also be offering products at a great price, but the products being sold are not the same as the products they advertise. This is known as the bait and switch scam.

Beware of posts on social media sites that appear to offer vouchers or gift cards, especially sites offering deals too good to be true, such as a free $500 gift card. Some may pose as holiday promotions or contests. It may even appear one of your friends shared the link with you. If so, it is likely your friend was duped by the scam after it was sent to them by one of their friends. Oftentimes, these scams lead to online surveys designed to steal personal information. Remember, if the deal looks too good to be true, it probably is. And never provide your personal information to an unknown party or untrusted website.

When purchasing gift cards online, be leery of auction sites selling discounted or bulk offers of gift cards. When purchasing gift cards in the store, examine the protective scratch off area on the back of the card to see if it has been tampered with.

Be on the lookout for mobile applications designed to steal your personal information from your smartphone. Such apps are often disguised as games and are often offered for free. Research the company selling or giving away the app and look online for third party reviews before installing an app from an unknown source.

Tickets to theater, concerts, and sporting events are always popular gifts during the holidays. If you purchase or receive tickets as a gift, do not post pictures of the tickets to social media sites. Protect the barcodes on tickets as you would your credit card number. Fraudsters will create a ticket using the barcode obtained from searching around social media sites and resell the ticket. You should never allow the barcode to be seen on social media.

If you are in need of extra cash at this time of year, beware of sites and posts offering work you can do from the comfort of your own home. Often, the work from home opportunities rely on convenience as a selling point for applicants

with an unscrupulous motivation behind the posting. You should carefully research the job posting and individuals or company contacting you for employment.

As a consumer, if you feel you are a victim of an Internet-related crime, you may file a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov.

Tips

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

- Check your credit card statement routinely.
- Protect your credit card numbers from "wandering eyes".
- 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 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.
- 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 on their official website.
- Remember if it looks too good to be true, it probably is.