apex
Computing Services

SENTINEL CYBER DIGITAL MAGAZINE

Cyber Security Awareness

A Message from Our LEADERSHIP TEAM

Dear Reader,

At Apex Computing, our mission is simple - to make IT simple - to empower North West businesses with the tools, knowledge, and confidence to thrive securely in a digital-first world.

Cyber threats are constantly evolving, but so too are the opportunities to strengthen your defences. For us, cyber security isn't just about technology - it's about people. It's about building awareness, good habits, and a culture of security across every team.

This magazine brings together our key insights; from phishing and password best practices, to leadership strategies that shape stronger security cultures. Each article is designed to help you take practical, meaningful steps towards greater cyber resilience.

We're proud to work alongside trusted partners like Pax8 and Huntress, but true cyber security begins with the mindset: staying alert, proactive, and ready for what's next.

Let's build a safer, smarter, and more resilient future - together.

Daniel Shone
Daniel Shone, Managing Director

C Gorman
Chris Gorman, CEO

CONTENTS

DON'T GET HOOKED: PHISHING SCAMS UNVEILED

85% of security breaches in UK businesses involve phishing. Greater Manchester is no exception - **phishing attacks here jumped by 30% in the last year**, contributing to an estimated £40 million in losses for local firms. Cyber criminals are casting wider and smarter nets, and no business is too small to take the bait. In this article, we'll pull back the curtain on phishing scams targeting SMEs and arm you with insights to stay safe.

The Rising Tide of Phishing Threats

Phishing remains the number one cyber threat to businesses. It's alarmingly prevalent - among companies that experienced a cyber attack, 85% said phishing emails were involved. Criminals send highly realistic emails or messages that look legitimate, hoping to trick someone into clicking a malicious link, handing over credentials, or transferring money. And it's getting worse...

...in Greater Manchester, phishing incidents spiked by 30% in the last year...

This surge has real consequences. Cyber scams cost North West businesses roughly £40 million in the past year - losses that hit SME owners particularly hard.

What's driving the spike? For one, phishing kits and stolen data are cheaply available on the dark web. Scammers have also upped their game with AI. The explosion of AI in the past few years has made scams far more convincing. Today's phishing emails are often polished - no more broken English - and some even use deepfake audio to mimic real executives on the phone. It's scary how real it all looks and sounds. In other words, the old advice of "watch for typos" isn't enough; phishing has grown sophisticated.

Local organisations are feeling the sting. SMEs are an attractive target - criminals know smaller businesses have fewer defences and busy, wear-many-hats staff who might click before thinking.

Real-World Tale: A Greater Manchester Business Nearly Hooked

Consider this close call that happened to a Greater Manchester firm last year. The finance manager at a Trafford manufacturing company receive an email from their Managing Director requesting an £18,000 urgent payment to a new bank account.

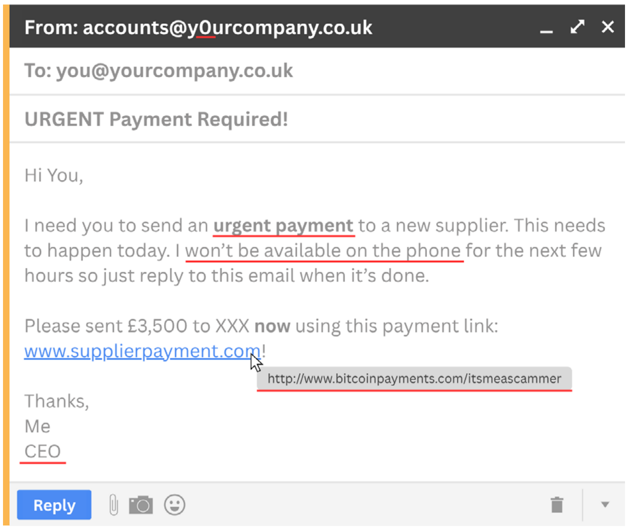
The message read: "*We need to pay this supplier today - I'm tied up in meetings, just get it done*." The sender's address looked right (it was spoofed), and it was signed off just like the MD's usual tone. Red flag? It was 4.45pm and the "MD" oddly said he couldn't be reached by phone.

Luckily, the finance manager felt uneasy and phoned the MD's known number anyway. He answered baffled - he'd sent no such email. Fraud averted. The company later found out that hackers had scraped the MD's publicly available information and crafted a believable story. This was a textbook example of CEO impersonation, also called "whaling" (harpooning a big phish).

What Does a Phishing Scam Look Like?

At first glance, many phishing messages appear innocently routine. It could be an email from “Microsoft Support” asking you to reset your password, or a WhatsApp message from a “supplier” about an unpaid invoice. The hallmarks of phishing include:

- **Impersonation of a trusted sender:** Attackers spoof the email address or display name of someone you know (a client, your bank, Microsoft, even your CEO). They may use a lookalike domain (e.g. @apexcomputing.com with ‘.com’ instead of ‘.co.uk’) to fool the eye.
- **Urgent or alarming language:** “Your account will be closed!” or “Payment overdue - action required immediately”. Phishers create panic so you rush without verifying.
- **Links and attachments:** The email urges you to click a link (to a fake login page) or open an attachment (laced with malware). Often the link URL is nearly identical to a real site’s URL (just one or two characters off)
- **Requests for sensitive info or payment:** They ask for passwords, bank details, or a quick bank transfer. A common ploy is telling you to “confirm” something - which actually means giving them your credentials.



From: accounts@y0urcompany.co.uk

To: you@yourcompany.co.uk

URGENT Payment Required!

Hi You,

I need you to send an **urgent payment** to a new supplier. This needs to happen today. I won’t be available on the phone for the next few hours so just reply to this email when it’s done.

Please sent £3,500 to XXX **now** using this payment link: www.supplierpayment.com!

http://www.bitcoinpayments.com/itsmeascammer

Thanks,
Me
CEO

In the above example, the email claims an urgent payment needs to be made and asks the employee to make a payment using a payment link straight away, as well as saying they will not be available for a phone call for the next few hours. Only by hovering over the link (revealing a strange URL) or noticing subtle anomalies could one detect the fraud.

This is how easily an untrained eye can be hooked. Even tech-savvy people can slip up if the bait looks legit.

Spear phishing is even more dangerous. Instead of blasting thousands of generic emails, attackers target your company specifically. They might scrape LinkedIn to learn your staff roles, then send a personalised email: e.g. the CFO gets an email from the CEO asking *“Are you in the office? I need a payment sent ASAP for XXX project”*. Because it references real names and projects, it feels authentic. These tailored scams - known as CEO Fraud or Business Email Compromise (BEC) - have tricked even seasoned professionals. In fact, in 2022 the most common frauds against UK businesses were invoice scams and CEO impersonation.

Hook, Line and Sinker: Why Phishing Works

Phishing succeeds because it exploits human nature. Scammers pray on our trust and our haste:

Trust in authority: If an email appears to come from your CEO, a supplier, or a government agency, you’re less likely to question it. Phishers often impersonate authority figures so you’ll comply reflexively.

Urgency by fear: By instilling panic (“Your account is compromised!”) or urgency (“Pay this now or lost that deal!”), they want you to act before you think. Under pressure, people skip the usual caution.

Greed or curiosity: Some phishing lures offera reward (e.g. a tax refund, a free gift) or pique curiosity (“See attached staff bonus list”). These temptations lead peopleto click impulsively.

