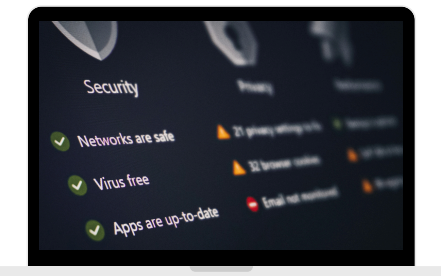


Your website is one of those things you set up once and then stop thinking about. It sits there doing its job, so there's no reason to touch it. That's exactly why a neglected website is one of the common ways a small business gets hacked. Most small-business sites run on WordPress, which powers more than 40% of all websites. WordPress itself is solid. The risk is usually the plugins and themes added to it, which often don't get updated for years.

Is Your Business Website a Security Risk?



How it happens

Attackers don't pick your business by name. They run automated tools that scan huge numbers of websites looking for known weak spots, like a plugin with a security hole that hasn't been fixed. When a plugin maker finds a flaw, they release an update. Until you install it, the hole stays open, and the scanners know exactly what to look for. Researchers who track WordPress flaws find the large majority are in plugins and themes, not in WordPress itself.

What a hacked site gets used for

A hacked site rarely announces itself. Attackers usually keep it running and use it for their own purposes:

- Serving malware to your visitors, or pushing them to a page that tries to install something.

- Hidden spam and scam pages that ride on your site's standing with search engines.
- Copying what people type into your contact or checkout forms, including payment details.

The damage lands on you. Search engines flag hacked sites and drop them down the rankings, and browsers may block them, so customers see a red "this site may be dangerous" warning instead of your homepage.

Is your site at risk?

It depends how it's built. If you use a hosted builder like Wix, Squarespace,

Shopify, most of the security and updates are handled for you, so your risk is lower.

If you have a self-hosted WordPress site, usually set up by a designer or agency on your own hosting, then keeping WordPress, the plugins, and the themes updated is someone's job. The question is whose. On a lot of small-business sites, the honest answer is that nobody has touched it since it launched.

What to do about it

- Keep WordPress, plugins, and themes updated, and turn on automatic updates where you can.
- Delete plugins you don't use, and replace any that the developer has abandoned.
- Use a strong, unique password on the admin login, with MFA if your setup supports it.
- Keep backups, so a hacked site can be restored instead of rebuilt.
- Decide who's responsible for all of the above: your designer, your host, or your IT provider.
- If you don't know when your site was last updated, ask whoever built it. That's the first thing to sort out.



ATTITUDE CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

Why Vetting Your Vendors Is No Longer Optional

98% of organizations have a relationship with a third party that's already been breached

Here's a number worth sitting with: 98% of organizations today have a relationship with a third party that has already been breached.

Your business almost certainly has that exposure too — the question is whether you know where it is.

For years, cybersecurity conversations focused almost entirely on your own environment: your firewall, your endpoints, your employees. That's still essential. But attackers have shifted their focus, and the numbers show it clearly.

Third-party involvement jumped 60% year-over-year in Verizon's 2026 Data Breach Investigations Report, now present in 48% of all breaches.

Nearly half of all breaches today trace back to a vendor, contractor, or service provider — not a direct attack on the business itself.

Why Vendors Have Become the Easier Target

It makes sense once you think about it from an attacker's perspective. Why spend weeks trying to breach a well-defended business directly when you can compromise one under-secured vendor and gain access to dozens of that vendor's clients at once?

Security researchers found that for every vendor breached in 2025, an average of 5.28 downstream companies were also compromised. One weak link doesn't just expose one business — it exposes everyone connected to it.

And the financial impact is significant on its own. Third-party and supply chain compromise was the second most common and second costliest attack type, averaging \$4.91 million per breach.

That's before accounting for the reputational damage, client notification obligations, and lost trust that follow.

“We Trust Them” Isn't a Security Policy

Most businesses vet a new vendor based on price, reputation, or a referral from someone they trust.

Almost none ask the vendor to demonstrate how they actually protect the data or access they're being handed. That gap matters most when a vendor will:

- Have remote access to your network, cloud environment, or email systems
- Access, store, or process your company, client, or employee data
- Communicate with your clients or partners on your behalf

If a vendor checks any of those boxes, a handshake and a good sales pitch aren't enough.

You're extending your own security perimeter to include theirs — and you have no way of knowing how strong that perimeter is unless you ask.

Continued on page 2...

continued from page 1

What a Real Vendor Vetting Process Looks Like

Vetting a vendor doesn't need to be complicated, but it does need to be structured and consistent. At minimum, a proper review should cover:

- Multi-factor authentication on any accounts with access to your systems
- Endpoint protection on the devices they use to do the work
- Patch management — are they running outdated or unsupported software?
- Data handling practices — how and where is your data stored, and is it encrypted?
- Remote access controls — no exposed, unprotected remote access tools
- Employee security training — do their staff know how to spot phishing?
- Incident response — will they actually tell you if something goes wrong, and how fast?
- Subcontractors — is your data being handed to a fourth party you've never heard of?
- Cyber insurance — do they carry coverage appropriate to the access they hold?

