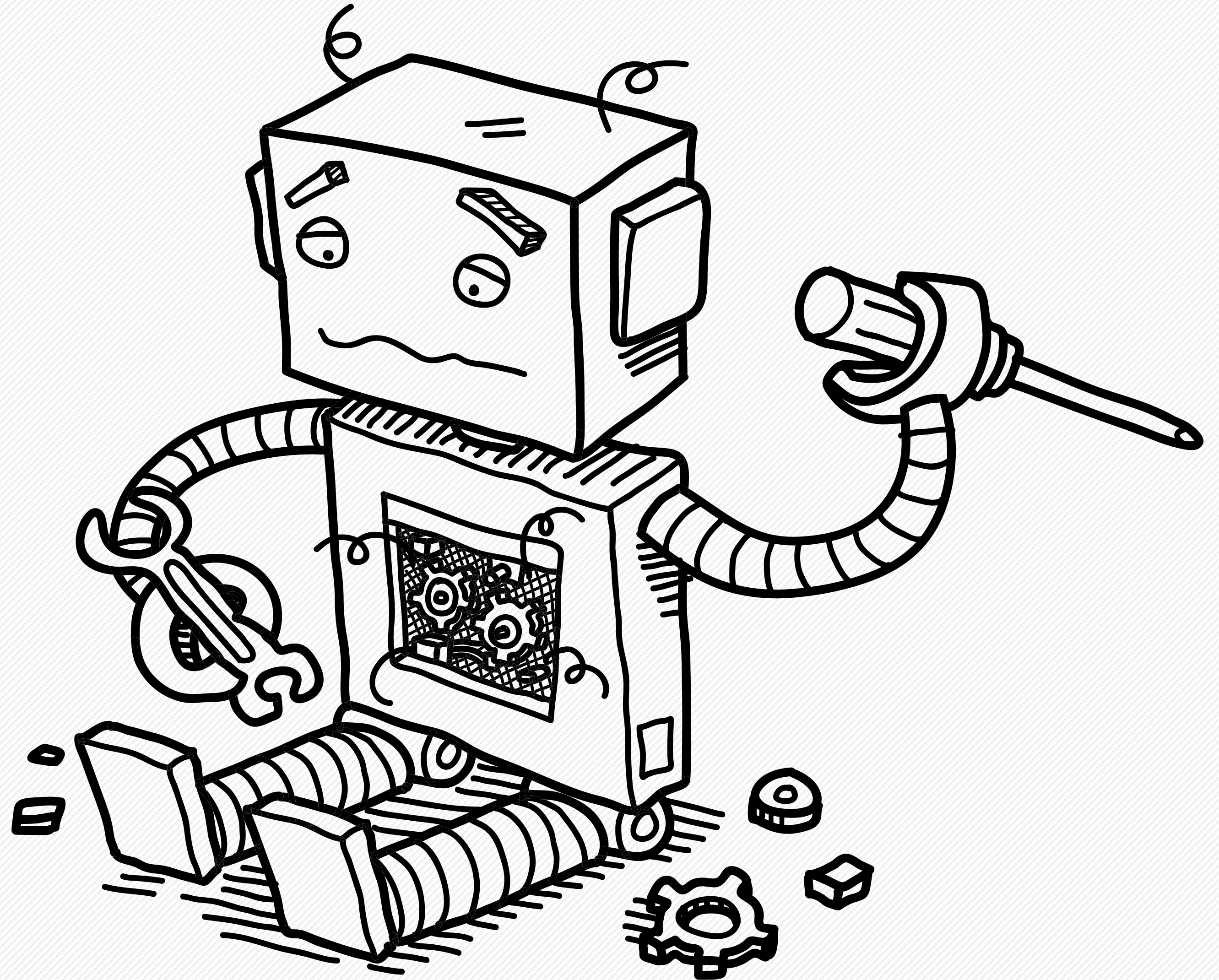


Website **Security** **Masterclass**

with Robyn Smart



Robyn Smart - Smart Robbie
smartrobbie.com.au



Why have things changed?



In the **1990's websites used to be 'set and forget'.**

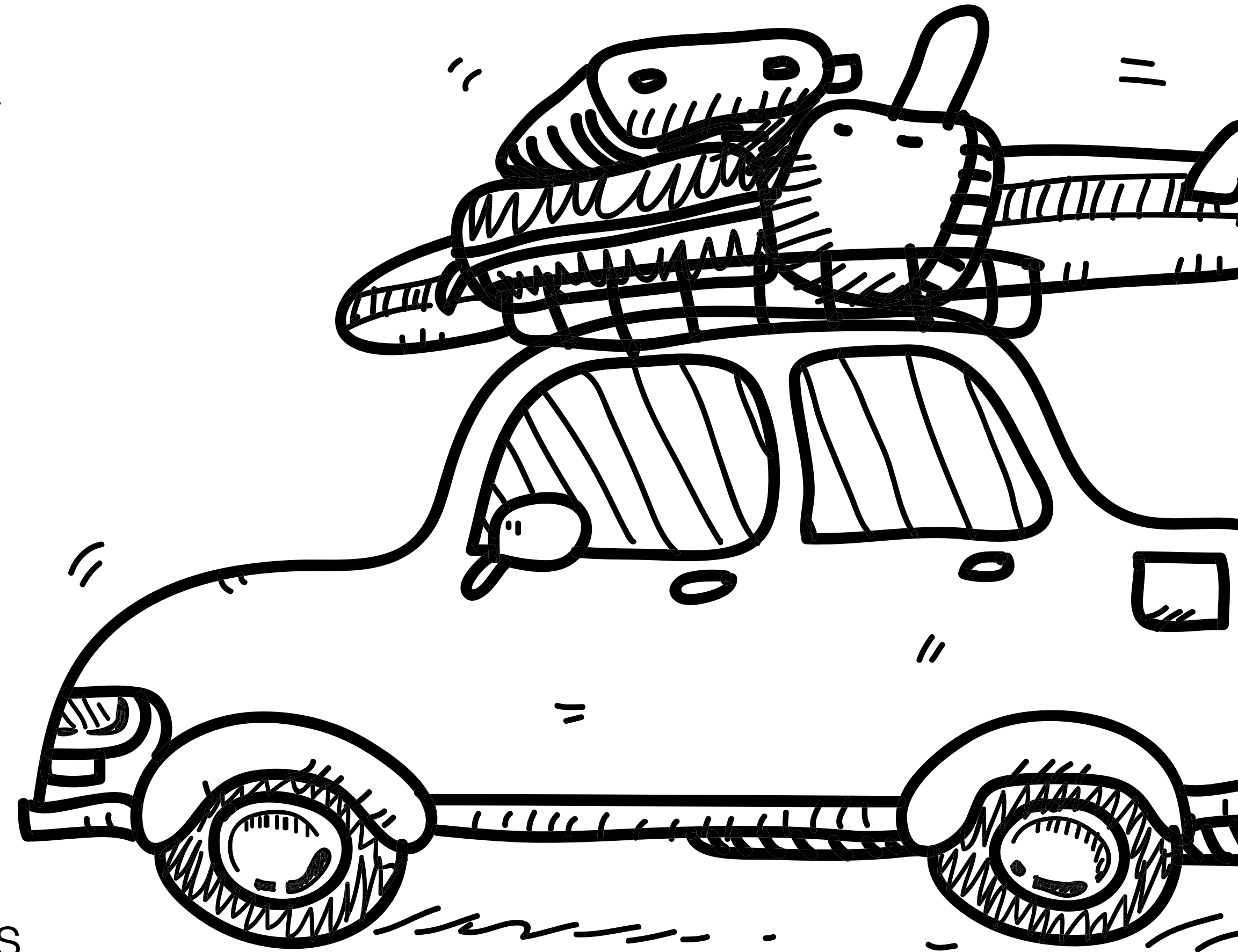
They were simpler websites, served as online brochures. WordPress maintenance didn't exist and website security was minor, it wasn't something you had to worry about.

Today, website are more complex.

Your website needs regular security monitoring and software updates.

Similar to physical store building, you need to have a security system.

Or like maintain your car, you have regular services on your car. If you don't service your car and something goes wrong, it's often more expensive to fix.



Why is website security **Important?**



WordPress Security



A hacked WordPress site can cause serious damage to your business revenue and reputation. Hackers can steal user information, passwords, install malicious software, and can even distribute malware to your users.

What types of hacks can happen to my site?

- redirect traffic to another website
- copy secure information such as email addresses, credit cards
- phishing (pretend they are you to get information)



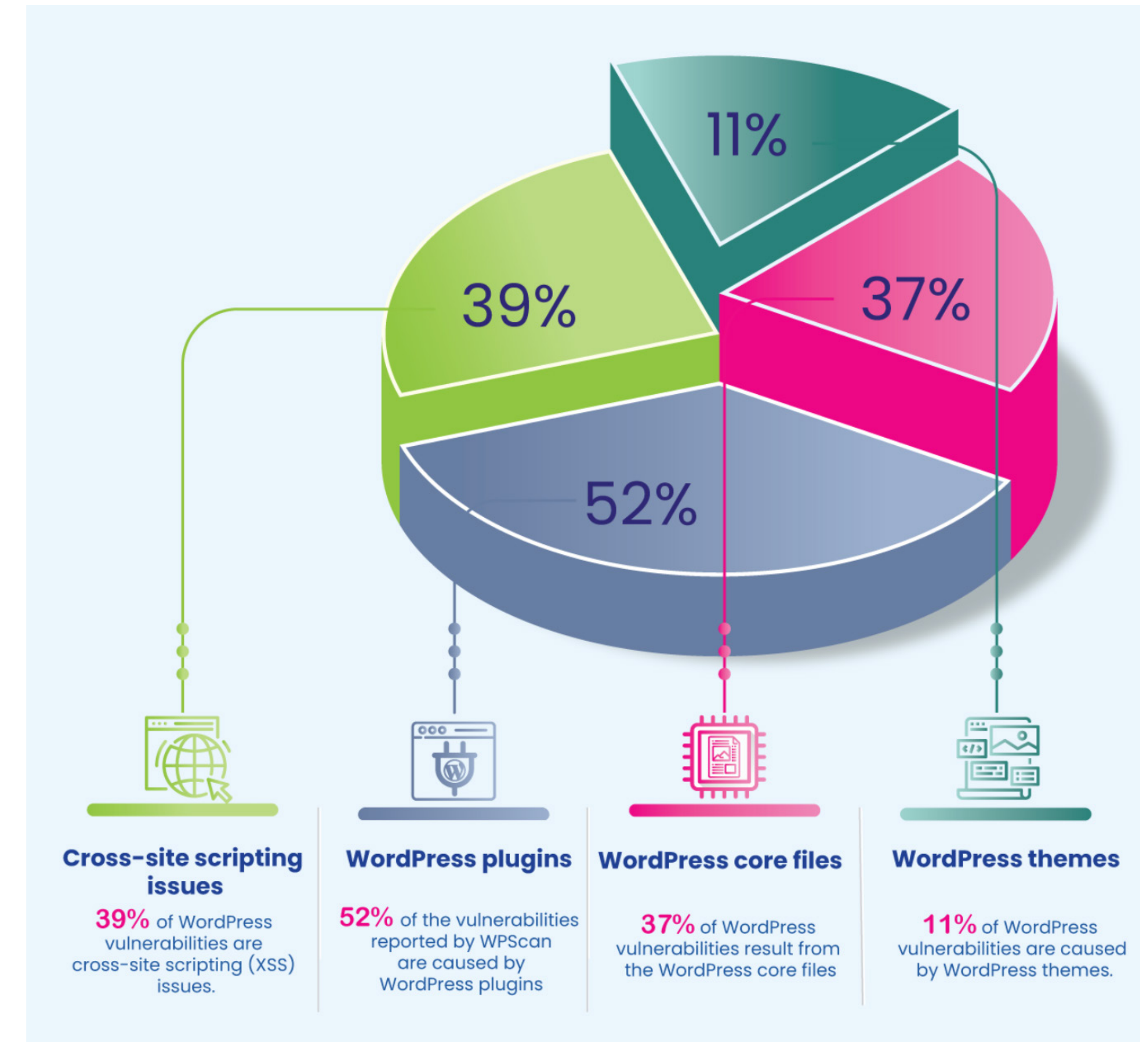
Why is website security important?



