# TALK NERDY TO ME

## INSIDE THIS ISSUE:



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

## 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 QR code scams get past your security**

Two things make these scams effective. First, the malicious link is hidden inside an image. Most email security tools scan the text of a message for known bad links. A QR code is a picture, so the link inside it is not text the filter can read. The UK's National Cyber Security Centre points out that not all phishing-detection tools scan images, which is the reason criminals started using QR codes to disguise their links in the first place.

Second, scanning a code moves you onto your phone. Your work computer probably has web filtering, endpoint protection, and DNS controls that block known bad sites. Your personal phone usually has none of that. So, the moment you scan, you step outside the protection your business pays for, often without realizing it happened.

**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 common are QR code scams?**

The volume is climbing fast. In its report on email threats for the first quarter of 2026, Microsoft said it detected around 8.3 billion email-based phishing threats in those three months.

QR code phishing rose 146% across the quarter, from 7.6 million attacks in January to 18.7 million in March.

By the end of the quarter it had reached its highest monthly volume in at least a year.

Microsoft also found that most of these attacks arrived as PDF attachments, growing from 65% of QR code attacks in January to 70% in March.

**How to protect your business from QR code scams**

Protecting yourself against Quishing comes down to a few habits:

- 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.

**What to do if someone already scanned one**

If you or someone on your team scanned a QR code and entered details on the page that opened:

1. Change the password for that account right away, along with any other account that used the same password.
2. Confirm multi-factor authentication is turned on for the account.
3. Tell whoever manages your IT, so they can check for unusual sign-ins.
4. If card or banking details were entered, call the bank and watch the account closely.

Acting quickly limits what an attacker can do with the details they captured.

## UNITEK ADJUSTABLE LAPTOP STAND

Unitek's laptop stand with detachable cooling fan elevates your laptop to a comfortable viewing angle while keeping it cool under load.

Adjust the height and tilt to suit your posture, then attach the built-in fan when running heavier workloads.

With a sturdy, foldable design and wide compatibility, it is ideal for home offices, hot desks, or anyone looking to reduce neck strain and improve airflow without adding clutter to your workspace.

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

Right now, with no special tools, someone could send an email that looks like it came from your company.

The From line would show your domain, your logo could be pasted into the message, and it could ask one of your clients to pay an invoice or update banking details. This is called email spoofing, and it is one of the most common ways fraud against your clients and suppliers begins. It works because email was never built to check that senders are who they claim to be.

## The three records that stop it

Three settings on your domain do the checking for you. You add them once at your domain host:

- 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 DMARC setting most businesses get wrong

DMARC has three policy settings, and choosing the wrong one is a common mistake.

• p=none tells receiving servers to do nothing when a message fails. It only monitors and sends you reports. Your domain can still be spoofed.
• p=quarantine tells them to send failing messages to the junk folder.
• p=reject tells them to block failing messages before they ever arrive.

A lot of businesses set up DMARC at p=none, watch the report come in, and never move past it. At p=none, you get reports but your domain still isn't protected.

Real protection only starts at quarantine or reject. Microsoft's own guidance is to work toward p=reject once you've confirmed your legitimate mail passes.

### 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.

## Why this matters even if you don't send bulk email

**The first reason is protection.**
These records stop scammers from impersonating your domain to your clients, your suppliers, and your own staff.

**The second is deliverability.**
The major mailbox providers now require these records from anyone sending in volume. 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 DMARC checker or ask your IT provider to confirm 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.
1. 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.
1. 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.

All of this is far easier if you've decided some of it in advance. You don't need a thick binder, just a simple plan that covers:

- Who to call first and their numbers, kept somewhere you can reach without your main systems.
- Where your backups are, and proof they've been tested by restoring from them.
- Which accounts and devices matter most, so you know what to protect first.

A single page covering those is enough for most small businesses, and it'll save you a lot of scrambling if the day ever comes.

# 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.
- Get everyone's consent before it starts recording.
- Check whether the tool uses your conversations to train its AI.
- Prefer a tool that keeps recordings inside your own storage.
- Check who the summary gets emailed to by default.
- Keep bots out of legal, HR, and confidential client meetings.

If you use Microsoft 365, an administrator can control what's allowed in Teams meetings. That gives you one place to set the rule, instead of relying on each person to get it right.

# 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.

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

People reuse passwords, 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: 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.