

Cyber Crime Centre – Digital Skimming



Police Service
of Northern Ireland

THE ACT OF STEALING PAYMENT DATA FROM ONLINE CUSTOMERS.

In the run up to the festive season, many organisations across Northern Ireland will be preparing for a seasonal increase in online sales to customers based both at home and abroad.

As part of this preparation, the Cyber Crime Centre would encourage all online retailers to consider the risks posed by Digital Skimming. Whether through vulnerabilities, configuration errors or brute force*, as experienced recently by a number of organisations in Northern Ireland, criminals can gain access to online stores with the aim of using malware to capture customer data.

WHAT TO DO IF YOU BECOME A VICTIM?*

- In case of malware infection, change all admin and database passwords immediately.
- Use a malware scanner to find any backdoors the attackers may have installed.
- Collect all available evidence and report the attack to [Action Fraud](#)
- In case of a personal data breach, comply with the applicable GDPR legislation ([ICO UK](#))

*For more information check out the [Europol EC3 Digital Skimming advisory](#)

DIGITAL SKIMMING

EUROPOL EC3 European Cybercrime Centre

WHAT IS IT?

A major cybersecurity threat

Digital skimming is the action of stealing credit card information or payment card data from customers of an online store. The transaction data is intercepted during the online purchase checkout process, without customers noticing anything unusual.

A crime known by many names

Digital skimming attacks are also known as web skimming, online card skimming, e-skimming, formjacking or **Magascan**.

Magento was the primary open source eCommerce platform initially targeted, inspiring the name "Magascan" (a combination of "Magento" and "shopping cart"), which also refers to the criminal group behind the attacks.

HOW DOES IT WORK?

In general, there are 3 stages in a digital skimming attack:

- Breach**: Criminals get access to the source code/server of an online store or the source code of a third party tool. This can happen through vulnerabilities, configuration errors or brute force.
- Inject**: Malware is inserted in the payment flow.
- Collect**: The customer and payment data is duplicated. Data can be collected immediately or hid in the server and collected later to minimize the risk of discovery.

Affected customers are unaware that their card was copied (skimmed). From their perspective, the order was placed and the item will be received, leaving no room for suspecting something went wrong.

Report online. Call 101. In an emergency call 999 [psni.police.uk](#)