NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER
BULLETIN

A-0001-NCCIC -150020111205

DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.

HOLIDAY PHISHING AND ONLINE CYBER SCAMS

EXECUTIVE SUMMARY

(U) This advisory provides general guidance to public and private sector organizations and individuals about potential holiday phishing and other online cyber scams. With the increase of buying goods and services online, especially during the holiday season (i.e. cyber Monday), the USG sees increased malicious cyber activity resulting in both online fraudulent activity and the loss of consumers' personal information. Cyber criminals often use multiple methods, such as phishing emails and phony websites, to attract online shoppers and gain access to and exploit their personal information. Additionally, attackers who pose as legitimate online businesses and services will use fraudulent emails and websites to infect an unsuspecting shopper's computer with malicious code. This advisory offers some suggested methods that may help minimize the likelihood of a consumer becoming successfully compromised. We encourage anyone receiving this advisory to distribute it widely.

BACKGROUND

(U) During the holiday season, many consumers will choose to buy gifts and services from online retailers. Malicious actors will take advantage of the increased volume of online consumers and try to exploit those who are unaware of cyber risks and gain access to their personal information. Public and private sector organizations and individuals should remain vigilant when purchasing online. Some of the current threat trends include, but are not limited to:

- Phony profiles on social networking sites such as Facebook and Twitter are claiming to be legitimate businesses. These fake profiles will look like their legitimate counterparts but clicking on links in these profiles could allow malicious code to be installed on the victim's computer compromising the victim's security and privacy[1].

- Emails from hotels claiming that a "wrong transaction" has been charged to a credit card have also been reported. The hotel will claim to offer a refund if the victim downloads and completes a refund form. Unfortunately, the form is embedded with malicious code and downloading it installs malware onto the victim's computer[2].

- Emails which are actually phishing scams involving bogus courier services during the holidays. The fake courier will send an email saying there is a package waiting for the victim and ask for personal information in order to retrieve it[2].

- Non-legitimate websites claiming to have the "hot" gift of the season when most legitimate retailers are sold out. The non-legitimate websites will tempt the victim to order from them when they actually do not have the item and will steal their personal information and charge their credit card[2].

PREVENTATIVE STRATEGIES

(U) The following preventative strategies are intended to help our public and private partners proactively look for emails attempting to deceive users into 'clicking the link' or opening attachments to seemingly real websites regarding holidays season 'deals'. The following represents some best practices to follow but is not an exhaustive list:

- NEVER click on links in emails. If you do think the email is legitimate, whether from a third party retailer or primary retailer, go to the site and log on directly. Whatever notification or service offering was referenced in the email, if valid, will be available via regular log on.
- NEVER open the attachments. Typically, retailers will not send emails with attachments. If there is any doubt, contact the retailer directly and ask whether the email with the attachment was sent from them.
- Do NOT give out personal information over the phone or in an email unless completely sure. Social engineering is a process of deceiving individuals into providing personal information to seemingly trusted agents who turn out to be malicious actors. If contacted over the phone by someone claiming to be a retailer or collection agency, do not give out your personal information. Ask them to provide you their name and a call-back number. Just because they may have some of your information does not mean they are legitimate! Again, be careful when providing any information over the phone. For further information regarding holiday scams, visit: http://www.us-cert.gov/current/index.html#holiday_season_phishing_scams_and

POINTS OF CONTACT

(U) While the U.S. Government does not endorse a particular solution, identifying vendors with experience managing cyber incidents may reduce the time it takes to mitigate damage and restore service or operations if compromised.

(U) Any cyber intrusion, including data breaches involving a monetary loss or financial nexus, can be reported to any of the FBI's 56 Field Offices. For FBI field office contact information, please consult your local telephone directory or see the FBI's contact information web page:

http://www.fbi.gov/contactus.htm

(U) US-CERT (www.us-cert.gov) offers a wide variety of technical and non-technical information to make use of both before and after an incident. A variety of documents with information regarding defensive measures to combat a computer network attack are available at:

http://www.us-cert.gov/nav/t01/

(U) Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement. Data breaches involving a monetary loss or financial nexus such as a compromise to your credit or debit accounts, or personal information can also be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

http://www.secretservice.gov/field_offices.shtml

(U) Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

ENDNOTES:

1. *'Tis the Season to Get Hacked: Don't Become a Holiday Cybercrime Victim,* socialmediatoday.com - http://socialmediatoday.com/jan-legnitto/395737/tis-season-get-hacked-don-t-become-holiday-cybercrime-victim
2. *12 Scams of the Holidays: Do Not Let Cybercriminals Steal Your Holiday Spirit*, blogs.mcafee.com - http://blogs.mcafee.com/consumer/12-scams-of-the-holidays-do-not-let-cybercriminals-steal-your-holiday-spirit