Federal Bureau of Investigation

Office of Public Affairs
National Press Office

'Tis the Season for Holiday Scams:
How to Protect Yourself

Talking Points
Updated 11/23/2016

With the holidays ramping up and seasonal shopping in full swing, criminals are also gearing up for a busy season. Cyber criminals don't take the holidays off. In fact, they're especially busy trying to steal your money and personal information. Shoppers should be more vigilant than ever for scams designed to steal their money and personal information. Though criminals are often aggressive and creative in their efforts to obtain such money and personal information, there are certain red flags and common schemes holiday shoppers can guard against this holiday season.

Online Shopping Scams

If a deal looks too good to be true, it probably is. Scammers often scheme to defraud consumers by offering too-good-to-be-true deals via phishing e-mails or advertisements. Such schemes may offer brand name merchandise at extremely low discounts or promise gift cards as an incentive to purchase a product. Other sites may offer products at a great price, but the products being sold are not the same as the products advertised.

Steer clear of un-trusted 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 except a compromised identity. In addition, do not open any unsolicited e-mails and do not click on any links provided.

In addition to securing your banking and credit accounts with strong and different passwords, secure all your other accounts that contain anything of value, such as: rewards accounts, online accounts that save your payment information, or accounts containing your private, personal information.

The emergence and prevalence of secondary markets for airline miles, gift cards, rewards credits, and the like have inadvertently increased the demand for, and resale value of, your stolen information.

Be vigilant when receiving items purchased from online auctions and third-party marketplaces. If an item arrives from some other online merchant, it may have been purchased using a stolen credit card number or stolen rewards points, etc. and then shipped directly to you. Report such cases to both the marketplace where you bought and the merchant who sent it.

Social Media Scams

Beware of posts on social media sites that appear to offer vouchers or gift cards, especially deals that are 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. Often, these scams lead you to participate in an online survey that is actually designed to steal personal information.

In addition, if you purchase or receive theater, concerts, or sporting event tickets as a holiday gift, do not post pictures of the tickets on social media sites. Fraudsters can create a ticket using the barcode obtained from the photo and resell the ticket. Protect ticket barcodes as you would your credit card number, and never display them on social media.

Smartphone App Scams

Be careful when downloading mobile applications. Some apps, often disguised as games and offered for free, may be designed to steal personal information. Before downloading an app from an unknown source, research the company selling it or giving it away, and look online for third-party reviews of the product. Also, be mindful that alternative app marketplaces available to "jailbroken" or "rooted" devices can potentially include copyright-infringing, stolen content and compromised versions of otherwise trustworthy applications.

Work-From-Home Scams

If you are in need of extra cash this time of year, beware of sites and postings offering work you can do from the comfort of your own home. These opportunities rely on convenience as a selling point for applicants, but often have unscrupulous motivations behind them. You should carefully research the job posting and individuals or company offering you employment.

Protect Yourself

Here are some additional steps you can take to avoid becoming a victim of cyber fraud this holiday season:

- Check your credit card statement routinely. If possible, set up credit card transaction auto alerts, or check your balance after every online purchase to ensure the proper amount was charged to your account. It is important to keep checking your card after the holiday season, as many fraudulent charges can show up even several weeks later.
- If purchasing merchandise, ensure it is from a reputable source.
- Ensure a site is secure and reputable before providing your credit card number online. Don't trust a site just because it claims to be secure.
- Do your research to ensure legitimacy of the individual or company you are purchasing from.
- Beware of providing credit card information when requested through unsolicited e-mails.
- Do not respond to unsolicited (spam) e-mails.
- Do not click on links contained within an unsolicited e-mail.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Be cautious of e-mails 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.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.
- Secure your credit card accounts, even rewards account, with strong passwords, change passwords and check your account routinely.
- Be wary when replying to unsolicited e-mails for work-at-home employment.
- Be cautious of exaggerated claims of possible earnings or profits.
- Beware when money is required up front for instructions or products for employment.

- Do not give out your personal information when first interacting with a prospective employer.
- Be leery when a job posting claims “no experience necessary.”
- Be cautious when dealing with individuals outside of your own country.

Who To Contact If You Suspect You’ve Been Victimized:

- Contact your financial institution immediately upon suspecting or discovering a fraudulent transfer.
- Contact law enforcement.
- Request that your bank reach out to the financial institution where the fraudulent transfer was sent.
- File a complaint with the FBI’s Internet Crime Complaint Center at www.IC3.gov, regardless of dollar loss. Provide all relevant information in your complaint.