OASIS TECHNOLOGIES

SEPTEMBER 2026

TECH TALK MONTHLY

How to Spot a Scam Email

Now That They Look Real

Inside:

What's Inside

Dear Fellow Business Owner 👋

Most of what causes trouble for a small business looks completely normal. Nothing about it stands out, so nobody checks it.

A scam email used to give itself away with bad spelling. Now AI writes them and they read perfectly. The first result on Google looks official, but anyone can buy that spot, including a scammer. A website that works fine can be running a plugin nobody has updated in three years.

The same goes for the things you assume are handled. Backups can fail every night for a month without anyone noticing, and you only find out when you need one. Accounts belonging to people who left last year are often still switched on. Half an hour a month spent checking would catch both.

That's what this month's issue is about: what to check, how often, and what to do when something does go wrong. If you'd like a hand setting any of it up, or you'd just like someone to look over how your business is protected, we're a phone call away.

Tony Loffi-Lara
CTO, Oasis Technologies, Inc.

DID YOU KNOW

Did you know? Wi-Fi doesn't stand for anything. A branding company invented the name in 1999, because the engineers' own term for it was "IEEE 802.11b Direct Sequence."

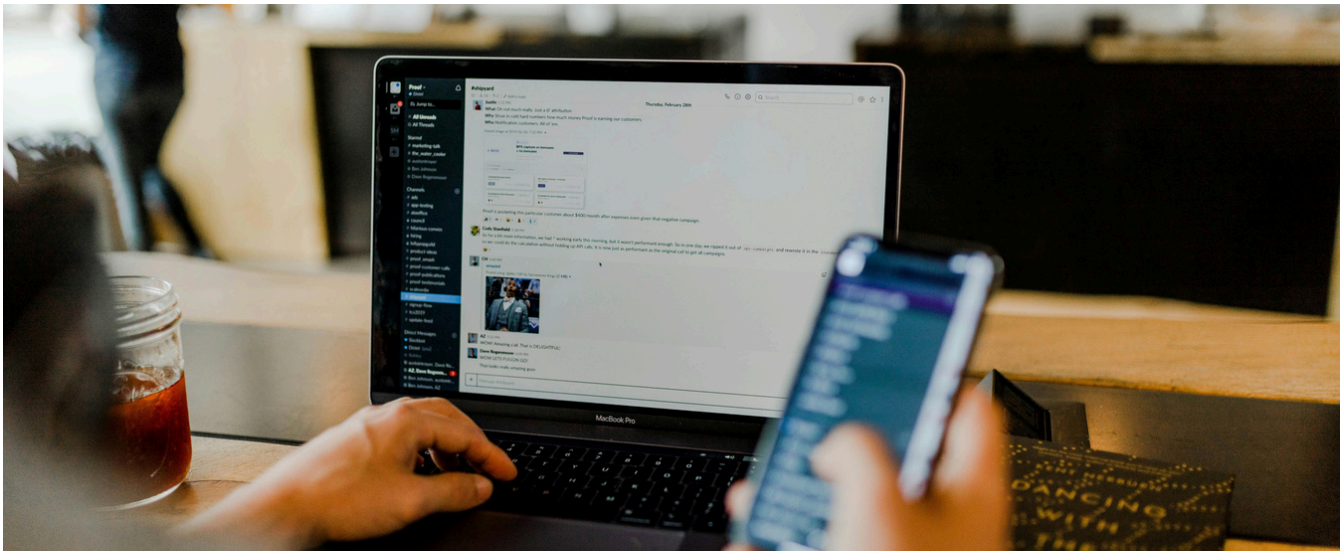
GET IN TOUCH

(405) 996-7124

oasis.tech/tony

tlara@oasis.tech

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 the 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.

What a scam email looks like now

Instead of "Dear customer, your account is suspended," someone in your finance team gets a message that looks like it came from a supplier they really deal with. It mentions a real project, and asks to update the bank details for the next invoice. It reads exactly like a real supplier email, and the only thing wrong with it is that the supplier never sent it. Your spam filter will catch a lot of these, but a well-written, personalized message with no obvious bad link doesn't always look dangerous to a filter.

How to protect your team

- Judge an email by what it asks for. How well it's written no longer tells you anything. Money, logins, and bank-detail changes are the warning signs.
- Confirm every change to a supplier's bank details by phone, on a number you already have, even when it's urgent.
- Stop telling staff to look for bad spelling. Tell them to slow down when a message involves money or logins.
- Turn on phishing-resistant MFA or passkeys, so a stolen password is harder to use.
- Make it easy to report a suspicious email, and make sure nobody feels silly for checking.

