Step by Step Security Cheat Sheet

Day 1 Assignment 1

HOW TO SELECT THE RIGHT BACKUP PLUGIN FOR YOU

Summary:

Use the 4 selection criteria to select the right backup plugin:

- ✔ Backup off site
- ✔ Easily restore backups
- ✔ Automatic backups
- ✔ Regular Plugin Safety Precautions

Day 2 Assignment 2

HOW TO UPGRADE WITHOUT AN ULCER

Summary:

Upgrades are **essential**. Use this formula to upgrade safely.

- ✔ Backup
- ✔ Upgrade plugins
- ✔ Clear cache and check site
- ✔ Upgrade theme & framework
- ✔ Clear cache and check site
- ✔ Upgrade WordPress
- ✔ Clear cache

Day 3 Assignment 3

THE NEWBIE MISTAKE EVERYONE STILL MAKES WITH PLUGINS

Summary:

- ✔ Plugins are inherently risky. Use with caution.
- ✔ Use plugins only when necessary. Always verify the source and test.
- ✔ Hard code functions whenever possible to restrict the usage of plugins.

Day 4 Assignment 4

USERS, PASSWORDS & SECURITY OOPSIES

Summary:

1. Users in WordPress are assigned roles. Ie: Admin, Author, Contributor, etc. Best practice is to give these users the fewest permissions necessary to do their jobs.
2. Passwords are extremely easy to guess - especially if you're a robot. So always use random passwords. Force users to change passwords regularly.
3. Restrict the number of login attempts.

Day 5 Assignment 5

SECURITY QUESTIONS FOR YOUR WEB HOST (WITH SCRIPTS)

Summary:

1. Secure File Permissions on the server to 755 (directories) and 644 (files)
2. Use .htaccess file to prevent access to sensitive information
3. Change your Unique Keys
4. Use one site per container

Bonus Security Tips

- Run a virus protection program on your computer/devices
- Use cloudflare (sometimes this is included with your hosting account)
- Check your theme - it's easy when you use this plugin: https://wordpress.org/plugins/theme-check/
- Generate new security keys
- Use a different database prefix
- Disable pingbacks - although I'm not sure how insecure that really is
- Disable XML-RPC (adding content via email)
- Use htaccess to prevent hot-linking and secure the rest of the files that a user doesn't need access to