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 21-060 **May 2021, Issue #50**

BusinesSafe Threat Topic: Credit Card Skimming

Credit card skimming is a type of credit card theft that captures credit and/or debit card information during otherwise legitimate transactions. Credit card skimming may be done through a physical device or through malicious software. A physical device, also known as a skimmer, may be placed on payment terminals such as gas pumps and ATM machines. Web skimming, or e-skimming, uses malicious software embedded in e-commerce websites which steal the customers' credit card and personal identifiable information. This information can be used to make fraudulent purchases with a counterfeit card or it can be used online to create other identities.

Criminal Activity:

1. **Physical skimmer devices** - Skimming devices can be placed on payment terminals in a way that makes the device appear as part of the terminal or placed inside the machine and undetectable. Skimmers have been found on the swipe slot of some ATMs and gas pumps, and some newer skimmers have also been found within the card reading mechanisms of these devices. Once the credit or debit card is swiped through a skimmer device, the device captures the card number, card holder's full name, expiration date and other data contained within the magnetic strip. Skimming devices may be accompanied by a hidden camera or fake keypad which is placed over the real keypad to obtain the information input by the cardholder such as their pin number or zip code. Criminals may also use Bluetooth technology that will transmit the stolen information to the criminals wirelessly. While there are safeguards in place to protect consumers from skimming devices, consumers shave to be vigilant as criminals have continued to develop new devices and workarounds to obtain credit card information.

   Men Caught Installing Credit-Card Skimmer at Delray Gas Station, Police Say
   Investigators Find 3 Credit Card Skimmers at Gas Stations In Brevard County

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.1, 1.3, 3.1, 3.4 FFC:1.1, 1.3, 4.1, 4.2,6.2

2. **E-Skimming** – E-skimming occurs when criminals use malicious software or codes that are embedded into compromised ecommerce websites allowing criminals to obtain consumer credit card information during the checkout process. Criminals can then collect this information and use it to make fraudulent purchases or commit identity fraud.

   Payment Card Skimming Hits 2,000 E-Commerce Sites
   Credit Card Skimmers Are Now Being Buried In Image File Metadata On E-Commerce Websites

Ways to Protect Yourself from Credit Card Skimming:

- **Look for signs of tampering:** Payment terminals should be regularly inspected by business employees to identify signs of tampering. Consumers should not use the gas pump or ATM if they appear to be opened, unlocked or if the security tape has been tampered with. This may be evidence that a skimming device has been installed.
- **Update and secure your platforms:** E-Commerce businesses can ensure their platforms are up to date and their security software is Payment Card Industry Data Security Standard compliant.
- **Pay inside:** To avoid credit card skimming devices at the pump, pay inside at the register.
- **Pay close attention to your bank account:** Check your credit or debit card statements regularly to ensure there are no fraudulent purchases and sign up for fraud alerts if applicable.

Resources:

- The Florida Department of Agriculture and Consumer Services offers information regarding credit card skimmers on their website. If you believe a gas pump has been tampered with notify the gas station management and file a complaint by calling 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832) or file a complaint online.
- The National Cybersecurity and Infrastructure Security Agency offers information on how businesses can identify and minimize the risks of E-Skimming on their platforms.
- To file a complaint regarding an E-Skimming incident call your local FBI field office or file online through the FBI Internet Crime Complaint Center.
- Computer crimes within Florida can also be reported through the Florida Department of Law Enforcement website.
- If you believe that your identity has been compromised the State Attorney's office website offers additional information and resources.
- Contact your local law enforcement to report suspected credit card compromises.

To sign up to receive BusinesSafe directly to your email, visit our website.

Florida Fusion Center
(800) 342-0820
FLBusinesSafe@FDLE.state.fl.us
Author: FL8642, Approval: FL8600, HSEC:1 FSIN:1.1, 1.3, 3.1, 3.4 FFC:1.1, 1.3, 4.1, 4.2,6.2