WHAT AI HASN'T CHANGED

- It asks for money, gift cards, or payment to a new account.
- It asks for a login, a verification code, or personal details.
- It pushes you with a deadline, a threat, or a "do this now."
- The display name looks right, but the email address behind it doesn't match.

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 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

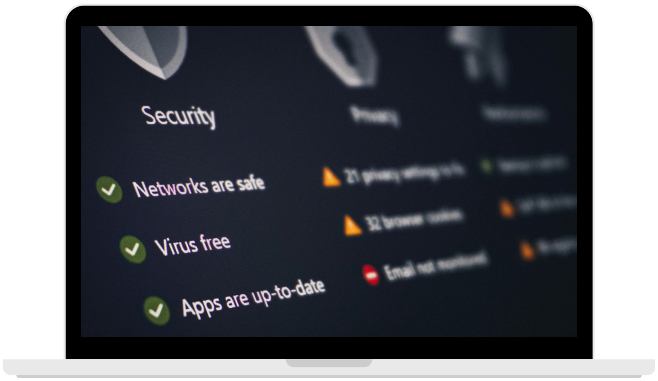
A hacked site rarely announces itself. Attackers usually keep it running and use it for their own purposes:

- 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,



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.

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.

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, so stop trying.

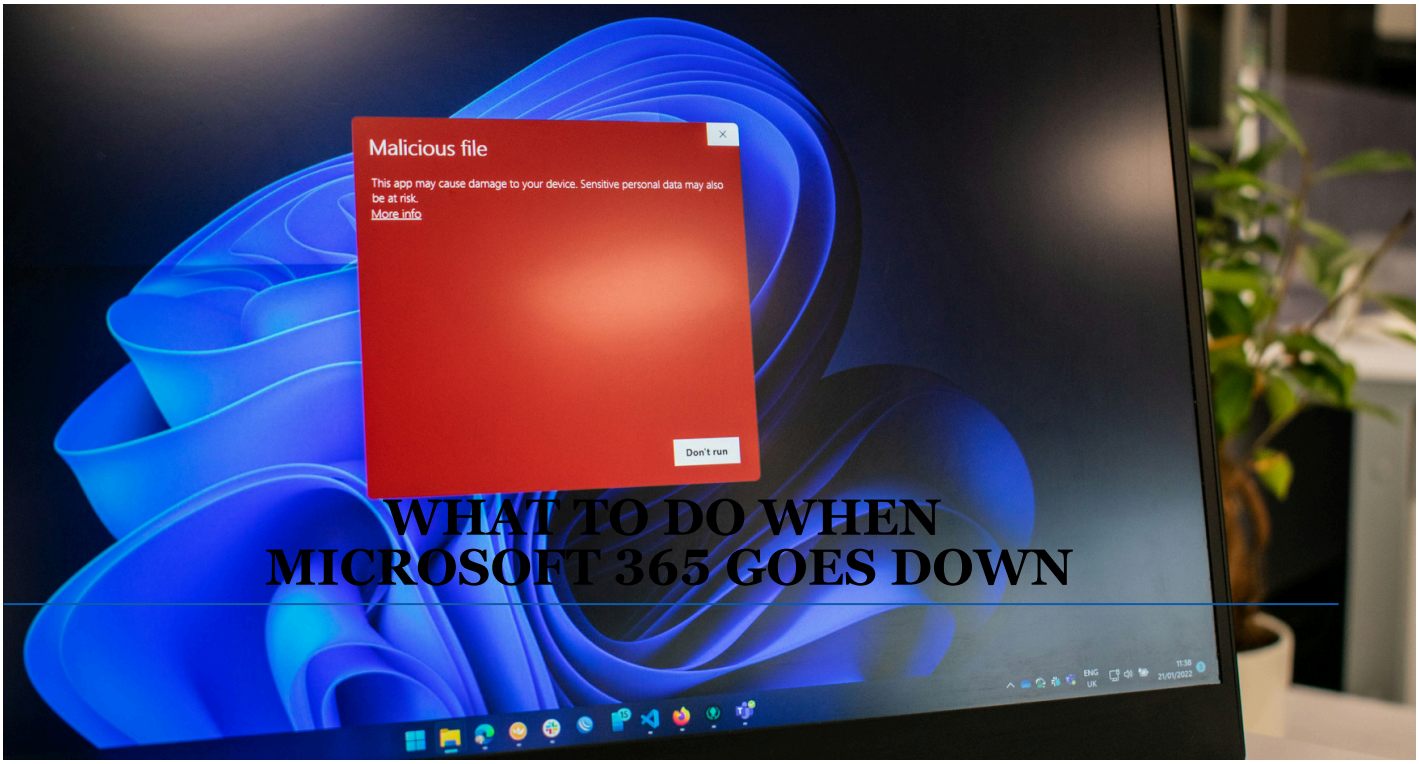
2. Tell your team what's down and what to use instead. Otherwise someone spends an hour rebooting a laptop that was never the problem.

3. Switch to your backup way to communicate. Move to the 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. 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.



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.

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.

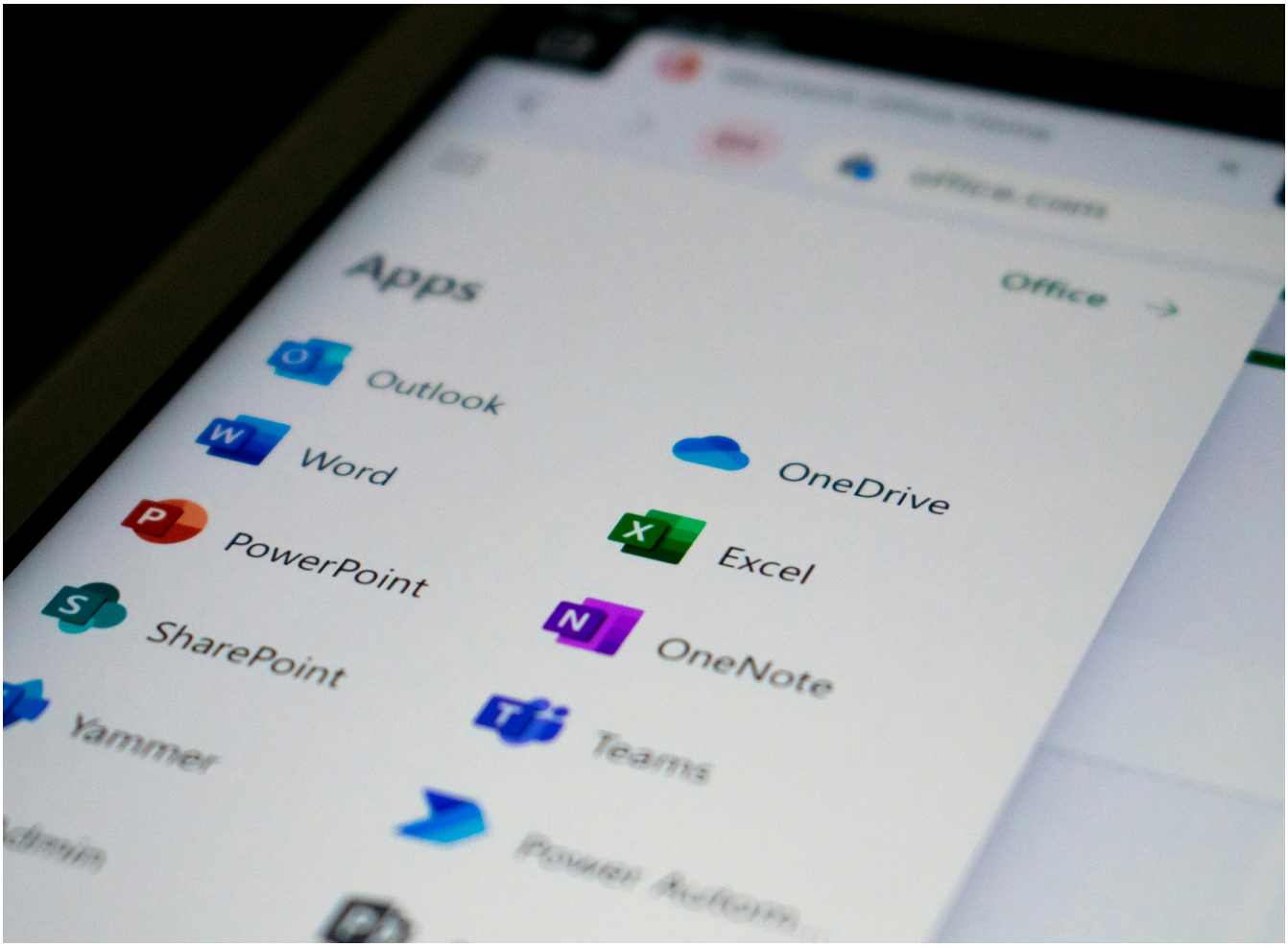
1. Put anything the team works on in SharePoint or a Teams channel, not in one person's OneDrive.

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.

Thank You!

Thanks for taking the time to read this month's newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW

OASIS TECHNOLOGIES

(405) 948-6500

info@oasis.tech

oasis.tech

6317 NW 23rd St.
Bethany, OK 73008