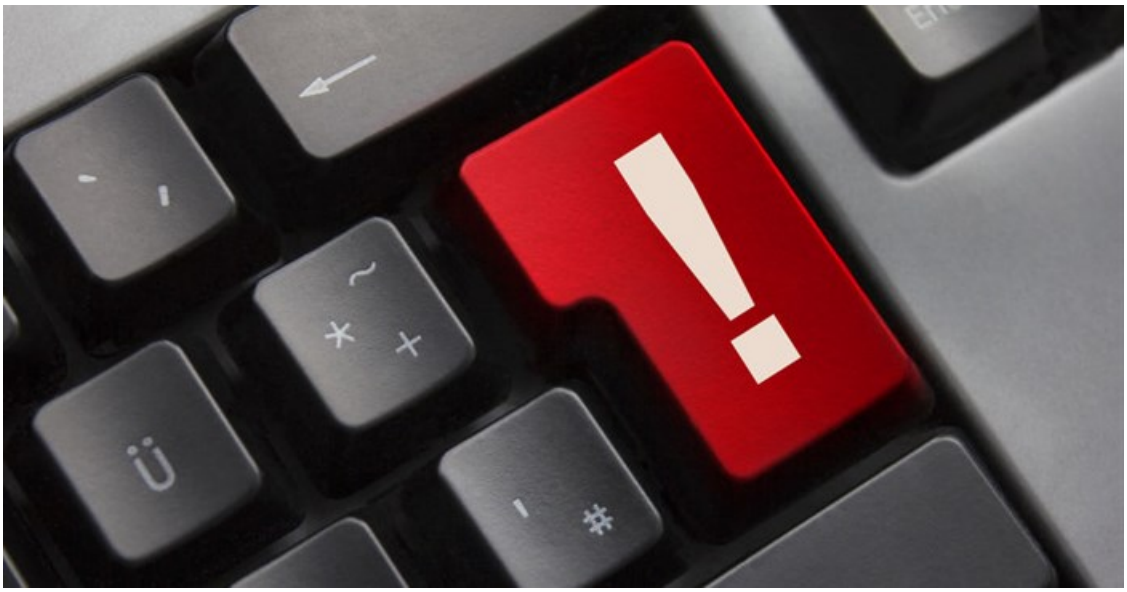
Top 10 website threats you should know about

If you are building and running your own websites or have an online business, the cyber-world can be a dark and daunting place. Cybercrime in the form of hacking could cause your site to be blacklisted by Google leading to a drop in search rankings, a damaged reputation, and a loss of revenue as you try to get your site back up.



©imilian via 123RF

"But there is no need to panic," says Myron Salant, web services product manager at Webafrica. "Many website owners only think about security after their site gets hacked, but knowledge is power: if you know what the threats are, you can arm yourself appropriately and get one step ahead of the hackers."

Salant identified the top 10 threats to your website that you should be aware of:

1. Injection

Injection happens when hostile data is sent to an interpreter as part of a query or command. This data tricks the interpreter, resulting in unintended commands and corrupt data. It's a common problem in web applications, particularly with SQL injection.

2. Cross-site scripting

When an application sends user-supplied data to a web browser without first validating or encoding it, cross-site scripting (XSS) can occur. This lets hackers execute scripts in the victim's browser that hijack user sessions or vandalise websites.

3. Insecure direct object references

Web applications don't always verify that the user is authorised for the target object. Without an access control check or similar protection, supposedly secure data can be accessed and stolen by attackers.

4. Cross-site request forgery

CSRF tricks a victim into submitting fake HTTP requests via cross-site scripting or image tags. It's an issue for web applications that inadvertently allows hackers to predict the details of a transaction - for example, automatically-generated

session cookies. Attackers create hostile web pages which generate forged requests indistinguishable from real ones.

5. Insecure cryptographic storage

It's hard to believe, but many web applications still do not properly protect sensitive data such as credit card numbers and personal details. Attackers can easily access poorly encrypted data and use it to commit credit card fraud, identity theft, and other data-related crimes.

6. Failure to restrict URL access

An application may protect sensitive functionality only by not displaying relevant URLs to unauthorised users. By accessing those ULRs directly, attackers can exploit this weakness to perform unauthorised operations.

7. Invalidated re-directs and forwards

Web applications may re-direct and forward visitors to other pages and websites without proper validation. Attackers can then redirect victims to phishing or malware sites or use forwards to access unauthorised pages.

8. Broken authentication and session management

Account credentials and session tokens are sometimes not properly protected. Attackers simply use stolen passwords, keys and authentication tokens to steal other users' identities and commit crimes.

9. Security misconfiguration

Attackers exploit security configuration weaknesses at any level whether it's the platform, web server, application server, framework or custom code. These flaws give attackers unauthorised access to default accounts, unused pages, unpatched flaws, unprotected files and system data.

10. Insufficient transport layer protection

When applications fail to authenticate, encrypt and protect sensitive network traffic, they may support weak algorithms, use expired or invalid certificates, or execute commands incorrectly.

"The above threats can simply be avoided by implementing an online security system, such as SiteLock, for example," says Myron. "If you are unsure about the right security solution for your website, speak to your web developer - as the cliché goes, prevention is better than cure!"