

WordPress Security Essentials

Facilitator Guide

Topic	WordPress Security Essentials
Duration	60 minutes
Audience	Beginner — no prior security knowledge required
Prerequisite	A modern browser with the latest update installed (Chrome or Firefox recommended); no WordPress account required
Environment	WordPress Playground (playground.wordpress.net) — no login or account needed
Materials	This guide and the companion slide deck

⚠ **WordPress 7.0 note:** This guide was written for WordPress 7.0 (released May 2026). Two changes affect this activity: (1) Administrator and Editor roles have been removed from the new-user default role selector in Settings > General; Site Health now alerts if either was previously set as default. (2) The dashboard uses a new 'Modern' color scheme -- the admin UI may look different from older screenshots or videos participants have seen.

Always walk through all steps in a fresh Playground before the session to confirm the current UI matches this guide.

Learning Objectives

By the end of this activity, participants will be able to:

- * Identify the security features WordPress provides out of the box, including automatic updates, user roles, and the password strength indicator. (Remember)

- * Use the WordPress dashboard to perform a basic security audit: check for pending updates, review user accounts, and evaluate installed plugins. (Apply)
 - * Configure two-factor authentication for the admin account using the Two Factor plugin. (Apply)
 - * Evaluate whether additional security plugins are warranted for a given site based on its complexity and traffic. (Evaluate)
-

Before You Run This Activity

Preparation checklist

- * Test playground.wordpress.net in the venue's browser at least 30 minutes before the session. The site requires internet access and loads best in Chrome or Firefox.
- * Walk through all hands-on steps yourself in a fresh Playground to confirm the current plugin UI matches this guide. The Two Factor plugin UI may change between versions.
- * Open your slide deck and confirm the slides display correctly on the projector.
- * Have a mobile device ready with an authenticator app (Google Authenticator, Authy, or 1Password) installed for the 2FA demonstration in Part 3.

A note on plugin philosophy

This activity deliberately keeps additional plugins to a minimum. WordPress provides a solid security baseline out of the box, and the most common attack vectors are outdated software and weak passwords, not missing security plugins. The only plugin installed during this activity is [Two Factor](#), a lightweight, single-purpose plugin maintained by WordPress contributors. Encourage participants to be skeptical of "all-in-one" security plugins that add significant complexity: the attack surface they add can exceed the protection they provide.

Part 1: Introduction and Discussion | 10 minutes

Background

Most WordPress security incidents are not sophisticated attacks. They follow a predictable pattern: an outdated plugin with a known vulnerability gets exploited by an automated scanner, a weak password gets brute-forced, or an admin account named "admin" gets targeted. Today's activity is about building the habit of auditing these basics before they become a problem.

Key concepts to introduce

- * **The most common entry points for WordPress hacks:** outdated plugins and themes, weak or reused passwords, and publicly known vulnerabilities in unmaintained software.
- * **Security is a spectrum, not a checkbox.** The goal is not a perfectly hardened site but a site that is not an easy target compared to neighboring sites.
- * **WordPress core is actively maintained.** The core team issues security releases quickly. The risk usually lives in plugins and themes, not in WordPress itself.
- * **The less plugins, the better.** Every plugin is a potential attack surface. A plugin that is no longer maintained should be removed, not just deactivated.

Opening discussion prompt

Ask the group one of the following to open the conversation:

- * Has anyone here had a WordPress site get hacked, or know someone who has? What happened? (A few honest stories from the group do more than any slide.)
- * What do you currently do to keep your site secure? Walk me through what happens after you publish a post and move on.

Facilitator note: You do not need to be a security expert to run this activity. The hands-on steps focus on the same audit process a professional would start with: check updates, review users, review plugins, and enable 2FA. If a question goes beyond your knowledge, it is fine to say so and point to the WordPress Security Whitepaper in the Sources section.

Part 2: What WordPress Provides Out of the Box | 10 minutes

Background

Before asking participants to add anything to their sites, establish what WordPress already provides. This reframes security from "I need to install a plugin" to "I need to use what I already have." Cover the following points with the slides.

