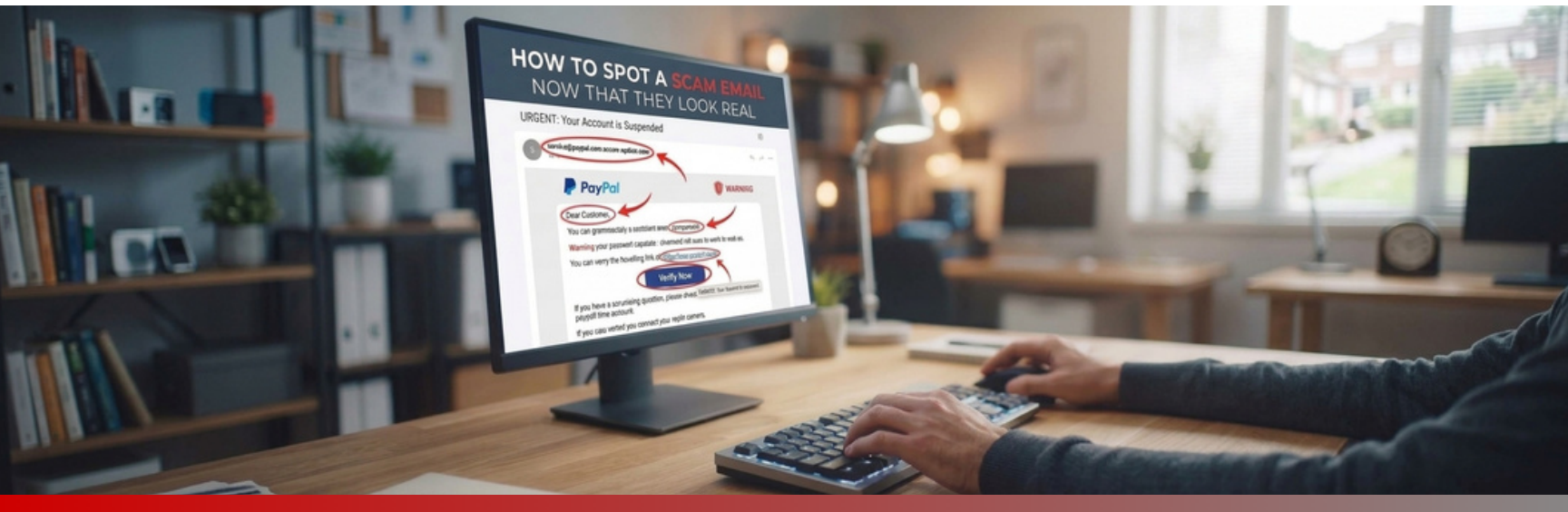
September 2026



TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

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
Technology Trivia — 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! -

Christopher McManus
President & CEO

HOW TO SPOT A SCAM EMAIL NOW THAT THEY LOOK REAL

For years, the advice was simple: watch for bad spelling and awkward grammar. Today, scammers use AI to write polished emails, so those warning signs are no longer enough. Messages arriving in your team's inbox can look just as professional as emails from a legitimate company.

Why the old advice stopped working

Spelling mistakes once helped expose scams because many attackers were writing in a language that wasn't their own. AI has changed that.

The UK's National Cyber Security Centre says generative AI can create convincing phishing messages without the translation, spelling, and grammar mistakes that once gave them away. The FBI has issued similar warnings.

Attackers can also use public information about your business to create messages with familiar names, job titles, and believable reasons for contacting your team.

Why these emails are so convincing now

• The writing is clean. AI can create professional-looking emails in seconds and match almost any tone the attacker wants.

• It's personal. Attackers can use information from your website, LinkedIn profiles, or public announcements to create messages tailored to your organization, including the right names, job titles, and a believable reason to respond.

• There's more of it. AI allows scammers to create messages much faster, making it easier to target more people. The FBI's Internet Crime Complaint Center reported more than 22,000 complaints involving AI and nearly $893 million in reported losses.

Your spam filter won't catch them all

It's tempting to assume your email security will stop every scam. But a well-written, personalized message asking a normal-sounding question may not look dangerous to a filter, especially when there's no obvious malicious link or attachment.

That's why your team is still an important line of defense.

