PEGGNET COMPUTERS



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 straightforward: look for spelling mistakes, awkward grammar, and clumsy wording. That advice is becoming less useful. Scammers now use AI to create polished emails that can sound just like messages from a legitimate business. A scam can look professional from the moment it reaches your team's inbox.

Why the old advice stopped working

Traditional phishing emails often contained obvious language mistakes because criminals were writing in a language that was not their own. AI has changed that. The UK's National Cyber Security Centre says generative AI can produce 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 organization to create a message that feels personal. Company websites, team LinkedIn profiles, and press releases can provide names, job titles, and other details that make a fraudulent request believable.

Why these emails are so convincing now

• **The writing is polished.** AI can create a professional-sounding message in seconds and match almost any business tone.

• **It's personal.** Attackers can combine public details about your organization with AI to create messages using familiar names, roles, and believable reasons for contacting your team.

• **There's more of it.** AI allows criminals to create convincing messages faster, so they can target more people. The FBI's Internet Crime Complaint Center included an AI section in its annual report for the first time, connected to more than 22,000 complaints and nearly $893 million in reported losses.

Your spam filter won't catch them all

It is easy to assume your email security will handle suspicious messages. But a polished, personalized email asking a normal-sounding question may not look dangerous to a filter, particularly when there is no obvious malicious link or attachment.

Both the NCSC and the FBI expect AI to increase the volume of these attacks. That makes your employees an important final layer of defense. They need to know what the message is asking them to do, not simply whether the writing looks professional.

It's not just email anymore

AI is also changing phone calls and text scams. The FBI warns that criminals can clone a voice from a short audio recording and create a voicemail that sounds like a boss or family member asking for urgent payment.

The defense is straightforward: if a call or voicemail asks for money or . login information, end the conversation and contact the person using a phone number you already trust.

Here are the signs you should still pay attention to

If you cannot judge an email by its writing, focus on the request:

• It asks for money, gift cards, or payment to a new account.
• It asks for a password, verification code, or personal information.
• It creates pressure through a deadline, threat, or urgent instruction.
• It asks you to change bank details for an invoice or supplier.
• It includes a link or attachment you were not expecting.
• The display name looks familiar, but the actual email address does not match.

The rule for your team is simple: when an email involves money, logins, or payment details, slow down before acting.

How to protect your team

• If an email requests payment to a new account or a supplier bank-detail change, 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.
• Create one clear rule for payment changes: verify every bank-detail change by phone, even when the request appears urgent.
• Turn on phishing-resistant MFA or passkeys, making stolen passwords harder to use if someone is tricked.
• Make suspicious-email reporting simple, and create a culture where employees feel comfortable checking before they act.
• Remind your team regularly that modern scam emails can look professional. A short five-minute conversation can be more effective than a poster nobody reads.

A professional appearance is no longer proof that a message is safe, so your team needs a process for verifying requests before money, credentials, or information leaves the organization before anyone clicks or pays.







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 easy to forget once it is live. It sits there doing its job, so it may seem fine to leave it alone. From an IT perspective, that is exactly why a neglected website can become an easy target for attackers. Many small-business sites run on WordPress, which powers more than 40% of all websites. WordPress itself is solid. The risk is often its plugins and themes, especially when they go years without updates.

How it happens

Attackers use automated tools to scan huge numbers of websites for known weaknesses, such as an outdated plugin with a security flaw. When a plugin developer discovers a problem, they release an update. Until that update is installed, the weakness remains open, and attackers know what to search for.

Researchers tracking WordPress vulnerabilities find that most flaws are found in plugins and fthemes rather than WordPress itself.

What a hacked site gets used for

A compromised website may not look hacked at all. Attackers often keep it running while quietly using it for their own purposes:

• Serving malware to visitors or sending them to pages designed to install malicious software.
• Creating hidden spam and scam pages that take advantage of your website's search-engine reputation.
• Capturing information entered into contact or checkout forms, including payment details.

The damage can quickly become your problem. Search engines may flag compromised websites and lower their rankings. Browsers may also block them, leaving customers with a warning that the site may be dangerous instead of your homepage.

Is your site at risk?

That depends on how your website is built. If you use a hosted platform such as Wix, Squarespace, or Shopify, much of the security and updating is handled by the provider, so your risk is lower today.

If you have a self-hosted WordPress website, often set up by a designer or agency on your own hosting account, someone needs to manage WordPress, plugins, and themes. The important question is who, exactly. On many small-business websites, the honest answer is that nobody has checked them since launch.

How to keep your website safe

• Keep everything updated. WordPress, plugins, and themes need updates when new versions are released. Many websites can enable automatic updates.
• Remove plugins you do not use. Every additional plugin creates another potential weakness.
• Choose established plugins. Look for options that are popular, well-reviewed, and recently updated.
• Watch for abandoned plugins. A plugin may stop receiving updates or be removed because of a security issue. Check periodically that yours are still supported and replace anything that is not.
• Secure the admin login. Use a strong, unique password for the website administrator account and enable multifactor authentication.
• **Add security protection.** A reputable security plugin or web firewall can block common attacks and alert you when something changes.
• **Keep backups.** If your website is compromised, a recent backup can help you restore it instead of rebuilding everything from scratch.

A website does not need to be famous to be targeted; scanners look for weaknesses, not reputation.

Know who's responsible

Decide who manages website updates and security, whether that is your web designer, IT provider, or hosting company. Then make sure the responsibility is clearly assigned to someone.

WHAT TO DO WHEN MICROSOFT 365 GOES DOWN

Your team relies on Microsoft 365 for email, files, meetings, and everyday communication. So when the service goes down, the natural reaction is to start troubleshooting. Before everyone starts restarting computers or changing settings, take a breath. If the problem is with Microsoft, there may be nothing to fix on your side.

In July 2024, a faulty software update caused around 8.5 million Windows computers to crash within a few hours. It wasn't a cyberattack. It was a bad update. Situations like this are a reminder that even reliable technology can experience unexpected outages. These five steps can help your business stay organized while you wait.

1. Check whether it's your environment or a wider outage. Start with the provider's status page and ask whether other users are experiencing the same issue. If Microsoft is having a broader problem, your team doesn't need to spend time troubleshooting devices that are working normally.

2. **Give your team clear instructions.** Tell employees which services are unavailable and what they should use instead. A simple message can prevent everyone from independently troubleshooting the same problem.

3. **Move to your backup communication method.** If Teams or email is unavailable, use phone calls, text messages, or another approved app. Your team should still be able to coordinate and communicate with customers.

4. **Keep customers informed.** If the outage prevents bookings, payments, or another customer-facing service, explain what's happening and tell customers when they should

5. Record what happened. Note when the outage started, which services were affected, and when they returned. That information gives your IT team a useful record for follow-up.

A few simple preparations can make outages easier

• **Keep important files available offline.** OneDrive and SharePoint can sync recent files to devices, allowing employees to access them when the service is unavailable.

• **Have another way to get online**. A mobile hotspot can help key employees stay connected if your primary internet connection fails.

• **Know where to check service status.** Provider status pages can quickly tell you whether the issue is widespread or specific to your organization.

• **Keep important contacts offline.** Store critical phone numbers somewhere that doesn't depend on your cloud systems or internet connection.

• **Ask your IT provider about outage alerts**. Early notifications can help your team understand what's happening before customers begin asking questions.

Keep this plan to one page and store it somewhere you can access without your main systems. Write down your critical tools, backup communication method, where essential information is stored, who is responsible, and who to call. Review it once or twice a year so the information stays current.

The outage may be outside your control. **How prepared your business is for it isn't.**

WHY YOU SHOULD SCROLL PAST THE FIRST RESULT ON GOOGLE

When you search Google for software, a login page, or a service you need, the first result isn't always the safest one. Sponsored results can appear above the legitimate website, and scammers can pay for those positions to make fake sites look trustworthy.

The goal is simple: get you to click before you stop to verify where you're going.

• Look past the sponsored results when searching for software or important login pages.

• Never download software from an advertisement. Instead, type the software maker's known website address directly into your browser.

• Bookmark the websites your team regularly uses for logins, so you don't have to search for them each time.

• Before entering a password, check the website address carefully. A familiar-looking page doesn't guarantee you're on the real site.

• Keep browsers and devices updated. Security updates can help reduce the chance that a malicious download can cause further problems.

• Make sure your team knows that the top Google result isn't automatically the right one. A quick reminder can prevent an unnecessary mistake.

• If someone clicks a suspicious link, don't ignore it. Change the affected password and have the device checked.

A few extra seconds of verification can be much easier than recovering from a compromised account.

ONEDRIVE OR SHAREPOINT? WHERE SHOULD YOUR BUSINESS FILES LIVE?

If your organization uses Microsoft 365, your team has access to both OneDrive and SharePoint. They serve different purposes, and knowing which one to use can prevent files from becoming difficult to find, share, or recover.

Think of OneDrive as your personal workspace and SharePoint as the organization's shared workspace. Files stored in a Teams channel are already stored in SharePoint.

1. Put documents your team works on together in SharePoint or the appropriate Teams channel. Don't make one employee's OneDrive the permanent home for a shared business file.

2. Use OneDrive for your individual drafts and files that don't need to be shared with the wider team.

3. Move important business files off local desktops. A document stored only on one laptop can be difficult to access when someone is away, and it isn't automatically a shared business resource.

4. Establish a simple company rule for where files belong. For example, "Client files live in the client's SharePoint folder." Clear rules remove guesswork and make files easier for everyone to manage.

There is another reason this matters: when an employee leaves, their OneDrive is retained for only 30 days by default before it is deleted. Anything the business needs should already be stored in the appropriate SharePoint location.

Good file organization isn't just about convenience. It helps your team maintain access to important business information when people, devices, or circumstances change.

THE 30-MINUTE IT CHECK TO DO ONCE A MONTH

Most owners check IT when something breaks. By then, issues cost more to fix. Verizon's 2026 Data Breach Investigations Report found 31% of breaches started with software that hadn't been patched. The fix existed. Thirty minutes can catch issues early.

- **Updates.** Confirm device and software updates are installing, not waiting at "restart required".
- **Backups.** Check when a file was last restored. If nobody has tested it, you don't know the backup works.
- **Who has access.** Make sure every user account belongs to an active employee.
- **Multi-factor authentication.** Confirm MFA is enabled for everyone.
- **Devices.** If there's a device you don't recognize, find out who is using it.
- **Subscriptions.** Review what you're paying for. Former employees may still have licenses, and multiple tools may do the same job.
- **Write down what you find and follow up afterward**.

  The 30-minute check works best when you review first and fix issues afterward.
- **Put it on the calendar for a fixed day and assign it to the same person each month.**

TECHNOLOGY TRIVIA TIME

Think You Know Your Tech?

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

Each month, **Peggnet 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