Built-in security features to cover

- * **Automatic background updates.** WordPress can auto-update core minor releases, plugins, and themes. Dashboard > Updates shows the current status and any pending items.
- * **Password strength indicator.** The password field in Users > Your Profile grades passwords in real time and enforces a minimum standard. WordPress will not save a password it considers too weak unless the user explicitly overrides it.
- * **User role system.** WordPress ships with five roles: Administrator, Editor, Author, Contributor, and Subscriber. Limiting who has Administrator access reduces risk.

- * **Nonces and permission checks.** WordPress core uses nonces (one-time tokens) to protect against cross-site request forgery. Well-written plugins follow the same pattern.
- * **Regular security releases.** The WordPress Security Team issues dedicated security releases quickly after vulnerabilities are found. The release notes always include the CVE identifiers for anything patched.

What is not included by default

Be honest with participants that WordPress does not include everything. The following require additional steps or plugins:

- * Two-factor authentication (added in Part 3 of this activity)
- * Login attempt rate limiting (some hosting environments add this; WordPress core does not)
- * File integrity monitoring
- * Web application firewall

Facilitation tip: Participants often ask about specific security plugins they have heard of (Wordfence, Sucuri, iThemes Security). Acknowledge them briefly but redirect: today's activity focuses on the built-in baseline and one targeted plugin for 2FA. Large security suites can be valuable for high-traffic or eCommerce sites, but add complexity that outweighs their benefit on a small blog or portfolio site.

Part 3: Hands-On Security Audit in Playground | 25 minutes

Background

Participants will walk through a security audit on a fresh WordPress Playground site. The audit mirrors the process they should run on their own sites. Because Playground resets between sessions, there is no risk to any real site. Encourage participants to open Playground on their own devices so they can follow along at their own pace.

Setup for participants

- * Open playground.wordpress.net in your browser. Wait for the WordPress dashboard to load (about 20 to 30 seconds).

Step-by-step: the security audit

1. In the left menu, click **Dashboard**. At the top of the screen, look for any "WordPress X.X.X is available" notices or plugin update banners. On a real site, these should never be ignored.

2. In the left menu, click **Dashboard**, then **Updates**. Review the current WordPress version, any plugins with pending updates, and any theme updates. Note how many are waiting.
3. In the left menu, click **Plugins**, then **Installed Plugins**. Review the list. Ask yourself: Do I know what each plugin does? Is each one still actively maintained? Are any deactivated but not deleted?
4. In the left menu, click **Users**, then **All Users**. Check for any accounts you do not recognize, and confirm that Administrator access is limited to people who actually need it.
5. Click your username to open your profile. Scroll to the **Account Management** section. Click **Generate Password** to see the password strength indicator. Notice how it grades password complexity in real time. Close without saving.
6. In the left menu, click **Settings**, then **General**. Verify the **Site Address (URL)** begins with https (on a live site). Confirm the **Administration Email Address** is one you actively monitor.

Discussion pause: Before moving to step 7, ask the group: Looking at what you just reviewed, what is the first thing you would fix on your own site? The most common answers are pending updates and weak passwords. This sets up the 2FA step naturally.

Step-by-step: adding two-factor authentication

7. In the left menu, click **Plugins**, then **Add Plugin**.
8. In the search box, type **Two Factor**. Find the plugin named **Two Factor by WordPress Contributors**. It is a lightweight, single-purpose plugin. Click **Install Now**, then **Activate**.
9. In the left menu, click **Users**, then **Your Profile**. Scroll down to the **Two-Factor Options** section.
10. You will see several methods listed: **Authenticator App** (recommended), **Recovery Codes** (recommended), **Email**, and **Dummy Method** (ignore this — it is a developer testing method). Enable **Email** as the primary method (no authenticator app needed for this demo). Click **Update Profile** to save.
11. Scroll back up to confirm the Two-Factor Options section shows Email as enabled. On a real site, the Authenticator App method (using an app like Google Authenticator or Authy) is the stronger option because it does not depend on email access. Recovery Codes should also be enabled alongside any primary method as a recovery option.

Facilitator note: If participants have an authenticator app on their phone, invite them to enable the Authenticator App method instead of Email. The plugin displays a QR code to scan and requires a 6-digit confirmation code. This is a good live demonstration of how app-based 2FA works in practice. Recovery Codes should also be enabled alongside any primary method as a recovery option.

