melapress

Quick (user) security wins

How to protect your WordPress website user accounts using free plugins

The most common reasons WordPress websites get hacked:

- Vulnerabilities in outdated software
- Compromised user accounts

Some numbers (for context):

- **96% experienced at least 1 security incident**
- **64% reported at least 1 security breach**
- **Only 26% train their team or have been trained**
  - Lack of user training strongly correlates with higher hack rates.

— *Melapress WordPress Security Survey 2025*

How websites user accounts get compromised?

- Weak & shared passwords
- Lack of controls
- No authentication hardening
- Lack of awareness & training

Why are user accounts a prime target?

- Poor security hygiene
- Easy to compromise. It happens to the best of us:
  - *Troy Hunt, March 2025*
  - *Josh Junon, September 2025*
- They open a lot of possibilities

Getting started with user security:

- Practice what you preach
- Assume most users are non-technical
- No expensive & complicated software required

Two types of users:

- **Your team**
  - Users who have access to the backend of your website / systems
- **Customers / business partners etc**
  - They have a user on the website but only access the front-end

Starting with the basics:

The security of your users' devices will become your WordPress website security problem.

Up to date software

- Enable auto updates
  - Keep users updated
- More than 5 users?
  - Use an MDM solution
    - Enforce OS updates (reduce attack surface)
    - Enforce browser and software versions

Step 1: The login process

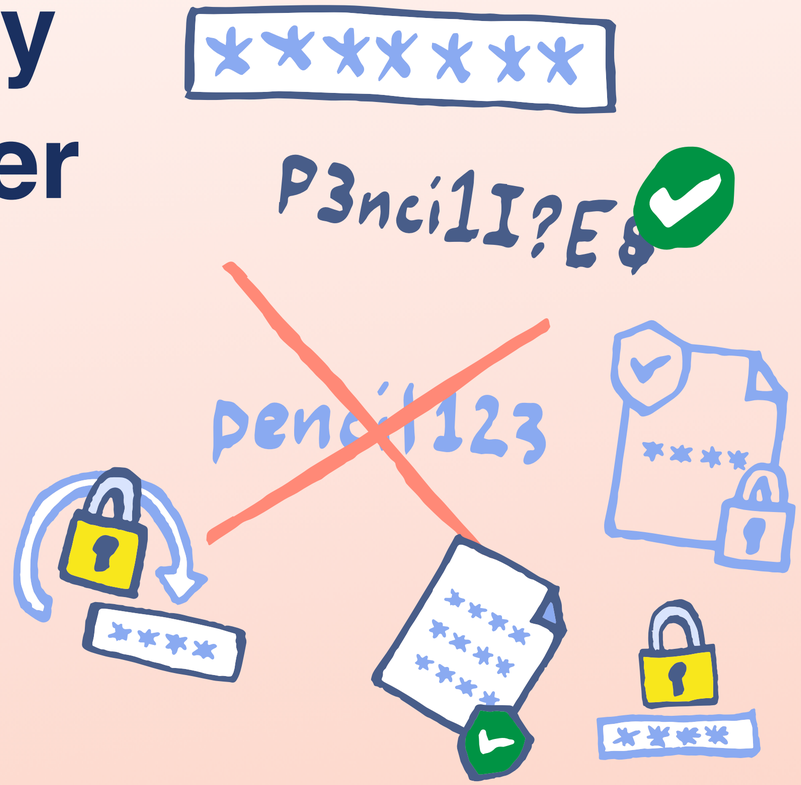
The first line of defence: passwords

Reality: lower your expectations

Solution: automate

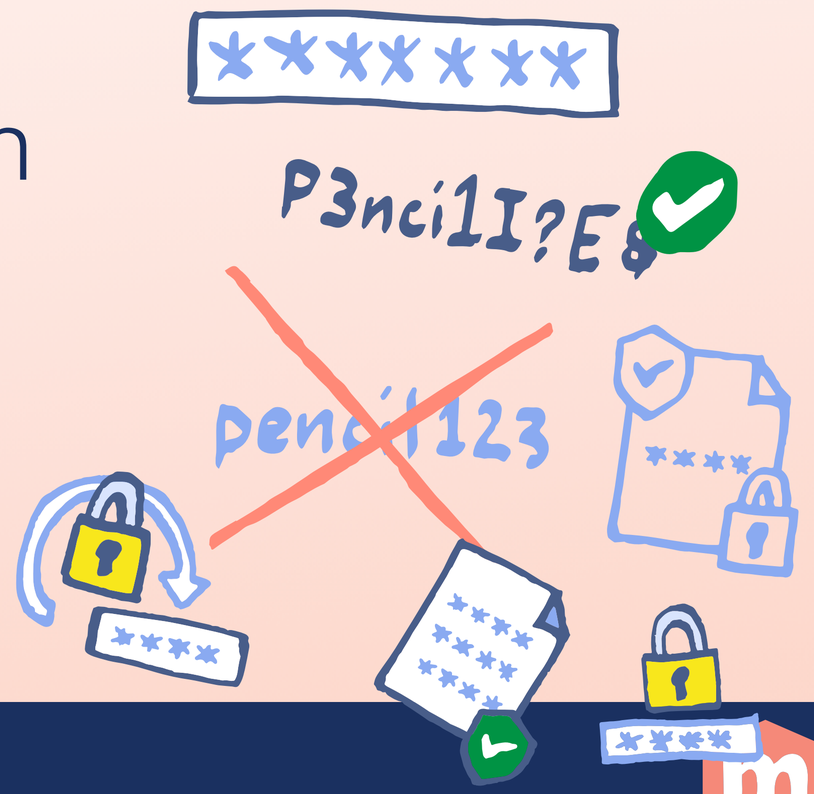
Apply strong password policies with a plugin:

