August 2026

powerPro computers

TECH TALK

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

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! -

Christopher McManus
President & CEO

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

QR codes have become part of everyday business. From making payments and accessing Wi-Fi to viewing digital menus and sharing files, they're a convenient way to connect people with information. Unfortunately, cybercriminals have found a way to turn that convenience into an opportunity for fraud.

Known as **QR code phishing** or **"quishing,"** these scams use malicious QR codes to direct users to fake websites designed to steal passwords, payment details, and other sensitive information.

Why QR Code Scams Are So Effective

Unlike traditional phishing emails that contain suspicious links, QR codes hide the destination inside an image. Many email security systems are designed to scan text-based links but may not detect malicious URLs embedded within QR codes.

Another challenge is that scanning a QR code usually switches you from your protected work computer to your mobile device. While your business network may have advanced security controls in place, your personal smartphone often doesn't, making it easier for attackers to bypass existing defenses.

Common QR Code Scams

Cybercriminals continue to find creative ways to trick users into scanning malicious codes. Some of the most common scams include:

- Emails claiming your Microsoft 365 account or business account requires immediate verification.
- Fake invoices containing a "Scan to Pay" QR code that redirects payments to a scammer.
- Fraudulent QR code stickers placed over legitimate payment terminals, parking meters, or public information displays.

How to Protect Your Business

Reducing the risk of QR code scams starts with employee awareness and a few simple security habits:

- Treat QR codes in emails with the same caution as unexpected links or attachments.
- Before opening a website, review the URL preview displayed on your phone after scanning.
- If something seems suspicious, avoid the QR code and visit the website by typing the address directly into your browser.
- Enable phishing-resistant Multi-Factor Authentication (MFA) to protect accounts even if passwords are compromised.
- Regularly educate employees about emerging phishing techniques so they can recognize and report suspicious activity.

If Someone Scans a Malicious QR Code

Quick action can significantly reduce the impact of an attack. If an employee enters login credentials or payment information after scanning a suspicious QR code:

- Change the affected account password immediately.
- Enable or verify Multi-Factor Authentication.
- Notify your IT provider so they can review account activity for unauthorized access.
- If financial information was entered, contact your bank immediately and monitor transactions for suspicious activity.

PowerPro Tip: Cybercriminals are constantly changing their tactics, but awareness remains one of your strongest defenses. A few moments spent verifying a QR code can prevent costly fraud and protect your business from unnecessary risk.

Stay One Step Ahead with PowerPro Computers

Cybersecurity isn't just about technology, it's about building smarter habits and stronger defenses. At **PowerPro Computers,** we help businesses strengthen email security, implement modern authentication, educate employees, and reduce the risk of phishing attacks before they become costly incidents.

Book a Free Technology Assessment to learn how we can help protect your business from today's evolving cyber threats.

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

Imagine one of your customers receives an email that appears to come from your business, complete with your company name and branding, asking them to pay an invoice or update banking details. The email looks legitimate, but it wasn't sent by you.

This type of attack is known as **email spoofing,** and it's one of the most common ways cybercriminals commit business email fraud. Without the right protections in place, attackers can impersonate your domain, putting your reputation, customer trust, and finances at risk.

Three Security Records Every Business Needs

Fortunately, protecting your domain doesn't require complicated software. Three email authentication standards work together to verify that emails sent from your business are legitimate:

1. **SPF** identifies which mail servers are authorized to send emails on behalf of your domain.
2. **DKIM** adds a digital signature that confirms an email hasn't been altered during delivery.
3. **DMARC** combines both technologies and tells receiving mail servers how to handle messages that fail authentication.

When properly configured, these records make it much harder for scammers to impersonate your business.

A Common DMARC Mistake

Many businesses enable DMARC in **monitoring mode** (p=none) but never move beyond it. While this setting provides useful reports, it doesn't stop fraudulent emails from being sent using your domain.

For real protection, your DMARC policy should gradually progress to **quarantine** and ultimately **reject**, blocking unauthorized messages before they ever reach your customers or employees.

Why It Matters

Email authentication isn't just about security. Major email providers, including Microsoft, Google, and Yahoo, increasingly expect businesses to use SPF, DKIM, and DMARC. A properly configured domain not only protects your organization from impersonation but also improves the chances that legitimate emails reach the inbox instead of the spam folder.

PowerPro Tip: If you're unsure whether your domain is properly protected, now is the perfect time for a review. A few simple configuration changes can significantly reduce your risk of email fraud while improving email deliverability.

Let PowerPro Help Protect Your Business

At **PowerPro Computers**, we help businesses strengthen their email security with correctly configured SPF, DKIM, and DMARC records, giving you greater confidence that your customers receive authentic communications from your organization.

Book a Free Technology Assessment to ensure your business is protected against email spoofing and other evolving cyber threats.

WHAT TO DO IN THE FIRST HOUR OF A CYBERATTACK

IfA cyberattack can unfold in minutes, but how you respond during the first hour can significantly reduce the damage. While the instinct is often to start fixing the problem immediately, taking the wrong steps can make recovery more difficult. A calm, structured response is the best way to protect your business.

