BUSINESSAFE

BusinesSafe is designed to aid businesses in protecting the safety and well-being of Florida's residents and visitors from threats. BusinesSafe provides private sector partners with open source information, analysis and resources to help protect their businesses and communities.

Florida Fusion Center 20-108 **May 2020, Issue #24**

BusinesSafe Threat Topic: Web Skimming

Due to social distancing efforts put in place to protect against the spread of COVID-19, many people are choosing to do more shopping online. Cyber criminals are likely to take advantage of this shift in consumer habits for financial gain. One likely method is web skimming, which occurs when malicious code is used on a legitimate website to obtain consumers' payment information.

Web skimming attacks are conducted when an attacker gains access to an online store and hides malicious code on the website to collect data while the customers are making purchases. Through this process, hackers gain the credit and debit card information of online shopper as they checkout. Web skimming has been discovered on a variety of websites that process online payments including retail establishments, health care entities, entertainment companies, and utilities.

Web skimming has been around since 2016 and has increased within the last two years. Due to the increase in online shopping during the pandemic, there has been an identified increase in web skimming incidents. Because experts expect this trend to increase, it is important for online shoppers to be aware of the threat and for businesses with online payment processing systems to remain vigilant in securing their online payment systems.

- In March 2020, the Tupperware website was reportedly targeted in a cyberattack that infected the company's website with card-skimming malware. The actors behind the attack were likely able to gather various forms of personally identifiable information from customers including full names, addresses, telephone numbers, and credit/debit card information.
  Criminals hack Tupperware website with credit card skimmer

- In February 2020, the NutriBullet company website was reportedly targeted by the notorious Magecart card skimming group. The group allegedly inserted malicious code into the website's checkout page.
  Magecart Cyberattack Targets NutriBullet Website

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1

Ways to Protect Yourself and Your Customers from Web Skimming

For consumers:

- **Use antivirus software.** Antivirus software can detect malicious code and may be able to alert you if a website is compromised.
- **Monitor your credit and debit card activity.** Review your banking statements for suspicious or unauthorized transactions.
- **Consider using alternative online payment services.** Using third-party payment services like PayPal, Apple Pay, and Google Pay when completing online transactions allows shoppers to avoid inputting their payment information for transactions.

For online retailers:

- **Keep your website's software updated.** Installing patches helps in addressing software vulnerabilities.
- **Use strong passwords.** Create long and complex passwords. Remember to also change the default login credentials for your system.
- **Implement multi-factor authentication (MFA).** MFA provides another layer of protection to your system and can help in thwarting attacks if cyber actors manage to guess your password.
- **Segment networks and functions.** Network segmentation separates components of your network from each other and can prevent attackers from navigating freely throughout your system.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8507, Approval: FL8600, HSEC-1, FSIN-1