How to Fight Formjacking and Win Back the Holiday Shopping Season

The 2018 holiday season brought a new kind of Grinch. Late in the year, Symantec revealed that hackers had begun to employ a nearly invisible new tactic called formjacking. According to the Internet Security Threat Report, Symantec blocked nearly four million formjacking attacks in 2018. One third of those attacks occurred during November and December.

Remember ATM skimmers that steal credit card information when you swipe your card? Think of formjacking as the online version of skimming. Hackers infect an online order form with malicious JavaScript. Then, when you enter your card information to make a purchase, the code transfers that data to the hackers.

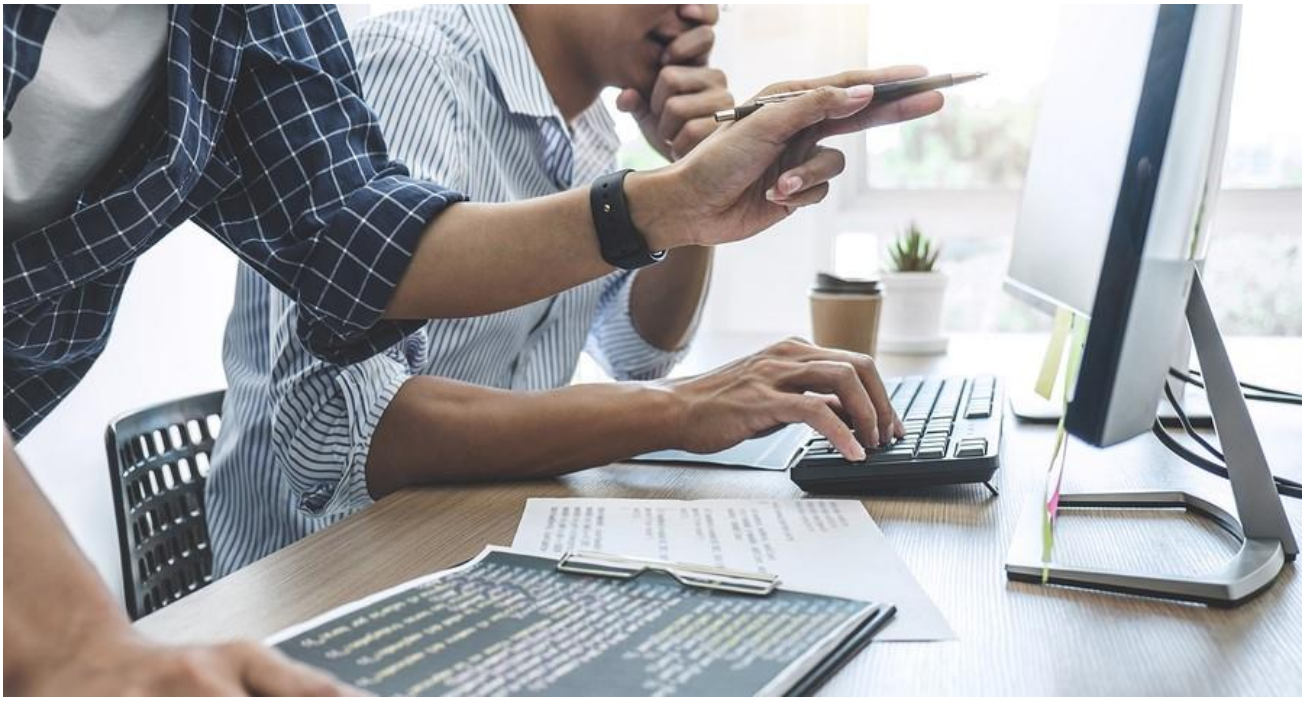
With formjacking, cyber-criminals gain a big payout for relatively little effort. First, they look for targets that process large amounts of sensitive data, particularly sites that use third-party JavaScript technology. Then they inject a small amount of code and sit back to wait for the data to arrive. Finally, they can sell stolen credit card information for about $45 per card.

Understand the Dangers

Some experts consider formjacking one of the most dangerous hacking methods yet, for several reasons. First, shoppers have almost no chance of detecting an attack until they see something unusual on their credit card statement. Even website owners struggle to detect anomalies in thousands of lines of code.

Second, because it can take days or weeks to discover that an attack has occurred, it can prove difficult to identify the compromised website. Meanwhile, shoppers suffer identity theft and financial loss. And vendors suffer more than a reputation hit. They may also find themselves in violation of privacy laws with stiff penalties.

Finally, while news reports have focused attention on the acquisition of credit card information, keep in mind that formjacking can capture anything entered into a form. This can include login credentials, health information, tax data and more.