87% of websites have high or medium cyber security risks

68% of websites doesn't have a recovery plan in place

52% of vulnerabilities are caused by plugins.



WordPress Security Stats 2020

Why is website security important?



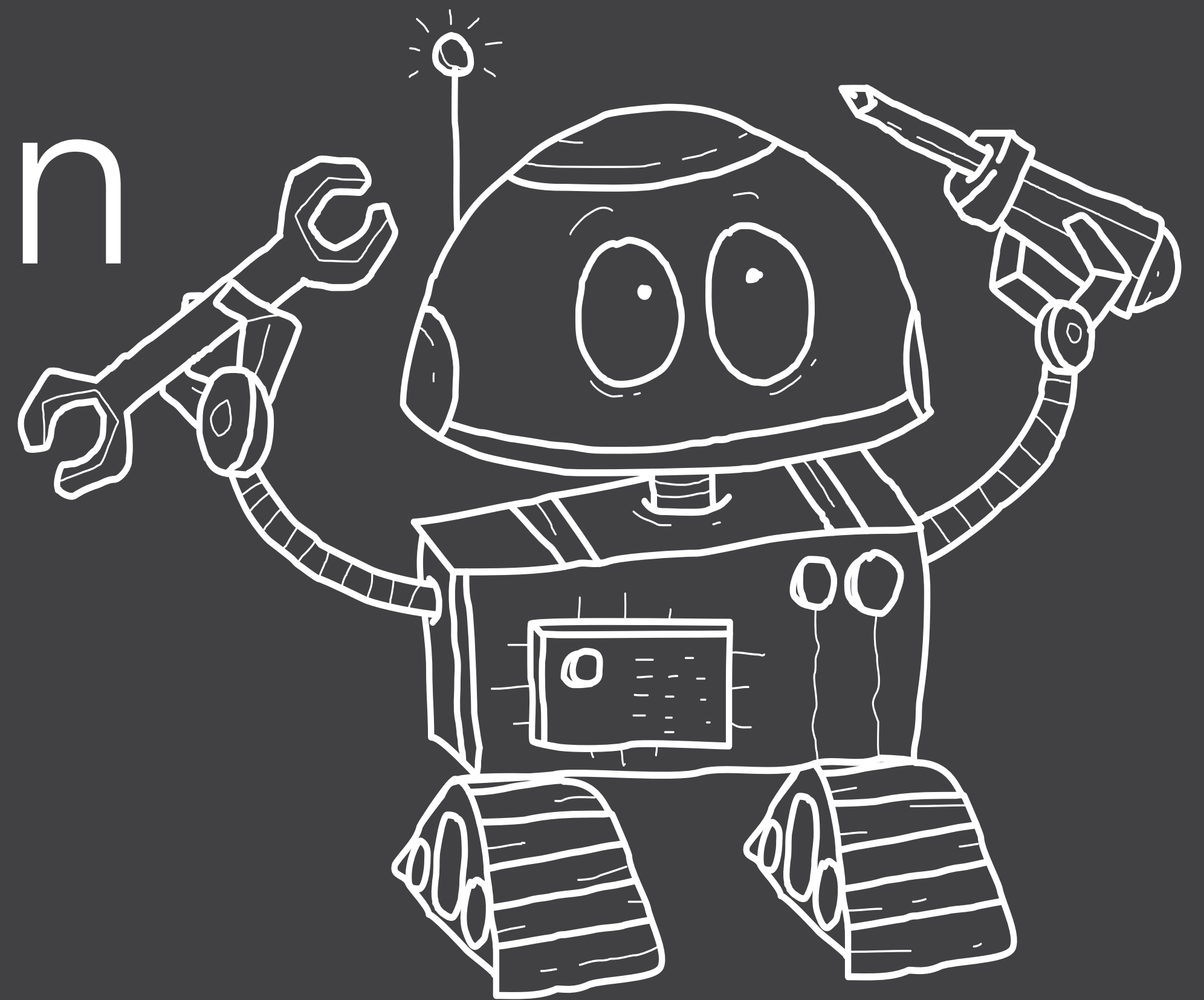
- 1. Protect your Customers**
- 2. Protect your Assets**
- 3. Protect your Reputation**
- 4. Prevent a loss in Revenue**
- 5. Your visitors expect it.**
- 6. Google likes secure websites.**
- 7. For Peace of Mind**

Good news... you can take some basic steps to secure and manage a safe WordPress website.



Tip

Secure your login
procedures



Secure logins - username and passwords



Use unique usernames:

don't use: domain name, test, demo, admin, administrator.

Use strong passwords:

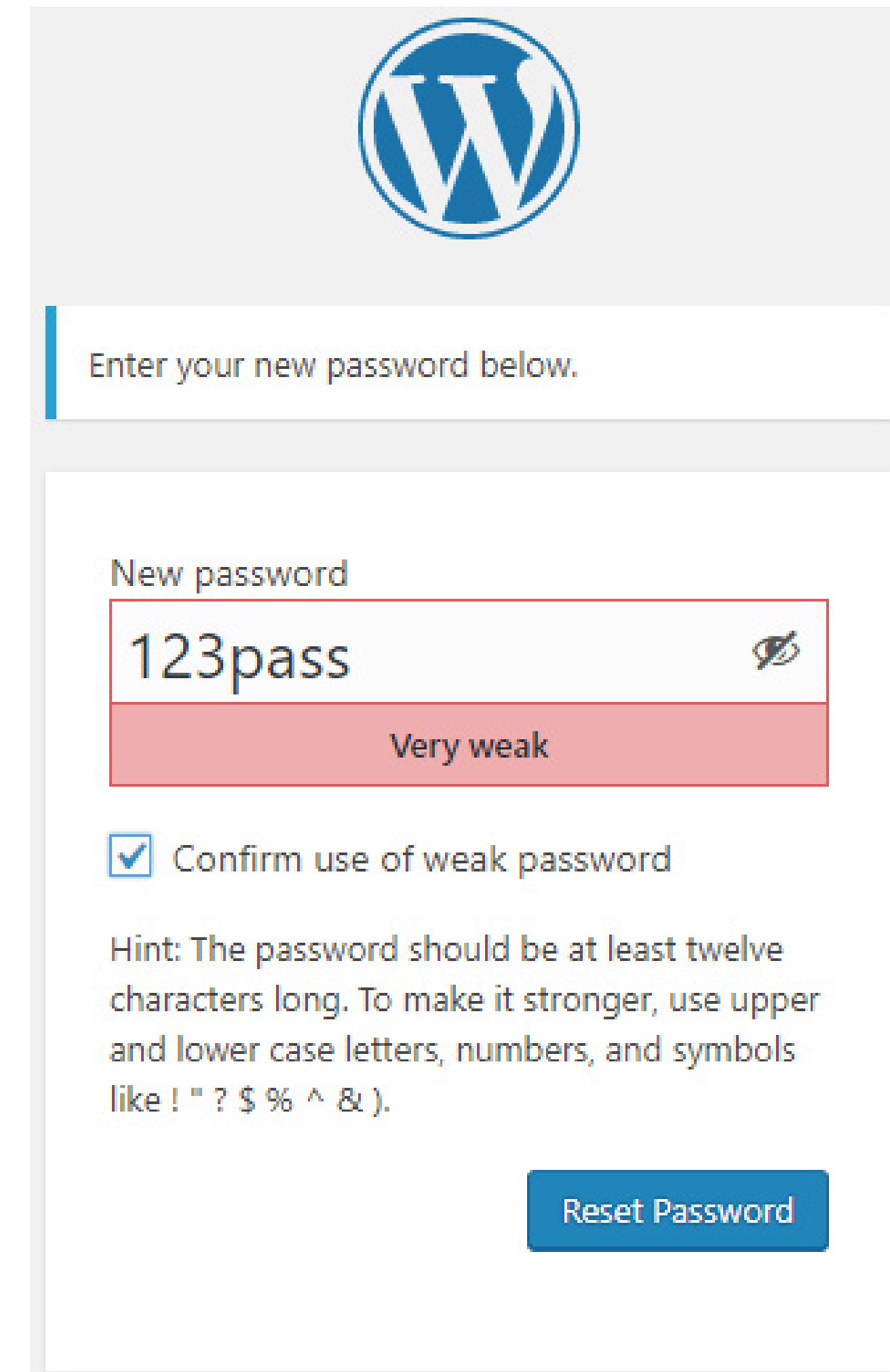
people are still using "123456" as a password.

Add a captcha:

Add an extra layer of security to your login by verifying that you are indeed a real person. You can use plugins to add a captcha to your site. reCaptcha by BestWebSoft is one we recommend

Change Login URL:

For example domainname.com.au/newlogin

A screenshot of the WordPress password reset form. At the top is the WordPress logo. Below it is a text box with the placeholder "Enter your new password below.". The main form area has a label "New password" above a text input field containing "123pass". To the right of the input is an eye icon. Below the input is a red bar with the text "Very weak". Underneath is a checkbox labeled "Confirm use of weak password" which is checked. A hint message states: "Hint: The password should be at least twelve characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! \" ? \$ % ^ &).". At the bottom right is a blue button labeled "Reset Password".

WordPress logo

Enter your new password below.

