ULTIMATE WEBSITE SECURITY MANUAL

Your Essential Black Friday Security Checklist

Harden your website's security before it would be too late.

In this handy checklist, you can find the most important things you should do to prepare for BFCM weekend and the holiday season. The best part? Most of the items on this website security checklist **don't require a developer!**

1. HOST YOUR WEBSITE ON A BITNINJA PROTECTED SERVER

Good Job! You are already protected against most of the dangerous cyberattacks, because your hosting provider has done the heavy lifting. BitNinja Server Security provides LogAnalysis, WAF, DoS Detection and realtime Malware Removal for your websites.

2. MAKE PASSWORDS SECURE (AND UPDATE THEM REGULARLY)

To create ultra-secure passwords for your website, use a password generator, like LastPass. By creating stronger and unique login credentials, you can quickly boost your website security. But never forget: regularly updating those credentials is also a must-have action.

3. INSTALL AN SSL CERTIFICATE

SSL security certificates encrypt the traffic from the visitor's web browser to your server. An SSL encrypted connection prevents sensitive information like login information, credit cards, and other customer data.

4. AUTOMATE AND TEST YOUR BACKUPS

When it comes to website security, backups are your best friend. Automate the process through your hosting provider. With a backup of your site, you can respond to a range of issues fast, whether it's a broken page or a hacked website.

5. UPDATE PLUGINS, CMS, AND MORE

Install the latest version of your CMS, as well as plugins, and any other tools / services that help operate your website, also, uninstall the outdated ones.This way you can keep your site protected from security vulnerabilities.

6. LIMIT USER PERMISSIONS

Limit the number of people that can access and modify your website with user permissions. Most of the CMSs allow you to instantly set different user permission levels by creating roles, like the ability to publish on your blog, install add-ons, or add another users.

7. ACTIVATE YOUR BITNINJA SITEPROTECTION FREE TIER

Log in to your control panel, and look for the SiteProtection button. After you logged in, you can start a full Malware Scan on your site for free, in order to detect even the hidden malwares uploaded.

8. SET UP ROBOT DEFENSE

In your SiteProtection free tier you can set up a CAPTCHA wall for your administrative login (like /wp-admin) to filter bots. This way you can make the prevention automated, and detect the malicious activities before it would be too late.

9. RUN AUTOMATED WEBSITE SECURITY TESTS

An external security test is always a good idea. You can hire a penetration tester to find the vulnerabilities like the enterprises do, but nowadays many SaaS tools offer similar services. SiteProtection Free Tier provides the following tests: SQL injection testing, XSS testing, general web testing, and CMS testing.

10. SET UP TWO-FACTOR AUTHENTICATION FOR ALL USERS

90% of passwords can be cracked in less than six hours. So-called "credential stuffing" or brute-force attacks can make it easy for hackers to break in and hijack people's online accounts in bulk. 2FA is one of the best ways to protect your online accounts, and only one more step is needed. Never skip this action.

COMPLETED EACH STEP?

EXCELLENT!

Now your websites are totally cyber safe for Black Friday.

Don't forget that we are always here to help you if you have any kind of questions , need extra services or to make any further configuration.