

# CYBER RISKS & LIABILITIES

## Formjacking Explained

As businesses increasingly rely on online transactions, cybercriminals have developed a scheme to exploit this process and steal sensitive information. This growing cyberthreat, known as formjacking, poses significant risks to businesses; it is difficult to prevent and can lead to major financial losses and reputational damage.

This article provides more information on formjacking and offers tips on how to mitigate its risks.

### What Is Formjacking?

Formjacking is a cyberattack in which a threat actor injects malicious JavaScript into a website, often one that contains an online payment form. Once the targeted page has been compromised, the added code allows the hacker to collect sensitive data, such as credit card numbers, addresses and phone numbers. This data is sent to the cyberattacker's domain after unsuspecting users enter their information and click "submit" to complete a transaction.

Malicious actors can then use the stolen data in identity theft schemes, payment card fraud scams and account takeover attacks or sell it to other criminals. Stolen information can also be used to create fraudulent accounts to distribute malware.

The hacker's code may be loaded through various methods, such as by exploiting a vulnerability in a business's website, employing a phishing scam in which the cyber intruder gains access to a company's checkout page, or compromising a third party's app or JavaScript used by a business.

### The Risks of Formjacking to Businesses

Formjacking attacks can have severe financial consequences, including lawsuits, fines, fees and penalties, as well as expenses related to remediation. Moreover, formjacking can damage a company's

reputation, as clients, vendors and other partners may lose their trust in the business due to cybersecurity incidents.

Formjacking is challenging to detect because the malicious code frequently changes, making it difficult for external scanners and firewalls to catch it. What's more, there are no apparent signs of formjacking, and the intended transaction is not affected, making it difficult to identify and stop the scam. As a result, formjacking attacks can go unnoticed for a long time.

### Mitigating the Risk of Formjacking

Although detecting malicious formjacking code and preventing attacks can be difficult, there are several measures businesses can take to identify potential issues and reduce the risk of it happening. Consider the following strategies:

- **Practice cyber hygiene** by keeping software, patches and extensions up to date. Establishing a content security policy and using firewalls and subresource integrity tags can also help prevent the injection of malicious data onto business websites and protect data. Additionally, complying with security standards and educating IT staff on the threats of formjacking are essential.
- **Scan and audit website code regularly** to check its integrity. Monitoring and analyzing web logs and JavaScript behavior can help detect malicious activity, and checking where a browser is sending data is also key in stopping formjacking attacks.
- **Utilize cyberdefense techniques** such as obfuscating JavaScript, which can make code more difficult for cyber attackers to understand. Implementing network segmentation can also limit network exposures and malicious actors' lateral



# CYBER RISKS & LIABILITIES

movement capabilities. An intrusion detection and prevention system can also help monitor potential threats and identify cyber intruders.

- **Implement ongoing cybersecurity measures**, such as thoroughly testing websites before they are publicly launched, executing penetration testing to discover vulnerabilities, and monitoring the supply chain to ensure vendors whose code is being used follow cybersecurity best practices.

Layering defenses can also reduce a business's vulnerability, and companies should consider leveraging artificial intelligence to help detect suspicious behavior.

## **Conclusion**

Formjacking is a cyberthreat that can significantly impact a business's finances, operations and reputation.

Because of this, companies should take steps to mitigate the risks associated with it.

Contact us today for more information.

---