New password

123pass

Very weak

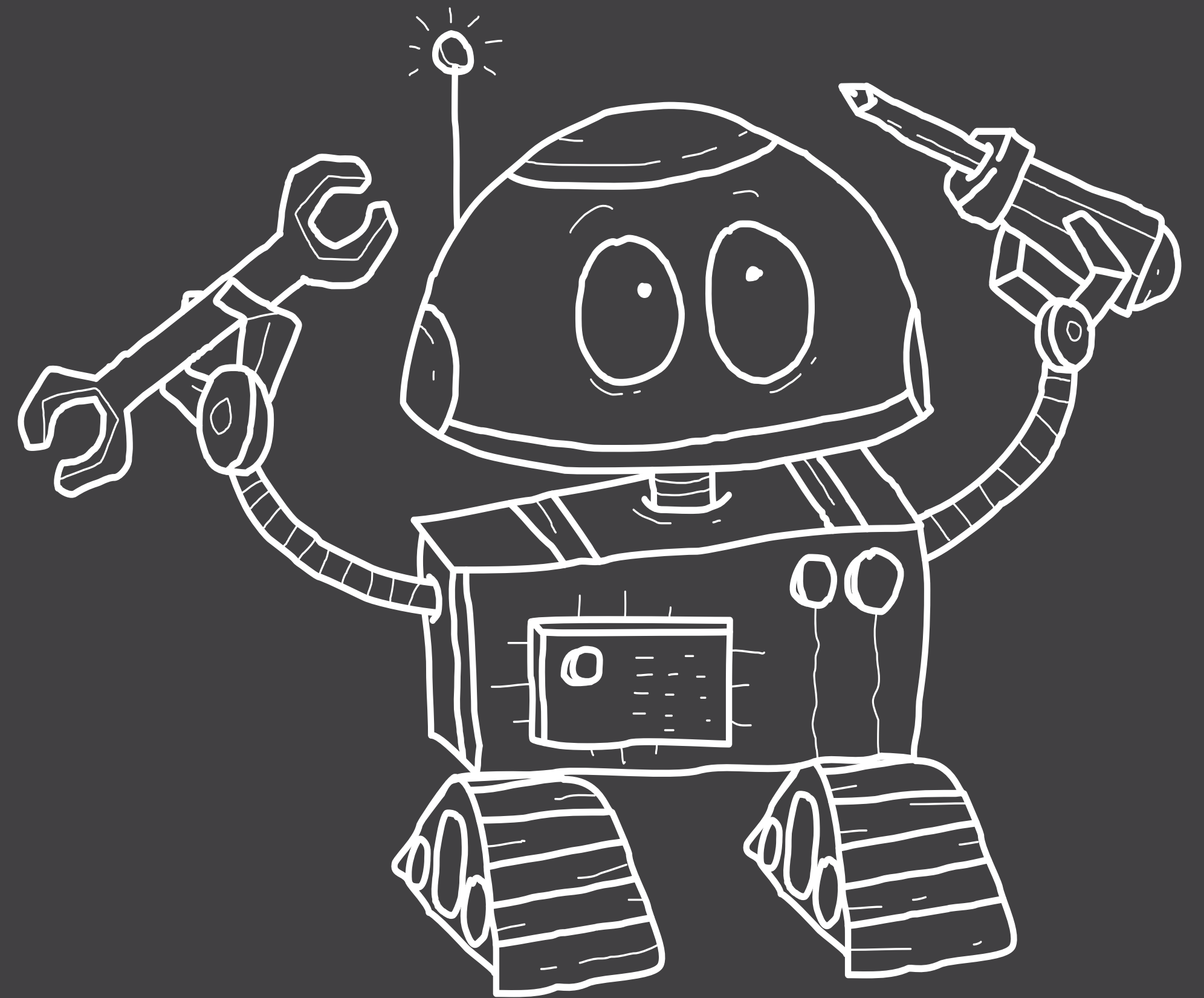
☒ Confirm use of weak password

Hint: The password should be at least twelve characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! \" ? \$ % ^ &).

Reset Password

Tip

Limit your login
attempts



Limit your login attempts




Limit login attempts:

Placing a cap on the number of times a user enters the wrong credentials in a certain amount of time will prevent hackers from brute-forcing a login.

Plugins that can do this:

- Security plugin like WordFence or iThemes Security
- Limit Login Attempts

A screenshot of the WordPress login page. At the top is the WordPress logo. Below it is a red-bordered box containing an error message. The message reads: "ERROR: Incorrect username or password." followed by "ERROR: Too many failed login attempts. Please try again in 20 minutes." and a link to "resetting your password". Below the error box are two input fields: "Username or Email Address" and "Password". At the bottom left is a checkbox labeled "Remember Me", and at the bottom right is a blue "Log In" button.



ERROR: Incorrect username or password.

ERROR: Too many failed login attempts. Please try again in 20 minutes.

You can also try [resetting your password](#) and that should help you to log in.

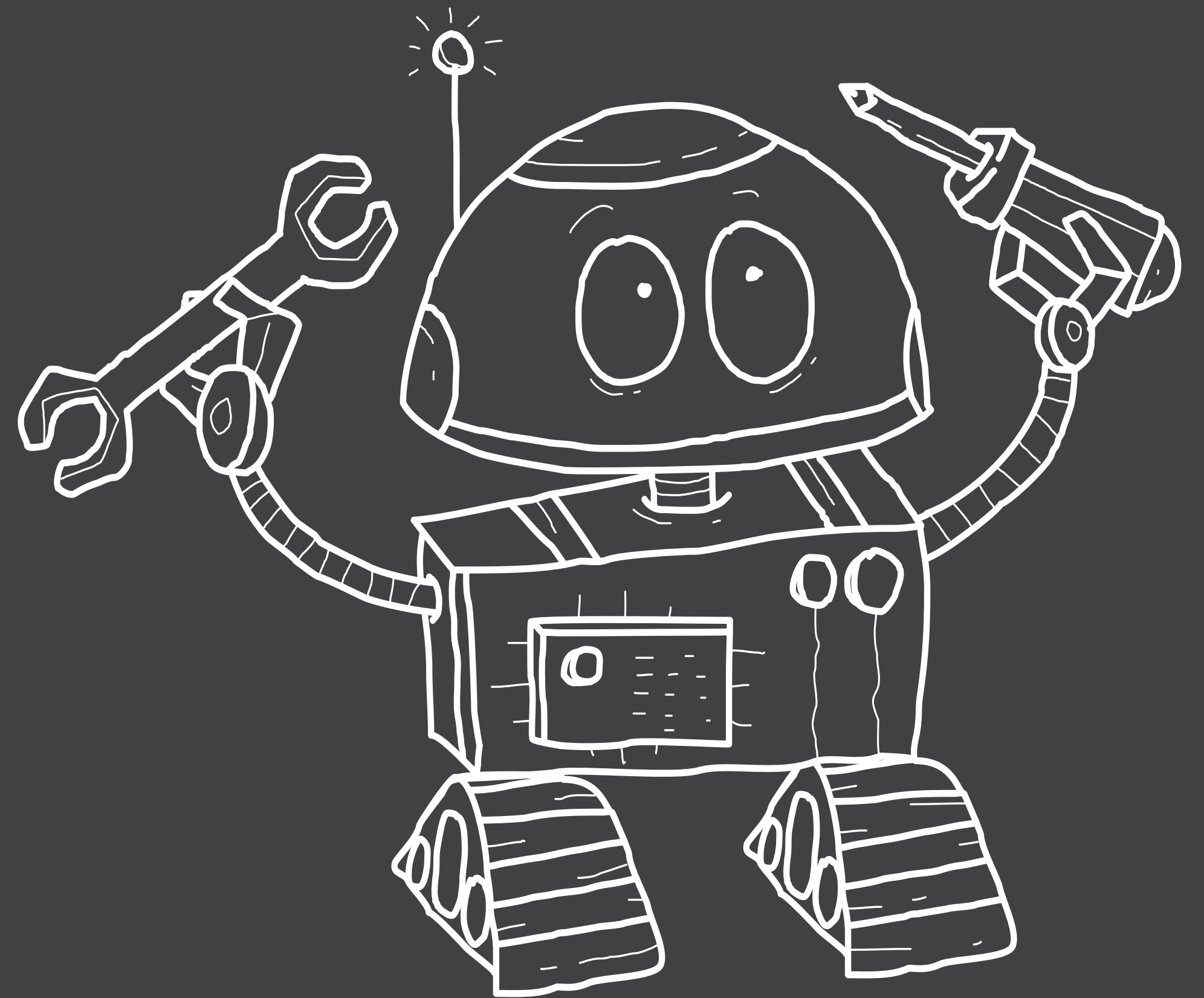
Username or Email Address

Password

☐ Remember Me

Tip

Who has
admin access
to your site?



Who has admin access?

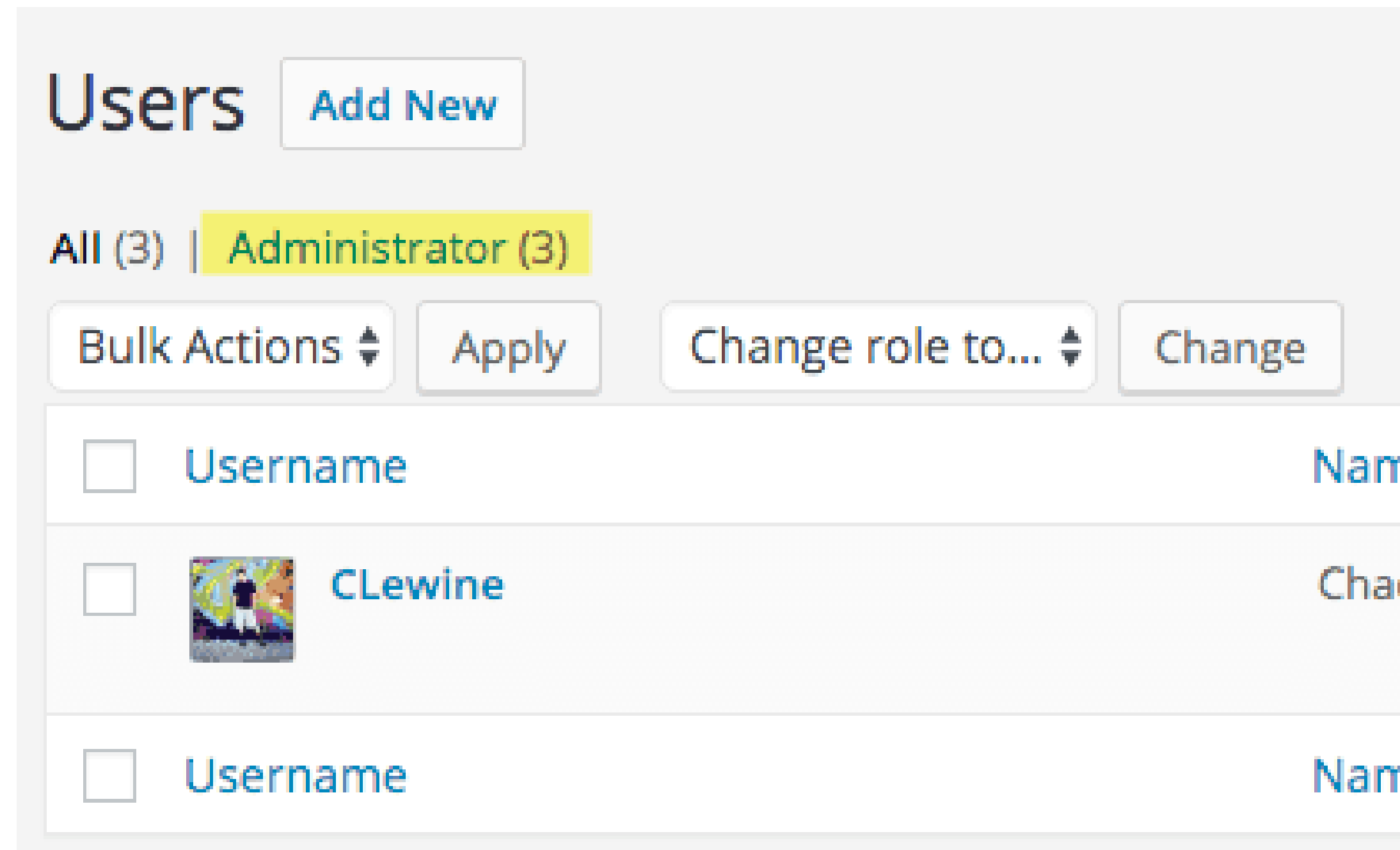


Administrator

Admin logins have complete control of your website.

