thefoodconnector

CLIENT INFORMATION

# How we keep your website secure

Website security is a set of protections stacked in layers, each looked after by the party best placed to manage it. This guide explains those layers, what The Food Connector does at each one, and the few steps that only you can take.

IN THIS GUIDE


- Security in layers, and who owns each one
- Hosting, server, and website protection
- Monitoring, backups, and recovery
- If something goes wrong
- Your part: a short checklist

OVERVIEW

# Security works in layers

No single product makes a website secure. Protection comes from several independent layers, so that if one is ever bypassed, the next is still in place. Just as important, each layer has a clear owner. Our hosting company protects the hardware and the network, we protect the server configuration and every website on it, and you control who holds a login to your site and your domain.

Good security also means more than keeping attackers out. It includes noticing problems quickly and recovering from them with little or no lost work. Our approach therefore rests on three goals: **prevent** what can be prevented, **detect** anything unusual quickly, and **recover** fast from a clean copy if the worst happens.

| | | |
|---|---|---|
| 1 | **Hosting and data center**<br>Physical security, network protection, and the server's operating system | HOSTING.COM |
| 2 | **Server firewall and malware protection**<br>Blocks attacks before they reach your site and removes malicious files | HOSTING.COM + THE FOOD CONNECTOR |
| 3 | **WordPress protection**<br>Security scanning, managed updates, and login safeguards on every site | THE FOOD CONNECTOR |
| 4 | **Monitoring and alerts**<br>Around-the-clock checks that flag problems before visitors notice them | THE FOOD CONNECTOR |
| 5 | **Backups and recovery**<br>Nightly offsite backups, verified every morning, ready to restore | THE FOOD CONNECTOR |
| 6 | **People and access**<br>Logins, passwords, two-factor authentication, and domain registrar access | YOU + THE FOOD CONNECTOR |

## Who is responsible for what

| PARTY | RESPONSIBLE FOR |
|---|---|
| **hosting.com** | The data center, power, network, server hardware, operating system updates, and server-level firewall and malware tools |
| **The Food Connector** | Server configuration, every WordPress site, updates, security scanning, monitoring, backups, and response when something goes wrong |
| **You, our client** | Who has a login to your website, the strength of those passwords, and the security of your domain registrar account |

PREVENTION

# Keeping attacks out

## 1 Hosting and data center

HOSTING.COM

- Websites run on a dedicated, professionally managed virtual private server (VPS), not on low-cost shared hosting, so The Food Connector controls who has access to the server and how it is configured.
- The server sits in a secured data center with redundant power and network connections.
- hosting.com keeps the operating system and core server software patched.
- CloudLinux walls each account off from the others, so a problem in one cannot spread to another.

## 2 Server firewall and malware protection

HOSTING.COM + THE FOOD CONNECTOR

- **Imunify360**, a server-level firewall, inspects incoming traffic and blocks known attack patterns, abusive bots, and repeated login attempts before they reach your website.
- **Monarx** scans every file on the server continuously and automatically neutralizes anything it identifies as malicious.
- When we see sustained abusive traffic, we block the source at the firewall, which stops it before it uses any of the server's resources.
- We add our own early-stage filters that turn away known attack signatures and bad bots before WordPress even starts to load.

## 3 WordPress protection on every site

THE FOOD CONNECTOR

- **Wordfence security scanning.** Every site is scanned daily for altered files, malware, unexpected administrator accounts, and plugins with publicly known vulnerabilities. These are WordPress-specific problems that a server firewall cannot see. On our server, Wordfence's own firewall is deliberately turned off, because Imunify360 already does that job and two firewalls conflict. Sites on client-owned hosting run Wordfence in full, firewall included.
- **Managed updates.** Plugins and themes are updated weekly from a central management system, with a follow-up check that confirms every update went through. WordPress security releases install as soon as they are published.
- **A vetted plugin set.** Each site runs a standard, maintained set of premium plugins. We remove plugins that are abandoned or carry unnecessary risk.
- **Encrypted connections.** Every site runs on HTTPS. Certificates renew automatically, and we monitor their expiry dates.
- **Session and spam safeguards.** Idle admin sessions sign out automatically. Email addresses and phone numbers on your site are encoded against harvesting bots. Site email is sent through an authenticated email service, which protects your domain from being spoofed.

# Catching problems early, recovering fast

## 4 Monitoring and alerts

THE FOOD CONNECTOR

- **Uptime monitoring.** Every live site is checked every few minutes, around the clock. Beyond confirming the site responds, we also check that its pages are displaying correctly.
- **Server health monitoring.** Our own monitoring watches server load and unusual activity and alerts us to sustained problems.
- **Error monitoring.** Serious site errors trigger an immediate alert, and a daily digest reports errors across all sites.
- **Domain monitoring.** We check the public registration records of every client domain daily and are alerted if a domain's settings change unexpectedly or its renewal date approaches. This guards against domain hijacking, one of the most damaging attacks a business can face.

## 5 Backups and recovery

THE FOOD CONNECTOR

- Every site's files and database are backed up automatically each night with UpdraftPlus Premium.
- Backups are stored offsite in **Amazon Web Services (AWS S3)**, so they survive even a complete loss of the server.
- An automated check runs every morning to confirm each backup completed, and alerts us if one did not.
- hosting.com also keeps its own separate server-level backups, an independent second copy.

## If something does go wrong

Even well-protected sites can be targeted, often through weaknesses that become public before a fix exists. When that happens, we follow a set process:

**Detect**
Monitoring, scanning, or an alert flags the problem.

›

**Contain**
We block the source and isolate anything suspicious.

›

**Check the fleet**
We sweep every site we manage for the same signs.

›

**Restore**
We clean the site or restore it from a verified backup.

›

**Harden**
We add protections so the same route cannot be used again.

We keep a written record of every security incident, including what happened, what we checked, and what we changed. If an incident affects your site, we will tell you what happened in plain language.

# Your part: a short checklist

Most real-world website break-ins do not involve hacking a server. They happen because someone obtains a valid password. These steps are in your hands, and they make a substantial difference.

- [ ] **One login per person.** Never share a single account among several people. Individual logins show who did what and can be removed one at a time.
- [ ] **Least access needed.** Give each person the lowest role that does the job. Most content editors do not need administrator rights. Ask us if you are unsure which role fits.
- [ ] **Strong, unique passwords.** Use a password manager and never reuse a website password anywhere else.
- [ ] **Remove people who leave.** When an employee or outside contractor no longer needs access, tell us and we will remove their account promptly.
- [ ] **Secure your domain registrar.** Turn on two-factor authentication for the account where your domain is registered (for example GoDaddy or Network Solutions), and keep the domain's registrar locks on. A hijacked domain can take your website and email offline even when the website itself is untouched.
- [ ] **Check with us before adding plugins or granting access.** If a vendor or freelancer asks for a login or wants to install something, let us know first so we can confirm it is safe.
- [ ] **Be cautious with unexpected emails.** We will never ask for your password by email. Forward anything that looks suspicious, such as urgent requests to "verify" your website, domain, or hosting, and we will take a look.

## What we can promise

Layered protection, continuous monitoring, verified nightly backups, and a fast, documented response. No honest provider can promise that a website will never be targeted. What we can promise is that problems are **caught early** and **fixed quickly**.

**Questions about security?**
Contact your Food Connector account team, or reach us through **thefoodconnector.com**. We are glad to walk you through how any of these protections apply to your site.

This guide describes The Food Connector's standard security practices as of November 2026. Protections for sites on client-owned hosting accounts may differ depending on the host, and we can describe the arrangements for your site on request. Product names are trademarks of their respective owners.