Terminology note: The section heading in the plugin UI is "Two-Factor Options" (with a hyphen). Participants may need to scroll below the password fields to find it. The methods listed are: Authenticator App (recommended), Recovery Codes (recommended), Email, and Dummy Method. Participants should ignore Dummy Method -- it is a developer testing method that has no effect. On first use, all options show as toggles.

Part 4: Closing Common Security Gaps | 10 minutes

Background

With the audit steps and 2FA complete, debrief the group on the four most common remaining gaps. Tie each back to the audit steps participants just completed.

The four gaps to cover

- * **Outdated plugins and themes.** This is the number one attack vector. Automated scanners run continuously, looking for sites running plugin versions with known CVEs. Keeping plugins updated is the highest-return security action most site owners can take.
- * **The "admin" username.** WordPress no longer allows the username "admin" to be set during installation, but older sites may still have it. If a participant has an admin account named "admin", the fix is to create a new Administrator account with a different username, log in with the new account, and delete the "admin" account.
- * **HTTPS.** Sites without HTTPS transmit login credentials in plain text. Most hosting providers include free SSL certificates. If a site still shows http:// in the address bar, this is the most urgent fix.
- * **Backups.** A backup is not a security tool, but it is the fastest recovery path after a compromise. Participants should know where their backups are, how recent they are, and how to restore from them. Many hosts include daily backups; many site owners have never tested restoring one.

Facilitator tip: Ask participants to check their own site's HTTPS status in a second browser tab while you are talking through this section. It is a quick visual check and often surfaces mixed-content warnings that participants did not know existed.

When to consider additional plugins

The following scenarios may justify adding a security plugin beyond Two Factor:

- * The site handles payments or sensitive user data (eCommerce, memberships)
- * The site is under active attack or has been compromised before

- * The hosting environment does not provide server-level protections
- * A compliance requirement (PCI-DSS, HIPAA) mandates specific controls

For most small blogs, portfolios, and local business sites, the steps in this activity plus a reliable hosting provider with HTTPS and daily backups represent a security posture that is well above average.

Part 5: Building a Security Routine | 5 minutes

Background

Security is not a one-time task. Close the session by helping participants turn today's audit into a repeatable routine.

The monthly security habit

1. Log into your WordPress dashboard. Check **Dashboard > Updates**. Apply all available updates.
2. Check **Users > All Users**. Remove any account(s) you do not recognize.
3. Check **Plugins > Installed Plugins**. Remove any plugin you are not actively using. Deactivated but installed plugins can still be exploited.
4. Confirm your hosting backup ran recently. If you are unsure, log into your hosting control panel and verify.

Before installing any plugin

Encourage participants to ask these questions before adding a plugin:

- * When was this plugin last updated? (More than 2 years: caution)
- * How many active installations does it have? (Under 1,000: caution)
- * Is it tested with the current version of WordPress?
- * Does the plugin do one thing, or does it bundle features I do not need?

Closing discussion prompt

- * **What is one thing you will check on your own site this week?**
- * What would it take to set a recurring reminder to do the monthly security check?

Stretch activity: Participants who finish early or want a deeper challenge: open a fresh Playground, go to Users > Your Profile, scroll to Two-Factor Options, and try enabling the Authenticator App method using a real authenticator app on their phone. The plugin displays a QR code to scan and requires a 6-digit verification code before saving. This is as close to the real 2FA setup experience as Playground allows.

Sources

All URLs verified as of May 2026. Check before running the activity.

1. [Two Factor — WordPress plugin](#): Lightweight, single-purpose 2FA plugin by WordPress contributors. Supports TOTP authenticator apps, email codes, and backup codes.
2. [Two Factor plugin changelog](#): Verify the current version and any UI changes to the Two Factor Options section before running the activity.
3. [WordPress Security Whitepaper](#): Official documentation covering the WordPress security model, core release process, and responsible disclosure.
4. [Hardening WordPress — WordPress Developer Resources](#): Official hardening guidance from the WordPress project covering passwords, file permissions, user roles, and more.
5. [Two-Factor Authentication for WordPress — Learn WordPress](#): Official Learn WordPress lesson on setting up 2FA; can be shared with participants as a follow-up resource.
6. [WordPress Security Checklist — iThemes](#): Practical checklist covering the most common security improvements; useful facilitator reference.