United States Secret Service Cybercrime Investigations

Merchant Tips for Securing Your Online Payment Platform 2020 Holiday Season

U.S. retail e-commerce sales are expected to explode this holiday season. With the ongoing COVID-19 pandemic changing shopping behaviors, retail online sales are predicted to increase by 25%-35% over last year's holiday season sales and generate up to $196 billion. With that much predicted revenue, the risk of online fraud increases exponentially. Online criminals will be stepping up their efforts to prey upon merchants' unsecured or outdated payment platforms. The U.S. Secret Service would like to remind you to stay vigilant and provide you with the following information and best practices to achieve a more secure online shopping experience this holiday season.

Software and Antivirus Updates: Install operating system and network software patches, firmware updates, and antivirus definitions as soon as they are available. Discontinue the use of outdated, unsupported operating systems.

Account Passwords: Immediately change factory preset passwords, change passwords regularly, and use different passwords for each system and account. Utilize multi-factor authentication and offer multi-factor authentication to customers.

Network Segmentation: Segregate payment system processing from other network applications, proper network segmentation and segregation lessens the network exposure.

Firewalls, Intrusion Prevention and Detection Systems: Use firewalls, properly configure and monitor intrusion prevention and detection systems for added defense.

Remote Access: Limit network remote access when and where possible. Always secure remote access and monitor for unusual activity to reduce risk. Identify a baseline of remote accessactivity for reference.

Backups: Have cold storage backups and test restoration of backup files regularly.

Online Payments: Utilize Payment Card Industry Data Security Standards (PCI DSS) for online transactions, to include encrypting (SSL encryption) customer PCI data being stored, processed, or transmitted. Verify card holder address and require Card Verification Value (CVV) code to help authenticate and validate card holder information.

Monitor: Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze web logs.

e-Skimming: The Silent Threat Lurking in Your Payment Platform

What is e-Skimming

Cybercriminals introduce malicious code on e-commerce payment card processing web pages with the intent to capture personally identifiable information (PII) and payment card industry (PCI) data. The malicious code is introduced through exploiting vulnerabilities on website e-commerce platforms or by gaining access to their network through third-party vendors who provide advertisements and web analytics on payment processing platforms. The captured data is then sent to domains under the cybercriminal's control.

How to Mitigate it

Malicious code signatures known to law enforcement are highly variable and are increasingly difficult to detect. Besides the best practices information listed above, continually monitor your payment website for software code changes. Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze the associated web logs.

For law enforcement assistance, please contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF), or visit www.secretservice.gov/investigation for additional information.