GUARDSIGHT

https://www.guardsight.com

ONLINE SHOPPING ALERT: WEB SKIMMERS

YOUR AWARENESS IS THE BEST DEFENSE

A web skimmer is a piece of malicious code embedded in web payment pages looking to steal your credit card and other personal information. Such malware arrives on target pages through a compromised 3rd party site that often has nothing to do with the vendor or customer. Web skimmers are passive in nature, making them harder than normal to detect. Follow the tips on the right to better protect yourself.

FACTS AND FIGURES

- Any given web store can have up to 67% of its shopping and checkout process outsourced to 3rd parties.
- Web skimmers sit on a compromised site and record payment information before it is encrypted. This is known as a passive attack.
- Web skimming attacks have risen 187% over the last year alone.

For additional advice or to learn more contact us: info@guardsight.com

1 SHOP SECURE

Shop on secure sites. Make sure you enter your information on site with an HTTPS prefix.

2 CHECKOUT AS A GUEST

Entering information repeatedly can be a hassle, but at least your information won't be stored on a vendor's server.

3 AVOID SHOPPING ON PUBLIC WIFI

Even with a VPN service, shopping online should be done on a trusted network such as your home network.

4 USE A VPN

Use a VPN whenever online and especially when online shopping. Avoid free VPN services.

5 MONITOR ACCOUNTS

Monitor all financial accounts for fraudulent activity. This includes banking accounts and online accounts such as Venmo, PayPal, and any frequented shopping site accounts.

6 IMPLEMENT MFA

Use Multi Factor Authentication (MFA) during checkout if the option is available.