PRASC

Project for the Regional Advancement of Statistics in the Caribbean

Projet régional pour l'avancement de la statistique dans les Caraïbes

Funded by the Government of Canada | Canada

WordPress
Security Guide for your website

Project for the Regional Advancement of Statistics in the Caribbean (PRASC)

Rhodz Lamarre
July 2020
Virtual Session

Contents

The content presented is sourced from WordPress on https://www.wpbeginner.com/wordpress-security/ (taken in July 2020).

Why Website Security is Important?

- Can cause serious damage to your site
- Reputation of the NSO
- Hackers can steal user information and passwords (Think of the admin portal)
- Install malicious software to the site
- Distribute malware to your users.
- Worst case : Ransomware

Keeping WordPress Updated

WordPress is an open source software which is regularly maintained and updated

- Minor updates - WordPress
- Major release - You
- Plugins and themes by 3rd parties
- Updates are crucial for security and stability (WordPress core, plugins, and theme)

Strong Passwords and User Permissions

The most common WordPress hacking attempts use stolen passwords.

Stronger passwords that are unique for :

- WordPress admin area
- FTP accounts
- Database (if you have access)
- WordPress hosting (if you have access)
- Custom email addresses (Contact page)

*Password manager

The Role of WordPress Hosting

- Continuously monitor the network for suspicious activity.
- Have tools in place to prevent large scale DDOS attacks
- Keeping the server software and hardware up to date to prevent hackers from exploiting a known security vulnerability in an old version.
- Have ready to deploy disaster recovery and accidents plans

* Shared hosting and cross-site contamination

WordPress Security

4 Easy Steps (no coding)

- Install a WordPress Backup Solution
- Best WordPress Security Plugin
- Enable Web Application Firewall (WAF)
- Move WordPress Site to SSL/HTTPS

Install a WordPress Backup Solution

- Allow you to quickly restore your WordPress
- You must regularly save a full-site backups to a remote location (not your hosting account)
- The ideal setting is once a week
- Can be easily done by using plugins like VaultPress , All-in-One Migration or UpdraftPlus.

WordPress Security Plugin

- Audit and monitor system that keeps track of everything that happens on your website.
  - Integrity monitoring,
  - Failed login attempts,
  - Malware scanning and etc.
- Cerber, Wordfence, Centrale IT

Enable Web Application Firewall (WAF)

Blocks all malicious traffic before it even reaches your website

- DNS Level Website Firewall
- Application Level Firewall

Both can be control by you but Central IT will probably take cake of that

SSL/HTTPS

- SSL (Secure Sockets Layer) is a protocol which encrypts data transfer between your website and users browser.
- Ranking in Google and Bing

Change the Default “admin” username

- The default WordPress admin username is “admin”. Should not be use.
- Usernames make up half of login credentials, this made it easier for hackers to do brute-force attacks.

Disable File Editing

For Central IT

- WordPress comes with a built-in code editor which allows you to edit your theme and plugin files right from your WordPress admin area
- Can be a security risk which is why we recommend turning it off.

Limit Login Attempts

- By default, WordPress allows users to try to login as many time as they want
- Limiting the failed login attempts a user can make.
- Web Firewall or plugin (Limit Login Attempts Reloaded)

Two Factor Authentication

Requires users to log in by using a two-step authentication method.

- Username and password
- Authentication using a separate device or app.

Plugin : Two Factor Authentication

Automatically log out Idle Users in WordPress

Leaving your session open.

- Someone can hijack your session, change passwords, or make changes to your account.
- Install and activate the **Inactive Logout** plugin

Add Security Questions to WordPress Login Screen

- Makes it harder for someone to get unauthorized access.

Plugin : WP Security Questions plugin.

Scanning WordPress for Malware and Vulnerabilities

WordPress security plugin installed, will routinely check for malware and signs of security breaches.

Run a scan if you notice a sudden drop in website traffic or experiencing slow speed.

Can only scan not remove or clean.

You can contact the PRASC team at:

statcan.prasc-prasc.statcan@canada.ca

Funded by the Government of Canada