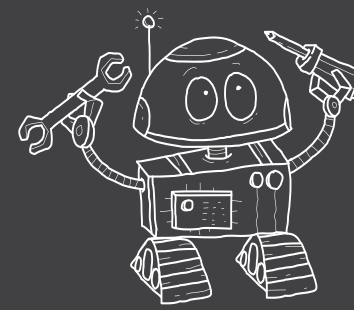
If you need people to have access to your site, it's best to give them their own login so you can remove them later.

It's always good to review who has access and adjust when needed.



Hosting/FTP logins

They are even more important than admin logins.

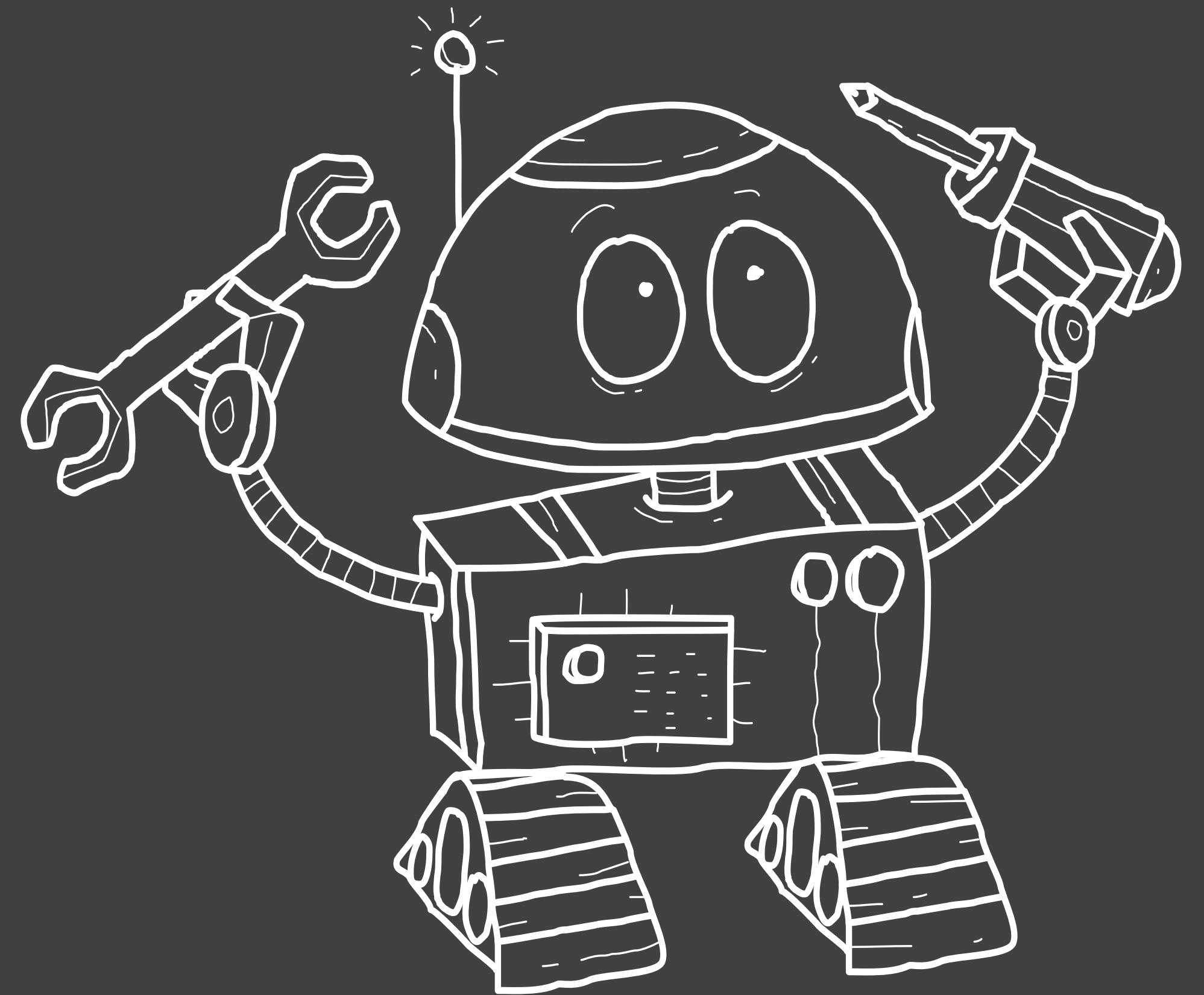


Pro Tip

Use LastPass to share access to hosting.

Tip

Are you using
2 factor
authentication?



2 Factor Authentication

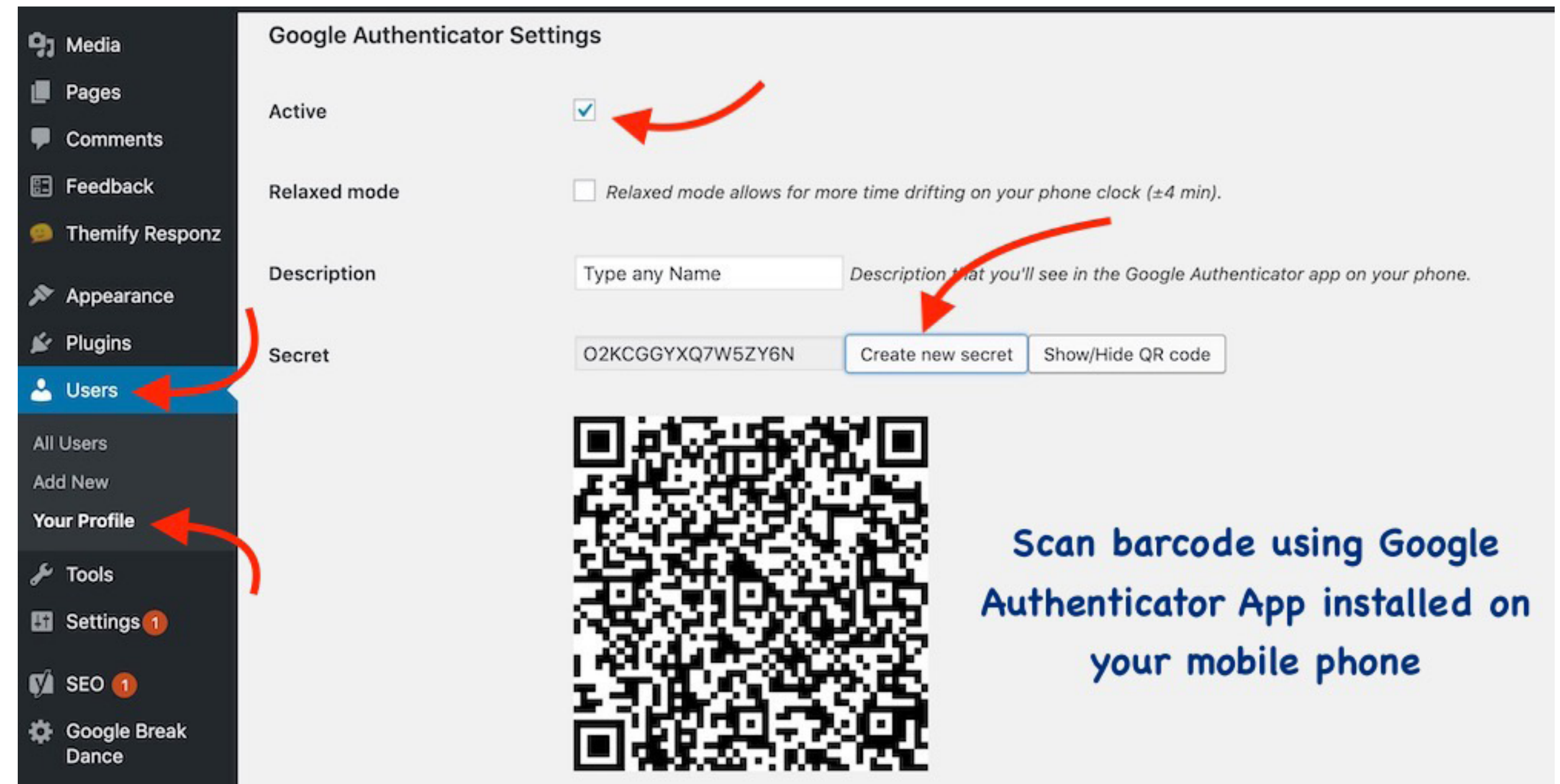


Enable two-factor authentication:

Two-factor authentication (2FA) requires users to verify their sign-on with a second device. This is one of the simplest, yet most effective tools to secure your login.