It's not just email anymore

AI is making phone and text scams more convincing too. The FBI warns that criminals can clone a voice from a short audio clip, creating a voicemail that sounds like your boss, coworker, or family member asking for an urgent payment.

The defense is simple: if a call or voicemail asks for money or login information, stop and verify it using a number you already trust.

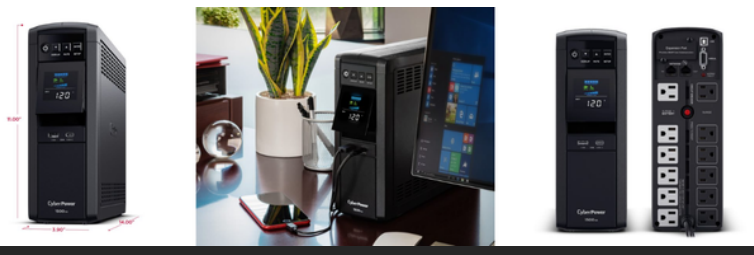
Here are the signs to still watch for

If you can't rely on how an email is written, pay attention to what it asks you to do:

- It asks for money, gift cards, or payment to a new account.
- It asks for a login, verification code, or personal information.
- It creates pressure with a deadline, threat, or "do this now" message.
- It asks you to change bank details for an invoice or supplier.
- It includes a link or attachment you weren't expecting.
- The display name looks correct, but the actual email address doesn't match.
- The rule for your team is simple: when it involves money, logins, or payment changes, slow down before you act.

How to protect your team

- If an email asks you to pay a new account or change supplier bank details, call the person using a number you already have.
- Teach employees to focus on what the message is asking them to do, especially when money or logins are involved.
- Make one rule for payment changes: confirm every bank-detail change by phone, even when the request sounds urgent.
- Turn on phishing-resistant MFA or passkeys, so a stolen password is harder to use if someone gets tricked.
- Make reporting suspicious emails easy, and remind employees that checking first is always encouraged.
- Remind your team that scam emails can look perfect today. A quick five-minute conversation can be more effective than a security 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 may be working perfectly today, but that doesn't mean it's being maintained properly. Many small businesses launch a website and rarely think about what happens behind the scenes.

That's where problems can begin.

WordPress powers more than 40% of websites, and the platform itself is well established. The bigger concern is often the plugins and themes added to it, especially when they haven't been updated in months or years.

How it happens

Attackers use automated tools to scan websites for known security weaknesses. When a plugin developer discovers a flaw, an update may fix it. Until that update is installed, the weakness can remain open.

Researchers regularly find that many WordPress vulnerabilities come from plugins and themes rather than WordPress itself.

What can happen after a website is compromised

A hacked website doesn't always look hacked. Attackers may quietly use it to:

- Send malware to visitors or redirect them to unsafe pages.
- Create hidden spam or scam pages using your website's reputation.
- Capture information entered into contact or checkout forms.

The impact can reach your customers and your reputation. Search engines may flag a compromised website, while browsers can display warnings that make visitors think twice before continuing.

How to keep your website safer

- Remove plugins you no longer need.
- Choose reputable, actively maintained plugins.
- Replace software that has been abandoned or unsupported.
- Protect administrator accounts with strong passwords and MFA.
- Consider a reputable security plugin or web firewall.
- Maintain recent backups so recovery is possible if something goes wrong.

Most importantly, know who is responsible for website updates, security, and backups. Whether that's your web designer, hosting company, or IT provider, make sure the responsibility belongs to someone.

WHAT TO DO WHEN MICROSOFT 365 GOES DOWN

Technology outages happen, even with services your business relies on every day.

In July 2024, a faulty software update caused around 8.5 million Windows computers to crash within hours. It wasn't an attack—it was a bad update.

When a service goes down, there may be nothing you can fix locally. What matters is having a simple plan that helps your team keep moving.

Five steps to take

1. Check whether it's just you. Visit the provider's status page or ask whether others are seeing the same problem. If it's a widespread outage, restarting every computer won't solve it.

2. Tell your team what's affected. Let employees know what is unavailable and what they should use instead.

3. Switch communication methods. Use phone calls, text messages, or another available app so your team can continue coordinating.

4. Keep customers informed. If an outage affects bookings, payments, or service, let customers know what's happening and when they should try again.

5. Record what happened. Note when the outage started, what was affected, and anything that needs attention afterward.

A little preparation goes a long way

- Keep important files available offline when possible.
- Have a backup internet option, such as a mobile hotspot.
- Know where to check service status.
- Keep important contacts available offline.
- Ask your IT provider about outage monitoring and alerts.

Keep your outage plan somewhere accessible even when your main systems aren't working. Include critical tools, backup communication methods, important contacts, responsibilities, and recovery steps.

Review it once or twice a year so the information stays useful.

WHY YOU SHOULD SCROLL PAST THE FIRST RESULT ON GOOGLE

When you search for software or a website to log in to, the first result may look like the obvious choice.

But the first result isn't always the safest.

Scammers can pay for search advertisements using familiar company names, putting fake websites above the legitimate ones.

A few habits can help:

- Scroll past sponsored results when you're looking for important software or login pages.
- Never download software simply because an advertisement appeared first. Go directly to the manufacturer's official website.
- Bookmark websites your team regularly uses.
- Check the web address carefully before entering a password.
- Keep browsers and devices updated.
- Remind your team that search results can be misleading.
- If someone clicks a suspicious link, change the affected password and have the device checked.

A few extra seconds can prevent a much bigger problem.

ONEDRIVE OR SHAREPOINT? WHERE YOUR BUSINESS FILES SHOULD LIVE

If your business uses Microsoft 365, your team has access to both OneDrive and SharePoint. The challenge is knowing which one should hold which files.

The simple rule is:

OneDrive is your personal work space. SharePoint is your team's work space.

Files shared through a Microsoft Teams channel are already stored in SharePoint.

Keep your files organized by following four simple rules:

1. Put shared work in SharePoint. If several people need access, don't keep the only copy in one employee's OneDrive.
2. Use OneDrive for personal working files. Drafts and documents you're working on alone can stay there, but shared business files should have a team-owned home.
3. Move important files off individual computers. A file stored only on someone's laptop can be difficult for others to access and may not have the protection your business needs.
4. Agree on a simple rule. For example, "client files live in the client's SharePoint folder." Clear rules eliminate guesswork.

This becomes especially important when someone leaves the organization. Their OneDrive should not be the only place where important company files exist.

Make sure shared business information is stored where the team—not one individual can access it.

THE 30-MINUTE IT CHECK TO DO ONCE A MONTH

Most business owners don't look closely at their technology until something breaks. By then, a small issue can become a bigger and more expensive problem.

Verizon's 2026 Data Breach Investigations Report found that 31% of breaches started with software that hadn't been patched. The fix already existed—the update simply hadn't been installed.

Set aside 30 minutes once a month to look for problems before they become disruptions.

Check these areas:

- Updates. Make sure device and software updates are actually installing, rather than sitting at "restart required."
- Backups. Check when a file was last restored successfully. If nobody has tested a restore, you don't really know whether the backup will work when needed.
- User access. Every account should belong to someone who still needs it. Remove access that is no longer necessary.
- Multi-factor authentication. Make sure MFA is enabled, especially for email and other important accounts.
- Devices. Review connected devices. If you don't recognize one, find out what it is and who is using it.
- Subscriptions. Review what your business is paying for. Former employees may still have licenses, while multiple tools may be doing the same job.
- Record what you find. Don't spend the entire 30 minutes fixing problems. Write them down and follow up afterward.

Make it a routine.

Put the check on the calendar for the same day every month and assign it to the same person.

Thirty minutes of attention each month can help your business catch small technology problems before they become expensive interruptions.

POWERPRO COMPUTERS

Technology should make running your business easier, not create more uncertainty.

PowerPro Computers helps businesses stay productive with practical technology guidance, dependable support, and solutions built around how you actually work.

Have a technology question or something that doesn't seem right? Talk with the PowerPro Computers team.

TECHNOLOGY TRIVIA TIME

Think You Know Your Tech?

It's time to put your technology knowledge to the test!

Each month, **PowerPro Computers** brings you a new Technology Trivia challenge. Answer correctly for your chance to win a **$50 Amazon eGift Card**

CLICK LINK & TAKE THE QUIZ

Click below to answer this month's Technology Trivia question and enter for your chance to win.

Click Here

A winner will be randomly selected for each newsletter from among those who answered correctly.

LAST MONTH'S ANSWER
Long Term Evolution