ithemes PRESENTS

THE ULTIMATE GUIDE TO WORDPRESS SECURITY IN 2020

+ TIPS FOR STAYING SECURE WHILE WORKING FROM HOME

TABLE OF CONTENTS

PART 1: GETTING STARTED WITH

WORDPRESS SECURITY IN 2020

WordPress security shouldn’t be so complicated that people are too intimidated to get started. Having the correct security measures in place is crucial to the success of any website and you can get started today.

The truth is, most hacks can be prevented with a few simple security measures. Let's take a look at some things that you can do to lock down your site.

KEYS TO A SUCCESSFUL WORDPRESS SECURITY STRATEGY

There are 4 keys to a successful WordPress security strategy.

1. Account Login Security
2. Security Monitoring
3. Plugin & Theme Management
4. Website Backup Strategy

ACCOUNT LOGIN SECURITY

The great thing about WordPress is how it makes creating a website accessible to just about anyone. But with that accessibility comes predictability. Anyone with experience working with WordPress knows where changes to the site are made: via the wp-admin area. They know where they need to go to access the **wp-admin**, the **wp-login.php** page.

By default, the WordPress login URL is the same for every WordPress site, and it doesn't require any special permissions to access. That's why the WordPress login page is the most attacked—and potentially vulnerable—part of any WordPress site.

“

BY DEFAULT, THE WORDPRESS LOGIN URL IS THE SAME FOR EVERY WORDPRESS SITE, AND IT DOESN’T REQUIRE ANY SPECIAL PERMISSIONS TO ACCESS. THAT’S WHY THE WORDPRESS LOGIN PAGE IS THE MOST ATTACKED—AND POTENTIALLY VULNERABLE—PART OF ANY WORDPRESS SITE.

”

HOW TO SECURE YOUR WORDPRESS LOGIN ACCOUNT

So what should you do? Here's a few tips to increase the security of your WordPress login account.

1. USE STRONG PASSWORDS

There is a lot of confusing and contradicting information about password security best practices on the internet. In an effort to clear up that confusion, let's break down the basics of how using a strong password improves your WordPress security.

Whenever creating a password, the first item that you will want to consider is the length of the password. The list below shows the estimated time it takes to crack a password using a four-core i5 processor.

The number of characters in your password matters! Take a look at these stats.

- 7 characters will take .29 milliseconds to crack.
- 8 characters will take 5 hours to crack.
- 9 characters will take 4 months to crack.
- 10 characters will take 1 decade to crack
- 12 characters will take 2 centuries to crack.

So as you can see, adding a single character to your password can significantly increase the security of your login. A password that it is at least 12 characters long, random and includes a large pool of characters like “lSt8XXa!28X3” will make it very difficult to crack.

Unfortunately, some hackers are leveraging GPUs and stronger CPUs to decrease the amount of time needed to crack passwords. So to strengthen your logins, also be mindful of your password entropy. The higher the password entropy is, the more difficult the password will be to crack.

For example, based on just the length requirement, a password like “abcdefghijkl” is 12 characters, which is great and should take 200 years to crack. However, since the password uses sequential strings of letters, it makes the password much more predictable compared with a password like “rfybolaawtpm” which has randomized characters.

Randomizing characters decreases the predictability and increases the strength of the password. But both of these passwords have one thing in common that ultimately reduces the password entropy. Both are only using lower case letters, limiting the pool of possible characters to 26. That’s why it’s vital to include alphanumeric, upper-case letters and common ASCII characters to increase the pool of characters needed to crack the password to 92.

A password that is at least 12 characters long, random and includes a large pool of characters like “lSt8XXa!28X3” will make it very difficult to crack.

2. REFUSE COMPROMISED PASSWORDS

Attackers often use compromised passwords as a starting point for hacking accounts because it is faster and easier than brute-forcing all possible password combinations. If your password has been exposed and you're reusing your credentials across multiple websites, attackers could compromise your account in just one or two attempts instead of millions.

A data breach is typically a list of usernames, passwords and often other personal data that was exposed when a site was compromised. Recently, Troy Hunt, creator of the haveibeenpwned API, reported on his blog about the "Collection #1" Data Breach. This data breach contained a staggering 1,160,253,228 unique combinations of email addresses and passwords.

iThemes Security Pro leverages the power of the haveibeenpwned API to prevent the use of known compromised passwords on your WordPress website. If your password was found in a data breach, iThemes Security will require you to update your account's password immediately.

If your password has been exposed and you're reusing your credentials across multiple websites, attackers could compromise your account in just one or two attempts instead of millions.

3. USE A UNIQUE PASSWORD FOR EVERY ACCOUNT

Another best practice for online security is using unique passwords for every account and website login you have. This is so important, we'll say it again: you should be using a different password for every site.

The more users you have that are reusing passwords, the weaker your WordPress login security will be. In a list compiled by Splash Data, the most common password included in all data dumps was 123456. The WordPress login security of your site is only as strong as the weakest link, so be proactive with strong password requirements.

Ultimately, using a password manager can help you keep track of your logins and unique passwords. With the help of a password manager, you don't have to remember your passwords.

“

THIS IS SO IMPORTANT, WE’LL SAY IT AGAIN: YOU SHOULD BE USING A DIFFERENT PASSWORD FOR EVERY SITE. WHY? IF YOUR PASSWORD HAS BEEN EXPOSED AND YOU’RE REUSING YOUR CREDENTIALS ACROSS MULTIPLE WEBSITES, ATTACKERS COULD COMPROMISE YOUR ACCOUNT IN JUST ONE OR TWO ATTEMPTS INSTEAD OF MILLIONS.

”

4. LIMIT LOGIN ATTEMPTS

By default, there isn't anything built into WordPress to limit the number of failed login attempts someone can make. Without a limit on the number failed login attempts an attacker can make, they can keep trying an endless number of usernames and passwords until they are successful.

