



Is It Safe to Connect My Clients' Sites to mySites.guru?

Security runs through everything mySites.guru does, from the platform and your data to the 100,000 connections it makes to remote sites each day.

Phil E. Taylor | 19 October 2026

YES!

An agency owner told me recently that she was holding off connecting her client sites because she'd be "sharing my clients' website access with strangers". It's the right instinct. Before you put a management tool between you and fifty client sites, you should know what that tool can do with them and who's behind it.

**mySites.guru is built to be secure in everything it does -
By Design**

That covers the platform, the data we hold, who on our side can reach it, your own login, and above all the connections to your sites. mySites.guru makes around 100,000 connections to remote sites every day for thousands of paying customers, and every one of them is encrypted, signed for the one site it is meant for, and validated through an independent callback before it runs.

You don't give us any client passwords, FTP details or hosting logins to get there. You install a connector plugin on each site, and the platform is built so that even someone with our entire database could not use it to run a command on your client's server. At least three read-only Docker containers, on three different physical servers behind our firewall, would all have to be compromised within seconds of each other to send a single forged request.

What you give us when you connect a site

Connecting a Joomla or WordPress site means installing the mySites.guru connector plugin, the same way you'd install any other extension. That's the whole setup. The admin password, FTP and the hosting control panel stay with you.

The only time I ever ask for FTP details is when a customer asks me to fix a site that won't connect, and they choose to send them through the support form. Day-to-day use never needs them.

Even a complete mySites.guru server compromise is not enough to access your sites

Most people picture a management tool as a big box of keys: break into the box, get every site. I built mySites.guru on the opposite assumption, that our own systems will eventually be attacked, and designed for what happens after that.





Validated, so the connector decrypts and runs it

Anything that fails a check is never decrypted

Every one of the roughly 100,000 requests a day takes this path.

The connector on your site authenticates every instruction before it acts on it. All communication with it is encrypted end to end, and a request is only valid if it has the correct signature for that specific site. Every single site gets its own cryptographic key pair, which isn't shared with any other site on the platform.

That encryption does more than one job. Besides protecting the request, it's how our requests tunnel through the restrictive firewalls and WAFs that some hosts put in front of their servers, which would otherwise block legitimate management traffic. Because each request is encrypted with that one site's keys, it can't be used against any other site. Each request is also time-boxed, and the connector won't act on it until the validation server has confirmed it.

A signature alone isn't the end of it. Every request to a connected site has a parallel connection to an independent validation server: before the connector runs anything, it calls back to check that the request really came from mySites.guru. If you've ever built a PayPal IPN listener, it's the same idea, and PayPal has relied on that pattern for decades. Every single request we make is signed and then validated before it runs.

mySites.guru also isn't one server. The platform is a layered, Docker-based service, with its layers distributed across different physical servers and run largely as read-only containers. To run a single command on any remote site, an attacker would need to compromise at least three different read-only Docker containers, on three different physical servers, within seconds of each other, all without tripping any of our defences, and all behind our main firewall on our private internal network. So even a complete compromise of one mySites.guru server, database included, is not enough to run a command on your site. I don't publish every layer of that design, because that would only help someone looking for a way in.

There's also a kill switch. In the unlikely event that mySites.guru itself had a security breach, I can stop every request to every connected site with a single command, by switching off the validation server. With nothing there to answer the callback, no connector will run anything until it's back.

This is not a theoretical concern. On 18 October 2026 TeamUpdraft confirmed that it had identified unauthorised access which it believes may have exposed UpdraftCentral connection keys. [One WordPress site owner on Reddit](#) found a backdoor plugin they never installed, dropped through two requests to UpdraftPlus's remote-control library with no wp-admin login, no plugin upload and no file editor use. TeamUpdraft's advice was to delete existing UpdraftCentral connection keys, change passwords and reconnect with a new key. If the same kind of breach happened at mySites.guru, it would not be enough to run a command on your site, because nothing stored in our service database is enough on its own to make the connector accept a request.

The same boundary holds in the other direction. If one of your client sites gets hacked, through a vulnerable extension or anything else, it has no path back into mySites.guru, and no path from there to your other sites.

An example: one-click login

[One-click login](#) is a good way to see all of this working, because it's the feature that sounds most like we must be holding your passwords. You press a button on your dashboard and you're in a client site's admin console, without typing a password.

Your password is never involved. We don't ask for it and we don't store it. Each login goes through the same signed and validated process as every other request:

1. Register

mySites.guru registers the upcoming request with our request validation service.