Asking these questions once, informally, isn't enough either. Vendor relationships change, staff turn over, and security postures drift. The businesses managing this well treat vendor review as a repeatable process, not a one-time gut check.

Turning This Into a Repeatable Process:



The Vendor Audit Form

This is exactly why we built a Vendor Cybersecurity Audit template — a standardized questionnaire you can send to any vendor who touches your systems, data, or clients, before you grant them access and again on a regular review cycle.

The form walks a vendor through each of the areas above, asks them to describe their controls in their own words, and — importantly — asks for actual evidence: a screenshot, a policy document, a certificate of insurance, or a written attestation from their IT provider.

It closes with a simple risk rating so your team can make a clear, documented decision: approved, conditionally approved pending fixes, or not approved.

Having this on file does more than reduce risk. It gives you a defensible, documented answer if a client, auditor, or insurer ever asks how you manage third-party risk — instead of “we’ve worked with them for years and they seem fine.”

Getting Started

You don't need to audit every vendor you've ever worked with overnight. Start with the ones that matter most: anyone with standing remote access, anyone holding sensitive data, and anyone who represents you directly to your clients. Build the habit from there.

If you'd like a copy of our Vendor Cybersecurity Audit template to start vetting your own vendors, reach out and we'll send it over.

Contact our team by phone so we can walk you through the vendor Audit form and process. and If you need additional support like a pen test and assistance with supporting documents that fit the bill. We can help with that too.

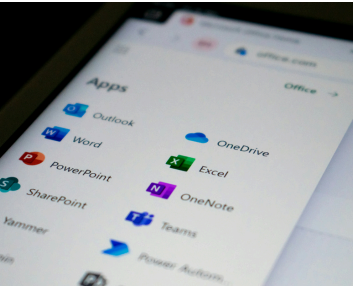


You may be experiencing these forms requested from your vendors. and clients. We can help you prove you have the right security in place too. Here is a 30-minute checklist you can start with: Updates. Check that device and software updates are installing, not sitting at "restart required".

- Backups. Check when anyone last restored a file. If it's never been tested, you don't know it works.
- Who has access. Every user account should belong to an active employee.
- Multi-factor authentication. Make sure it's on for everyone.
- Devices. If there's a device you don't recognize, find out whose it is.

Write down what you find and fix it afterward.

ONEDRIVE OR SHAREPOINT? WHERE YOUR FILES SHOULD LIVE



If your business runs on Microsoft 365, you have two places to keep files, and most people were never told the difference.

OneDrive is your own space, for drafts and work only you need. SharePoint is the team's space, for anything shared. Files in a Teams channel are already in SharePoint.

- Put anything the team works on in SharePoint or a Teams channel, not in one person's OneDrive.
- Keep OneDrive for your own drafts, and don't let it become the only home for a shared file.
- Get important files off local desktops. A file only on a laptop isn't backed up or shared.
- Agree a simple rule, like "client files live in the client's SharePoint folder," so nobody has to guess.

When someone leaves, their OneDrive is only kept for 30 days by default before it's deleted, so anything the team needs should be in SharePoint before that happens

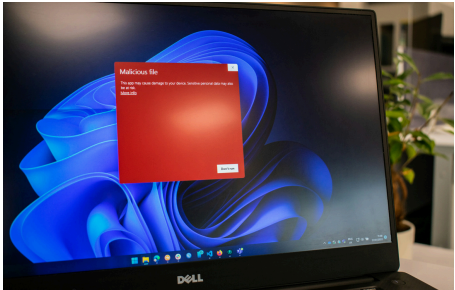
Why You Should Scroll Past the First Result on Google

When you search for a program to download or a site to log in to, the first thing you see is usually an ad. Scammers buy those ads on trusted names, so their fake site sits above the real one.

- Scroll past the sponsored results. The real website is usually just below.
- Never download software from an ad. Type the maker's address yourself.
- Bookmark the sites you log into, like your bank and Microsoft 365.
- Check the web address before you type a password into anything.
- Keep browsers and devices updated, so a bad download is less likely to work.
- Tell your team the top result can be a trap. Most have never been warned.
- If someone clicked one, change the password and have the device checked



What to Do When Microsoft 365 Goes Down



In July 2024, a faulty software update crashed around 8.5 million Windows computers in a few hours. It wasn't an attack, just a bad update. When a service you depend on goes down, there's nothing for you to fix. These five steps keep you working while you wait.

- Check whether it's just you. Look at the provider's status page, or ask whether anyone else has the same problem. If it's a wider outage, there's nothing to fix on your end, so stop trying.
- Tell your team what's down and what to use instead. Otherwise someone spends an hour rebooting a laptop that was never the problem.
- Switch to your backup way to communicate. Move to the phone, text, or another app so the team can still coordinate and reach customers.
- Tell customers if it affects them. If you can't take bookings or payments, say so, and tell them when to try again.
- Note when it started and what's affected. A couple of lines is enough, and it helps you follow up once things are back.

Write the plan down before you need it. One page covers it: which tools would stop the business, how people reach each other when the usual way is down, where your essential information lives, who's in charge, and who to call. Keep it somewhere you can reach without your main systems, and review it once or twice a year.