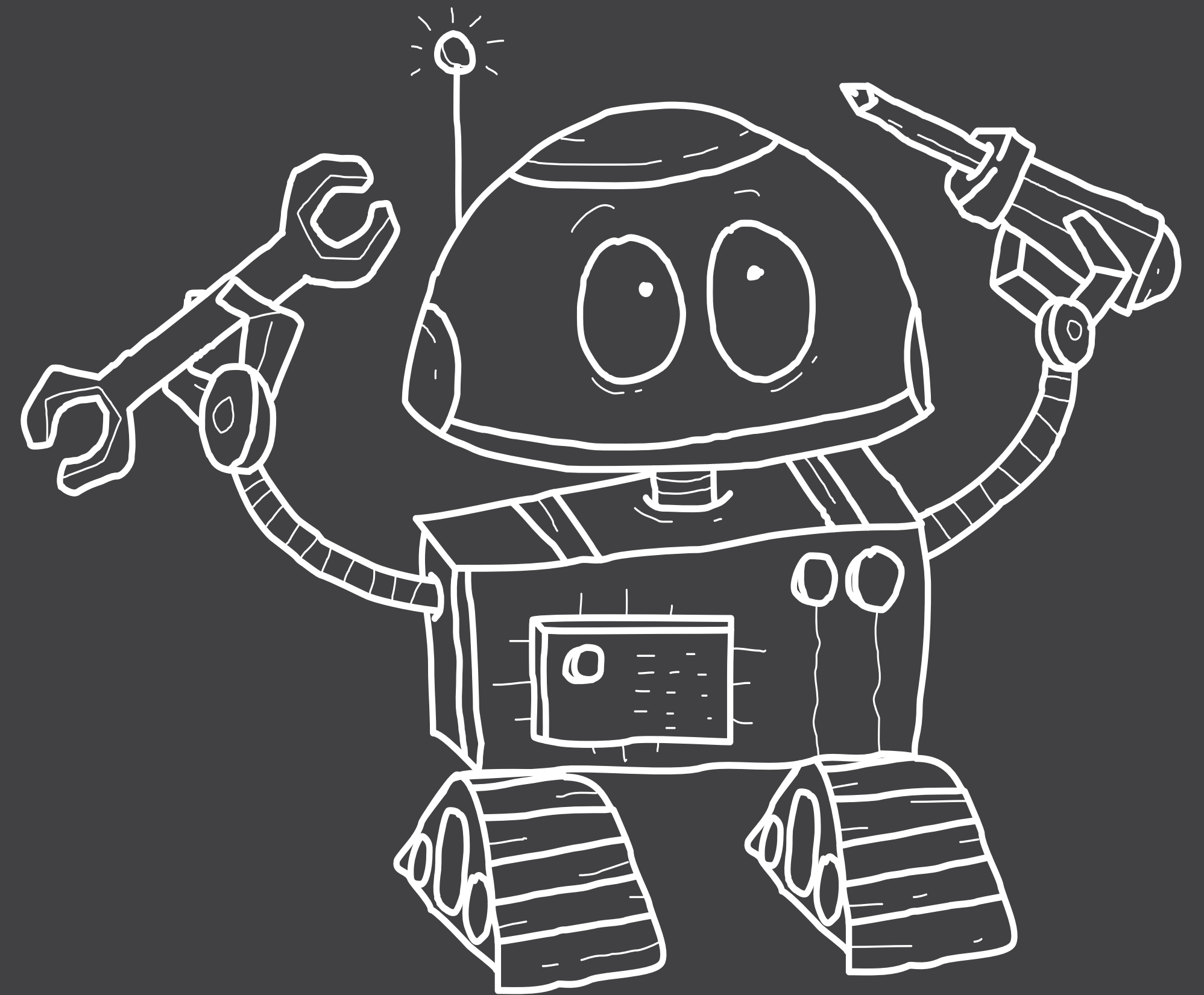
Plugins that can do this:

- Security plugin e.g. WordFence
- Google Authenticator



Tip

Do you have
a backup
solution?



How can I backup?



Plugins

Use a plugin like UpdraftPlus or Backup Buddy

Paid Services

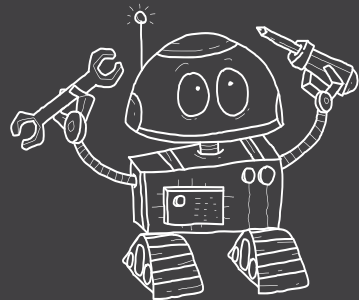
Use paid services such as BlogVault/VaultPress



Hosting Provider

Not all hosting providers have backups.
Check this is activated and working.

Don't rely on just your hosting provider backups.
keep your own copy.



Pro Tip

Know how to restore from a backup. Don't want your site to crash and not sure what steps to take to restore your website.



How often should I backup?



Daily Backups

Good for basic sites

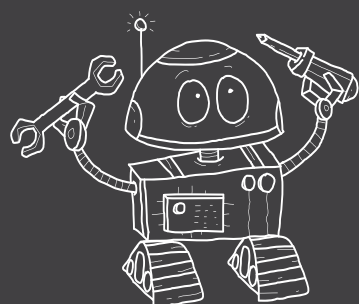
Hourly/Real Time Backups

Good for WooCommerce Sites - keep customer orders and data history



Restore

You can restore when something goes wrong.

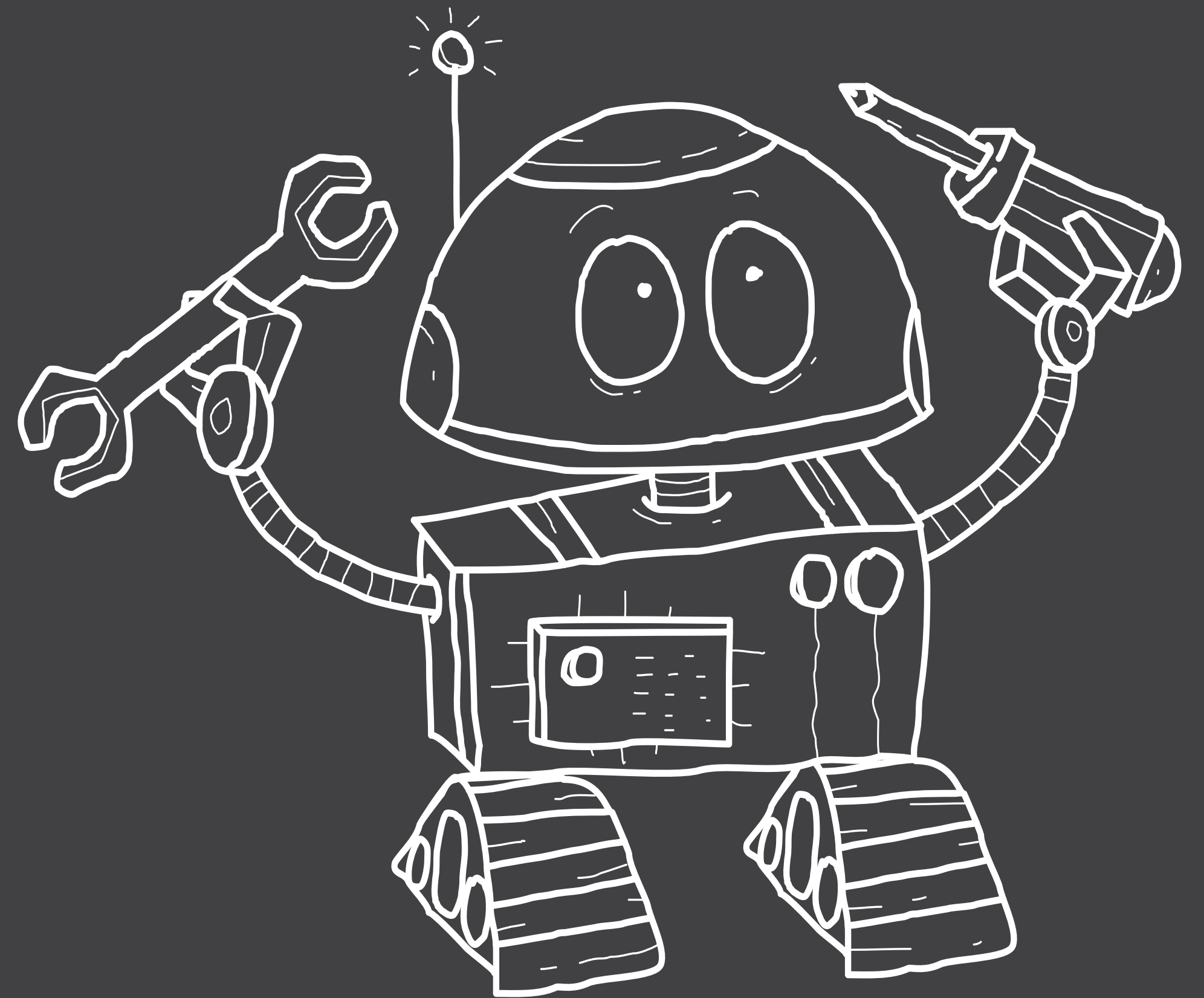


Pro Tip

You can never have enough backups!

Tip

Is your software
updated?



Get all the essential logins



Before you start your maintenance, it's important you get **all the core logins** for your website.

Domain Login:

Username and Password for where your domain is registered e.g. Netregistry

Hosting Login:

Where your website is hosted. e.g. WP Engine, Ventra IP etc. Find your login and check you also have access to your cPanel and FTP login.

WordPress Login:

Administrator login for your WordPress website to perform the updates.

Pro Plugins and Themes:

For example Elegant themes, Elementor Pro, WP Rocket, WooCommerce, ThemeForest etc.

Technical Details

URL/Website Address	https://
Login URL	https://
Username	Username
Password	Password
Hosting Provider	Hosting Provider Name
Server IP Address	1.1.1.1
Domain Registrar	Domain Registrar Name
DNS Records	DNS Provider Name
Email Provider	Email Provider Name
Content Delivery Network (CDN)	CDN Provider Name
Content Management System	WordPress
Theme	Theme Name
Premium (Paid) Software	Plugin 1 Plugin 2 Plugin 3 Plugin 4 Plugin 5 Plugin 6 Plugin 7

Have a Process / Checklist to follow



Have a process / checklist to follow

Ensures you don't miss steps

Update Weekly / Monthly

e.g. Wednesdays - low traffic, support available if needed. If you leave it to a Friday, you might loose the weekend troubleshooting.

Staging site

If you have a complex site or one that could potentially break, consider testing updates on a staging site before doing them on your live site.

Regular updates

Don't leave updates for too long as they may get harder and hard to update.