- Melapress Login Security
- Password Policy Manager
- WP Password Policy



Also for step 1:

- Use Password managers
  - *SaaS VS installed software*
- Automatic password generation
  - *Via own password generator*



Use Passkeys

- They replace passwords
  - strong single-factor (device + biometric)
- Not guessable
- Cannot be phished
- Not reusable
- But…

Passkeys do not replace 2FA/MFA

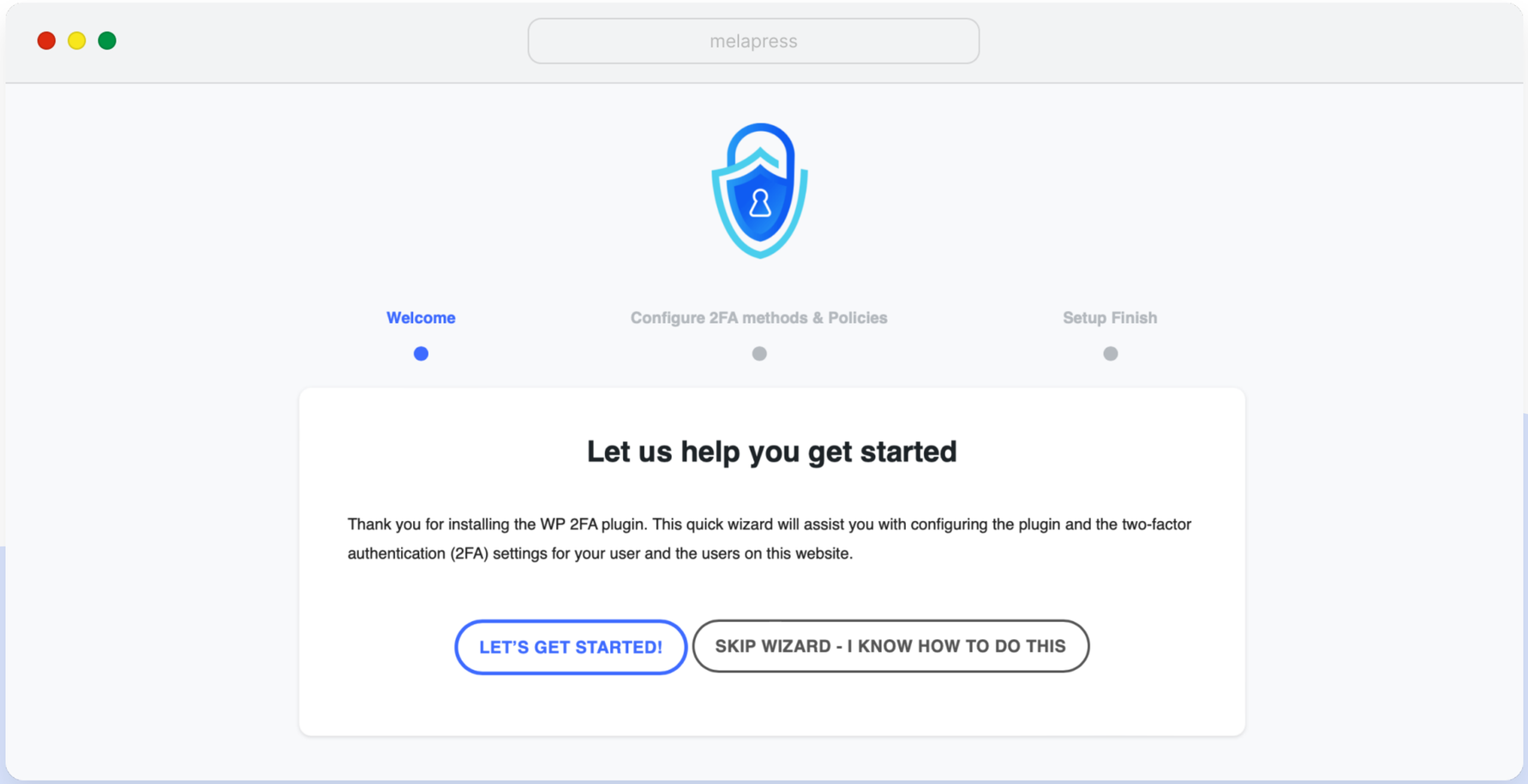
unless you switch to passkeys exclusively

