How to protect your business from Formjacking

Formjacking, a new and effective cyber-attack that rapidly increased in popularity in 2018, involves threat actors inserting malicious code into a legitimate web-based form to collect data submitted. While formjacking is typically used to collect payment card data (this has often been described as the cyber version of card skimming), it has also been used to collect personally identifiable information (PII).

According to the Symantec Internet Security Threat Report, 4,800 websites on average are compromised with formjacking code each month. If a formjacking attack is successful, your payment card information and/or PII can be sold on the dark web between $50 to several hundred dollars.

Fraudsters often target small and medium sized businesses; however, large companies can also fall prey to this attack. So, what should you do to protect your company's website? Below are some recommendations to help you mitigate this risk.

- **Consider using an intrusion detection and prevention system (IDPS)**. IDPS is a security tool used to identify intruders before they can do serious damage. Using an IDPS could help ensure the malicious code is never inserted into your website.
- **Complete regular code audits**. Fraudsters alter the site code slightly. Become familiar with your code so you can quickly detect changes.
- **Monitor outbound traffic**. Using a firewall or other security application, screen your websites outbound traffic to see if it is going somewhere it isn't supposed to.
- **Use Subresource Integrity (SRI) tags**. Using cryptographic hashes, SRI tags ensure files that web applications and documents gather do not contain unexpected content.
- **Use anti-virus software and keep your systems up to date**. Install software updates as soon as possible.

As with any cyber-attack, there are many risks to your data being exposed. Some of the greater risks your business should consider include:

- **Reputation**. Your business' good reputation that you've worked hard to build could quickly turn to bad once your customers data has been compromised.
- **Liability**. Since your business owns the data that has been compromised, your company could take a significant financial loss.
- **Reduced revenue**. Your business may have to postpone operations while you work to identify what has been compromised, and how to fix it.

Cyber threats are constantly evolving. The dramatic increase in formjacking last year proves this. As always in cyber security and fraud prevention, using the right defense strategies could help protect your website from these types of attacks, keep your customers data safe while also keeping your business assets secure and preserving your reputation.

How to Protect Your Business and Yourself from Formjacking. (2019. May 10) Retrieved from https://teresarothaar.com/how-to-protect-your-business-and-yourself-from-formjacking-bd166c41fe88?gi=42d7445cadcb

You Need to Protect Your Website Against Formjacking Right Now. (2019. February 27) Retrieved from https://www.pcmag.com/article/366770/you-need-to-protect-your-website-against-formjacking-right-n

How to Protect Your Business Website from Formjacking. (2019. May 1) Retrieved from https://securityboulevard.com/2019/05/how-to-protect-your-business-website-from-formjacking/

Formjacking: The Online Scam Hidden in Your Website Code. (2019. May 14) Retrieved from https://www.insightsforprofessionals.com/blog/formjacking-online-scam-hidden-in-website-code

Cyber Criminals Cash in on Millions with Formjacking, Posing a Serious Threat to Businesses and Consumers. (2019. February 20) Retrieved from https://www.businesswire.com/news/home/20190219006067/en/Cyber-Criminals-Cash-Millions-Formjacking-Posing-Threat

Symantec, 2019 Internet Security Threat Report (2019). (Volume 24) Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf