TALK NERDY TO ME

INSIDE THIS ISSUE:

How to Spot a Scam Email Now That They Look Real — Page 1

Gadget of the Month — Page 1

Is Your Website a Security Risk? — Page 2

When Microsoft 365 Goes Down — Page 2

Why You Should Scroll Past the First Result on Google — Page 2

OneDrive or SharePoint? — Page 2

30-Minute IT Check — Page 2

Phishing vs. Fishing — Page 2

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- Jason Horne
CEO

HOW TO SPOT A SCAM EMAIL NOW THAT THEY LOOK REAL

For years the advice was simple: watch for bad spelling and clumsy grammar. Scammers now use AI to write their emails, so that advice no longer helps. The messages arriving in your team's inbox read as well as anything from a real company.

Why the old advice stopped working

That worked because many scammers were writing in a language that wasn't their own, and mistakes showed. AI removed that. The UK's National Cyber Security Centre says generative AI can now produce convincing phishing without the translation, spelling and grammatical mistakes that used to reveal it. The FBI says the same. Attackers can also feed public details about your company into an AI tool and get back a message with the right names, the right job titles, and a believable reason to be in touch.

Why these emails are so convincing now

- The writing is clean. A scam email reads like a normal business email, because a machine wrote it in seconds, in whatever tone the attacker asked for.
- It's personal. Attackers can feed public details about your company into an AI tool, pulled from your website, your team's LinkedIn profiles, or a press release, and get a message tailored to you: the right names, the right job titles, and a believable reason to be in touch.
- There's more of it. AI makes each message faster to produce, so attackers send far more. The FBI's Internet Crime Complaint Center added a section on AI to its annual report for the first time, tied to more than 22,000 complaints and nearly $893 million in reported losses.

Your spam filter won't catch them all

It's tempting to assume your email security will handle this but a well-written, personalized email that asks a normal-sounding question doesn't always look dangerous to a filter, especially when it carries no obvious bad link or attachment. Both the NCSC and the FBI expect AI to push more of these messages through, which is why the last line of defense is a person who knows what to check.

It's not just email anymore

AI has done the same thing to phone calls and texts. The FBI warns that criminals can clone a voice from a short audio clip, enough to leave a voicemail that sounds like your boss or a family member asking for an urgent payment. The same thing that makes AI emails so convincing makes AI phone scams convincing too. The defense is the same: if a call or voicemail asks for money or logins, hang up and call the person on a number you already have.

Here are the signs you should still pay attention to

If you can't trust how an email is written, look at what it's asking you to do:

- It asks for money, gift cards, or a payment to a new account.
- It asks for a login, a verification code, or personal details.
- It creates pressure: a deadline, a threat, or a "do this now."
- It asks you to change the bank
- details for an invoice or a supplier.
- It comes with a link or attachment you weren't expecting.
- The display name looks right, but the actual email address doesn't match it.

So, the rule to teach your team is simple: when it is about money, logins, or how you pay someone, slow down before you act.

How to protect your team

- If an email asks you to pay a new account or change a supplier's bank details, call the person on a number you already have.
- Tell them to look at what the email is asking for, and to slow down when it's about money or logins.
- Make one rule for payment changes: confirm every change to bank details by phone, even when it's urgent.
- Turn on phishing-resistant MFA or passkeys, so a stolen password is harder to use even if someone gets tricked.
- Make it easy to report a suspicious email and make sure nobody feels silly for checking.
- Remind the team now and then that scam emails look perfect these days. A quick five-minute chat beats a poster nobody reads.

CYBERPOWER PFC SINEWAVE UPS

The CyberPower PFC Sinewave UPS is basically a battery in a box that your computer plugs into instead of the wall socket, so it keeps running through a cut and gives you time to save everything and shut down properly.

It diverts excess voltage away from sensitive electronic equipment during an AC power surge or power spike to prevent damage.

At around $270, it's cheap protection against losing a day's work to a power cut.

IS YOUR BUSINESS WEBSITE A SECURITY RISK?

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.

How it happens

Attackers 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, or 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.

How to keep your website safe

- Keep everything updated. WordPress, plugins, and themes all need updating when new versions come out. Many sites can be set to update automatically.
- Remove plugins you don't use. Every extra plugin is another thing that can go wrong.
- Stick to well-known plugins. Use ones that are popular, well-reviewed, and updated recently.
- Watch for abandoned plugins. Sometimes a plugin stops getting updates or gets removed from the store because of a security problem. Check now and then that your plugins are still supported and replace any that aren't.
- Lock down the admin login. Use a strong, unique password for the website's admin account, and turn on multi-factor authentication.
- Add a security plugin or web firewall. A reputable one can block common attacks and warn you when something changes.
- Keep backups. If the worst happens, a recent backup lets you restore the site instead of rebuilding it from scratch. Know who's responsible. Decide who looks after updates and security, whether that's your web designer, your IT provider, or your hosting company, and make sure it's clearly somebody's job.

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.

1. 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.
2. Tell your team what's down and what to use instead. Otherwise, someone spends an hour rebooting a laptop that was never the problem.
3. Switch to your backup way to communicate. Move to phone, text, or another app so the team can still coordinate and reach customers.
4. Tell customers if it affects them. If you can't take bookings or payments, say so and tell them when to try again.
5. Note when it started and what's affected. It helps you follow up afterward and spot anything that needs fixing once things are back.

A few things that make outages hurt less

- Keep key files available offline. With OneDrive or SharePoint, recent files can sync to the device so you can still open them when the service is down.
- Have a backup way to get online. A mobile hotspot from a phone can get a few key people working again if your main internet drops.
- Know your status pages. It's the fastest way to tell whether the problem is them or you.
- Keep contacts off the cloud. Have your important phone numbers and contacts somewhere that doesn't need the internet.
- Ask your IT provider about alerts. Many can set up a warning that tells you about an outage before your customers do.

Keep this to a single page, somewhere you can reach without your main systems, whether on paper or on an app. Write down your critical tools, your backup way to communicate, where the essentials live, who's in charge, and who to call. Review it once or twice a year so the names and numbers stay current.

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.
- Never download software from an ad. Type the maker's address yourself.
- Bookmark the sites you often log into.
- 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 top results can be a trap. Most have never been warned.
- If someone clicked a bad link, change the password and have the device checked.

ONEDRIVE OR SHAREPOINT? WHERE FILES SHOULD LIVE

f 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.

1. Put anything the team works on in SharePoint or a Teams channel, not in one person's OneDrive.
2. Keep OneDrive for your own drafts, and don't let it become the only home for a shared file.
3. Get important files off local desktops. A file only on a laptop isn't backed up or shared.
4. 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.

THE 30-MINUTE IT CHECK TO DO ONCE A MONTH

Most owners only look at their IT once something has broken, and by then it costs more to fix. Verizon's 2026 Data Breach Investigations Report found that 31% of breaches started with software that hadn't been patched. The fix already existed. Half an hour a month catches most of it.

- 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.
- Subscriptions. Read what you're paying for. Licenses for people who left are common, and so are two tools doing the same job.
- Write down what you find and fix it afterward. Thirty minutes only works if you don't stop to fix things along the way.
- Put it in the calendar on a fixed day and give it to the same person each month.

PHISHING vs. FISHING