Step 2: Deploy & enforce Two-Factor Authentication (2FA)

Do not just rely on Passwords. Use a plugin such as:

- **WP 2FA**
- **Two-factor**
- **Two Factor Authentication**

Also in step 2:
Use an intuitive solution



Concerns about users getting locked out because of 2FA?

- Give the users the tool they need
  - *Backup methods*
- Explain to the users
  - *Tell them what the changes are etc*

Step 3: Additional user login hardening & policies:

- Limit failed login attempts
  - Lock user accounts instead of blocking IP addresses
- Deactivate public password resets
- Add HTTP authentication
- Restrict IP addresses

Allowing access to third parties?

Use temporary logins with plugins like:

- *Melapress Login Security*
- *Temporary Login without Password*

So you can:

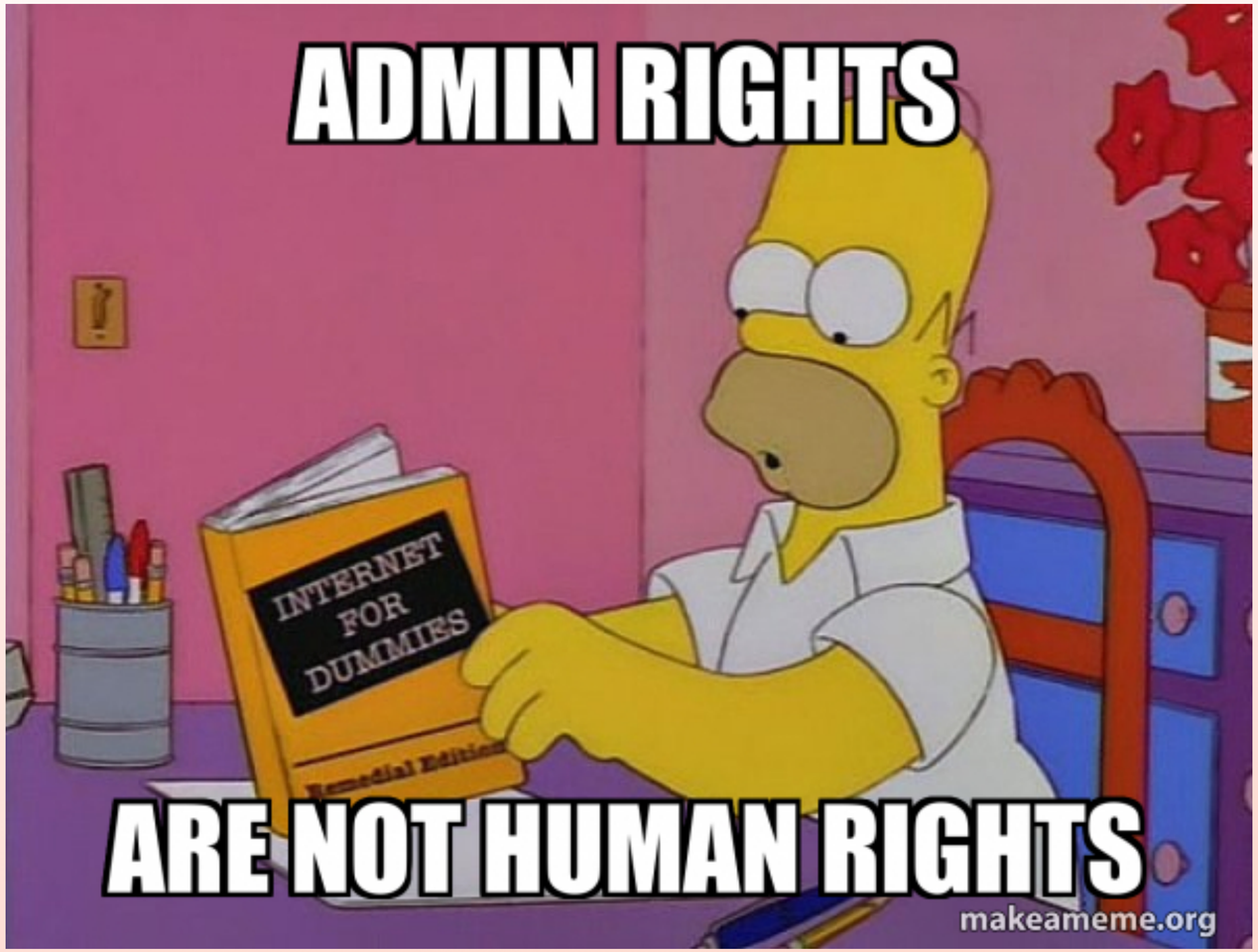
- *Control how many times they can log in*
- *Control what they can access*
- *Link expires automatically*

Should strict login security policies be applied for all users?

