United States Secret Service Cybercrime Investigations

PREPARING FOR A CYBER INCIDENT

E-SKIMMING

Online shopping has steadily increased in recent years, which has led to an upsurge in e-Skimming. E-Skimming poses a threat to U.S. businesses, consumers, and the financial sector.

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. Cybercriminals then send the stolen data to network domains under their control.

How e-Skimming Works

Malicious code can be introduced through exploiting vulnerabilities on website e-commerce platforms, or by gaining access to networks. Malicious code signatures known to law enforcement are highly variable and are increasingly difficult to detect.

Who is at Risk

Businesses accepting online payments on their websites and third-party vendors who provide online advertisements and web analytics on payment processing platforms.

HOW TO PROTECT FROM E-SKIMMING

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 access activity 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.