NATIONAL CYBERSECURITY AWARENESS MONTH

DO YOUR PART.
#BECYBERSMART

E-SKIMMING

The Internet touches almost all aspects of our daily lives. We are able to shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information. #BeCyberSmart when sharing personal information online to reduce the risk of becoming a cybercrimes victim.

WHAT IS IT?

Cyber criminals introduce skimming code on e-commerce payment card processing web pages to capture credit card and personally identifiable information and send the stolen data to a domain under their control.

HOW DOES IT WORK?

Skimming code is introduced to payment card processing websites by:

- Exploiting a vulnerability in the website's e-commerce platform
- Gaining access to the victim's network through a phishing email or brute force of administrative credentials
- Compromising third-party entities and supply chains by hiding skimming code in the JavaScript loaded by the third-party service onto the victim website
- Cross site scripting which redirects customers to a malicious domain where malicious JavaScript code captures their information from the checkout page

The malicious code captures credit card data as the end user enters it in real time. The information is then sent to an Internet-connected server using a domain name controlled by the actor. Subsequently, the collected credit card information is either sold or used to make fraudulent purchases.

WHO IS BEING TARGETED?

Any business accepting online payments on their website is at risk of an e-Skimming attack. This threat has impacted e-commerce companies in the retail, entertainment, and travel industries as well as utility companies and third-party vendors. E-Skimming is also commonly targeting third-party vendors such as those who provide online advertisements and web analytics. The cyber criminals are evolving their tactics and have also been seen using malicious code that targets user and administrative credentials in addition to customer payment information.