Step 4: Use user roles

- What information users can see
- Which sections of the website users can access
- What changes they are allowed to apply on the website
- What processes can they trigger

Not everyone needs admin rights!



Free plugins to create & manage user roles:

- Melapress Role Editor
- User Role Editor
- PublishPress Capabilities

User onboarding process

Define and create correct roles

- *Use the principle of least privileges*
- *Assign restrictions from day one*

Document everything

- *Write down what users can access*
- *Keep the documentation up to date*

User off boarding process

Refer to the documentation and:

- *Disable / delete accounts (do not change password)*
- *Revoke API keys*
- *Reset shared credentials*
- *Revoke any other type of access*

Use cases for WordPress user roles

Agency and client scenario:

- Allow client to:
  - *Change specific theme settings*
  - *Update the theme & plugins*
- Limit client from:
  - *Installing new plugins*
  - *Changing WordPress site settings*

e-Commerce store scenario:

- Part of the team updates products’ metadata (e.g. stock qty)
- Order processing only need to access and process orders
- Marketing needs access to on-page SEO

So far we have covered

- Secure passwords (& password managers)
- Use 2FA / MFA (hardened authentication)
- Use user roles (and document)

but there is (always) more you can do…

The most important part:

Educate users about
security best practices

Security best practices

- Do not use public or others’ computers
- Avoid public (insecure) WIFI’s and networks
- Always use VPN
- Credentials hygiene
- Recognize potential attacks
- Secure file handing
  - *No email attachments*
- How and where to report incidents & suspicious activity

And keep repeating…

- Send occasional emails
- Drop hints during meetings
- Explain everything to the users
- Keep them in the loop

"*The faintest ink is better than the strongest memory*"

The breach numbers don’t lie

“64% reported at least 1 security breach”

- Outdated plugins/themes (predictable entry points)
- Weak or recycled passwords (instant takeover)
- No 2FA/MFA (attackers only need the credential)
- Poor onboarding/offboarding (old accounts > open doors)

Most hacked sites didn’t fail on firewalls.

They failed on basic user issues

So...

If an attacker wants to get into a WordPress website, what's the easiest way for them to do it?

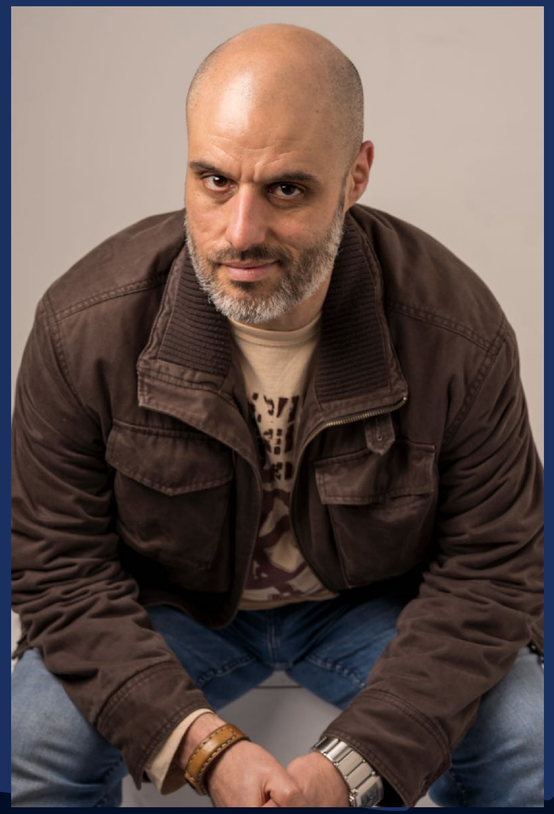
Actionables

Checklist for the next 48 hours:

- [ ] Enable auto updates
- [ ] Install a password policy plugin (and enforce)
- [ ] Start using password managers
- [ ] Require 2FA (start with admins)
- [ ] Create non-admin roles
- [ ] Brief your team on security best practices (educate)

That’s all folks!

- Implement (systems & policies)
- Automate (the processes)
- Educate (the users)
- Take Action!



Robert Abela

CEO & Founder of melapress