BIZCOMMUNITY

How to protect yourself from the latest online security threat - formjacking

The latest *Symantec's Internet Security Threat Report* lists formjacking as one of the most dangerous attacks in the history of cybercrime. About 4,800 websites get infected with formjacking software every month globally.

©avemario via 123RF

Formjacking is like virtual ATM skimming. First, cyber criminals inject malicious code into an online shopping website to steal victims' payment card details. The code reads credit card information as the person enters it, and then sends that information to the hacker.

"Formjacking is becoming more and more used by cybercriminals because of the simplicity to carry out it. The actual e-commerce transaction goes through as if nothing has happened. The victim usually realises that they have been attacked just when charges start showing up on credit card statements," says Daniel Markuson, a digital privacy expert at NordVPN.

Symantec's research revealed that small and medium-sized retailers are the most widely compromised, although no company is immune. Even the online payment websites of such well-known retailers as Ticketmaster and British Airways suffered from formjacking code.

6 tips to stay safe

It's hardly possible for users to detect this kind of attack until it's too late. That's why it's mainly up to e-shops and other e-commerce platforms to defeat this threat. Nevertheless, good online shopping practices can still protect you from the risk of losing your money.

There are a couple of ways to stay safe, according to Markuson:

1. Shop only at reputable websites: Avoid making impulsive purchases from online shops you don’t know. Keep in mind that smaller sites that do not have enough resources and the same level of protection as major sites are more likely to host a formjacking script.

2. Carefully read other customers’ reviews: If someone has already been hit by a formjacking attack, it‘s very likely that you’ll find a comment about that. Always do your research in advance and if you notice something suspicious, better look for another store.

3. Always check the URL of the website: Make sure that the address bar says “https” instead of “http.” Check whether the store’s privacy policy clearly communicates how it collects, uses, and protects your data.

4. Provide companies only with necessary information: The less data they have, the less they can leak. Don’t provide your date of birth, social security number, or bank account number just because someone asks for it.

5. Use a browser-based script blocker: Consider adding one of the script-blocking extensions to your browser. This will provide you with significantly more protection against formjacking attacks. You can try NoScript software extension for Mozilla-based web browsers. It allows JavaScript to be executed only by trusted websites and provides extra security for your browser.

6. Stay organised: Make sure to keep all your documentation, such as receipts or order confirmation numbers to prove your online purchase. It is also important to constantly check your credit card statements. If you see any activities on your balance that you don’t expect to find, try to recall whether you really authorised the charge. If you can’t recall it, inform your bank or credit card issuer, and they should be able to help you.