2. Send

An encrypted login request is sent to the connector on the site.

3. Validate

The site checks back with the validation service to confirm the request is real.

4. Decrypt

Only then does the site decrypt the request, which was encrypted with that site's own keys so it is useless anywhere else, and see that it's a login instruction.

5. Create session

The site creates a new session for the admin user you chose in mySites.guru.

6. Redirect

You're redirected to the site, and your browser picks up that session.

No password crosses the wire at any point, and not even a username. The login request names the admin user by a number, the user's ID on that site, and we don't store usernames in our database at all. One-click login is also opt-in: it does nothing until you pick, per site, which admin user it should log you in as.

Who is on our end

Me, Phil Taylor. I've been involved in Mambo and then Joomla for decades, starting as one of the original five core developers of Mambo Open Source 4.5. I was also one of the top code contributors to Joomla 4, and I'm on the Joomla Security Strike Team's honour roll. If you run Joomla, you are probably already running code I wrote on your

sites! Tens of thousands of people trust me with their sites, and you can read what they say.

I've run mySites.guru for more than a decade and I answer all the support email myself. Support isn't outsourced, so there's no overseas helpdesk with a login to your account.

Access to the production systems is restricted to named personnel, over key-based authentication on a private network. The application servers and the database aren't reachable from the public internet.

If I ever need to see your dashboard as you see it to sort out a support problem, that admin impersonation is restricted, logged, and shows up in your own account activity log. You'll always be able to see that it happened.

Some jobs can't be done through the connector at all: a hacked site, a half-finished update, a site that won't boot. For those, fix.mySites.guru is my paid, hands-on repair service, and it does need your site's credentials. That process is locked down too. Credentials are encrypted at rest, field by field, with the encryption key on different hardware to the database, and they are never emailed to anyone, including me. Only I can see them, and every time they're opened that's recorded. They're also time-boxed: a scheduled job destroys them seven days after you send them unless a job is still under way, nothing survives thirty days under any circumstances, and you can destroy them yourself from your account at any time.

Securing mySites.guru since 2012

mySites.guru has been running since 2012, and for all of that time securing it has been part of the job, along with defending it against abuse and attacks. The security architecture above has been part of the platform from day one.

Security is also what I do outside mySites.guru. I'm security educated and trained, and I design and build complex security architecture for other organisations as well as for our own platform.

We've also responsibly disclosed over 100 security issues in other people's products, including Joomla core and many of the extensions your sites run, and [a month of our Joomla security disclosures](#) shows what that work looks like. That work has been recognised outside the Joomla world too, including a Digital Jersey Tech Awards nomination for helping secure government COVID digital certificate platforms.

What data does mySites.guru store about a site?

Very little, and most of it is integers and flags: counts, and [yes-or-no answers to the checks the connector runs](#). Anything more detailed is pulled from the site in real time, only when you open [one of the investigate tools](#).

All the alerting and notifications you get from mySites.guru come from those integers and flags. We don't pull your site's files or database into our service to work out whether something needs your attention.

The heavy lifting happens on your own server. [Scanning file contents and database content is done by the connector](#), in your environment, with your own settings, your own PHP and your own versions. What comes back to us is the answer, not your content.

The little we do hold is protected like this:

In transit

All traffic to the platform is end to end encrypted.

At rest

Personal data is encrypted in the database, and the encryption keys are held on different physical hardware to the database.

Backups

Encrypted with a modern cipher, held off-site, and kept for at most a month.

Your password

Stored one-way hashed, so it can never be recovered in plain text.

To be clear: Your clients personal data on their sites

Data protection law defines “processing” personal data very broadly. Showing you the names of the users on a client site in the user management tools could count, so we treat ourselves as processing that data and go over and above what’s required of us as your sub-processor.

We don’t harvest or otherwise process the personal data found on your sites, and we don’t store any of it in our service. We only read it from your site in real time, while you’re using the tools, and it stays on your site.

The only other personal data we process is about our own account holders: your name, IP address, location, billing and payment details and the like. We handle that securely and in full adherence with international data protection law, going over and above what it requires. Our Data Processing Agreement covers the data on your sites, and our Privacy Policy covers yours.

The weakest point is your own login

Your own mySites.guru login is the weakest point, and securing it is your responsibility, not ours. This is by design.