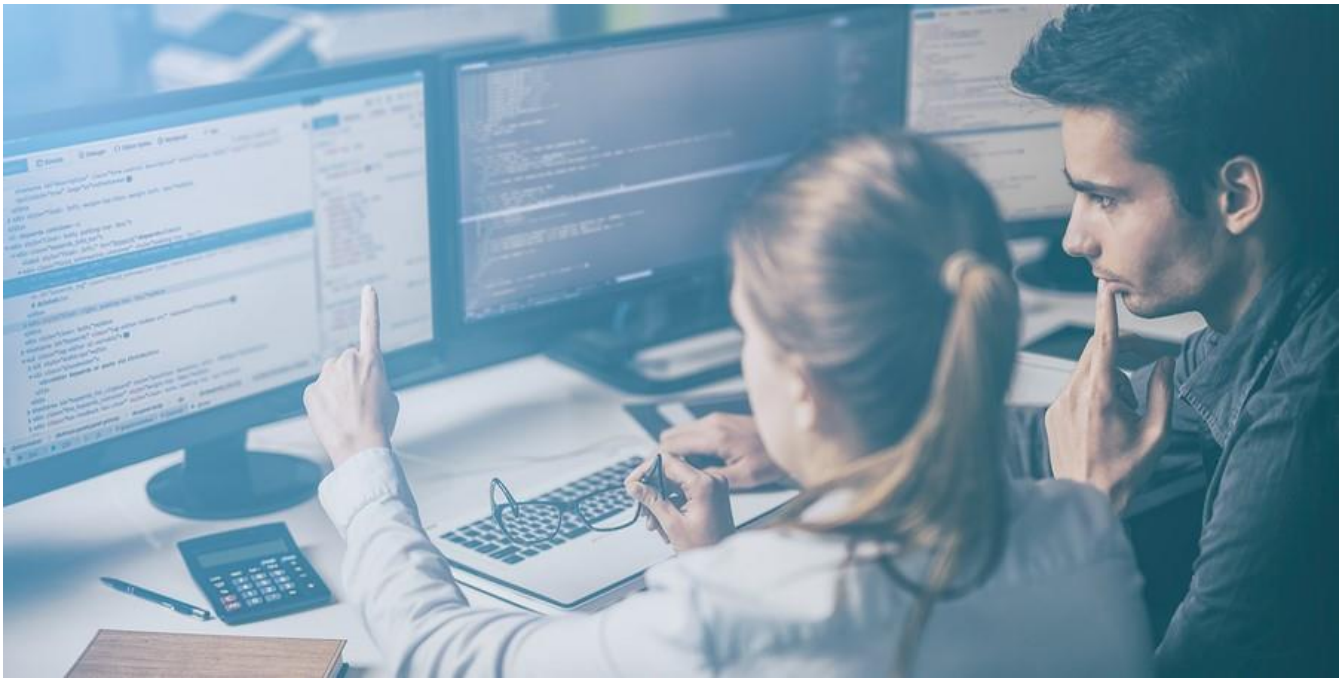
Best Practices for Vendors to Detect and Prevent Formjacking

Symantec reports that hackers infect approximately 4,800 sites each month. Small to medium-size businesses take the biggest hit, due to less robust cyber-security. However, larger companies, such as British Airways and Ticketmaster, have suffered attacks, as well. In many cases, the criminals gain entry by infecting smaller businesses in the supply chain.

The onus for preventing and detecting formjacking attacks falls to the e-commerce provider. Vendors must apply a defense-in-depth approach to e-commerce cyber-security, including measures like the following:

- **Address vulnerabilities in your supply chain** – Cyber-criminals look for e-commerce sites that use embedded JavaScript technology such as chatbots, marketing analytics and advertisements. Consequently, you should monitor the security practices of third-party vendors that deploy such technology on your website.
- **Look for unexpected code** – Monitor your websites regularly to look for unusual code. For example, you can employ Subresource Integrity (SRI) tags. SRI tags use hashes to verify that web material does not contain unexpected content.

- **Practice** **e-commerce cyber-security best practices** – Implement known best practices for website security. For instance, install security updates promptly and use strong passwords.
- **Consider setting up a honeypot** – In computing terms, a honeypot consists of a bait to catch criminals. In this case, a honeypot might include a decoy web server that looks like a high value target. When attackers touch the decoy, the action triggers an alert.
- **Monitor outbound traffic** – A compromised form will send data to the hackers. Thus, any data being transmitted to an unknown source could indicate that criminals have compromised your website.



While no silver bullet exists to halt hackers in their tracks, you can take control of your cyber-security and reduce the risk. The retail cyber-security experts at eMazzanti can help you design a layered strategy to protect you and your customers from formjacking and other cyber-security threats.