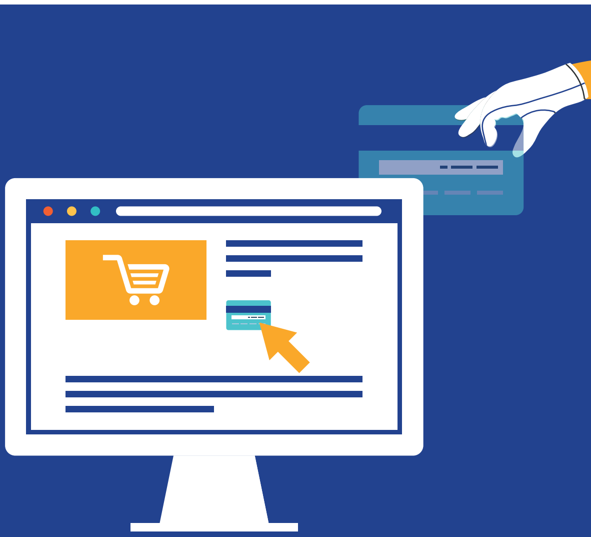
DIGITAL SKIMMING

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 **Magecart.**

Magento was the primary open source eCommerce platform initially targeted, inspiring the name **'Magecart'** (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 bruteforce.

Inject
Malware is inserted in the payment flow.

Collect
The customer and payment data is duplicated. Data can be collected immediatly 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.

DIGITAL SKIMMING

EUROPOL
EC3 | European Cybercrime Centre

WHY DO YOU NEED TO KNOW?

Digital skimming attacks are rising.
The attacks can go undetected for a long time.
When a breach is eventually discovered,
it can bring reputational damage for the online store,
because the users will question the safety of the service.

HOW CAN YOU PROTECT YOUR BUSINESS?

You can make it harder for cybercriminals by:

Using a malware monitor with web skimming-specific capabilities.

Ensuring MFA and strong password policies for staff. Training your staff to deal with spearphishing attacks.

Running automated vulnerability audits on the ecommerce platform including installed third party components on a regular basis.

Ensuring that only specific IPs can access the control panel of your store. Deny staff access from unknown locations.

Ensuring timely installation of security patches and critical software updates.

Implementing Content Security Policy (CSP) and Subresource Integrity (SRI). This will make it harder to inject malicious code into your store.

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 your national police.
- In case of a personal data breach, comply with the applicable GDPR legislation.