Public Service Announcement

Prepared by the Internet Crime Complaint Center (IC3)

November 26, 2013

Holiday Shopping Tips

The FBI reminds holiday shoppers to beware of cyber criminals who are out to steal money and personal information. Scammers use many techniques to defraud consumers, from phishing e-mails offering too good to be true deals on brand-name merchandise to offering quick cash to victims who will re-ship packages to additional destinations. Previously reported scams are still being executed today.

While monitoring credit reports on an annual basis and reviewing account statements each month is always a good idea, consumers should keep a particularly watchful eye on their personal credit information at this time of year. Scrutinizing credit card bills for any fraudulent activity can help to minimize victims' losses. Unrecognizable charges listed on a credit card statement are often the first time consumers realize their personally identifiable information has been stolen.

Bank transactions and correspondence from financial institutions should also be closely reviewed. Bank accounts can often serve as a target for criminals to initiate account takeovers or commit identity theft by creating new accounts in the victims' name. Consumers should never click on a link embedded in an e-mail from their bank, but rather open a new webpage and manually enter the URL (web address), because phishing scams often start with phony e-mails that feature the bank's name and logo.

When shopping online, make sure to use reputable sites. Often consumers are shown specials on the web, or even in e-mail offers, that look too good to be true. These sites are used to capture personally identifiable information, including credit card numbers, addresses and phone numbers to make fraudulent transactions. It's best to shop on sites with which you are familiar and that have an established reputation as trusted online retailers, according to the MRC, a nonprofit that supports and promotes operational excellence for fraud, payments and risk professionals within eCommerce.

If you look for an item or company name through a search engine site, scrutinize the results listed before going to a website. Do not automatically click on the first result, even if it looks identical or similar to the desired result. Many fraudsters go to extreme lengths to have their own website appear ahead of a legitimate company on popular search engines. Their website may be a mirrored version of a popular website, but with a slightly different URL.

Purchases made on these sites could result in one or more of the following consequences: never receiving the item, having your credit card details stolen, or downloading malware/computer virus to your computer. Before clicking on a result in a search engine, inspect the URL of the

destination website. Look for any misspellings or extra characters such as a period or comma as these are indicative of fraud. When taken to the payment page of a website, again verify the URL and ensure it is secure by starting with "HTTPS," not just "HTTP."

Here are some additional 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; 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 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 that the e-mail is genuine.
- If you are requested to act quickly or there is an emergency that requires your attention, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Remember if it looks too good to be true, it probably is.

Finally, check these additional sources to become even more informed on safe online shopping. Previous Holiday Shopping Tips public service announcements can be viewed on IC3.gov at the following links: http://www.ic3.gov/media/2012/121120.aspx, http://www.ic3.gov/media/2011/111121.aspx and http://www.ic3.gov/media/2010/101118.aspx.

US-CERT posted a Holiday Season Phishing Scams and Malware Campaigns release on Nov. 19, 2013, reminding consumers to stay aware of seasonal scams. The entire alert can be viewed at **MailScanner has detected a possible fraud attempt from "www.ic3.gov" claiming to be** https://www.us-cert.gov/ncas/current-activity/2013/11/19/Holiday-Season-Phishing-Scams-and-Malware-Campaigns.

To receive the latest information about cyber scams, go to FBI.gov 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, 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 **MailScanner has detected a possible fraud attempt from "www.ic3.gov" claiming to be** http://www.fbi.gov/scams-safety/e-scams.