What is Formjacking? How to prevent?

Formjacking, commonly known as e-skimming or credit card skimming, is a tactic used by hackers and scammers to shop online for the purpose of stealing personal and financial information. victims when they shop on legitimate online sites.

What is Formjacking?

Formjacking is a relatively new online scam that was most popular in 2018 and 2019 after several major online retailers, such as Target and British Airways, were hacked and their private credit card information was hacked. hundreds of thousands of customers stolen.

How does E-Skimming work?

Unlike system hacks or data breaches that steal saved information, formjacking involves hacking into an online store and placing JavaScript code in payment-related forms. This JavaScript code allows ordering online as usual on the hacked site, but also sends a copy of all customer entered information, such as name, address, and credit card information, to hacker.

Formjacking scammers have also been known to hack third-party shopping cart providers, allowing them to simultaneously skim credit card and banking information from various online stores at the same time.

The hacker can then use the collected information to fulfill online orders. Often, the data will be sold online to other parties and may result in the victim becoming the target of other online scams in the future.

How to avoid this scam?

There are several ways to prevent yourself from falling victim to hackers when shopping online.

1. **Use Apple Pay or Google Pay** : Both services completely hide your credit card information when making online purchases.
2. **Use PayPal** : PayPal and other similar online financial services are mostly protected against form hacking because they don't ask you to enter any banking information.
3. **Save payment information on the website** : If your credit card information is already connected to your account, you won't need to enter it in the form. However, your financial information may be exposed if the website or database is hacked.
4. **Check the security status of the website** : While not a complete guarantee, if the web store's website address starts with https, not http, it may indicate Security is enhanced. The padlock icon next to the address bar also indicates a site is using security precautions.
5. **Disable scripts in web browsers** : Most Internet browsers will have an option to disable JavaScripts in the settings. Browser plugins can also be used.
6. **Use a privacy-focused web browser** : Some browsers, such as Brave, have a strong focus on privacy and security and disable many scripts by default.
7. **Check your bank statements** : The easiest way to make sure your information isn't stolen or sold online is to check your monthly financial statements for any suspicious or unusual transactions.

What to do if you have become a victim?

If you suspect that you have been the victim of credit card information theft, the first thing you should do is contact your bank or credit card provider and freeze all transactions.

The credit card provider, depending on the card you use, may also refund any suspicious charges that were made. You may be encouraged to get a new credit card because once your credit card information is exposed, you won't be able to secure it again.

If you accidentally enter a phone number into a hacked form, you could become the target of many phone scams. Be very careful with suspicious phone calls.

You may also want to notify the owner of the site where you suspect your information has been exposed, as they may not be aware of such a hack.