Increase your WordPress login security by installing a WordPress security plugin like iThemes Security Pro to limit the number of failed login attempts. The iThemes Security Pro WordPress Brute Force Protection feature gives you the power to set the number of allowed failed login attempts before a username or IP is locked out.

A lockout will temporarily disable the attacker's ability to make login attempts. Once the attackers have been locked out three times, they will be banned from even viewing the site.

5. LIMIT OUTSIDE AUTHENTICATION ATTEMPTS PER REQUEST

There are other ways to log into WordPress besides using a login form. Using XML-RPC, an attacker can make hundreds of username and password attempts in a single HTTP request.

The brute force amplification method allows attackers to make thousands of username and password attempts using XML-RPC in just a few HTTP requests. When you know an attacker can use database dumps as a starting point and make thousands of guesses per request, it makes the importance of WordPress login security much clearer.

In addition, when you are developing your WordPress login security plan, it is important to be aware that the WordPress Rest API adds additional ways to authenticate a WordPress user.

Cookie authentication is one method authentication when you login WordPress automatically stores a cookie so plugins and themes can perform a function on your behalf. Cookie authentication will benefit from the protections you have added to the wp-login.php.

6. USE TWO-FACTOR AUTHENTICATION

We saved the best way method to increase WordPress login security for last: WordPress two-factor authentication. Two-factor authentication requires an extra code along with your WordPress username and password to log in.

There are many methods of two-factor authentication, but not all methods are created equal. If you can, avoid using text for two-factor authentication. The National Institute of Standards and Technology no longer recommends using SMS to send and receive authentication codes.

Using a WordPress security plugin, like iThemes Security Pro, you should enable either the email or mobile app method of two-factor.

Just note that many sites require you to use an email address as a username. If an attacker hacks one of these sites, the next step will be to try to log into email accounts using the new email addresses and passwords they stole. If one of your users or clients are reusing compromised passwords on every site, their email account, along with their two-factor email codes, will be compromised.

7. PASSWORDLESS LOGINS

Passwordless login is a new way to verify a user's identity without actually requiring a password to login. Passwordless login is both safe and simple, increasing the likelihood that the average person will secure their account. Passwordless logins lock down your accounts and are much easier to use than traditional credentials.

You may already be using a form of passwordless login without realizing it. For example, if you are using a thumbprint or Face ID to open your phone, you are using a form of passwordless login. Keep in mind that a passwordless login doesn't necessarily mean a password isn't assigned to the user. Your phone still requires you to set a password or a PIN, but you do not need to enter it every time you unlock your phone.

There is a balance to WordPress security. You want your website to be secure while not getting in the way of your users and customers.

The Passwordless Login method provided by iThemes Security Pro will send you an email with a "magic link," or a link that will log you into WordPress with a click of a button. This way, the passwordless login requires you to have access to the actual email account associated with the user, providing another layer of security.

SECURITY MONITORING

Every day, activity takes place on your website that may indicate nefarious activity. What are these events and are you actively monitoring them? The next section will cover security monitoring on your website.

WORDPRESS SECURITY LOGS

WordPress security logs provide detailed data and insights about activity on your WordPress website. If you know what to look for in your logs, you can easily identify and stop malicious behavior on your site.

WordPress security logs have several benefits in your overall security strategy. If your site does get hacked, you will want to have the best information to aide in a quick investigation and recovery.

Here are a few ways WordPress security logging helps with your security monitoring strategy:

1. Identity and stop malicious behavior.
2. Spot activity that can alert you of a breach.
3. Assess how much damage was done.
4. Aide in the repair of a hacked site.

Now let's talk about what acitvity you should monitor.

“

IF YOUR SITE DOES GET HACKED, YOU WILL WANT TO HAVE THE BEST INFORMATION TO AIDE IN A QUICK INVESTIGATION AND RECOVERY.

”

1. BRUTE FORCE ATTACKS

Brute force attacks refer to the trial and error method used to discover usernames and passwords in order to hack into a website. WordPress doesn't track any user login activity, so there isn't anything built into WordPress to protect you from a brute force attack. It is up to you to monitor your login security to protect your WordPress site.

Luckily, a brute force attack isn't very sophisticated, and it is pretty easy to identify in your logs. You will need to record the username and IP that is attempting to login and whether or not the login was successful. If you see that a single username or IP has consecutive multiple failed login attempts, the chances are you are under a brute force attacks.

The iThemes Security Pro's Local Brute Force Protection feature automatically monitors failed login attempts and blocks brute force attacks.

2. FILE CHANGES

Even if you follow WordPress security best practices, there is still a chance for your site to become compromised. A compromise means the site has had malicious changes, and that is why is it is so important to stay on top of the file changes on your site by recording them in your WordPress security logs.

File change entries include files added and removed and modifications to existing files. Now that you have the changes recorded in your security logs, you should schedule the time to audit them. If you are an iThemes Security Pro user, remember to enable File Change notifications to be notified when a file changes.

There are several legitimate reasons you would see new file change activity in your logs, but if the changes made were unexpected, you should take the time to assure the changes were not malicious. For example, if you see a change made to a plugin at the same date and time you updated the plugin, there would be no reason to investigate.

3. MALWARE SCANS

Not only should you run malware scans, you should also be recording the results of every malware scan in your WordPress security logs. Some security logs will only record scan results that fund malware, but that isn't enough. It is crucial to be alerted as quickly as possible of a breach to your site. The longer it takes for you to know about a hack the more damage it will do.

While it feels good to see the history of a proactive approach to security paying off, that is just a bonus and not the reason to record malware scans. If you aren't documenting your scheduled scans, then you will have no way of knowing if there are any scan failures.

Not recording failed scans could result in you thinking that your site is being checked daily for malware but, in reality, the scan is failing to complete.

4. USER ACTIVITY

Keeping a record of user activity in your WordPress security logs can be your saving grace after a successful attack.

1. Logins & Logouts (+ When & Where) - The first type of user activity you should track is when users log in and log out of your site and from where. Monitoring time and location of user's logins can help you spot a user that is compromised. Did that user login at an unusual time or from a new place? If so, you may want to start your investigation with them.

2. New Users - The next activity you should keep a record of is user creation. A common practice for a hacker to perform is to create a new admin user in an attempt to be covert. It is easy for you to notice something strange with your account but it is much more difficult to identify malicious activity on another user.

3. Add/Remove Plugins - We should now check to see if the new user has added or removed any plugins from the site. It is vital to make a record of who adds and removes plugins. Once your site has been hacked, it will easy for the attacker to add their own custom plugin to inject malicious code into the site. Even if they don't have access to your server, your WordPress site can access it. Using a plugin they can add redirects to your site to use in their next spamvertizement campaign. After their malicious code is executed, they can then delete the plugin to remove evidence of their crime. Lucky for us we won't miss any of it because it was all documented in our WordPress security logs.

4. Add/Edit Pages - Now it is time to look to see if our new user has added any new or made changes to existing pages or posts on the site. Have they added links to send your traffic to other sites? You will be able to see if any embarrassing pages have been added to the site and get them taken down.

PLUGIN & THEMES MANAGEMENT

Plugin and theme management play a big role in the health of your site. In this section, we'll cover what that means.

1. UPDATE EVERYTHING

When your WordPress site is running outdated versions of plugins, themes or WordPress, you run the risk of having known exploits on your site.Updates are not just for new features or bug fixes; they can also include security patches for known exploits. Even though this is the easiest of the WordPress security vulnerabilities to prevent, most successful hacks use exploits that are found in outdated software.

You can automate updates on your site Using the iThemes Security Pro WordPress version management feature. Automating your updates ensures you get the critical security patches that protect your site against WordPress security vulnerabilities and as a bonus, it reduces the amount of time you spend maintaining your WordPress site.

Keep everything on your site updated. 60% of breaches involved vulnerabilities for which a patch was available but not applied.

1. AUTOMATICALLY PATCH KNOWN VULNERABILITIES

Having software with known vulnerabilities installed on your site gives hackers the blueprints they need to take over your site. It is hard to keep track of every disclosed WordPress vulnerability and compare that list to the versions of plugins and themes you have installed on your site.

The improved WordPress Security Site Scan powered by iThemes performs automatic checks for known vulnerabilities installed on your site. And if a patch is available, iThemes Security Pro will now automatically apply the fix for you.

2. REMOVE UNUSED PLUGIN & THEMES

The PHP code on your WordPress site should also be included in the WordPress security vulnerabilities list. Exploiting PHP code is a common method used by hackers to gain access to your WordPress site, so it is crucial you reduce the risk by limiting exploit opportunities. Uninstall and completely delete any unnecessary plugins and themes on your WordPress site to limit the number of access points and executable code on your website.

In addition, avoid using abandoned WordPress plugins. If any plugin installed on your WordPress site has not received an update in six months or longer, you may want to make sure it hasn't been abandoned. A plugin not having any recent updates doesn't necessarily mean it has been abandoned, it could just mean it is feature complete and will only receive updates to ensure compatibility with the latest versions of WordPress and PHP.

3. ONLY INSTALL SOFTWARE FROM TRUSTED SOURCES

Only install WordPress plugins and themes from trusted sources. You should only install software that you get from WordPress.org, well-known commercial repositories or directly from reputable developers.

You will want to avoid “nulled” version of commercial plugins because they can contain malicious code. It doesn’t matter how you lock down your WordPress site if you are the one installing malware.

If the WordPress plugin or theme it isn’t being distributed on the developer’s website, you will want to do your due diligence before downloading the plugin. Reach out to the developers to see if they are in any way affiliated with the website that is offering their product at a free or discounted price.

Avoid “nulled” or bootleg version of premium plugins because they usually contain malicious code. It doesn’t matter how you lock down your WordPress site if you are the one installing malware.

“

AVOID “NULLED” OR BOOTLEG VERSION OF PREMIUM PLUGINS BECAUSE THEY USUALLY CONTAIN MALICIOUS CODE. IT DOESN’T MATTER HOW YOU LOCK DOWN YOUR WORDPRESS WEBSITE IF YOU ARE THE ONE INSTALLING MALWARE.

”

WORDPRESS SECURITY MYTHS

You'll find lots of security advice floating around the internet from well-intentioned people who genuinely want to help.

Unfortunately, some of this advice is built on WordPress security myths and don't actually add any additional security to your WordPress website. In fact, some WordPress security "tips" may increase the likelihood you will run into issues and conflicts.

We have plenty of WordPress security myths to choose from, but we are only going to focus on the top 5 we have consistently seen in over 20,000 support tickets. These conversations were used as a basis for the following criteria to select the top myths.

The Top 5 WP Security Myths

1. You Should Hide Your /wp-admin or /wp-login URL (Also Known As "Hide Backend")

The idea behind hiding the wp-admin is that hackers can't hack what they can't find. If your login URL isn't the standard WordPress /wp-admin/ URL, aren't you protected from brute force attacks?

The truth is that most Hide Backend features are simply security through obscurity, which isn't a bullet-proof security strategy. While hiding your backend wp-admin URL can help to mitigate some of the attacks on your login, this approach won't stop all of them.

2. You Should Hide Your /wp-admin or /wp-login URL (Also Known As Hide Backend)

The idea behind hiding the wp-admin is that hackers can't hack what they can't find. If your login URL isn't the standard WordPress /wp-admin/ URL, aren't you protected from brute force attacks?

The truth is that most Hide Backend features are simply security through obscurity, which isn't a bullet-proof security strategy. While hiding your backend wp-admin URL can help to mitigate some of the attacks on your login, this approach won't stop all of them.

3. You Should Hide your Theme Name and WordPress Version Number

If you use your browser's developer tools, you can pretty quickly see the theme name and WordPress version number running on a WordPress site. The theory behind hiding your theme name and WP version is that if attackers have this information they will have the blueprint to break into your site.

The problem with this myth is that there isn't an actual guy behind a keyboard looking for the perfect combination of theme and WordPress version number to attack. However, there are mindless bots that scour the internet looking for known vulnerabilities in the actual code running on your website, so hiding your theme name and WP version number won't protect you.

4. You Should Rename Your wp-content Directory

The wp-content directory contains your plugins, themes and media uploads folder. That is a ton of good stuff and executable code all in one directory, so it's understandable that people want to be proactive and secure this folder..

Unfortunately, it's a myth that changing the wp-content name will add an extra layer of security to the site. It won't. We can easily find the name of your changed wp-content directory by using the browser developer tools. Changing the name of the directory will not add any security to your site, but it can cause conflicts.

5. WordPress is an Insecure Platform

The most damaging WordPress security myth is that WordPress itself is insecure. This is simply not true. WordPress is the most popular content management systems in the world, and it didn't get that way by not taking security seriously.

The truth is that the biggest WordPress security vulnerability is its users. Most WordPress hacks on the platform can be avoided with a little effort from the site owners.

Keep in mind that the number one reason for successful WordPress hacks is outdated software. To get a patch for a security vulnerability, you have to keep things updated. WordPress even allows you to enable automatic updates so you don't have to manually run updates. But some people still don't make it a priority to update their sites on a regular schedule. So these sites are filled with outdated software that makes them ripe for attack. When a hacker uses a security hole it isn't a WordPress flaw, it is a user flaw.

“

THE TRUTH IS THAT THE BIGGEST WORDPRESS SECURITY VULNERABILITY IS ITS USERS. MOST WORDPRESS HACKS ON THE PLATFORM CAN BE AVOIDED WITH A LITTLE EFFORT FROM THE SITE OWNERS.

”

SIGNS OF WEBSITE INFECTION

Finding yourself asking “Is my WordPress site hacked?” means you’ll want some quick answers. In this post, we cover seven signs of infection and what to do if you discover you’ve been hacked.

The faster you notice the signs of a website breach, the quicker you can get your site cleaned up. The quicker you can get your website cleaned, the less damage the hack can do to your website.

Not all hacks have the same goal, so the signs of a website compromise will depend on the attackers motive. Here are 7 different symptoms you need to look out for when you are monitoring the health of your site.

1. Your Homepage is Different

Changes to your homepage seem like an obvious sign. But how many times do you actually run a thorough check or your homepage? I know I typically go straight to my login URL and not my home URL. From there, I log in, update my site or edit a post. After I finish what I came to do, I often leave without looking at my website’s home page.

The primary goal of some hacks is to troll a website or gain notoriety. So they only change your homepage to something they find funny or to leave a hacked by calling card.

2. Your Website Performance Has Dropped

Your site may feel sluggish when it has an infection. You can experience slowdowns on your website if you are experiencing brute force attacks or if there is a malicious script using your server resources for cryptocurrency mining. Similarly, a DDoS (or denial of service attack) happens when a network of IPs simultaneously sends requests to your website in an attempt to cause it to crash.

If your site is running slowly, check the server access logs for an unexpected number of requests. You can also use a web application firewall like the one provided by Sucuri to help protect your website against a DDoS attack.

3. Your Website Contains Malicious or Spam Popups Ads

There is a good chance a hacker has compromised your website if your visitors see popups that redirect them to a malicious website. The goal of this type of attack is to drive traffic away from your site to the attacker's site so they can target users with click fraud for Pay Per Click advertising. The most frustrating thing about this type of hack is you may not be able to see the popups. A popup hack can be designed to not show for logged in users, which decreases the odds of website owners seeing them. So even when the site owner logs out, the popups will never display.

Your view of the popups can also be limited if you use an ad blocker extension in your browser. For example, a customer reported a popup hack and shared screenshots and a video of the popups. After I spent hours running through their website, I was not able to recreate anything they were reporting. I was convinced that their personal computer had been hacked and not the website.

Finally, it dawned on me why I wasn't able to see the popups. I had installed an ad blocker extension on my browser. As soon as I disabled the ad blocker extension, I was able to see popups everywhere. I share this embarrassing story to hopefully save you from running into the same mistake.

4. You Notice a Decrease in Website Traffic

If you log into your Google Analytics account and you notice a steep decline in website traffic, your WordPress site could be hacked. A drop in site traffic deserves an investigation. There could be a malicious script on your site that is redirecting visitors away from your site or Google could already by blacklisting your website as a malicious site.

The first thing you want to look for is your website's outbound traffic.
By tracking your website with Google Analytics, , you will need to configure your site to track the traffic leaving your site. The easiest way to monitor outbound traffic on your WordPress site is to use a WordPress Google Analytics plugin. A good Google Analytics plugin will allow you to track specific activity with a click of a button.

5. Unexpected File Changes

If files on your website have been changed, added or removed, it could be a sign that your site has been compromised. That's why it is essential to have a notification system in place to alert you of website file changes. You can investigate any unexpected changes by comparing the changed file to a version in a recent backup.

Using a WordPress security plugin like iThemes Security can help you track file changes. Because of the number of notifications this setting can generate, you can exclude files and directories in the File Change Detection settings. It is okay to exclude directories that you know are going to be regularly updating. Backup and cache files are a perfect example of this and excluding them will reduce the number of notifications you will receive.

6. Unexpected New Admin Users

If your website has any unexpected registrations of new admin users, that's another sign your WordPress site has been hacked. Through an exploit of a compromised user, an attacker can create a new admin user. With their new admin privileges, the hacker is ready to cause some major damage to your site.

In November of 2018, we had several reports of new admin users being created on customer websites. Hackers used a vulnerability in the WP GDPR Compliance plugin
(vulnerability patched in version 1.4.3)
to create new admin users on WordPress sites running the plugin. The plugin exploit allowed unauthorized users to modify the user registration to change the default new-user role from a subscriber to an admin.
Unfortunately, this wasn't the only vulnerability and you can't just remove the new users the attacker created and patch the plugin.