With everything above in place, the easiest way into your sites through mySites.guru is your own dashboard login. If you choose a weak or reused password, choose not to set up passkeys or two-factor authentication, or choose to switch off login notifications, that's on you rather than on the platform.

mySites.guru gives you all the tools to lock your account down. Using them is up to you:

Passkeys and hardware keys

Sign in with a [passkey](#) using Face ID, Touch ID, Windows Hello or your Android phone, or plug in a hardware security key such as a YubiKey. Passkeys can't be phished or reused on another site.

Two-factor authentication

Codes from an authenticator app, backup codes for when your phone isn't to hand, and the option to trust a device for 60 days.

A nudge on every sign-in

Until you set up two-factor or a passkey, every sign-in without one prompts you to do it.

Login notifications

An email every time someone signs in to your account, with the IP address and time. If it wasn't you, reply and I'll help you lock the account down. You can switch them off in your [notification settings](#), but please don't: they're your early warning.

Brute-force blocking

Ten failed sign-ins from one IP address within five minutes and that address is blocked.

No password reuse

Your last five passwords can't be used again.

Team member logins

Give staff their own logins instead of sharing yours, limited to the sites they need, each with their own second factor. You can remove one person without changing anything for the rest.

A locked-down File Manager

The Web File Manager is off until you switch it on for a site, needs two-factor, and asks for your password again before it switches on.

And use a strong, unique password, ideally generated and stored in a password manager.

mySites.guru plugin security updates are automatic

You never need to update our plugin. We do that for you automatically, as and when we release new code, so you're fully protected and have the very latest features deployed for you. Even this process is locked down: an update only runs inside an authenticated, validated request from mySites.guru, the new version downloads from our own CDN over HTTPS, and every file is checked against the release manifest after it's installed, so a partly applied update gets caught rather than reported as done.

You can cut off access yourself, at any time

mySites.guru can only reach a site while the connector and its keys are on it, so ending access is in your hands, and it takes seconds. Any one of these does it:

Delete the Keys folder

plugins/system/bfnetwork/bfnetwork/Keys on Joomla, or wp-content/plugins/mywpguru/bfnetwork/Keys on WordPress.

Uninstall the plugin

Use the normal Joomla extension manager or WordPress plugin uninstaller.

Delete the files

Remove the plugin's files over FTP.

Delete the site from your dashboard

Every site has its own key pair, and deleting the site destroys our half of it, so we can't reach the site afterwards even if we wanted to.

What to tell your clients

If a client asks where their data goes, our Data Processing Agreement covers the usual agency setup: your client is the controller, you are the processor, and mySites.guru is your sub-processor. It's about how personal data is handled rather than how the platform is secured, but it's the document a client's compliance person will expect to see.

And if you're a security researcher who has found something we've missed, our security_policy explains how to report it.

Don't take our word for it. See what other people have to say.

Hundreds of agencies and site owners who manage their Joomla and WordPress sites with mySites.guru have reviewed it, and WP Mayor rated it 4.6/5. Read the reviews.

Further Reading

- [Backdoor plugin dropped on my WordPress site](#) - the October 2026 UpdraftCentral connection key incident, with TeamUpdraft's confirmation
- [Data Processing Agreement](#) - how personal data on your connected sites is handled, for when a client asks
- [Security policy](#) - how to report a vulnerability in mySites.guru or the connector, and our response targets
- [One-click login to any Joomla or WordPress admin](#) - how the passwordless handshake works day to day
- [Passkeys for secure login to mySites.guru](#) - lock down your own dashboard login
- [Manage multiple sites with your whole team](#) - give staff their own logins instead of sharing yours

Frequently Asked Questions

Is it safe to connect my clients' sites to mySites.guru?

Yes. mySites.guru is built to be secure in everything it does. You don't give us any passwords or FTP details, every request to a site is encrypted with that site's own keys, time-boxed and confirmed by an independent validation server before it runs, and even a complete compromise of one mySites.guru server is not enough to run a command on your site.

Do I have to give mySites.guru my clients' admin passwords or FTP details?

No. You connect a site by installing the mySites.guru connector plugin on it. You don't give us admin passwords, FTP or hosting logins to use the service. One-click login to a site's admin from your dashboard uses an encrypted session handshake, so no passwords are stored or transmitted.

Could someone at mySites.guru, or an attacker inside mySites.guru, take over my clients' sites?

The connector authenticates every instruction before acting on it, and a request is only valid with the correct signature for that specific site. Before running anything, the connector also calls back to an independent validation server to confirm the request really came from mySites.guru. Even complete access to the mySites.guru database could not be used to run a command on a customer's server. At least three read-only Docker containers, on three different physical servers behind our firewall, would all have to be compromised within seconds of each other to send a single forged request.