3 Different Types of Updates



Functional Releases

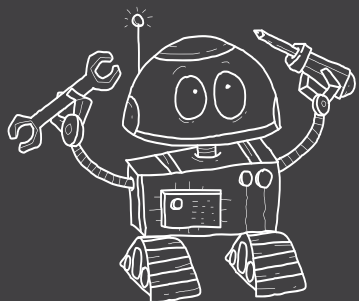
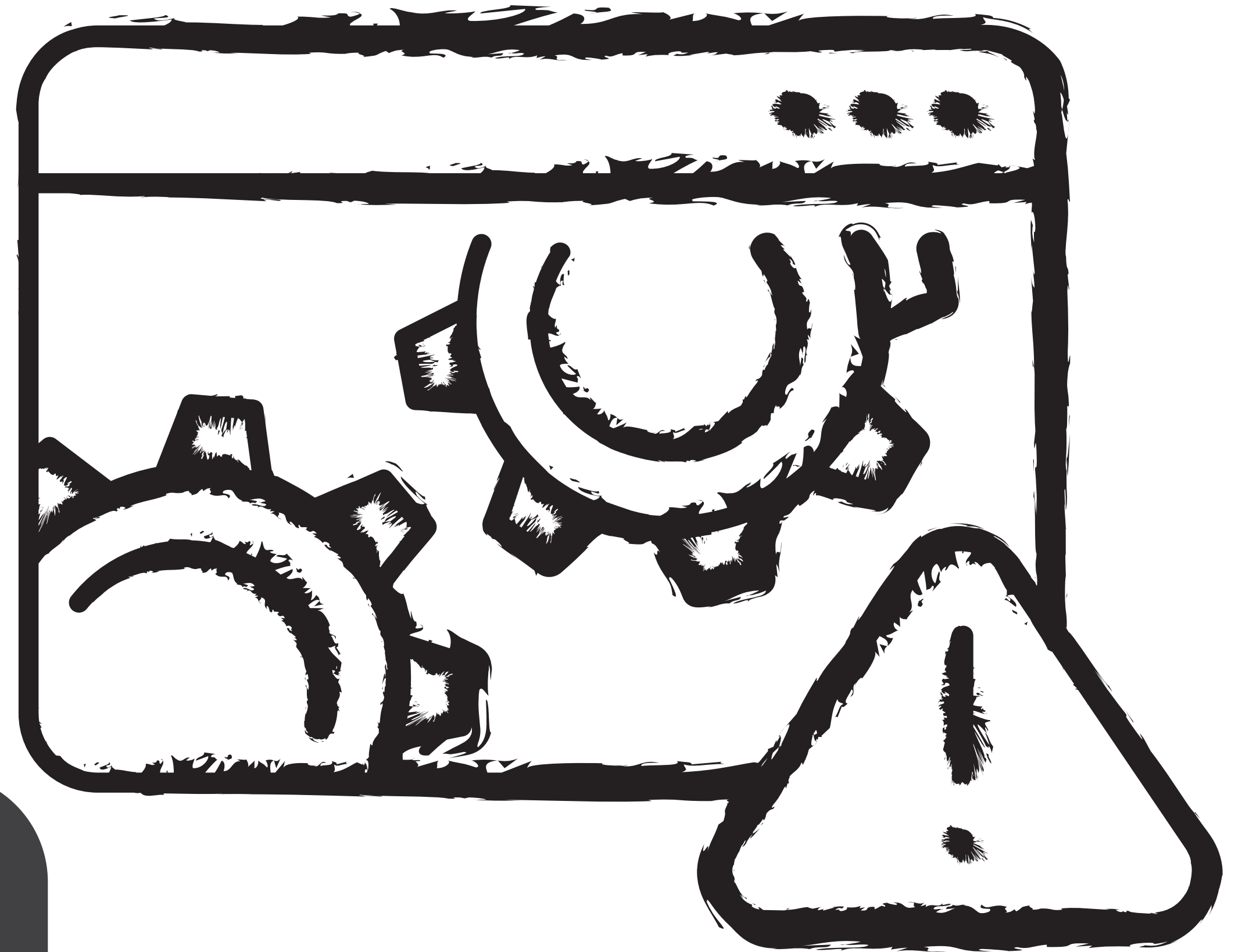
Updates adds features and options.

Maintenance Releases

These updates are generally minor updates fixing bugs that have already been reported.

Security Releases

These updates contain security to repair a vulnerability in the plugin, theme or WordPress core. (update ASAP)



Pro Tip

Security plugins like WordFence and iThemes Security will let you know when there is a vulnerability.



Update Plugins

Check if there are plugins that need updating and if there are any notices.

Manual Updates

Some plugins may need to be updated via FTP - easier if you can activate licenses for updates.

Remove unused plugins

Remove inactive or unused plugins. Audit your plugins and see what doesn't need to be there anymore.

Dashboard

Home

Updates 12

Insights

Elementor

Settings | Deactivate

The Elementor Website Builder has it all: drag and drop page builder, pixel perfect design, mobile responsive editing, and more. Get started now!

Version 3.2.5 | By [Elementor.com](#) | [View details](#) | [Docs & FAQs](#) | [Video Tutorials](#)

There is a new version of Elementor available. [View version 3.3.1 details](#) or [update now](#).

Heads up, Please backup before upgrade!

The latest update includes some substantial changes across different areas of the plugin. We highly recommend you [backup your site before upgrading](#), and make sure you first update in a staging environment

Compatibility Alert - Some of the plugins you're using have not been tested with the latest version of Elementor (3.3.1). To avoid issues, make sure they are all up to date and compatible before updating Elementor.

Plugin	Tested up to Elementor version
Elementor Pro	3.2.0
Ultimate Addons for Elementor	3.2.4
JetElements For Elementor	Unknown
JetTabs For Elementor	Unknown

Smart Robbie Masterclass | [smartrobbie.com.au](#)

Activate Licenses



Add your license to premium plugins and themes

This will make it easier for you to update the software. Otherwise you will need to do it manually via FTP.

License Settings

Status: **Active**

[My Account](#)

You're connected as **robyn@smartrobbie.com.au**. Want to activate this website by a different license?

[Switch Account](#)

Want to deactivate the license for any reason?

[Disconnect](#)

☐ **JetElements For Elementor**

[Deactivate](#)

Brand new addon for Elementor Page builder. It provides the set of modules to create different kinds of content, adds custom modules to your website and applies attractive styles in the matter of several clicks!

Version 2.5.5 | By [Crocoblock](#) | [View details](#)

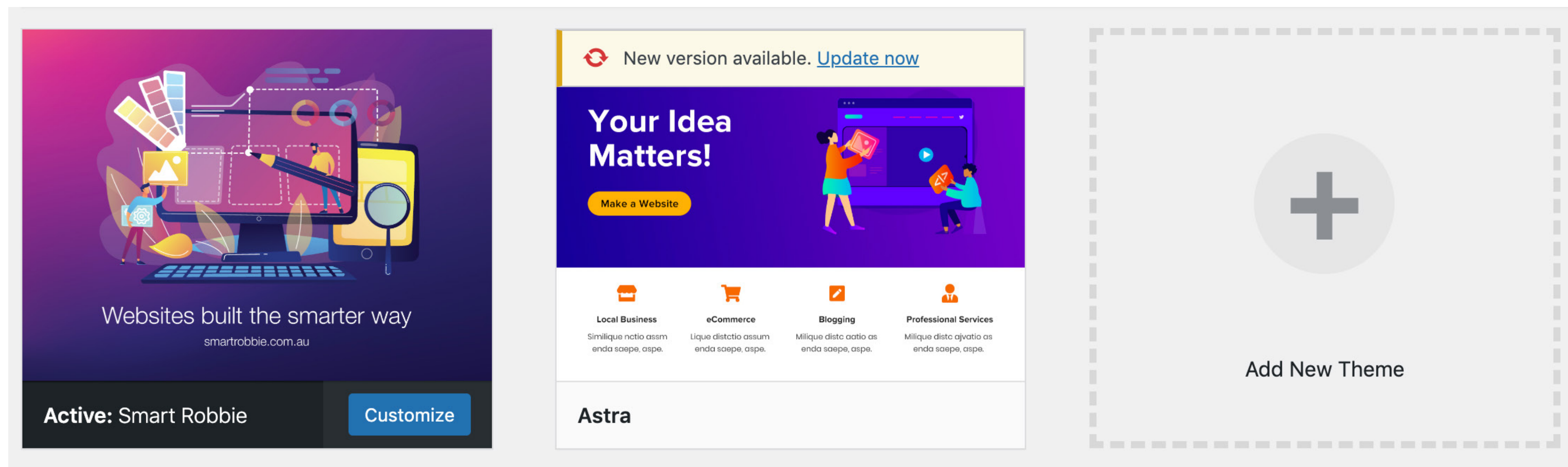
 There is a new version of JetElements For Elementor available. [View version 2.5.8 details](#). Automatic update is unavailable for this plugin. [Activate your license for automatic updates.](#)

Update Themes

Ensure you have a child theme active.

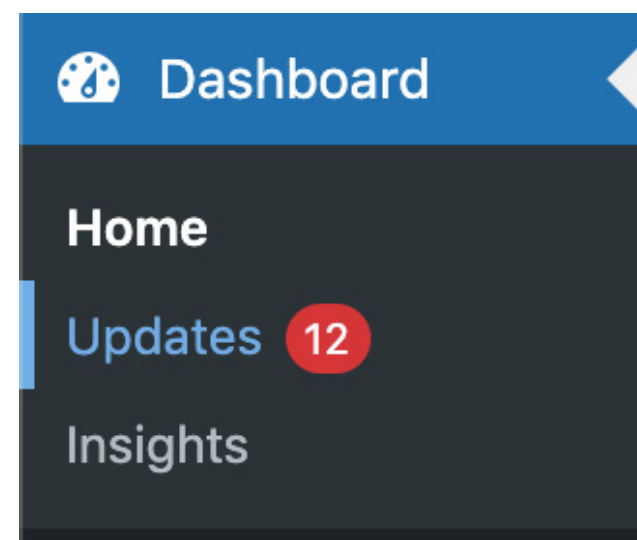
Remove Un-used Themes

One less thing to worry about, remove unused themes.



Update WordPress Core

Become familiar with what is a minor or major update.



[WordPress 5.7.2](#) is available! [Please update now.](#)

An updated version of WordPress is available.

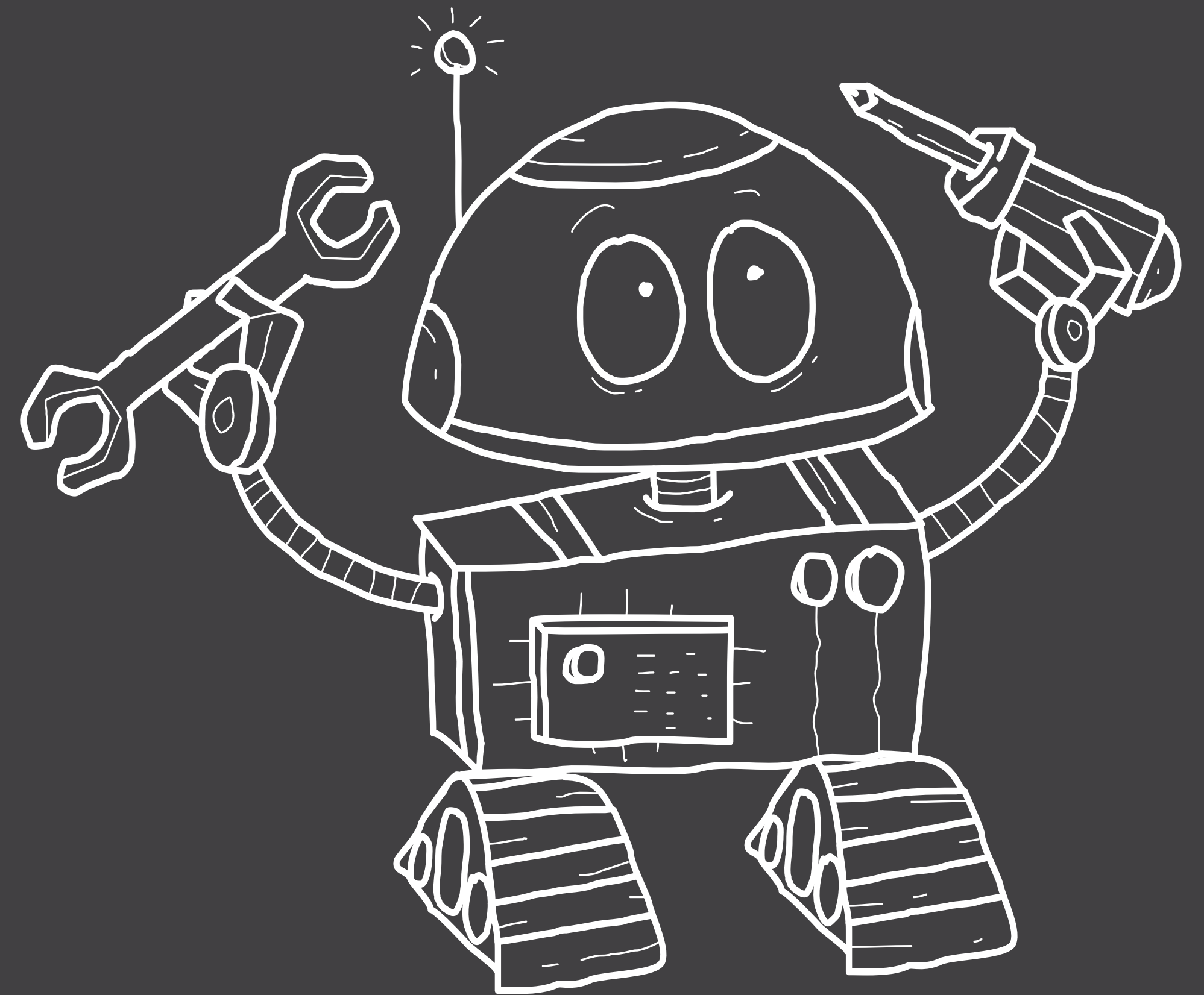
You can update to [WordPress 5.7.2-en_US](#) automatically:

[Update Now](#)

While your site is being updated, it will be in maintenance mode. As soon as your updates are complete, this mode will be deactivated.

