Holiday Scams and Malware Campaigns

TLP:WHITE

Original release date: November 16, 2017

US-CERT reminds users to remain vigilant when browsing or shopping online this holiday season. Emails and ecards from unknown senders may contain malicious links. Fake advertisements or shipping notifications may deliver attachments infected with malware. Spoofed email messages and phony posts on social networking sites may request support for fraudulent causes.

To avoid seasonal campaigns that could result in security breaches, identity theft, or financial loss, users are encouraged to take the following actions:

- Avoid following unsolicited links or downloading attachments from unknown sources.
- Refer to our Tips to learn more about Shopping Safely Online and Avoiding Social Engineering and Phishing Attacks.
- Read the Federal Trade Commission's blog: Holiday Shopping Tips from the FTC.
- Visit the Federal Trade Commission's Consumer Information page on Charity Scams.

If you believe you are a victim of a holiday phishing scam or malware campaign, consider the following actions:

- File a complaint with the FBI's Internet Crime Complaint Center (IC3).
- Report the attack to the police and file a report with the Federal Trade Commission.
- Contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed and do not use that password in the future. Avoid reusing passwords on multiple sites. See Choosing and Protecting Passwords for more information.

TLP:WHITE

Security Tip (ST07-001)

Shopping Safely Online

TLP:WHITE

Original release date: December 06, 2010 | Last revised: October 01, 2016

Why do online shoppers have to take special precautions?

Online shopping has become a popular way to purchase items without the hassles of traffic and crowds. However, the Internet has unique risks, so it is important to take steps to protect yourself when shopping online.

The Internet offers convenience not available from other shopping outlets. From the comfort of your home, you can search for items from multiple vendors, compare prices with a few mouse clicks, and make purchases without waiting in line. However, the Internet is also convenient for attackers, giving them multiple ways to access the personal and financial information of unsuspecting shoppers. Attackers who are able to obtain this information may use it for their own financial gain, either by making purchases themselves or by selling the information to someone else.

How do attackers target online shoppers?

There are three common ways that attackers can take advantage of online shoppers:

- **Creating fraudulent sites and email messages** – Unlike traditional shopping, where you know that a store is actually the store it claims to be, attackers can create malicious websites or email messages that appear to be legitimate. Attackers may also misrepresent themselves as charities, especially after natural disasters or during holiday seasons. Attackers create these malicious sites and email messages to try to convince you to supply personal and financial information.
- **Intercepting insecure transactions** – If a vendor does not use encryption, an attacker may be able to intercept your information as it is transmitted.
- **Targeting vulnerable computers** – If you do not take steps to protect your computer from viruses or other malicious code, an attacker may be able to gain access to your computer and all of the information on it. It is also important for vendors to protect their computers to prevent attackers from accessing customer databases.

How can you protect yourself?

- **Do business with reputable vendors** – Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information. (See Avoiding Social Engineering and Phishing Attacks and Understanding Web Site Certificates for more information.) Attackers may obtain a site certificate for a malicious website to appear more authentic, so review the certificate information, particularly the "issued to" information. Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill.
- **Make sure your information is being encrypted** – Many sites use secure sockets layer (SSL) to encrypt information. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser; for example, it may be to the right of the address bar or at the bottom of the window. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
- **Be wary of emails requesting information** – Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. (See Avoiding Social Engineering and Phishing Attacks.) Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email. If you receive an unsolicited email from a business, instead of

TLP:WHITE

clicking on the provided link, directly log on to the authentic website by typing the address you (See Recognizing and Avoiding Email Scams.)

- **Use a credit card** – There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. You can minimize potential damage by using a single, low-limit credit card to making all of your online purchases. Also use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.
- **Check your shopping app settings** – Look for apps that tell you what they do with your data and how they keep it secure. Keep in mind that there is no legal limit on your liability with money stored in a shopping app (or on a gift card). Unless otherwise stated under the terms of service, you are responsible for all charges made through your shopping app.
- **Check your statements** – Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately. (See Preventing and Responding to Identity Theft.)
- **Check privacy policies** – Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used. (See Protecting Your Privacy.)

Author

US-CERT Publications