Tips for Secure Holiday Online Shopping

As the holiday shopping season approaches, the U.S. Secret Service and the Cybersecurity & Infrastructure Security Agency want to remind you that the risk of online fraud increases dramatically. U.S. retail e-commerce spending for the 2019 holiday shopping season is forecasted to top $135 billion. Online criminals will utilize this busy time to prey even more upon those consumers and businesses who are unsuspecting or unprepared. The following information and best practices are provided to help both the consumer and the merchant achieve a more secure online shopping experience during the holidays and beyond.

FOR THE CONSUMER

Here are some considerations that are within the consumer's control to aid in protecting their online transactions.

- **Software and Antivirus Updates –** No matter what device you shop from, the operating system updates and antivirus definitions should to be installed as soon as they are available to help protect yourself online.
- **Account Passwords –** Passwords to online shopping sites and other accounts should be changed regularly and the same password should not be used on multiple accounts. If offered by the site, take advantage of multi-factor authentication for an added layer of security. Passwords on home networking equipment such as Wi-Fi routers should be changed from the default password they are configured with from the factory.
- **Payment Cards –** Credit cards should be used instead of debit cards. Credit cards have better protections for the consumer if fraud occurs. Debit cards have no limit to the amount of loss the consumer can suffer. Verify online transactions by checking your credit card and banking statements routinely.
- **The Use of Public Wi-Fi –** Online shopping or banking should **NOT** be conducted over publicly available Wi-Fi networks. While the network in a restaurant, coffee shop or store may require a password, there is no guarantee as to how secure the network is or who may be monitoring and intercepting your online transactions.
- **Beware of Phishing Emails and Social Engineering –** This is the time of year when our inboxes are flooded with offers of all sorts which increases the possibility of encountering fraudulent websites and emails. Avoid opening attachments and clicking on links within emails from senders you do not recognize. Often, these attachments or links can contain malicious content that can infect your device or computer (i.e. ransomware) and steal your information. Type the hyperlink manually into your browser (hover over to reveal the URL) to see what happens and avoid the possible unsuspecting download. Also, be wary of emails or calls requesting that you verify your account by providing information such as your login, password, account number, etc. Legitimate businesses will never call you or email you directly for this information. Utilize the customer service numbers on your credit/debit cards/bank statements or the merchants website to verify any information requests. Lastly, remember that if the offer sounds too good to be true, then it probably is.
- **Who You Conduct Business With Online–** Extra consideration should be given to merchants and businesses you provide your personal and payment card information to online. Reputable and established online businesses utilize encryption, such as Secure Socket Layer (SSL), to protect your information as it is transmitted to and from your computer or device. Also, to lessen the risk of visiting fraudulent or "spoofed" websites, consider how you get there. Certificate "errors" can be a warning sign that something is not right with the website. Verify the hyperlink website address from hyperlinks within emails or access the website from an internet search. When shopping from your phone, only consider vetted apps from trusted businesses and download only from your device's designated app store.

For law enforcement assistance, please contact your local U.S. Secret Service Electronic Crimes Task Force (ECTF), Field Office or visit https://www.secretservice.gov/. For more information on securing your computer, devices or networks visit https://www.cisa.gov/.

Tips for Secure Holiday Online Shopping

FOR THE ONLINE MERCHANT OR BUSINESS

- **Software and Antivirus Updates –** Operating system and network software patches, firmware updates and antivirus definitions should to be installed as soon as they are available. Discontinue the use of outdated, unsupported operating systems such as Windows XP.
- **Account Passwords –** Network or system passwords should be changed regularly and the same password should not be used on multiple systems or accounts. Offer and utilize multi-factor authentication for an added layer of security for you and your customers. Passwords on all equipment should be immediately changed from the default password they are configured with from the factory.
- **Network Segmentation –** Segregate your payment system processing from other network applications such as email and non-payment system related processes. Proper network segmentation and segregation lessens the network exposure if a cyber criminal were to gain access to your system.
- **Firewalls, Intrusion Prevention and Detection Systems –** The use of a firewall and properly configured and monitored intrusion prevention and/or detection system are recommended for added defense of your network.
- **Remote Access Considerations –** Remote access into your network should be limited, secured and monitored for unusual activity in order to reduce the amount of risk. Have a baseline of remote access activity for reference.
- **Back Up Your System –** A back up of your system may help limit unnecessary downtime and losses if needed.
- **Online Payments –** Utilize Payment Card Industry Data Security Standards (PCI DSS) protocols for your online transactions. This includes encrypting (SSL encryption) your customer's payment card data whether it is being stored, processed or transmitted. In addition, verification of the cardholder's address and requiring the Card Verification Value 2 (CVV2) code (3 or 4 digit number on the front or back of the card) can help authenticate the transaction and validate the cardholder and account.

E-Skimming

E-Skimming has become a significant threat to U.S. businesses and the financial sector. E-Skimming is the sophisticated fraud technique where cyber criminals introduce malicious code on e-commerce payment card processing web pages to capture payment card and personally identifiable information and send the stolen data to a domain under their control. Any business accepting online payments on their website is at risk. The malicious code can be introduced through exploiting a vulnerability on a website's e-commerce platform or through unauthorized access into a victim's network. E-Skimming is also commonly targeting third-party vendors, such as those who provide online advertisements and web analytics on payment processing platforms, to introduce the code onto the victim's website. The malicious skimmer code does not have a specific set of indicators of compromise and therefore is increasingly difficult to detect. In addition to the network security considerations already listed above, the following E-Skimming precautionary measures are recommended:

- Perform all regular updates to payment software.
- Install patches from payment platform vendors.
- Implement software code integrity checks. Many of the payment platform vendors now offer tools on their websites to scan your payment website for irregularities within the software code (JavaScript).
- Monitor and analyze your web logs.

For law enforcement assistance, please contact your local U.S. Secret Service Electronic Crimes Task Force (ECTF), Field Office or visit https://www.secretservice.gov/. For more information on securing your computer, devices or networks visit https://www.us-cisa.gov/.