If you had WP GDPR Compliance and WooCommerce installed, your site might have been injected with malicious code. The attackers were able to use the WooCommerce plugin background installer to insert a backdoor installer in the database.

7. Admin Users Removed
If you are unable to log into your WordPress site, even after a password reset, it may be a serious sign of infection.

When the Gentoo Github repo got hacked the first thing the attacker did was delete all admin users. So how did this hacker even get into their Github account? A Gentoo admin user's password was discovered on a different site. I am guessing that the username and password was discovered either through scraping or a database dump. Even though the admin's password for their Gentoo Github account was different than one used on the compromised account, it was very similar. So this would be like me using iAmAwesome2017 as a password on one account and iAmAwesome2019 on another site. So the hackers were able to figure out the password with a little effort.

You can also enable the Trusted Devices feature in iThemes Security Pro to restrict admin capabilities for logins from untrusted devices. If an attacker successfully logs into your site as an existing admin user–either by a brute force attack or if the user's credentials were part of a database dump–they will not have full admin capabilities.

Even with the password being compromised, this breach could have been prevented if the admin was using two-factor authentication. Two-Factor authentication requires an extra code along with your username and password credentials to log in. iThemes Security Pro allows you to enable WordPress two-factor using a mobile app or email to receive your access additional code.

WEBSITE RECOVERY

What should you do if your website is a complete loss? What if you've been hacked and you can't get back in? The easiest and fastest way to come back from a hack is to restore from a backup. Here are ten tips to create a backup strategy and peace of mind.

ELEMENTS OF A SOLID BACKUP STRATEGY

1. Choose a Backup Method - Find a dedicated backup solution like BackupBuddy.

2. Decide What to Backup - Your backups should include your plugins, themes. media, uploads and database.

3. Choose Your Backup Frequency - What is your tolerance for lost data. If you are making daily changes to your site, you should have daily backups.

4. Schedule and Automate - Find the best time to backup your site and then use a backup plugin to automate your backups.

5. Choose an Offsite Location to Store Your Backups - Store your backups in a different location than your site's server.

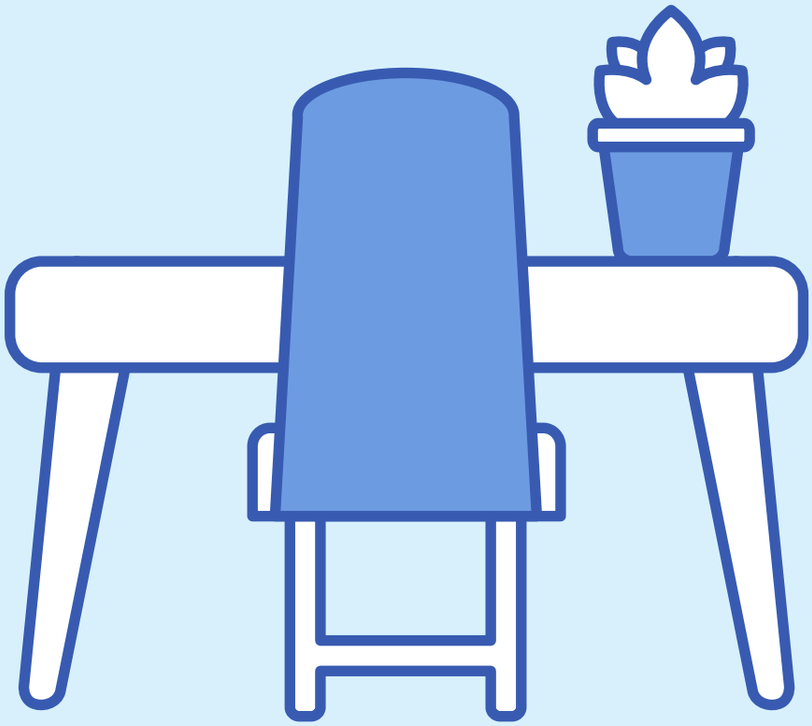
6. Scan Your Backups - If your backup is infected it won't help you to clean your site.

7. Audit Your Backup Schedules - It is important to do periodic checks to make sure your backup automations are still in working order.

8. Practice Restoring - When things go wrong, you will need to know how to use your backup to restore your site.

9. Know the Limitations of Your Environment - If you are on poor hosting make sure your backup strategy is right for your site.

10. Be Prepared to Migrate - Sometimes the problem is the host. Knowing how to move your site will give you the freedom to move when things go wrong.



PART 2: STAYING SECURE WHILE

WORKING FROM HOME

With more of us working from home than ever, it has never been more important to be vigilant of possible attacks.

Our friends at Cloudflare recently revealed that hacking and phishing attempts have been up by 37% and, on some days, they are blocking between four and six times the number of attacks they would usually see, since the start of the COVID-19 pandemic.

Let's take a look at what you can do to protect to create a secure at home work environment

THE IMPORTANCE OF USING UPDATED SOFTWARE & TOOLS

Updates aren't just for cool new features and bug fixes, they can also include critical security patches. Knowing what to update and how to update is the first step in create secure and safe while working from home.

WHAT TO UPDATE & HOW TO AUTOMATE YOUR UPDATES

- YOUR OPERATING SYSTEM
- APPLICATIONS INSTALLED ON YOUR DEVICES
- WEB BROWSERS
- ROUTERS

1. YOUR OPERATING SYSTEM

The device you're working on has an Operating System which you will see written shorthand as OS. The operating system is the software that works between your hardware and and the applications installed on your device. Your OS handles everything from print jobs to divvying out resources such as CPU and memory usage to the programs running on your computer.

Your operating system plays a major role on any device you use. That is why it is so important to keep the OS updated. It doesn't matter what other security measures you have in place if you are running an older, vulnerable version of your OS.

It doesn't matter what other security measures you have in place if you are running an older, vulnerable version of your operating system.

TYPES OF OPERATING SYSTEMS

- **Server OS** - A server OS is an operating system specifically designed to run on a server. Server operating systems are light weight and focused network computing.
- **Desktop OS** - A desktop OS is an operating system designed to run on a Desktop PC or Laptop. The three most common desktop operating systems are Windows, macOS, and Linux.
- **Mobile OS** - A mobile OS is an operating system designed to run on a phone or tablet. The two most popular mobile operating systems are iOS and Android.

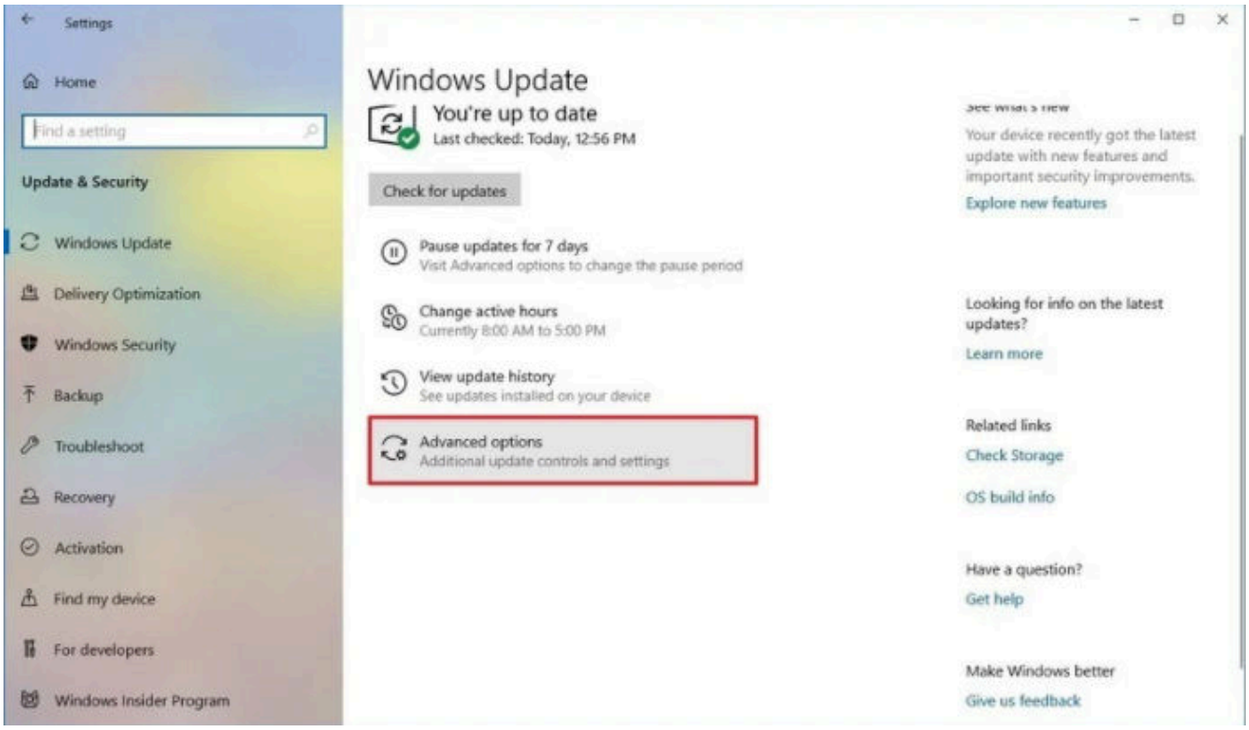
AUTOMATING UPDATES

It is best practice to configure your operating system to update automatically. Auto-updating your OS means that the latest security patches will download and install on your device without you needing to do anything.

HOW TO SET AUTOMATIC UPDATES IN MACOS

1. On your Mac, choose Apple menu > System Preferences, then click Software Update.
2. To automatically install macOS updates, select “Automatically keep my Mac up to date.”
3. To set advanced update options, click Advanced, then do any of the following:
    - To have your Mac check for updates automatically, select “Check for updates.”
    - To have your Mac download updates without asking, select “Download new updates when available.”
    - To have your Mac install macOS updates automatically, select “Install macOS updates.”
    - To have your Mac install app updates from the App Store automatically, select “Install app updates from the App Store.”
    - To have your Mac install system files and security updates automatically, select “Install system data files and security updates.”
4. Click OK.

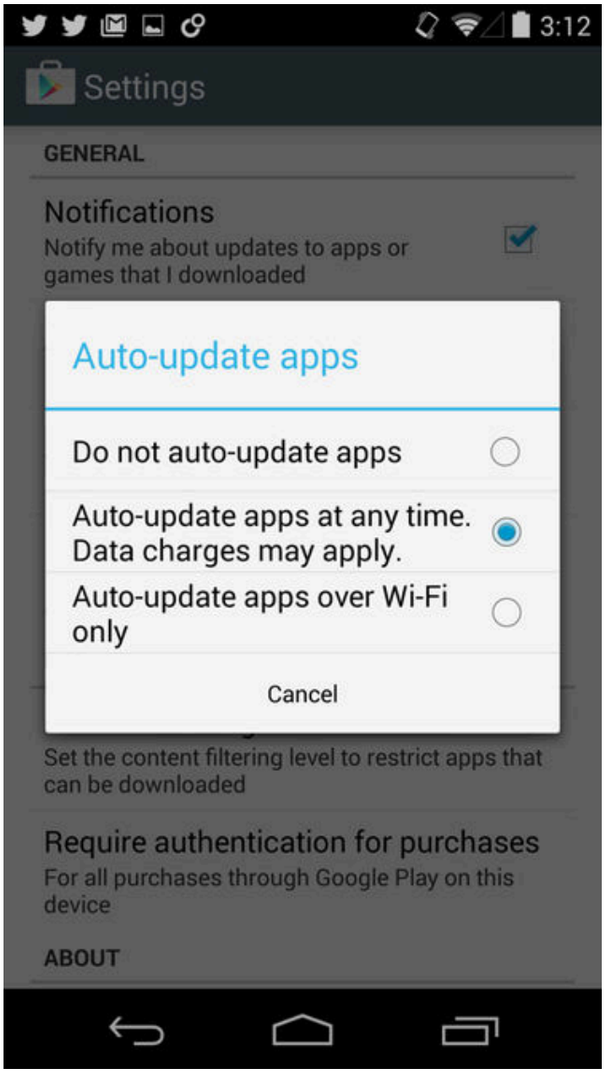
HOW TO SET AUTOMATIC UPDATES IN WINDOWS 10



1. Open Settings
2. Click on Update & Security
3. Click on Windows Update
4. Click the Advanced Options button

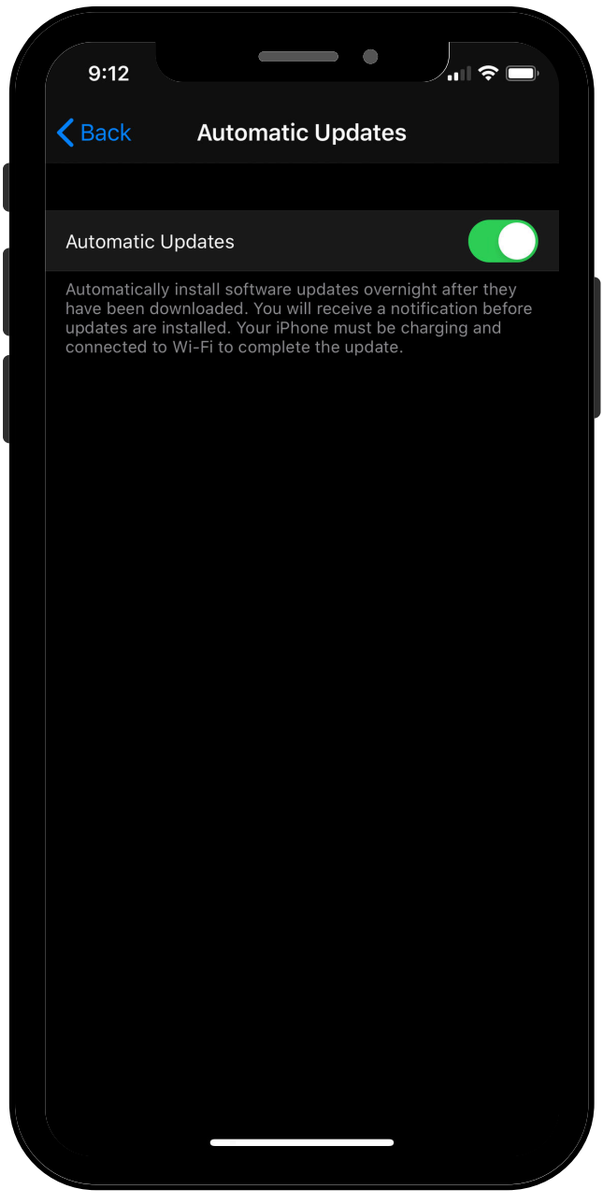
HOW TO SET AUTOMATIC UPDATES IN ANDROID

1. Open Settings
2. Tap on Software Update
3. Tap Download Updates Automatically



HOW TO SET AUTOMATIC UPDATES IN IOS

1. Open Settings
2. Tap or Click on General
3. Tap or Click on Software Updates
4. Tap or Click on Automatic Updates



2. APPLICATIONS INSTALLED ON YOUR DEVICES

Your next line of defense is to keep the applications you install on your devices up to date. You can set your apps to auto-update if you downloaded them from your operating system's app store.

HOW TO SET YOUR ANDROID APPS TO AUTO UPDATE

1. OPEN THE GOOGLE PLAY STORE APP.
2. TAP MENU > SETTINGS.
3. TAP AUTO-UPDATE APPS.
4. SELECT AN OPTION:
   - OVER ANY NETWORK TO UPDATE APPS USING EITHER WI-FI OR MOBILE DATA.
   - OVER WI-FI ONLY TO UPDATE APPS ONLY WHEN CONNECTED TO WI-FI.

HOW TO SET YOUR MICROSOFT STORE APPS TO AUTO UPDATE

1. SELECT THE START SCREEN, THEN SELECT MICROSOFT STORE.
2. IN MICROSOFT STORE AT THE UPPER RIGHT, SELECT THE ACCOUNT MENU (THE THREE DOTS) AND THEN SELECT SETTINGS.
3. UNDER APP UPDATES, SET UPDATE APPS AUTOMATICALLY TO ON.

HOW TO SET YOUR MAC STORE APPS TO AUTO UPDATE

1. OPEN THE APP STORE PREFERENCES.
2. CLICK THE AUTOMATIC UPDATES CHECKBOX.

HOW TO SET YOUR IOS APPS TO AUTO UPDATE

1. OPEN SETTINGS.
2. TAP [YOUR NAME].
3. TAP ITUNES & APP STORE.
4. TAP APP UPDATES TO ENABLE AUTOMATIC UPDATES.

3. WEB BROWSERS

With more of our work being done in the browser it has never been more important to keep your browser up to date. If you didn't get your desktop browser (like Safari) from your operating system app store, you will need to make sure it stays up to date.

HOW TO UPDATE CHROME

1. ON YOUR COMPUTER, OPEN CHROME.

2. AT THE TOP RIGHT, CLICK MORE .

3. CLICK UPDATE GOOGLE CHROME.
Important: If you can't find this button, you're on the latest version.

4. CLICK RELAUNCH.
The next time you restart your browser, the update will be applied.

HOW TO UPDATE EDGE

1. ON YOUR COMPUTER, OPEN EDGE.

2. ON THE TOP RIGHT CLICK THE MENU ICON.

3. ON THE TOP RIGHT CLICK THE MENU ICON.

4. CLICK ABOUT MICROSOFT EDGE.

5. CLICK UPDATE.

4. ROUTERS

The United States Air Force knows what can happen when you don't secure your router. A dumb security flaw let a hacker download US drone secrets, which could have been easily prevented.

The vulnerability allowed anyone to use the router's FTP server using the username: admin and password: password. The hack could have been prevented by either applying the security patch that had been released prior to the attack or updating the default passwords.

Always Change the Default Username & Password
A would be attacker can easily find your default router login details, so it is crucial for you to update the username and use a strong password.

The instructions to update your router's firmware will vary by device. Locate your router's Manufacture and model number, which can typically be found on the back of your router. Go to the manufacture's website to find how to update the firmware.

PROTECTING YOURSELF AGAINST PHISHING

Cybercriminals are taking advantage of the uncertainty and the increased stress that the pandemic has caused all of us. Not to mention that we all have received an increased number of emails due to updates regarding COVID-19.

Phishing is a method of cyber-attack using email, social media, text messages, and phone calls to trick the victim into giving up personal information. The attacker will then use the information to access personal accounts or commit identity fraud.

Another goal for a phishing attack is to trick the mark into downloading and installing malware on their personal device.

How do phishing attacks work?

Email is the most common tool used in Phishing attacks. The attacker will disguise the email to look like it was sent from a legitimate company. For example, an attacker could craft an email to look like it was sent from your bank.

HOW TO SPOT A PHISHING EMAIL

1. Look at the from email address - If you receive an email from a business, the portion of the sender's email address after the "@" should match the business name.

If an email is representing a company or government entity but is using a public email address like "@gmail" is a sign of a phishing email

Keep an eye out for subtle misspellings of the domain name. For example, let's look at this email address support@netflixx.com. We can see that Netflix has an extra "x" at the end. The misspelling is a clear sign that the email was sent by a scammer and should be deleted immediately.

2. Look for grammatical errors - An email that is full of grammatical mistakes is a sign of a malicious email. All of the words may be spelled correctly, but sentences are missing words that would make the sentence coherent. For example, "Your account is been hacked. Update password to account security".

Everyone makes mistakes, and not every email with a typo or two is an attempt to scam you. However, multiple grammatical errors warrant a closer look before responding.

3. Suspicious attachments or links - It is worth pausing for a moment before interacting with any attachment or links included in an email.

If you don't recognize the sender of an email you shouldn't download any attachments included in the email as it could contain malware and infect your computer. If the email claims to be from a business, you can Google their contact information to verify the email was sent from them before opening any attachments.

If an email contains a link, you can hover your mouse over the link to verify the URL is sending you where it should be.

4. Watch out for urgent requests - A common trick used by scammers is to create a sense of urgency. A malicious email might manufacture a scenario that needs immediate action. The more time that you have time to think, the greater the chance you will identify the request is coming from a scammer.

You may receive an email from your "boss" asking you to pay a vendor asap, or from your bank informing you that your account has been hacked and immediate action is required

PHISHING CHECKLIST

- [ ] CHECK SENDER'S EMAIL ADDRESS
- [ ] LOOK FOR GRAMMATICAL ERRORS
- [ ] WATCH FOR SUSPICIOUS ATTACHMENT & LINKS
- [ ] BE WARY OF URGENT REQUESTS

SECURE YOUR INTERNET

There has never been a better time to do an audit of our internet security. Now that some of us are working from home for the first time. We no longer have the protection that our office IT provided, and it is our responsibility to protect the sensitive information we have trusted with.

Luckily for us, there are some easy things we can do to increase the security and privacy of our internet traffic drastically.

1. Update Your WiFi Password - Some manufacturers use the same default passwords for all of their devices.

If you are using the password that came with your WiFi router, it is time to update your password.

2. Use a VPN - A VPN, or Virtual Private - Network is used creates a secure connection to another network over the internet. Using a VPN will keep whatever you are looking at on the internet private.

3. Use an Ad Blocker - A good ad blocker doesn't will not only block ads but will prevent your from visiting known phishing and malware sites.

SERVER SECURITY

Server security isn't something that is always on the top of our minds. However, sever security is a critical part of every security plan. Here are some tips that you can use to start securing your server today.

CHOOSE THE RIGHT WEB HOST

Not all web hosts are created equal and choosing one solely on price can end up costing you way more in the long run with security issues. Most shared hosting environments are secure, but some do not properly separate users accounts.

Does your host:

- Update server software regularly?
- Does your host enable logging?
- Does your host offer sFTP?

HTTPS & SSL

SSL encrypts the communication that your customers type in their browser and send to your site. With SLL, when someone enters their account name and password, it will be protected when that information is sent to your site's server for confirmation.

Encrypting the username and password will make it harder for an attacker to intercept the username and password in transit from their browser to your server.

USE A CDN & WAF

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defense against a range of attack vectors.

Encrypting the username and password will make it harder for an attacker to intercept the username and password in transit from their browser to your server.

A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content

A properly configured CDN may also help protect websites against some common malicious attacks, such as Distributed Denial of Service (DDOS) attacks..

WRAPPING UP: A SECURITY CHALLENGE

We covered a lot of ground in this ebook, from securing your WordPress website to working securely from home. By adopting a few best practices and adopting good habits, you can greatly strengthen your defenses against the most common types of attacks.

Ready to take the challenge? Right now is a great time to do a security audit of your website and work-from-home setup to be sure your are using security best practices. Let's go!

“

READY TO TAKE THE CHALLENGE? RIGHT NOW IS A GREAT TIME TO DO A SECURITY AUDIT OF YOUR WEBSITE AND WORK-FROM-HOME SETUP TO BE SURE YOUR ARE USING SECURITY BEST PRACTICES.

”

iThemes Security Pro

THE #1 WORDPRESS SECURITY PLUGIN

Get started with our single site iThemes Security Pro plan for just $49* with coupon code **SECUREMYWP**

LEARN MORE

*Offer good on any *new* iThemes Security Pro (1 site) plugin purchase. Coupon can't be used to renew or extend an existing iThemes Security Pro (1 site) plugin membership.