Your First Five Steps

1. Isolate the affected device

Disconnect the computer from your network by turning off Wi-Fi or unplugging the network cable. This helps prevent malware or ransomware from spreading to other devices and shared files. Avoid shutting the computer down unless your IT provider instructs you to do so.

2. Contact your IT provider immediately

Call your trusted IT support team instead of sending an email, as email systems may already be compromised. If your business has cyber insurance, notify your insurer as soon as possible so their incident response process can begin.

3. Preserve the evidence

Resist the urge to reinstall software or delete suspicious files. The information left behind can help identify how the attack happened and speed up recovery. If possible, take photos or screenshots of any error messages or ransom notes.

4. Protect your accounts and finances

If you suspect banking or payment details have been exposed, contact your financial institution immediately. Then, using a trusted device, change passwords for critical accounts such as Microsoft 365, email, and administrator accounts, and ensure multi-factor authentication (MFA) is enabled.

5. Have a recovery plan ready

The easiest cyber incidents to recover from are the ones you've prepared for. Keep an offline list of emergency contacts, regularly test your backups, and identify your most critical systems before an incident occurs.

PowerPro Tip: A simple, tested incident response plan can save valuable time and reduce costly downtime when every minute matters.

We're Here When You Need Us

No business wants to experience a cyberattack, but preparation makes all the difference. At **PowerPro Computers,** we help businesses strengthen their cybersecurity, protect critical data, and recover quickly when incidents occur. If you're unsure whether your current security measures are enough, **book a free Technology Assessment** and let our team help you stay one step ahead.

WHO CAN SEE WHAT YOUR AI NOTE-TAKER RECORDS?

AI meeting assistants can save time by automatically recording conversations, generating transcripts, and summarizing action items. However, every recording may contain sensitive business information, client discussions, or confidential employee data. Before introducing an AI note-taker into your meetings, it's important to understand where that information goes and who can access it.

Before You Press "Record"
To reduce privacy and security risks, make sure your business follows a few simple best practices:

- **Use one approved AI note-taking platform** across your organization instead of allowing employees to connect different third-party tools.
- **Disable automatic meeting joins** so recordings only begin when someone intentionally enables them.
- **Always obtain consent** before recording meetings, especially when clients or external partners are involved
- **Review the vendor's privacy policy** to understand whether meeting data is used to train AI models.
- **Choose solutions that keep recordings within your organization's secure storage** whenever possible.
- **Verify who receives meeting summaries** by default to prevent sensitive information from being shared unintentionally.
- **Avoid AI recording tools in confidential meetings**, such as HR discussions, legal consultations, financial reviews, or sensitive client conversations.

A Smarter Way to Manage AI

If your business uses Microsoft 365, administrators can control which AI apps are permitted within Microsoft Teams. Centralized management helps enforce consistent security policies across your organization instead of relying on individual users to make the right decisions.

PowerPro Tip: AI tools should improve productivity—not create new security risks. Establishing clear policies for meeting recordings helps protect your business while allowing your team to benefit from AI responsibly.

PowerPro Can Help
AI is transforming the workplace, but it should be implemented with security and privacy in mind. At **PowerPro Computers,** we help businesses securely deploy Microsoft 365, configure collaboration tools, and establish practical AI governance policies that protect sensitive business information.

Book a Free Technology Assessment to ensure your business is using AI tools safely, securely, and with confidence.

STILL USING WINDOWS 10? IT'S TIME TO MAKE A PLAN

If your business is still running Windows 10, now is the time to take action. Although your computers may continue to work normally, Microsoft ended security support for Windows 10 in October 2025, meaning newly discovered vulnerabilities are no longer being patched.

Without ongoing security updates, unsupported devices become increasingly vulnerable to cyberattacks, ransomware, and data breaches. They can also create compliance challenges and may impact cyber insurance requirements, leaving your business exposed to unnecessary risk.

What Should You Do Next?
A smooth transition doesn't have to be complicated. Start with these simple steps:

- Identify every device in your business still running Windows 10.
- Check Windows 11 compatibility using Microsoft's PC Health Check tool to see which computers qualify for a free upgrade.
- Upgrade eligible devices to Windows 11 while keeping your files, applications, and settings intact.
- Plan for older hardware that can't be upgraded. Depending on your needs, replacing outdated devices or using Microsoft's Extended Security Updates as a temporary solution may be the best option.

Don't Wait for a Security Problem

Delaying your upgrade increases the risk of security incidents and unexpected downtime. Planning ahead allows you to spread costs, minimize disruption, and ensure your business continues operating securely.

PowerPro Tip: Don't wait until an unsupported computer causes a security issue. A proactive upgrade plan is far less costly than recovering from a cyberattack or unexpected system failure.

Let PowerPro Help
At **PowerPro Computers**, we can quickly assess your current devices, identify which systems are ready for Windows 11, and recommend the most cost-effective upgrade strategy for your business.

Book a Free Technology Assessment and let our experts help you transition to a secure, supported, and future-ready IT environment.

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.

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
Zune