Wordpress Security

All About Security:
- Safety Precautions and Strategies
- Wordpress admin panel Area Security
- User Access Control
- Wordpress Plugin
- Server and File Security
- Secure Media
- Copyright and Protected Text

Safety Precautions and Strategies	Secure passWords Password ALgoridms Software Updates Protect Media and Content Use Secure FTP and Private SSH Keys Take Frequent BackUps
Secure Wordpress Setup	**Secure DataBase:** Safe Server, Secure UserName and password and Change Prefix **Secure Installation:** Change Admin Username, Setup SALT encryption Keys **Secure Configuration:** Move and Secure wp-config.php and wp-admin folder
.htaccess File	Restricting access to contain files and folder Restrict by ip Prevent Directory Browsing Redirects
Plugin	Akisment, Limit login Attemps,2 Factor Authentication, All Round Security Plugins, Wps Hide Login
Meida Protection	Protect Copyright Text Prevent Image Saveing and Right Click Use private plugin for video rather than posting on youtube and embedding Password protect files

20 Best WordPress Security Plugins to Protect Your Business Website: Link

WpScan AntiMaware Security Astra MalCare CleanTalk Wp-Cerber SheildSecurity WpActivityLog

Titan Wp Hide and Security BBQFireWall WpFail2Ban SecurityNinJa BulletProof DefenderSecu

Sucuri IThme AIOS SecuPress Wordfence

-- Updates are Annoying!

Many people, especially end users consider updating to be disruptive and annoying. While that is true, a small annoyance is worth the damage that can be done to an out of date system

-- What Kinds of Software Should Be Updated?

Web Content Management Systems – Wordpress, Joomla, Drupal and custom systems
Web Shopping Carts
Other Web Software
Computer Operating Systems – Windows, OSX, Linux Distributions
Mobile Operating Systems – iOS, Android, Blackberry, Windows 8 Mobile
Customer and Product Management Systems

-- Why Do We Need Updates?

Bug Fixes – No program is perfect. Most need at least a little debugging.
Security – Hackers can study programs and find the security flaws. Updates can close up the flaws
Improvement – Systems are always improving. Without updates we wouldn't get better functionality as well as better UI and design.

-- Wordpress - What Should I Update

Wordpress Core Updates – Bug fixes, security updates and major updates
Update Wordpress Plugins
Update Your Themes

-- Backup Backup Backup!

It is crucial that you backup your entire site
All Server Files
All Database Tables & Data
You can do this manually or use a 3rd party plugin. Here are some plugins
Backup Wordpress - http://wordpress.org/plugins/backupwordpress/
BackWPup Free - http://wordpress.org/plugins/backwpup/
6Scan Backup - http://wordpress.org/plugins/6scan-backup/
UpDraftPlus - https://wordpress.org/plugins/updraftplus/

-- We Do Everything Online

Manage Finances
Network with friends and family
Take classes
Converse, blog, forums, etc
Shop
Create
Just about everything else

-- Basic Rules For Secure Passwords

At least 8 characters
At least one uppercase letter
At least one lowercase letter
At least one number
At least one symbol character

-- Do NOT use the same password

This is used because it is easy to remember
If you have 200 accounts at 200 different sites, a hacker only needs to get into one and he
will have control of your entire web presence
Learn to manage your different passwords

-- Use A Simple But Secure Algorithm

Lets say you live at
"323 Broadway Street Boston Massachusetts".
You could use
323bsBM#

For even more security, use a random phrase
"I have a cat named spot that's 4"
You could use
IhacnSt4!

-- Do not use real words

Many hacker tools like brute force attacks work by quickly testing random words. Using
random strings of characters severely decreases the chance of a hacker getting in using this
kind of method

-- Password Generators

Password generators can generate the most secure passwords possible.
The only thing to question is the generator app itself. Are they really random?, are they
saved?, etc

Some Reputable Generators
strongpasswordgenerator.com
identitysafe.norton.com/password-generator
random.org/passwords

-- Password Managers

Software that solves the problem of remembering many different passwords

Risk: If someone gains access to your computer, it will not be hard to access the passwords

Built-in Browser (Chrome, Firefox)
3rd Party Local (more secure less convenient) – KeyPass
3rd Party Cloud Based (less secure more convenient) - LastPass

-- Worlds Dumbest Passwords

password
123456
Abc123
123123
111111
qwerty
Your name or kids names
Your pets name
Your phone number
Your birth date
Welcome
letmein

Preventing Attacks:

Limit Login Attemps, 2 Factor Auth, Protecting Bruteforcing,Backup and Restore, Prevent HotLinking

https://wordpress.org/plugins/limit-login-attempts-reloaded/
https://www.cloudways.com/blog/two-factor-authentication-plugins-wordpress/
https://wordpress.org/plugins/two-factor-authentication/
https://wordpress.org/plugins/guardgiant/
https://wordpress.org/plugins/updraftplus/
https://blogvault.net/5-best-wordpress-backup-plugins/

Protect Your Content:

https://wordpress.org/plugins/wp-protect-content/
https://wordpress.org/plugins/secure-copy-content-protection/
https://wordpress.org/plugins/wp-content-copy-protector/
https://betterstudio.com/wordpress-plugins/best-wordpress-content-protection-plugins/

Conclution::

--Installing Wordpress Security:

* Create a Secure database
* Secure Installation with encryption keys
* Secure configuration and file placement

-- We learned How to be Cautious

* The importance of secure passwords
* Password algorithms to remember passwords
* The importance of software Updates
* How to protect our content and media
* how to log in Security
* The importance of backing up our Wordpress Site

-- Using wordpress Security Plugin

* AKismet to stop Spam
* Limit login Attemps with lockout Options
* 2 factor Authentication
* Plugin with all around Security Options

-- Protect your Media

* Protect COpyWritten Text
* Prevent Right click image save
* Private video plugin
* Password Protecting Server Files

-- How to Create an .htaccess file using it to..

* Restrict user access to server files and Folders
* Blacklisting by IP
* Whitelisting by IP
* Prevent Browsing Server Files
* Enable 301 Redirects