Who on your side can see my account?

Phil runs mySites.guru and answers all support himself, and support is never outsourced. Access to production systems is restricted to named personnel over key-based authentication on a private network. If an admin ever impersonates your account to help with a support request, that is restricted, logged, and shown in your own account activity log.

If one of my client sites gets hacked, can that spread to my other sites through mySites.guru?

No. The boundary runs both ways: a site that gets compromised, through any route, has no path back into mySites.guru itself, and so no path from there to the other sites on your account.

Do you have a Data Processing Agreement I can show my clients?

Yes. Our DPA at mysites.guru/dpa/ covers the usual agency arrangement, where your client is the controller, you are the processor, and mySites.guru is your sub-processor. It covers how personal data on your connected sites is handled, which is usually what a client's compliance team asks about.

How do I disconnect a site?

Delete the connector's Keys folder (plugins/system/bfnetwork/bfnetwork/Keys on Joomla, wp-content/plugins/mywpguru/bfnetwork/Keys on WordPress), uninstall the plugin with the Joomla or WordPress uninstaller, or delete its files over FTP. Any one of those ends all access from mySites.guru. Deleting the site from your dashboard also destroys our half of that site's key pair.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

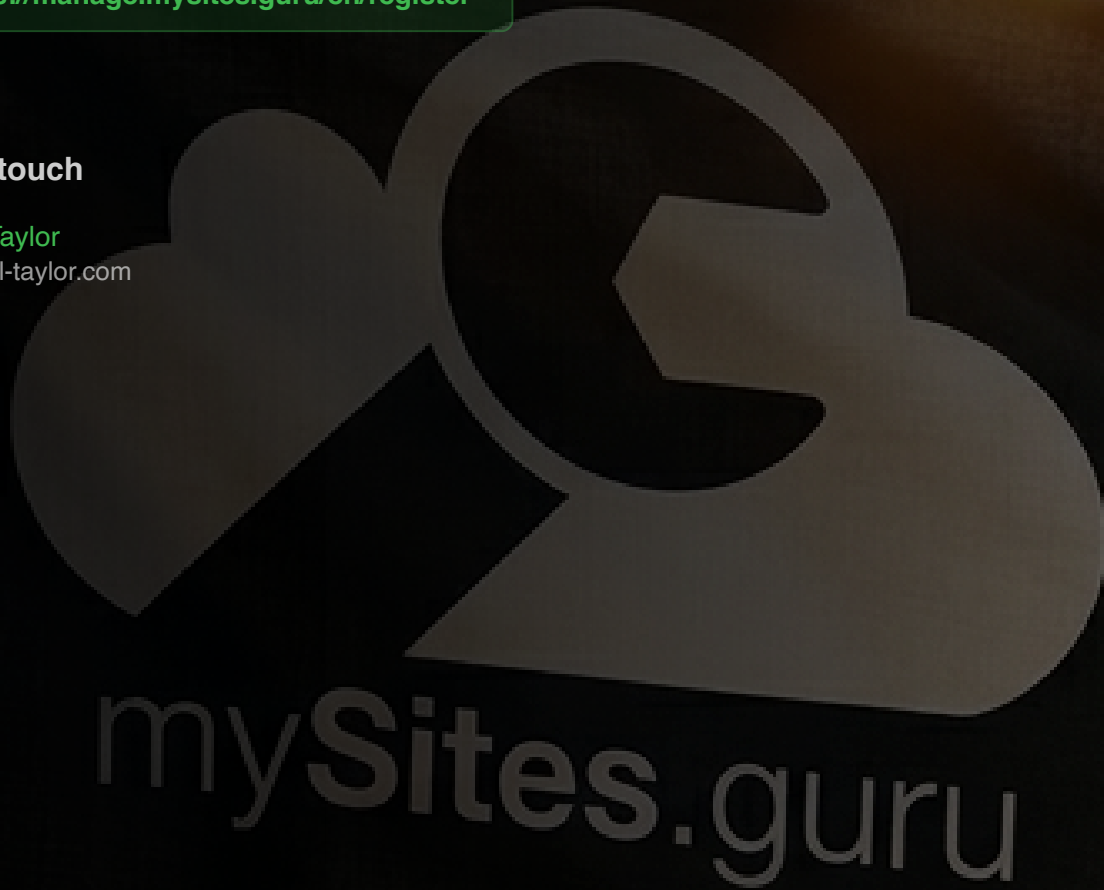
Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru

