OASIS TECHNOLOGIES

AUGUST 2026

TECH TALK MONTHLY

QR CODE SCAMS:
What They Are and How to Spot Them

Inside:

What's Inside

Dear Business Owner 👋

Most of the businesses we talk to have some security in place. Far fewer have a plan for the first hour after something goes wrong.

That first hour matters more than almost anything that comes after it. When a cyberattack hits, the instinct is to start fixing things, and that's often what makes it worse: turning off the affected computer and wiping the evidence, replying from an email account the attacker is already reading, or paying a ransom before anyone understands what's going on.

Most of this is avoidable with a plan agreed before anything happens, and it doesn't need to be long. A single page covering who to call first, which devices to disconnect and which to leave alone, and where your backups are, kept somewhere you can reach without your main systems, is enough for most small businesses.

This month's issue walks through the threats we're seeing most, from QR-code scams to fake emails sent in your name, and what to do if one of them gets through. If you'd like help putting a simple plan together before you ever need it, we're a phone call away.

Tony Loffi-Lara
CTO, Oasis Technologies, Inc.

DID YOU KNOW ?

Did you know? The world's first webcam, set up at Cambridge University in 1991, was pointed at a coffee pot so researchers could see if it was empty before walking over.

GET IN TOUCH

(405) 996-7124

oasis.tech/tony

tlara@oasis.tech

QR CODE SCAMS: WHAT THEY ARE AND HOW TO SPOT THEM

QR codes are part of everyday business now. You scan them for menus, payments, Wi-Fi, and shared files. Scammers know that, and they've started hiding their links inside QR codes to get past the security that would normally catch a bad link in an email.

What a QR code scam is

A QR code scam, sometimes called “quishing,” swaps a written link for a QR code. You scan it with your phone, it opens a web page, and you land on a fake login or payment screen built to steal your details. The QR code is only the way the scammer gets you there. The page on the other end is the same kind of fake you'd see in any phishing attack, made to look like Microsoft 365 or your bank.

Why it gets past your security

Two things make these scams work. First, the link is hidden inside an image, and most email security scans the text of a message, not the picture, so the link can slip through. The UK's National Cyber Security Centre points out that this is exactly why criminals started using QR codes to disguise their links. Second, scanning a code moves you onto your phone, which usually has far less protection than your work computer. Microsoft reported that QR-code phishing jumped 146% in the first few months of 2026, most of it arriving as a code tucked inside a PDF attachment.

How to protect your team

- Treat a QR code in an email with the same caution as a strange link, especially if it asks you to log in or pay.
- Before you act, check the web address your phone previews when you scan. If it isn't the site you expected, close it.
- When in doubt, skip the code and go to the site directly by typing the address yourself.
- Use phishing-resistant MFA, so a stolen password is harder to use.
- Tell your team what these look like, with a real example, because most people have never been warned about this.

COMMON QR SCAMS TO WATCH FOR

- A fake “scan to keep your account active” email, often from “Microsoft” or “IT.”
- A QR code inside a PDF invoice, with a “scan to pay” prompt that sends your money to the scammer.
- A sticker placed over a real QR code on a parking meter or payment terminal.

HOW TO STOP SCAMMERS SENDING EMAIL IN YOUR COMPANY'S NAME

Right now, with no hacking at all, someone could send an email that looks like it came from your company. They put your domain in the “from” line and email your clients or suppliers, asking them to pay a fake invoice or move money to a new account. Because the message carries your name, the people who trust you are far more likely to act on it. It works because email was never built to check that senders are who they claim to be.

The three records that stop it

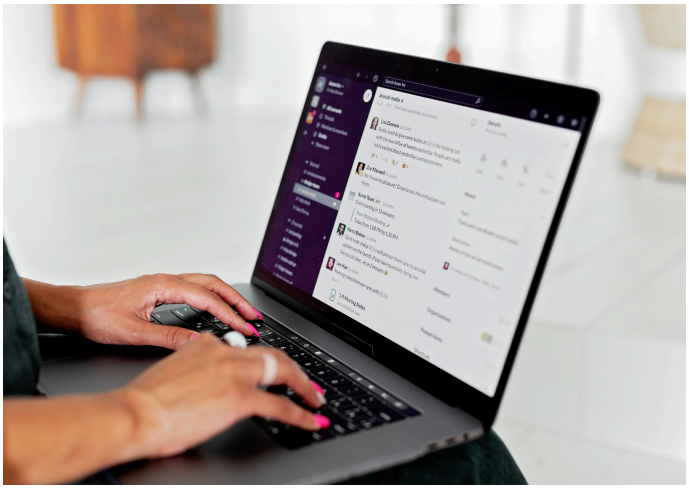
- **SPF** is a list of the mail servers allowed to send email for your domain.
- **DKIM** adds a tamper-proof signature that proves a message really came from you and wasn't changed on the way.
- **DMARC** ties the two together and tells receiving mail servers what to do with anything that fails the check.

The setting most businesses get wrong

Having the records isn't quite enough. DMARC has three settings, and most businesses stop at the wrong one. On “monitor only,” it watches and reports but never blocks a fake. Real protection starts when it's set to “quarantine” or “reject.” One thing these records don't stop: a lookalike domain (like yourcompany-invoices.com), or a display name that shows your company over a random address. So staff should still check the full email address before acting on any payment request.

How to switch it on without blocking your own email

DMARC is best turned up in stages. Start on “monitor only” and read the reports it sends, which show every



source sending email as your domain, including the ones that shouldn't. Once you've confirmed your real email passes, move to “quarantine,” then to “reject.” Done gradually, you close the door on impersonation without sending your own invoices and quotes to the spam folder.

Worth having even if you barely send email

Beyond protecting your name, these records help your messages arrive. Since early 2024, Google and Yahoo have required bulk senders to use SPF, DKIM, and DMARC, and Microsoft began applying similar rules to Outlook.com in 2025. Even below those volumes, a properly set-up domain is more likely to land in the inbox than the spam folder. You can check what yours has in place with a free DMARC checker, or ask your IT provider to confirm it and walk the policy up to full protection safely.

WHAT TO DO IN THE FIRST HOUR OF A CYBERATTACK

If your business is hit by a cyberattack, the first hour decides how bad it gets. The instinct is to start fixing things, and that's usually what makes it worse. Work through these five steps instead.

1. **Disconnect the affected devices from the network.** Unplug the network cable and turn off Wi-Fi so the problem can't spread to other computers or your backups. Try not to power the machine off, because that can wipe evidence of what happened.

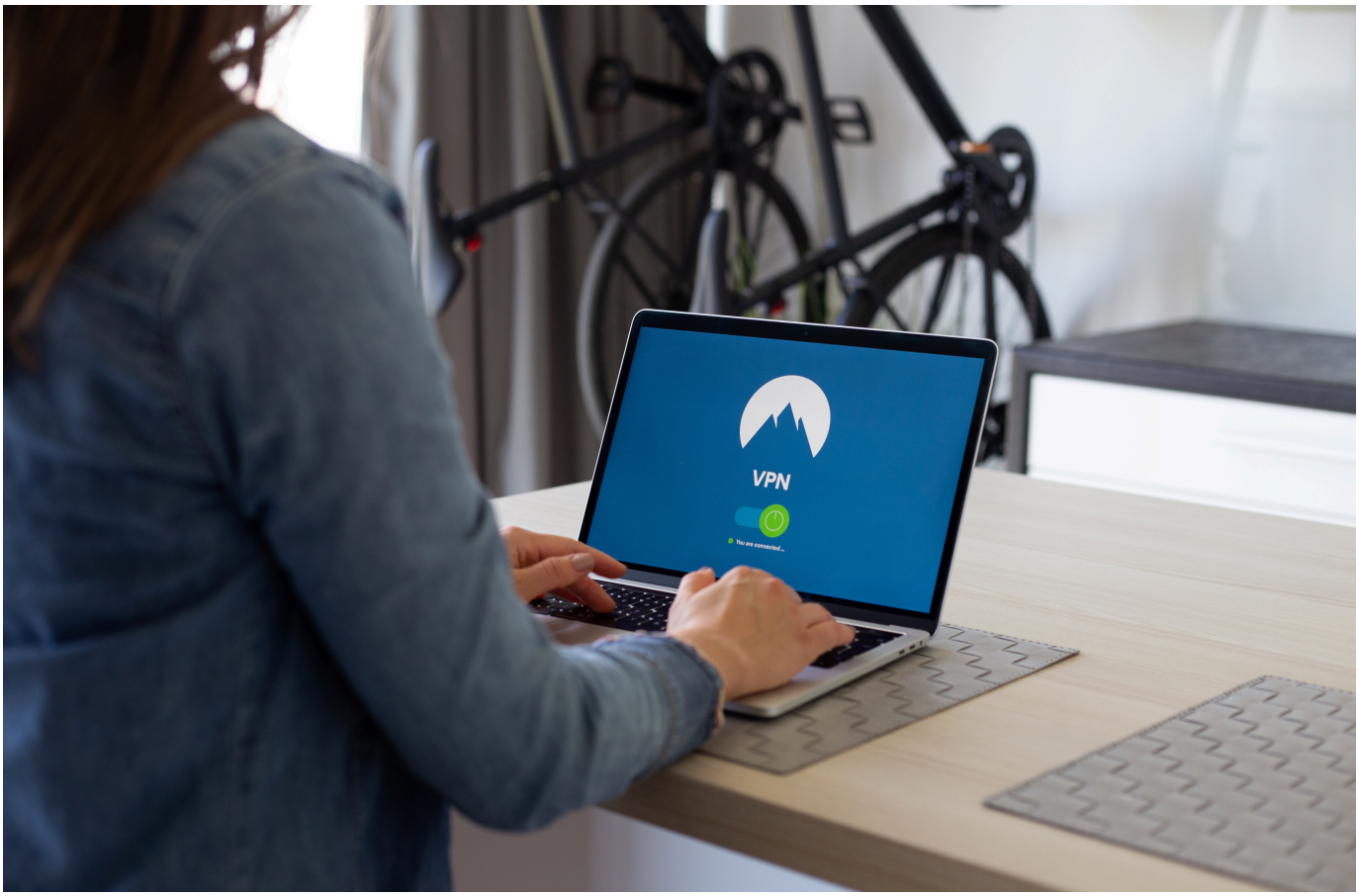
2. **Call your IT provider, by phone.** Don't email, in case the attacker is watching your inbox. If you have cyber insurance, call them next, since many policies want their incident team involved early.

3. **Leave the evidence alone.** Don't wipe, reinstall, or tidy up the affected machines yet. Screenshots are fine, but keep the originals.

4. **If money was sent, call your bank immediately.** Ask them to recall the transfer. With wire fraud, the first few hours make the biggest difference.

5. **Reset passwords from a clean device, and turn on MFA.** Start with email and admin accounts, using a device you know isn't affected.

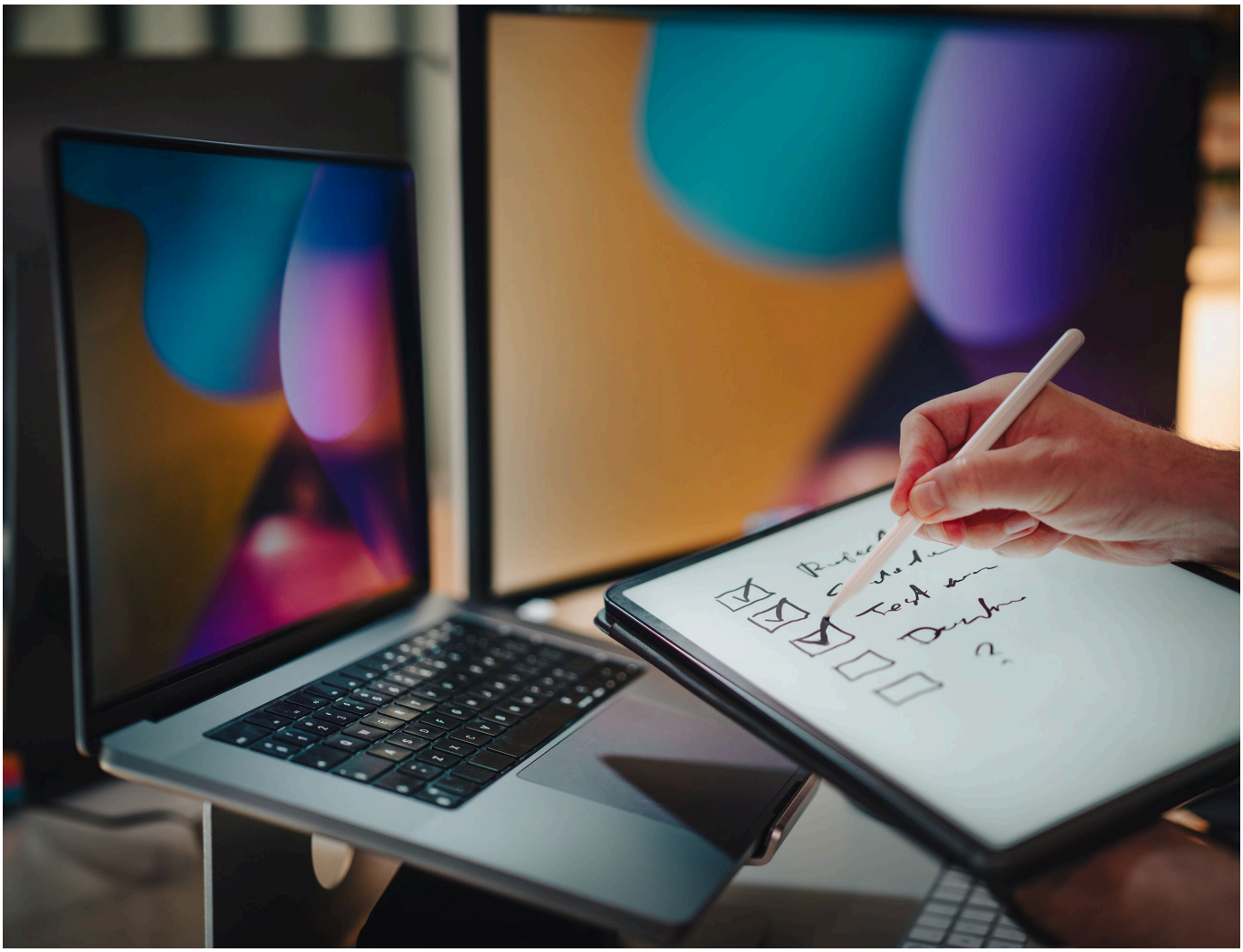
Then report it: in the US to the FBI's IC3, in the UK to the NCSC, in Australia to ReportCyber. And don't pay a ransom on the spot. The FBI doesn't recommend paying, and it's a decision to make with law enforcement and your insurer, not in the first panicked hour.



WHO CAN SEE WHAT YOUR AI NOTE-TAKER RECORDS?

AI note-takers join your meetings, record every word, and store it on the vendor's servers. They're worth using, but before you let one into a client or staff meeting, run these quick checks.

- Pick one approved tool, and ask staff not to connect others to company meetings.
- Turn off auto-join, so it only records when someone chooses to.
- Announce the recording and get everyone's consent before it starts.
- Check whether the tool uses your conversations to train its AI.
- Prefer a tool that keeps recordings inside your own Microsoft or Google account.
- Check who the summary gets emailed to by default.
- Keep bots out of legal, HR, and confidential client meetings.

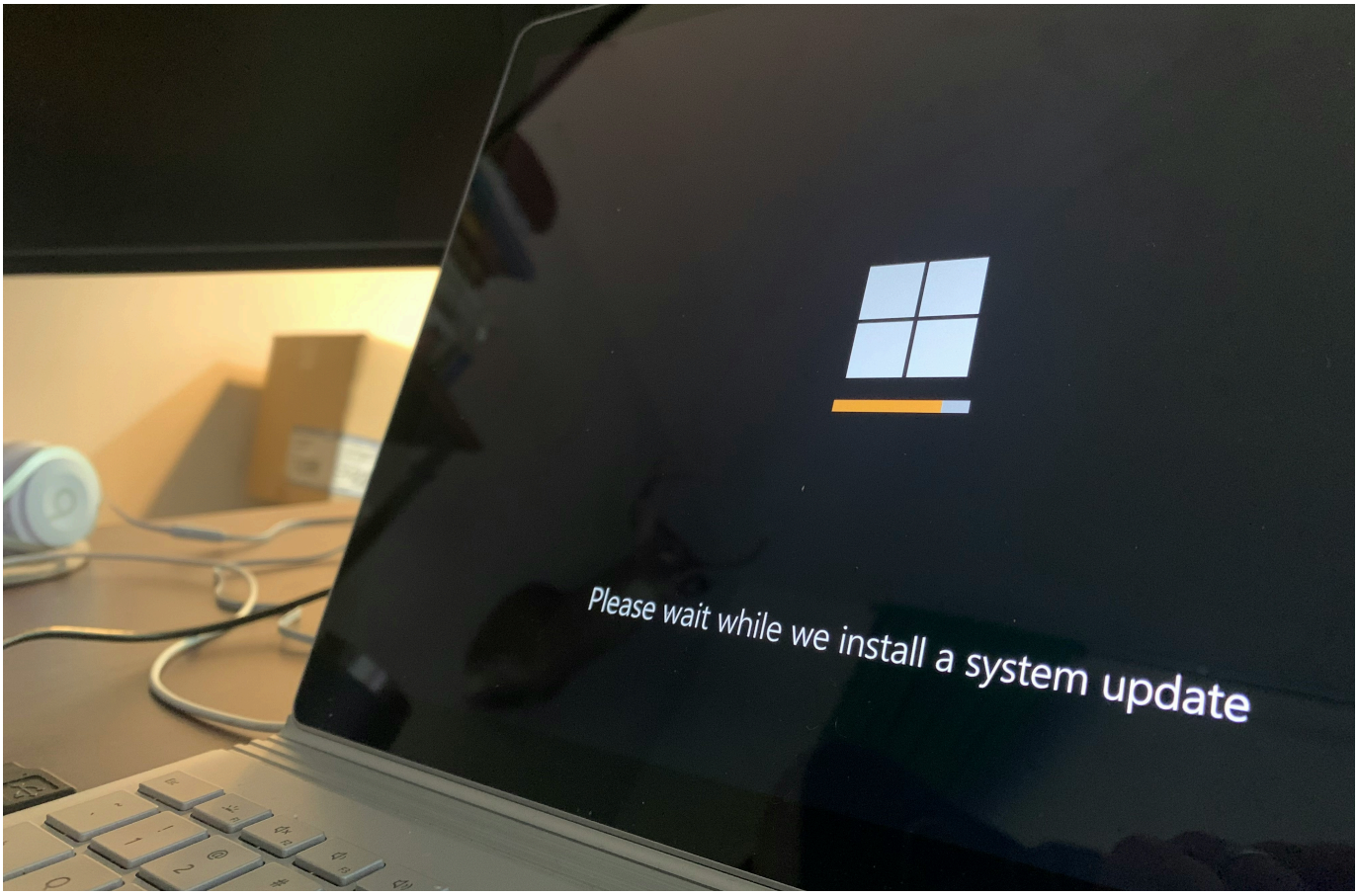


STILL ON WINDOWS 10? HERE'S WHY IT'S A RISK NOW

Windows 10 stopped getting security updates in October 2025. The computers still work, which is why it's easy to leave them, but every new flaw found now stays unpatched. That makes those machines easier to attack and can cause problems with compliance and your cyber insurance. Here's how to move off it:

1. List every computer still running Windows 10.
2. Check which ones can upgrade to Windows 11 (free if the hardware qualifies) using Microsoft's free PC Health Check app.
3. Upgrade the ones that qualify. The upgrade keeps your files and programs in place.
4. For the rest, choose between paid Extended Security Updates as a short-term bridge or replacing the PC.
5. Your IT provider can run this inventory quickly and tell you the best option for each machine.

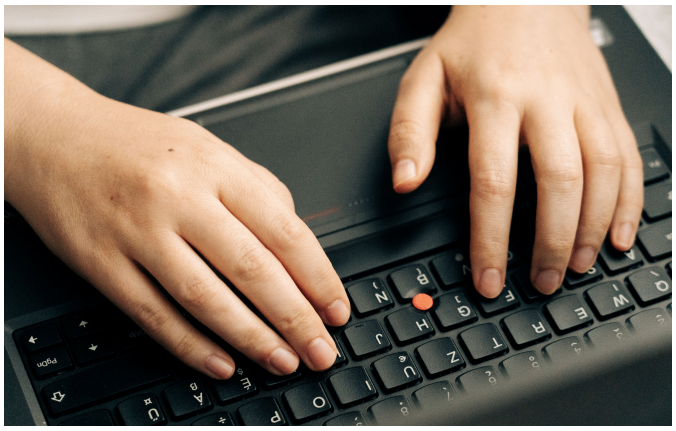
Your IT provider can run this inventory quickly and tell you the best option for each machine.



PASSKEYS: THE LOGIN THAT CAN'T BE PHISHED

Passwords are the weak point in most businesses. People reuse them, write them down, and type them into fake login pages. Passkeys replace them: you sign in with the same fingerprint, face, or PIN you use to unlock your phone, and there's no password for anyone to steal, guess, or phish.

- **Why they're safer:** nothing to phish, nothing for a hacker to steal in a breach, and nothing to reuse or forget.
- **Where they work:** Microsoft, Google, and Apple accounts, plus a growing list of banks and business tools.
- Included with Microsoft 365 at no extra cost.
- **They're faster:** Microsoft says a passkey sign-in takes about 3 seconds, against 69 for a password plus a code.
- **Two types:** a synced passkey is backed up to your account and works across your devices, while a device-bound passkey stays on one device or a physical security key.
- **Start with your most sensitive accounts:** administrators, finance, and anyone who can move money.



- **Let everyone else add a passkey** alongside their password at first.
- **Give each person a backup,** like a second device or a security key, so a lost phone doesn't lock anyone out.
- **Keep passwords** for the few systems that don't support passkeys yet.

Passwords won't disappear overnight, but passkeys are the strongest login upgrade most businesses can make.

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 N.W. 23rd St.
Bethany, OK 73008