Tip

Hosting



What type of hosting do you have?



Where is your site hosted?

Having a good hosting provider is important.

Is it on a shared server?

Is it cheap?

Do they provide backups?

Latest PHP version are you running?

Do they provide support?

The Benefits of Managed Wordpress Hosting



Specifically Optimized
for WordPress



Auto-updates



Bulletproof
Security



Super Speed



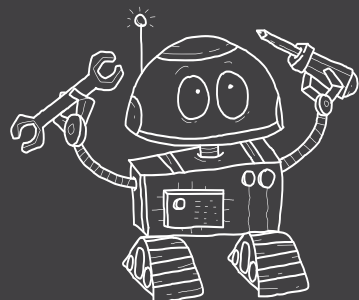
Auto-backups



24/7 Support



Flexible & Scalable
for Huge Traffic

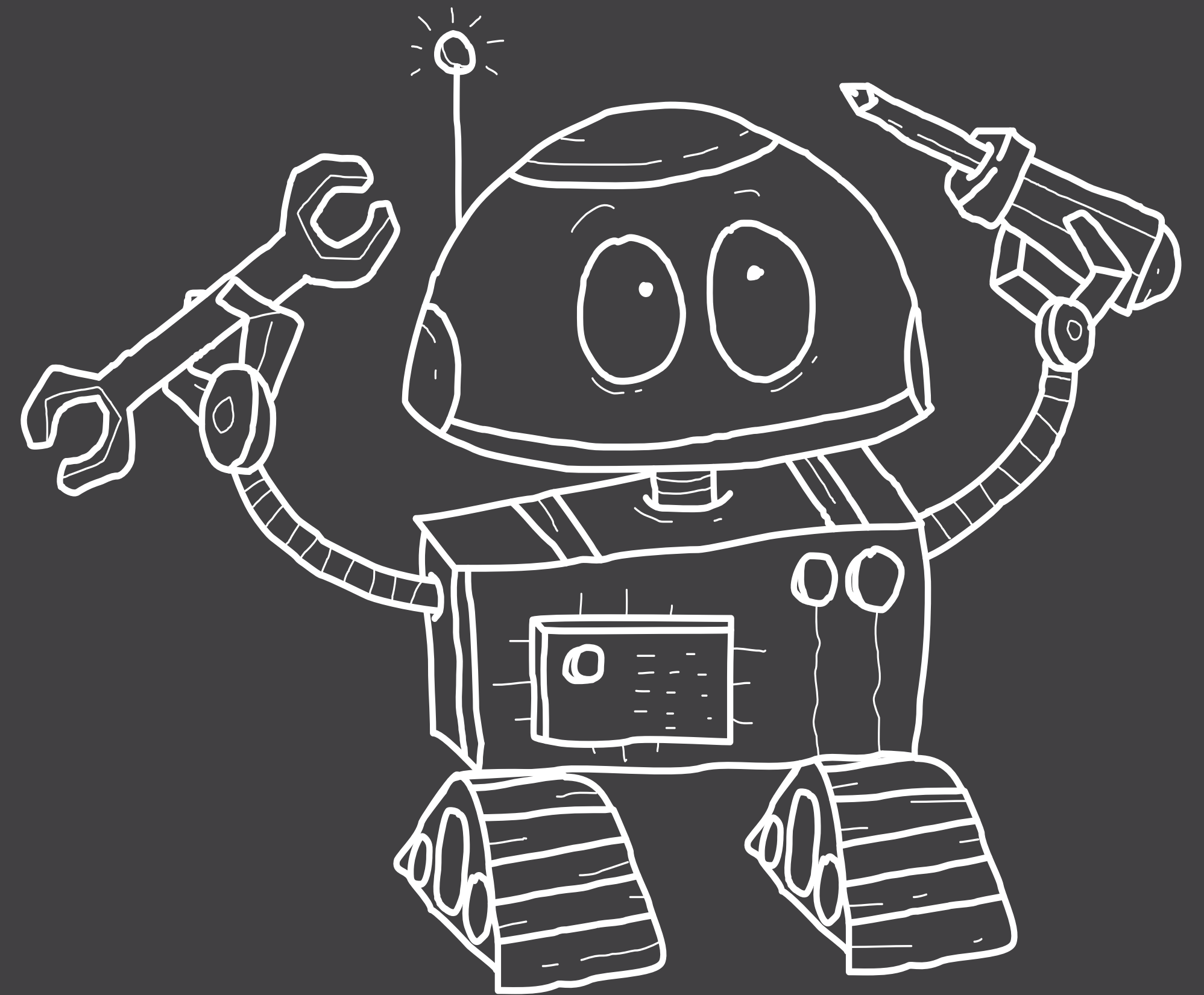


My recommendations:

WP Engine, Ventra IP, Siteground

Tip

SSL Certificate



Limit your login attempts



SSL Certificate

SSL (Secure Sockets Layer) is the technology that encrypts connections between your website and visitors' web browsers, ensuring that the traffic between your site and your visitors' computers is safe from unwelcome interceptions.

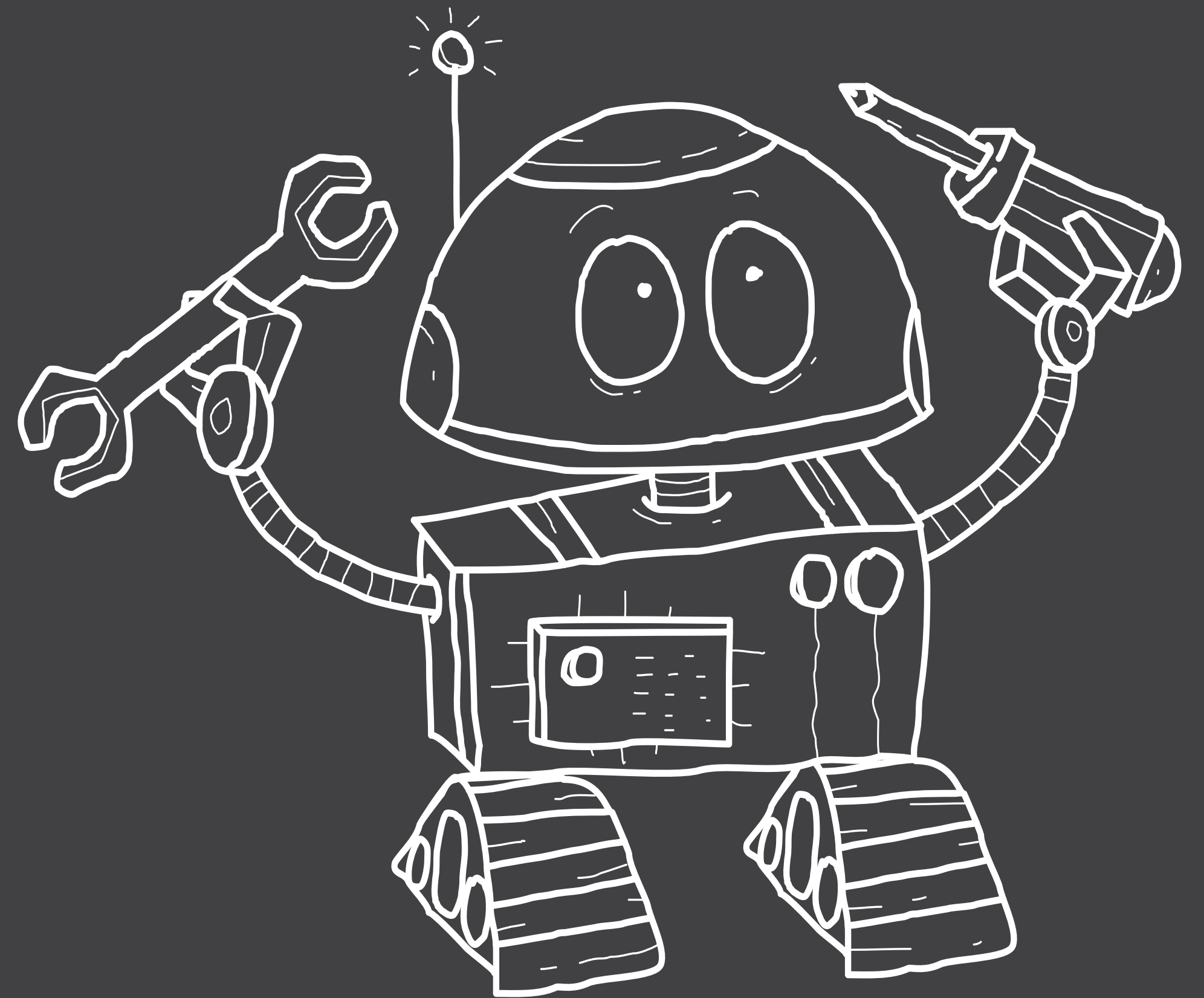
Not only will it boost SEO, but it also plays directly into your visitors' first impression of your website. Google Chrome will even warn users if the site they're visiting doesn't follow the SSL protocol, which directly reduces website traffic.

If the homepage URL begins with "https://" (the "s" stands for "secure"), your connection is secured with SSL. If the URL begins with "http://", you'll need to obtain an SSL certificate for your website.



Tip

Have a
security plugin

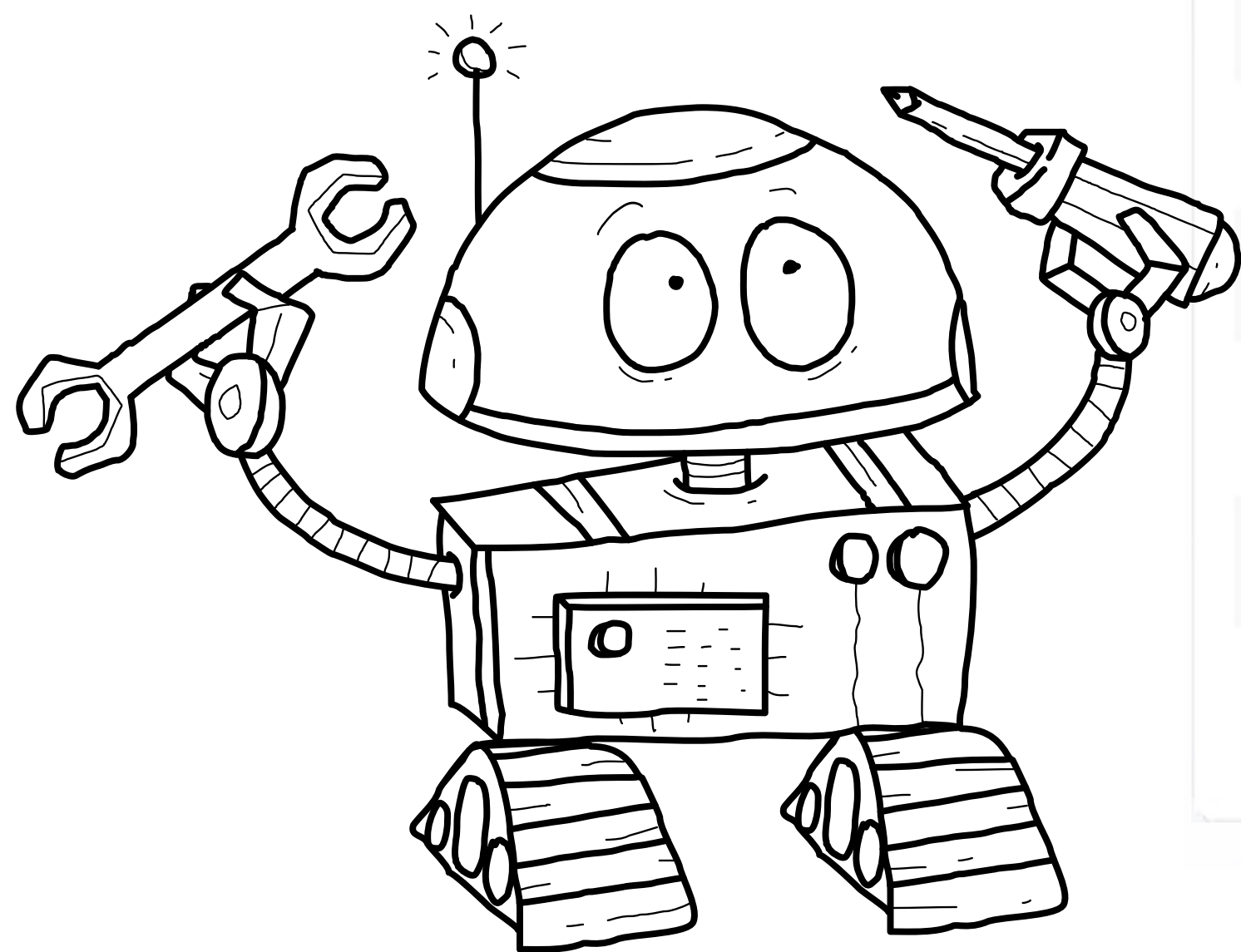


Security Plugins



Security plugins we love:

- WordFence
- iThemes Security
- WPScan



Plugins		
Name	Vulnerabilities	
✓ Akismet Anti-Spam Version 4.1.8	No known vulnerabilities found to affect this version	
✓ Controlled Admin Access Version 1.5.2	No known vulnerabilities found to affect this version	
! Give - Donation Plugin Version 2.9.7	High	GiveWP < 2.10.0 - Reflected Cross Site Scripting (XSS) - Fixed in version 2.10.0
✓ Hello Dolly Version 1.7.2	No known vulnerabilities found to affect this version	
✓ Log HTTP Requests Version 1.2	No known vulnerabilities found to affect this version	
! PhastPress Version 1.110	Medium	PhastPress < 1.111 - Open Redirect - Fixed in version 1.111
✓ Tawk.to Live Chat Version 0.4.1	No known vulnerabilities found to affect this version	
! Web-Stat Version 1.1.8	High	Web-Stat < 1.4.1 - API Key Disclosure - Fixed in version 1.4.1

Security Checks



Use plugins such as WordFence or iThemes Security to review any security issues that your site may have.

Check for any Flags

In particular critical updates.

Are plugins abandoned?

These plugins may not have alerts for vulnerability.

Run a extra security scan

You can run your site through Sucuri for a free check: <https://sitecheck.sucuri.net/>


















Username/Passwords

Use unique usernames and strong passwords

Good hosting

A good hosting provider will also help monitor any security vulnerabilities.

Also good plugin developers will also send you alerts e.g. WooCommerce.

Results Found (14)		Ignored Results (0)		DELETE ALL DELETABLE FILES		REPAIR ALL REPAIRABLE FILES								
Posts, Comments, & Files		0	Themes & Plugins		0	Users Checked		0	URLs Checked		0	Results Found		14
<div><div></div><div><p>The Plugin "WPBakery Page Builder" needs an upgrade (5.5.5 -> 6.7). Type: Plugin Upgrade</p></div><div><p>Issue Found July 20, 2021 11:22 pm ● Critical</p></div><div><div> IGNORE</div><div> DETAILS</div></div></div>														
<div><div></div><div><p>Need help with a hacked website? Our team of security experts will clean the infection and remove malicious content. Once your site is restored we will provide a detailed report of our findings. Includes a 1-year Wordfence Premium license.</p></div><div><div>GET HELP</div></div></div>														
<div><div></div><div><p>WordPress core file modified: wp-includes/default-constants.php Type: File</p></div><div><p>Issue Found July 19, 2021 6:15 pm ● High</p></div><div><div> REPAIR</div><div> IGNORE</div><div> DETAILS</div></div></div>														
<div><div></div><div><p>Your WordPress version is out of date Type: Core Upgrade</p></div><div><p>Issue Found July 20, 2021 11:22 pm ● High</p></div><div><div> IGNORE</div><div> DETAILS</div></div></div>														
<div><div></div><div><p>The Plugin "SEO Auto Image Tags" appears to be abandoned (updated October 31, 2017, tested to WP 4.8.17). Type: Plugin Abandoned</p></div><div><p>Issue Found July 19, 2021 6:35 pm ● Medium</p></div><div><div> IGNORE</div><div> DETAILS</div></div></div>														
<div><div></div><div><p>The Plugin "Contact Form 7" needs an upgrade (5.4.1 -> 5.4.2). Type: Plugin Upgrade</p></div><div><p>Issue Found July 20, 2021 11:22 pm ● Medium</p></div><div><div> IGNORE</div><div> DETAILS</div></div></div>														

Thank You

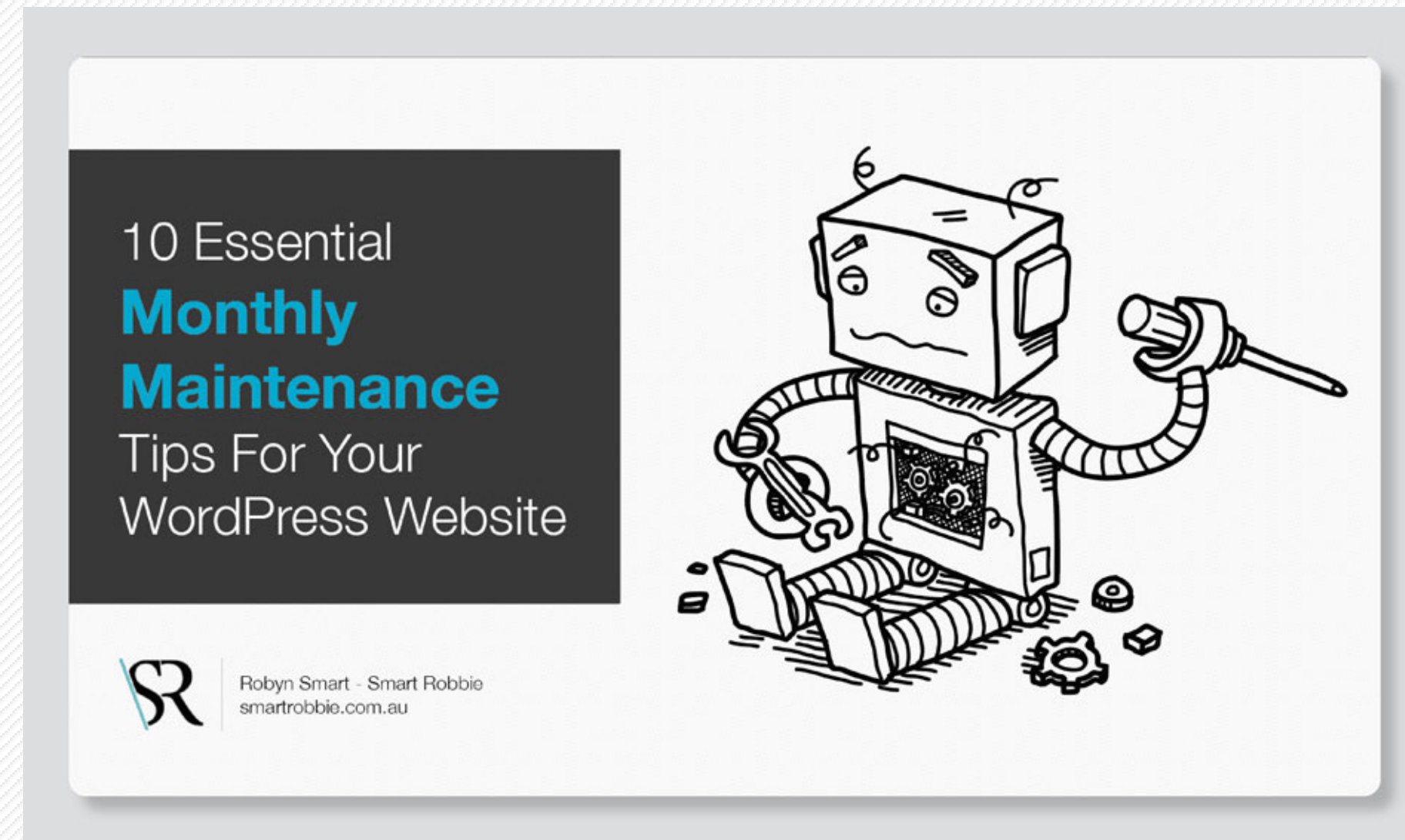


Thank you!

If you want to learn more from me,
feel free to go to:
Smartrobbie.com.au

Robyn

Director and Developer,
Smart Robbie



Visit the link below for additional resources:

Free 10 Essential Monthly Maintenance Tips for your WordPress Website
50% off our Performance and Security Assessment

<https://smartrobbie.com.au/security-masterclass/>