Professional spoofing: Today’s phishing emails look incredibly authentic. With stolen graphics and well-written copy, a spoofed email or website is nearly indistinguishable from the real thing. Even the sender’s domain can be forged or subtly altered. Without technical email filters, these messages will land in your user’s inboxes.

Given these tactics, it's no surprise that phishing remains the most disruptive type of cyber attack facing businesses. But you are now powerless against it. Let's look at how you can strengthen your defences.

Smart Tips to Outsmart the Phishers

Most Managed Service Providers (MSPs) will tell you the basics: "*Think before you click*" and "*Don't trust unknown senders*". Important advice, yes - but to truly phish-proof your organisation, you need more robust strategies.

Here are some insider tips you might not hear every day, straight from our expert team

1 Implement Multi-Factor Authentication (MFA) Everywhere

Ensure all email accounts, portal logins, VPNs, and even your social media logins have MFA. If an employee inadvertently gives away their password, a hacker still can't log in without that second factor.

2 Verify Requests Offline

Treat any request involving payments or sensitive data with healthy scepticism - especially if made by email. Have a clear policy that any wire transfer or change of bank details must be verified by phone or face-to-face with the supposed requester. This thwarts most CEO and invoice scams.

3 Use Safe "Out-of-Band" Confirmation

For transactions, use a second channel to confirm (e.g. if you get an email request, verify via a known phone number from your records, not from the email). Never used contact info provided in a suspicious message.

4 Tighten Payment Controls

Work with your bank to enable protections like "Confirmation of Payee" on transfers. This service checks if they payee's name matches the account, helping catch when a fraudster is posing as a supplier. Also, set lower daily transfer limits and require dual approval for larger payments.

5 Educate and Test Your Team

Regularly train employees on phishing red flags and do periodic simulated phishing exercises. It's better they fail a fake phishing test than a real attack. Foster a culture where staff feel safe to report a mistaken click immediately (rather than hide it). Speedy reporting can contain damage.

6 Warn of External Emails

Consider an email banner or tag for external emails (e.g. "[External]" in the subject line). This alerts staff that an email came from outside the company, making impersonation attempts more obvious.

7 Lock Down Your Domain

Protect your own email domain from being spoofed. Configure SPF, DKIM and DMARC records - these email authentication tools verify that messages actually come from your domain. (If this sounds like jargon to you, don't worry - our Managed Email Authentication service can handle it).

8 Keep Software Updated and Scanned

Phishing links often deliver malware. Ensure all PCs have updated anti-malware and that security patches are applied promptly. This helps contain the fallout if someone does click a bad link.

9 Encourage "Stop and Think"

Remind your team: it's OK to slow down. A quick call or double-check with IT is encouraged if something seems off. Create an environment where no one gets scolded for asking, "Is this email legit?". It could save your company.

By implementing the tips above, you create layers of defence - covering people, processes, and technology. Phishing protection isn't one silver bullet, it's body armour made of many layers.

TOP 5 CYBER SECURITY MYTHS BUSTED

MYTH...

“Cyber criminals only target large corporations”

THE TRUTH...

Over 40% of UK cyber attacks hit SMEs. Hackers automate their scams - not their ethics.

MYTH...

“Strong passwords mean I’m safe”

THE TRUTH...

Only with MFA! Passwords are breached daily (even complex ones); MFA is your bodyguard.

MYTH...

“We use the Cloud - it’s automatically secure”

THE TRUTH...

Shared responsibility model: Cloud secures the platform, *you* secure the people and data.

MYTH...

“Antivirus is enough”

THE TRUTH...

It’s like locking your front door but leaving the windows open. Layered defence is essential.

MYTH...

“We’ll know if we’ve been hacked”

THE TRUTH...

Many breaches sit undetected for over 200 days! Silence is the real danger.

SECURING THE HOME OFFICE: CYBER SAFETY FOR REMOTE AND HYBRID WORK

Over 64% of UK SMEs now have hybrid or fully remote teams. And while flexible work boost productivity, it also broadens your attack surface - every home network, personal laptop, or mobile phone accessing your systems introduces a new risk.

In this article, we're covering how to secure remote, hybrid, and Bring Your Own Device (BYOD) setups, so your business stays protected - no matter where your team logs in from.

"Remote Work is Convenient" - For Hackers Too

Cyber criminals love remote workers. Why? Because home setups often lack the layers of protection you'd find in the office:

- Weak or unchanged router passwords
- Outdated devices with no antivirus
- Personal email, apps, or downloads mixing with work activity
- Unsecured file sharing or USB use
- No centralised monitoring by IT

And then there's the biggest vulnerability: **human error on an unmonitored device**.

"We've had cases where staff were unknowingly sharing sensitive data over public Wi-Fi, or using outdated antivirus on their home machines. They weren't reckless, they just didn't realise the risks," said one of our customers when onboarding with us.

Real-World Example: BYOD Gone Bad

A 20-person marketing agency in Manchester suffered a breach when a freelancer's laptop - with poor antivirus and a pirated PDF reader - was used to access the team's shared drive. The device was infected with a keylogger, which silently harvested login credentials for multiple platforms. It took days before unusual activity was spotted. By then, two client Dropbox folders had been compromised.

The cost? Client trust, incident response bills, and weeks of cleanup.

DOWNLOAD YOUR FREE COPY OF OUR **CYBER SECURITY GUIDE FOR** *Remote Working Businesses*

HERE

Flexibility Shouldn't Equal Vulnerability

Working from anywhere is here to stay, but so are the threats that come with it. Now is the time to:

- Review how your team accesses business systems
- Tighten up home network and device policies
- Deploy the right tools and training

Common Remote Work Mistakes (and How to Fix Them)

Here's what we see most often with remote and hybrid clients:

Weak or Default Wi-Fi Passwords

Many home routers still use the factory password or something guessable.

✓ **Fix it: Staff should change router logins, use WPA3 if available, and update firmware regularly.**

Sharing Devices with Family or Friends

A partner using the same laptop for streaming or downloading is a hidden risk.

✓ **Fix it: Use company-issued devices or enable profiles with restricted access.**

No Mobile Device Management (MDM)

Phones accessing company email without encryption or passcode? That's a risk.

✓ **Fix it: Use Microsoft InTune or other MDM tool to remotely wipe lost or compromised files.**

Skipping VPNs or Firewalls

Remote workers using open Wi-Fi without encryption put data in transit at risk.

✓ **Fix it: Provide a Business VPN to all staff - encrypts traffic and keeps prying eyes out.**

Delayed Patch Updates

Without enforced policies, home machines often skip critical security updates.

✓ **Fix it: Centralised patch management or cloud-based endpoint protection can enforce updates remotely.**

apex's Top Remote Security Tips for SMEs

Create a Remote Work Policy

Outline what's allowed, what's not, and who's responsible for device management

Mandate Multi-Factor Authentication (MFA) on All Accounts

Ensure MFA is required for Microsoft 365, CRM, and any cloud platform access remotely

Provide Secure, Managed Devices

Even just for key roles - company-managed devices with endpoint protection are 10 time easier to monitor

Use a Business VPN

Encrypt traffic between remote workers and your systems, especially if staff work from cafes, shared spaces or travel frequently

Enable Mobile Device Management (MDM)

Use MDM to secure mobile phones and tablets that access business apps or email

Monitor and Audit Access

Review login logs, locations, and devices regularly to spot unusual behaviour

> *"A good remote setup is invisible to the employee - but tight in the background. They get the freedom to work from anywhere. You get the peace of mind that every endpoint is protected."*

#CaseStudy

EMPOWERING GROWTH WITH SCALABLE, SECURE IT SOLUTIONS

Roma Finance is a specialist commercial lender established 15 years ago, helping clients realise their property ambitions - from auction purchases to land development. As the business scaled rapidly and envisioned a more technology-forward future, Roma Finance needed a managed service provider (MSP) that could match its ambitions, enhance its infrastructure, and improve cyber security - all without disrupting day-to-day operations.

"One of the most immediate benefits of working with Apex was their approach to cyber security... There have been occasions where an issue was resolved before we were even aware of it," said Roma's Finance's Business Architect, Adam Bates.

The Challenge: Scaling for Strategic Growth

Prior to engaging Apex Computing, Roma Finance managed its IT support in-house as part of its facilities management function. While this was suitable during their earlier growth phases, it began showing limitations as the company expanded in both headcount and digital complexity. Roma needed:

- A scalable IT infrastructure to support team growth
- Strong cyber security tailored for the financial sector
- Flexibility to accommodate hybrid working patterns
- A collaborative partner and strategic advisor, not just a vendor

"When we first met Apex, it felt like we'd found a partner we could growth with"

Solution Highlights

Infrastructure Overhaul

One of the first major projects Apex delivered was a complete office Wi-Fi overhaul - ensuring the network was robust, secure, and scalable. Despite the inevitable teething problems, Apex's hands-on, on-site approach ensures swift resolution and minimal disruption.

Cyber Security Excellence

With a focus on financial services, Apex implemented a layered cyber security approach, providing:

- Proactive threat monitoring for instant alerts
- Transparent reporting for compliance and visibility
- Peace of mind with issues resolved before detection by the clients

Apex also guided Roma Finance through both Cyber Essentials and Cyber Essentials Plus certifications, significantly enhancing its security posture.

Supporting a Hybrid Workforce

Roma Finance operates across office, home, and field environments. Apex provided:

- Seamless remote support, including outside regular hours
- Device deployment and configuration for field agents

- Rapid-response services for emergencies and accidents

This flexibility empowered Roma Finance's team to stay connected and effective - regardless of location.

Relationship-Driven Service

Beyond ticket resolution, Apex demonstrated genuine partnership. Examples include:

- Personally delivering laptops to team members at home
- Responding with empathy and urgency when the client had an incident
- Maintaining clear SLAs and always prioritising emergencies

Watch: Roma Finance's Business Architect, Adam Bates speak about his experience with Apex

Roma

apex Computing Services

Roma F[illegible]e:

Building a[illegible]g-Term IT Partnership with Apex

Why Roma Finance Chose Apex

Roma Finance evaluated several providers but chose Apex Computing based on trust, transparency and commercial clarity. Apex was open about what it could - and couldn't - deliver, which built confidence from the start. The decision was further cemented by Apex's:

- Transparent and scalable pricing model
- Willingness to align with Roma Finance's technology roadmap
- Clear communication and structured onboarding process

> ***"It's not transactional, but ongoing and collaborative... Speak to Apex. If you're looking for a long-term, professional IT relationship, it's hard to go wrong"***

The Results

Apex ensured a smooth IT transition from Roma Finance's outgoing provider

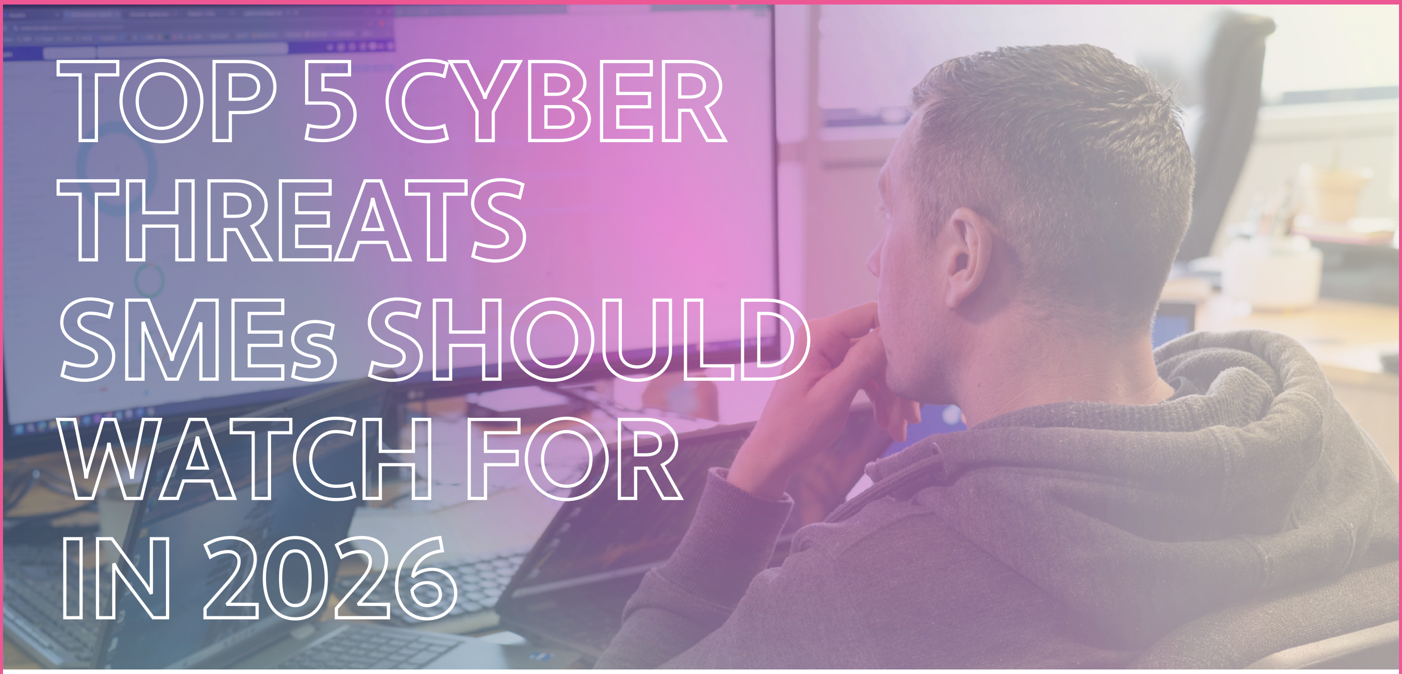
Robust and scalable IT infrastructure

Cyber Essentials Plus certification

Increased confidence in cyber security

Full support for hybrid and remote workers

Strong long-term partnership



TOP 5 CYBER THREATS SMEs SHOULD WATCH FOR IN 2026

Cyber threats are evolving faster than ever - and for small and medium-sized enterprises (SMEs), the risks are multiplying. As 2026 approaches, attackers are combining automation, artificial intelligence (AI), and social manipulation to outsmart traditional defences. Here are the top 5 threats every business should keep on their radar.

THREAT #1...

Phishing and Business Email Compromise (BEC)

Phishing remains the number one way cyber criminals infiltrate businesses - and BEC attacks are becoming increasingly personal.

In 2026, expect to see highly convincing emails that appear to come from trusted contacts, complete with correct branding, tone, and even AI-generated writing styles.

Attackers are using stolen data from previous breaches to craft believable messages that trick staff into transferring money or credentials.

TIP

Regular staff training, multi-factor authentication (MFA), and real-time threat monitoring are key to defending against BEC scams.

THREAT #2...

Ransomware-as-a-Service (Raas)

Ransomware is no longer the domain of elite hackers. Ransomware-as-a-Service gives anyone with bad intentions access to ready-made malware kits and payment portals. The result? A surge in low-skill but high-volume attacks targeting SMEs - the most profitable "sweet spot" for criminals who know smaller firms often lack enterprise-grade protection.

TIP

Keep offline backups, patch systems regularly, and use endpoint detection and response (EDR) solutions to detect suspicious activity early.

THREAT #3...

Cloud Misconfiguration and Data Theft

As more businesses move data and applications to the cloud, misconfigurations are fast becoming one of the biggest sources of data leaks.

From poorly configured access controls to unencrypted storage buckets, even small errors can expose sensitive data publicly or to cyber criminals scanning for vulnerabilities.

TIP

Regularly audit your cloud security settings and use automated configuration tools to ensure compliance and visibility.

THREAT #4...

Deepfake Voice Fraud and AI Engineering

AI has created a new class of threats. Deepfake voice scams are on the rise, with attackers cloning voices of executives or suppliers to authorise payments or extract confidential information.

Meanwhile, "AI engineering" - the malicious manipulation of AI systems or data sets - is emerging as a powerful attack vector. Compromised AI models can produce misleading results, corrupt data, or open back doors for attackers.

TIP

Establish strict verification processes for voice or video instructions and monitor AI systems for abnormal activity or data drift.

THREAT #5...

Supply Chain Compromise

In 2026, attackers are increasingly bypassing direct defences by targeting suppliers, software vendors, and managed service providers.

A single compromised partner can create a cascade of risk across the entire business ecosystem - something SMEs often overlook. Cyber criminals know this and are exploiting trusted relationships to deliver malware or steal credentials through legitimate channels.

TIP

Evaluate the security posture of your suppliers, insist on transparency in cyber security practices, and segment your network to reduce the blast radius of a breach.

Final Thought

For SMEs, cyber security in 2026 isn't just about defending against attacks - it's about building resilience. With threats becoming more sophisticated, prevention, detection and response must all work together. The businesses that thrive will be the ones that treat cyber security not as a checkbox, but as a culture.

LOCKING DOWN YOUR BUSINESS: PASSWORDS AND BEYOND

One weak password could cost your company thousands. Over half of UK SME employees (52%) have never received cyber security training, and far too many are still using passwords like 'CompanyName2025!'. It's time to change that.

Passwords remain a central line of defence in business security - and also one of the weakest. In this article, we're taking a closer look at how SMEs across the North West can drastically reduce risk by tightening up password habits and enabling modern authentication.

Weak Passwords Are Still the #1 Access Point for Hackers

Most cyber breaches don't start with Hollywood-style hacking. They start with an email or a stolen credential.

- 81% of hacking-related breaches involve stolen or weak passwords
- 59% of people reuse passwords across work and personal accounts
- Criminals often buy stolen password databases on the dark web for pennies

> *"You'd be surprised how many staff at SMEs still use passwords like 'Password123!' or 'Summer2024', especially under time pressure. We once onboarded a 40-user account where half the team had variations of the company name as their login. Easy pickings for a brute attack,"* said one of our cyber team.

If your team uses the same login for email, payroll, Microsoft and Team - you're at serious risk.

Case in Point: A Manchester Firm's Close Call

Recently, a locally-based accountancy firm to Manchester reached out to Apex after an employee's password was compromised. A cyber criminal used stolen Office 365 credentials (from a previous data breach) to log in and sit silently in their inbox for days.

The attacker watched conversations, then jumped in pretending to be the employee - emailing a client to "update payment details". The client paid a £6,000 invoice to the scammer before realising it wasn't legitimate.

The password was one that was being used across multiple platforms. Had multi-factor authentication (MFA) been enabled, the breach could've been prevented entirely.

Beyond Passwords: Full Identity Protection

Your passwords are just one part of a wider access control strategy. Here's what Apex helps North West businesses implement:

- **Conditional Access Policies:** Only allow logins from trusted devices or locations. Block access from high-risk countries of IPs
- **Single Sign-On (SSO):** Consolidate multiple logins to one secure portal (e.g. Microsoft Entra

ID), reducing password fatigue and human error

- Account Lockout Policies: Prevent brute force attacks by auto-locking accounts after a set number of failed attempts
- Access Reviews and User Audits: Ensure ex-employees and dormant accounts are removed or disabled. Many breaches occur via unused or forgotten logins
- Privileged Access Management: Admins and finance users need stricter access controls. Don't let everyone have full control in every system

Think You're Already Covered? Ask Yourself:

?

Are your staff using unique passwords for every platform?

?

Do you know who in your business has admin-level access and for what?

?

Is MFA enabled on all critical apps or just "recommended"?

?

When was the last time you ran a user access audit?

?

Are you alerted if a staff email or password appears in a data breach?

If you answered "No" or "I'm not sure" to any of the above, it's time to talk to an IT and cyber security partner like Apex

Don't Leave the Front Door Open

Passwords are the digital keys to your business - don't leave them under the mat.

Start by making MFA non-negotiable across your company. It's simple, cost-effective, and stops over 99% of account takeover attempts. Pair that with smart policies and password manager rollouts, and you'll be miles ahead of the average SME.

5 Ways to Upgrade Your Password Practices Now

Consider Using Passphrases, Not Passwords

Encourage your team to use memorable passphrases instead of single words. 'BlueCoffeeRocket2025@' is much stronger than 'Manchester1!'.

Enable MFA Everywhere

MFA adds a second layer of security. Even is a password is stolen, it's useless without the MFA code.

Introduce a Password Manager

Avoid sticky notes and spreadsheets. A secure password manager like Keeper (that's what we use here at Apex) or 1Password generates and stores long, random credentials that staff never have to remember.

Set Minimum Standards for Passwords

- Minimum of 12 characters
- Mix of upper and lower case letters, number and symbols
- No company names, birthdays, or pet names

Use group policies (especially in Microsoft 365) to enforce strong password creation across all users.

Regularly Review Compromised Passwords

Check is any work email accounts or passwords have been exposed on the dark web. Apex can provide ***Dark Web Monitoring*** and run these kinds of reports for your domains, altering you to compromised credentials in real time.

HOW APEX CAN HELP...

Apex offers tailored identity security solutions designed for SMEs in Greater Manchester just like you. We help you: deploy password managers; enforce MFA; secure user accounts with intelligent detection and lockdown policies; provide security awareness training; and support real-world phishing simulations

Cyber Hygiene Checklist

Essential daily, weekly, and monthly actions for SMEs

Core Security Foundations

	☑ Download **the Apex Cyber Hygiene Checklist**
Whenever created	□ Use strong, unique passwords (or pass-phrases) of 12+ characters and a reputable password manager
Review monthly	□ Enable Multi-Factor Authentication (MFA) on all business-critical accounts (email, cloud services, remote access)
Review weekly	□ Keep all devices patched and updated (operating systems, browsers, apps)
Review weekly	□ Install and regularly update endpoint protection (antivirus/EDR)

Email and Account Safety

Review monthly	□ Activate advanced email filtering to block phishing and malicious attachments
Frequently	□ Train staff to spot phishing emails (hover over links, check sender addresses) - ensure full training annually
Check weekly	□ Immediately disable access for leavers and rotate shared account credentials as soon as a staff member leaves

Data Protection and Backups

Daily (automated)	□ Back up all critical data daily (on-site and off-site/cloud)
Monthly	□ Test backups monthly to ensure quick and clean recovery
Review weekly	□ Apply least privilege access: staff only see what they need - review permissions
Review monthly	□ Encrypt sensitive files and devices (laptops, USB drives)

Secure Devices and Networks

Check weekly	□ Ensure business-grade firewalls are in place and regularly updated
Review quarterly	□ Lock down WiFi networks with strong encryption (WPA3) and unique passwords/pass-phrases
Review monthly	□ Deploy Mobile Device Management (MDM) to control and wipe stolen/lost devices
Monthly	□ Remove unused hardware and decommission old equipment securely

People and Training

Annually	□ Provide annual cyber security awareness training to all staff; also do frequent reminders
Frequently	□ Run regular phishing simulations to keep vigilance high
Review monthly	□ Establish a clear Incident Response Plan and make sure everyone knows how to report issues

Compliance and Oversight

Review Annually	□ Review and update cyber security policies at least once per year, plus monthly quick reviews
Review Monthly	□ Check that you meet GDPR and industry-specific compliance requirements
Review weekly	□ Keep a log of all security incidents and responses for auditing as they occur
	□ **Optional:** Work towards achieving a Cyber Essentials and Cyber Essentials Plus certification

Quick Win Actions

- Change any weak or reused passwords **today**
- Set up MFA for all email accounts **this week**
- Verify that backups are working and accessible **this month**

Why This Maters

Cyber attacks on UK SMEs are rising sharply. Good cyber hygiene reduces the risk of ransomware, phishing, and data breaches - protecting your customers, reputation, and bottom line.

Visit Our Cyber Awareness Hub Here

MANIFESTO FOR BUSINESS LEADERS WHO WANT TO INSPIRE SECURITY-FIRST CULTURES

VISION, NOT VIGILANCE

Leaders don't need to be cyber experts - they need to make cyber a business priority. Ask: *"How secure are we compared to where we want to be?"*

RECOGNISE SECURITY CHAMPIONS

When someone reports a phishing email or flags a risk, celebrate it like a sales win. Reward curiosity.

> ***"Security culture isn't a policy - it's a posture. And it starts with the people who set the tone".***

TALK ABOUT IT OFTEN

Include a "Cyber Moment" in every board meeting. Two minutes on one security update. Keep it visible.

BUILD A CULTURE OF CURIOSITY

Empower teams to question unusual emails, challenge requests, and learn. Make security approachable, not fearful.

PARTNER POWER

Collaborate with partners (like Apex) for regular audits, tabletop exercises, and roadmap sessions. Cyber maturity is a journey, not a checkbox.

#CaseStudy

NAVIGATING DIGITAL CURRENTS: ENHANCING SAFETY AND EFFICIENCY

We spoke to Mathew Wilkinson from Pyranha Mouldings Ltd about their experience with Apex Computing.

Could you introduce Pyranha Mouldings Ltd?

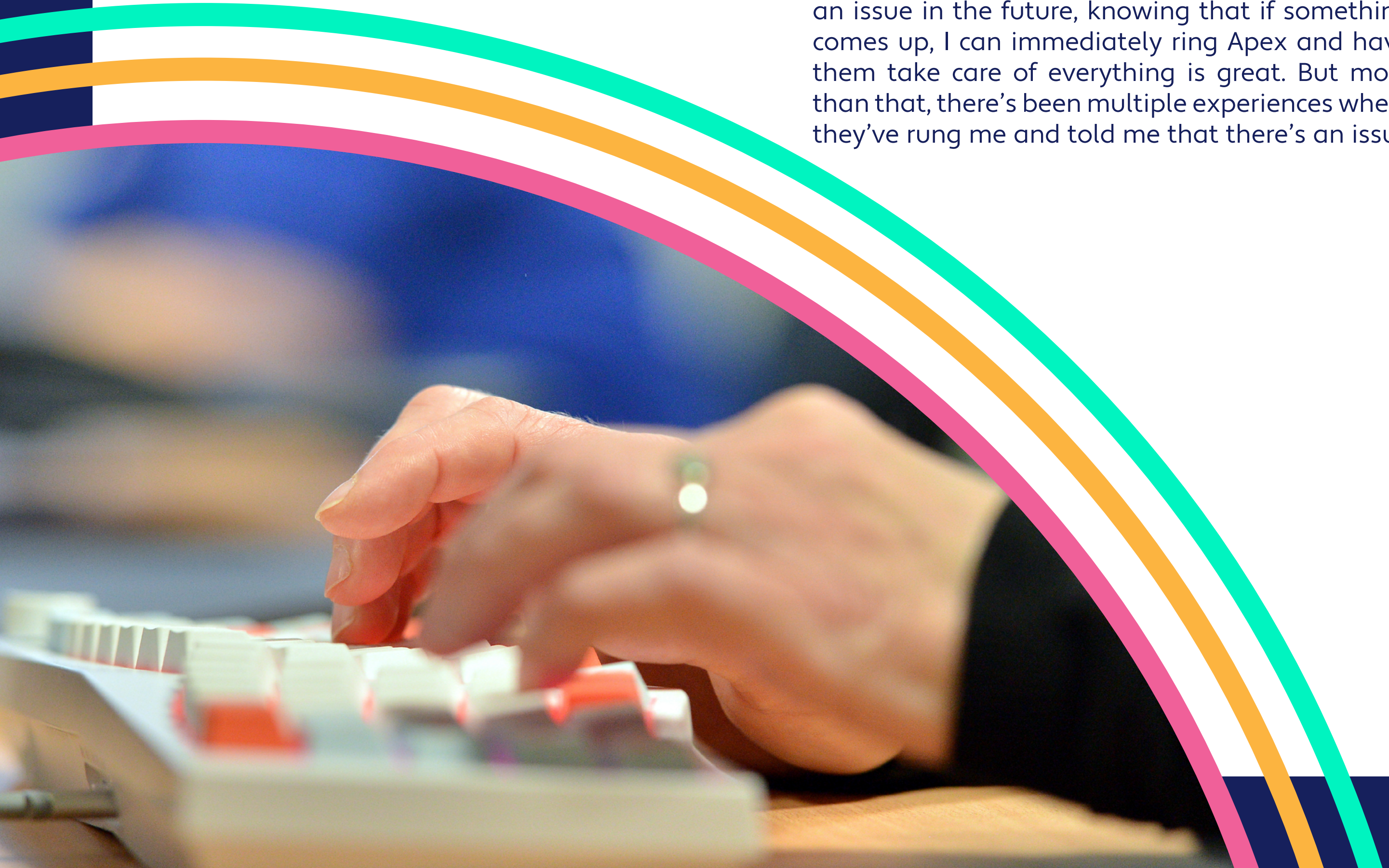
Pyranha Mouldings was founded in 1971. We're a company that makes canoes and kayaks, and we do those across three different brands. We have Pyranha Kayaks, which is mainly a whitewater brand. PH Sea Kayaks does sea kayaks in both plastic and composite, and Venture, which makes recreational kayaks and canoes.

How did you come across Apex Computing Services?

We interviewed a number of companies and went and visited them, had them visit us, and Apex came out on top of that. They were really nice people to work with, super friendly, super helpful, even before we started working with them. And we just knew that we could rely upon them and that we could treat them as part of our team.

How have Apex's services contributed to the smooth operation of your business?

Apex really does take care of everything. They're proactive and watching for any issues that might come up and preempting anything that could be an issue in the future, knowing that if something comes up, I can immediately ring Apex and have them take care of everything is great. But more than that, there's been multiple experiences where they've rung me and told me that there's an issue



and that they're already working on it, and it just gives me complete peace of mind and I can get on with my main duties.

Could you highlight a situation where Apex's prompt response or proactive measures made a difference?

Just earlier this week, we had a firmware update on our firewalls, and that unfortunately, got stuck in a loop and led to our Internet access being cut off for a brief period of time. The first I found out about that was when I was driving into work and I got a call from Nathaniel, from Apex letting me know what had gone on and that he was already on his way to the site to fix it. So what better can you ask for than that, really?

Have you seen any notable improvements in data security or business continuity since partnering with Apex?

We've definitely noticed a huge improvement in business continuity and security since working with Apex. We, unfortunately, were the victims of a ransomware attack prior to working with Apex and specifically looked for a company that would look after us in the event of anything like that in the future, but more importantly, prevent it.

"Apex has certainly been very open about the threats that are around, what we can afford as a business to put in place and what we really should be considering having in place"

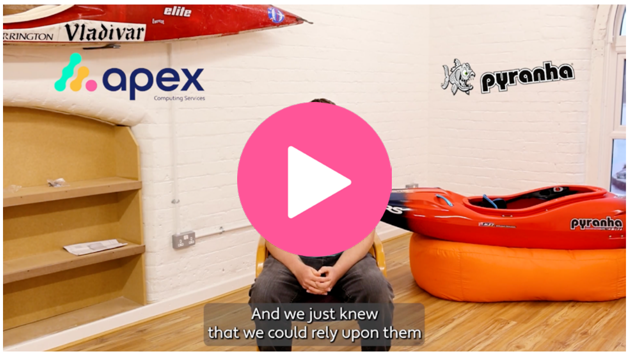
How has Apex's support enhanced the overall productivity and efficiency of Pyranha Mouldings?

With Apex's support, we've had way less downtime than we have previously. Whenever an issue has come up, generally it's fixed before we know about it, and when it isn't, it's fixed very quickly.

What is the key takeaway for other Manchester-based Manufacturers considering Apex Computing's Services?

They are great people. You can really get to know them, really kind of welcome them into your team, and they'll welcome you into their company, and they'll support you in the best way that they can. I can't recommend them enough.

Watch: Pyranha Mouldings Ltd's Mathee Wilkinson talk about their experience with Apex

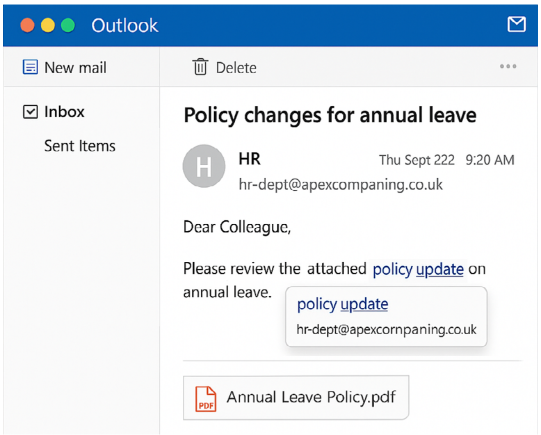


QUIZ:
CAN YOU SPOT THE PHISH?

FOUR EMAILS. ONE REAL. CAN YOU TELL WHICH?

How to Play:
Below are four examples of emails - one is genuine, three are phishing attempts.

01 | HR UPDATE



Policy changes for annual leave

HR Thu Sept 222 9:20 AM
hr-dept@apexcompaning.co.uk

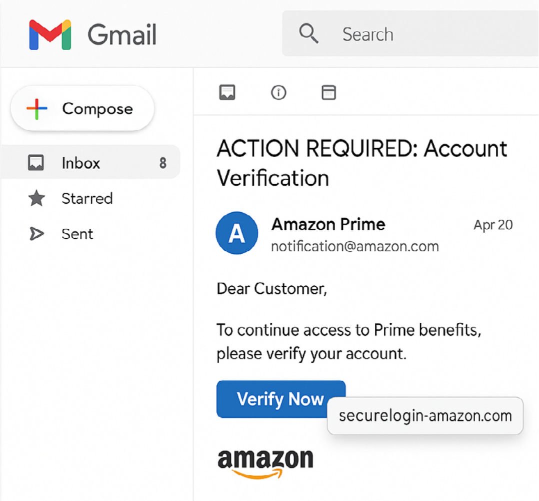
Dear Colleague,

Please review the attached policy update on annual leave.

policy update
hr-dept@apexcornpaning.co.uk

Annual Leave Policy.pdf

02 | VERIFICATION



ACTION REQUIRED: Account Verification

Amazon Prime Apr 20
notification@amazon.com

Dear Customer,

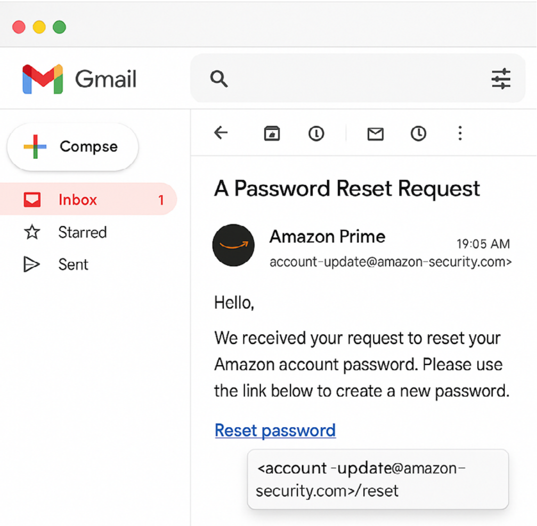
To continue access to Prime benefits, please verify your account.

Verify Now

securelogin-amazon.com

amazon

03 | PASSWORD



A Password Reset Request

Amazon Prime 19:05 AM
account-update@amazon-security.com>

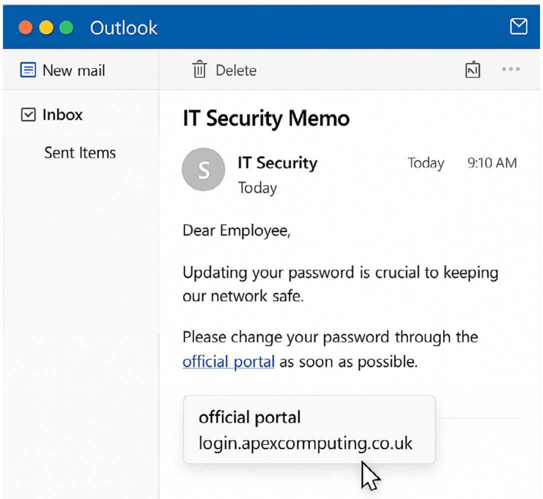
Hello,

We received your request to reset your Amazon account password. Please use the link below to create a new password.

Reset password

<account -update@amazon-security.com>/reset

04 | UPDATE DETAILS



IT Security Memo

IT Security Today 9:10 AM
Today

Dear Employee,

Updating your password is crucial to keeping our network safe.

Please change your password through the official portal as soon as possible.

official portal
login.apexcomputing.co.uk

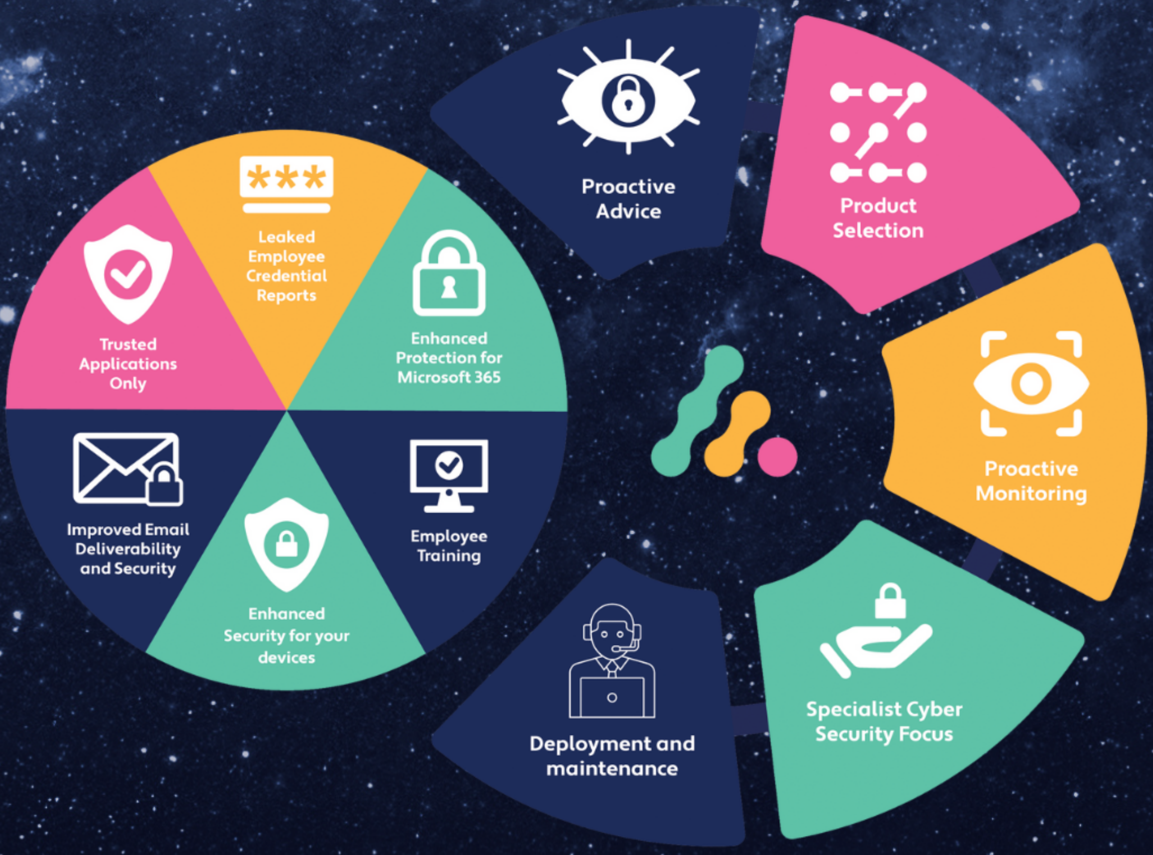
Need a Clue? Find clues and answers on Page 29.

apex
Computing Services

Cyber Security Expertise with Sphere at the Core

The *Apex Cyber Security Sphere* is a comprehensive solution, bringing together the best tools to keep your business secure and future-ready

Firewalls and Network Defence
Endpoint and User Protection
24/7 SOC Monitoring
Backup and Recovery
Awareness and Compliance


Leaked Employee Credential Reports
Trusted Applications Only
Enhanced Protection for Microsoft 365
Improved Email Deliverability and Security
Employee Training
Enhanced Security for your devices
Proactive Advice
Product Selection
Proactive Monitoring
Specialist Cyber Security Focus
Deployment and maintenance

make IT simple

www.apexcomputing.co.uk/cyber-security-sphere
0161 233 0099

CYBER HYGIENE 101: SIMPLE DAILY PRACTICES FOR SMES

32% of UK SMEs still have no cyber security measures in place. That's not just risky - it's an open door for ransomware, data loss, and downtime.

The good news? You don't need a six-figure IT budget to build strong defences. In this article, we'll break down daily and weekly habits that protect your business, your team, and your clients - all without slowing you down.

Let's make cyber hygiene second nature in your workplace

What is Cyber Hygiene?

Think of cyber hygiene like personal hygiene: brushing your teeth, washing your hands, getting check-ups. You don't wait for a problem to appear - you take small, regular actions to stop issues before they start.

Cyber hygiene is the same idea.

- It's keeping your system clear
- Your data backed up
- Your people aware
- Your defences up to date

"We've stopped countless ransomware attacks simply because our clients had good cyber hygiene. The biggest mistake we see is businesses assuming they're fine because 'nothing's gone from yet'. That's like never locking your office because you haven't been burgled - yet," said one of cyber experts.

Your 10-Point Cyber Hygiene Checklist

Here are the essentials every North West SME should be doing - no excuses, no jargon.

1. Keep software updated
2. Use antivirus and endpoint protection
3. Backup your data (and test it)
4. Remove ex-employee access
5. Secure admin accounts
6. Block unused ports and applications
7. Train staff regularly to spot threats
8. Regularly review devices
9. Monitor for breach signs
10. Have a simple incident recovery plan

"It's not about perfection. It's about progress. We help clients build simple, repeatable routines. If you do these basics well, you block 90% of threats before they start."

Think This is Too Basic?

Here's the truth: most breaches happen because of the basics being skipped. Not because you didn't have AI cyber tools or a SOC team.

- WannaCry hit the NHS because of an unpatched Windows system
- Small firms across the North West have been crippled by ransomware because their backups failed, or no one tested them
- Most phishing attacks work because users haven't had training in months

How Apex Keeps You Covered

We work with over 180 businesses across Greater Manchester - from legal firms to manufacturers - to keep their cyber hygiene tight and consistent. Here's what we can take off your plate:

- Fully Managed Cyber Security: From patching to backups to antivirus and email filtering - all in one service

- Routine System Checks: Automated alerts, scheduled health checks, and proactive issue fixing

- Staff Awareness Training: Phishing simulation training, cyber attack simulations, password safety, and Bring Your Own Device (BYOD) devices

- Backup and Disaster Recovery: We configure, test, and manage secure backups for total peace of mind

- 24/7 Threat Detection: Get alerted the moment something suspicious appears on your network or devices

- Cyber Essentials Certification Support: We help SMEs achieve and maintain Cyber Essentials and Cyber Essentials Plus - including hygiene audits and remediation

Small Habits = Big Protection

You lock your office doors every night - cyber security should be just as routine. You don't need to do everything at once. Start with Apex's Cyber Security Hygiene Checklist, automate what you can, and review your habits monthly.

If you need help, we're just down the road (and only a phone call away).

Resources to Help You Start Today...

Download

Our FREE Cyber Hygiene Checklist for SMEs - print it, pin it, use it!

Read

Our Cyber A-Z Jargon Buster.

Explore

Our all-inclusive cyber security package - the Apex Cyber Security Sphere.

Talk to Us

Get a free cyber health check for your business. Contact our team - no hard sell, just honest advice.

#CaseStudy

SECURING ELEGANCE: A SUCCESS STORY WITH LOCAL JEWELLERS

We spoke to Paweł Klamannm, Project & Operations Manager of David M Robinsons the Jewellers about their experience with the Apex Cyber Security Sphere.

Could you provide a brief overview of your business and the industry you operate in?

Our company specialises in offering a premium selection of high-end jewellery and watches. We operate both through our physical chain of stores and our online platform. Our collection is carefully curated to cater to discerning customers who value quality and luxury. As the Project & Operations Manager, I play a pivotal role in ensuring that our operations run smoothly, that our products meet the highest standards, and that we consistently provide exceptional service to our customers. We operate in the luxury retail industry, which is characterized by its focus on exclusivity, craftsmanship, and customer experience. Our brand's reputation is built on trust, quality, and the timeless appeal of our products.

Why is IT critical to your business operations, particularly around security of your data?

IT plays an indispensable role in our business operations, especially when it comes to the security of our data. Given that we handle a vast amount of sensitive information about our clients, it's paramount that we ensure its absolute safety. Our clients trust us not only with their luxury purchases but also with their personal and financial information. Breaches in data security could not only lead to significant financial repercussions but also erode the trust we have established over the years. In our industry, trust is paramount. Data, in many ways, is the most valuable asset in our business, and its protection is non-negotiable. We invest in state-of-the-art IT infrastructure and security measures to ensure that our client data remains confidential and protected at all times.

In today's digital landscape, cyber security is paramount. What were some of the specific cyber security challenges or concerns your business faced before implementing the Apex Cyber Security Sphere?

Before adopting the Apex Cyber Security Sphere, our business faced fragmented cybersecurity solutions, gaps in staff training, and the challenge of keeping pace with rapidly evolving cyber threats. The Sphere streamlined our defences by centralizing our security tools and measures. Additionally, it provided comprehensive training for our staff, ensuring they're equipped to handle emerging threats. With the dynamic nature of cyber threats, having the Sphere ensures we stay current, safeguarding our most critical asset: data.

> *"The decision-making process for adopting the Apex Cyber Security Sphere was rooted in thorough research and analysis of our cyber security needs," said Paweł. "Since the implementation of the Sphere, we've observed a marked shift in our team's engagement with cyber security... The ongoing training provided by the Sphere has been pivotal in fostering a heightened sense of security."*

Were there any specific threats or concerns that highlighted the need for enhanced cyber security measures?

One of the primary threats we identified was the vulnerability posed by the end user. Often, even with the best technical defences in place, human error or oversight can become the weakest link in the security chain. Given this, we felt an urgent need to reinforce our cybersecurity measures with consistent and updated training. The ongoing training provided by the Sphere directly addresses this concern, ensuring that our team is always well-informed and vigilant, significantly reducing the risk of potential breaches or compromises.

What aspects of the Sphere caught your attention and made it seem like a suitable solution for your business?

The standout feature of the Sphere that truly captured our interest was its holistic approach to cybersecurity. Instead of juggling multiple solutions or being concerned about individual components, the Sphere provides a comprehensive solution that addresses all facets of cybersecurity under one umbrella. This not only streamlines our defences but also offers peace of mind, knowing that every potential vulnerability is being actively monitored and addressed. For a business like ours, where data protection is paramount, such an all-encompassing solution is invaluable.

Could you share insights into the decision-making process within your organisation when considering the adoption of the Sphere?

Watch: David M Robinson's Project & Operations Manager, Paweł's video interview below

Securing Eleg
A Cyber Security Success story with **David M Robinsons** the Jewellers

The decision-making process for adopting the Apex Cyber Security Sphere was rooted in thorough research and analysis of our cybersecurity needs. Initially, I reviewed and evaluated several solutions available in the market against our specific requirements and concerns. Once I was convinced of the Sphere's holistic approach and its potential benefits for our organization, I prepared a detailed recommendation highlighting its features, benefits, and how it could address our specific challenges. Subsequently, I presented this recommendation to John, emphasizing the urgent need for enhanced cybersecurity measures and how the Sphere could be the answer to our concerns. Given the importance of this decision, we discussed potential implications, costs, and benefits in detail. After weighing all factors, John signed off on the adoption of the Apex Cyber Security Sphere based on my recommendation, demonstrating the trust in my judgment and the evident merits of the Sphere itself.

Were there any particular features that played a crucial role in choosing this solution over the other cyber security solutions?

While the technical features of the Apex Cyber Security Sphere were compelling, a decisive factor in our choice was our existing trust in Apex as a brand. The relationship we've nurtured with Apex over the years has been characterized by reliability, responsiveness, and a deep understanding of our needs. Such a history of positive interactions and their reputation for excellence made the decision easier, as we felt confident in their commitment to providing a top-tier cybersecurity solution tailored for our specific requirements.

"In the high-end jewellery and watch industry, where transactions incolce significant monetary values and sensitive data, ensuring cyber security is paramount," said Paweł. *"The Apex Cyber Security Sphere, by offering a comprehensive and holistic approach, has become a cornerstone for our industry's cyber security needs."*

How has the Sphere addressed the specific challenges you were facing?

Since the implementation of the Apex Cyber Security Sphere, we've observed a marked shift in our team's engagement with cybersecurity. Traditionally viewed as a complex and, admittedly, somewhat dry topic, cybersecurity has now become a more approachable and understood subject within our organisation.

How have these features contributed to a stronger sense of security and risk mitigation?

The ongoing training provided by the Apex Cyber Security Sphere has been pivotal in fostering a heightened sense of security within our organisation. By focusing on the end users – often considered the weakest link in cybersecurity chains – the Sphere has turned a potential vulnerability into a strength. As our staff undergoes regular training, they're not just passively absorbing information but actively engaging with it, leading to a deeper understanding and retention of cybersecurity best practices.

Can you share examples of how the solution has addressed industry-specific threats or compliance regulation?

The Apex Cyber Security Sphere has been instrumental in addressing our industry's specific needs and compliance requirements. During our regular annual audits, the Sphere's comprehensive protective features and protocols readily demonstrate our adherence to robust cybersecurity standards. Additionally, when pursuing the Cyber Essentials Certification, a testament to a business's cybersecurity commitment, the Sphere ensured we met all best practices, simplifying the certification process. In essence, the Sphere not only provides top-tier cybersecurity but also positions us favourably in a competitive industry that highly values trust and reliability.

Have you noticed any changes in user behaviour and adherence to security protocols since implementing the Sphere?

The implementation of the Apex Cyber Security Sphere has had a noticeable impact on our employees' awareness of cybersecurity practices. Before its integration, while there was a general understanding of the importance of cybersecurity, the depth of this understanding was sometimes limited.

Looking ahead, how do you see the Sphere aligning with your business's future growth and cyber security strategies?

Looking forward, as our business expands and evolves, the Apex Cyber Security Sphere will remain a pivotal component of our cybersecurity strategy. The dynamic nature of the digital landscape demands that security solutions not only address present concerns but are also equipped to anticipate and mitigate future threats. Our hope and expectation are that the team behind the Sphere will remain vigilant and adaptive, ensuring that the platform continually evolves in response to the changing cybersecurity landscape. This would entail routinely assessing the Sphere's components and making necessary adjustments, be it adding new features or refining existing ones, to remain at the forefront of cybersecurity. Such proactive adaptability is crucial for ensuring that as our business grows and diversifies, our cybersecurity posture remains robust and aligned with both current and future challenges.

What advice would you offer to other businesses considering the adoption of the Apex Cyber Security Sphere?

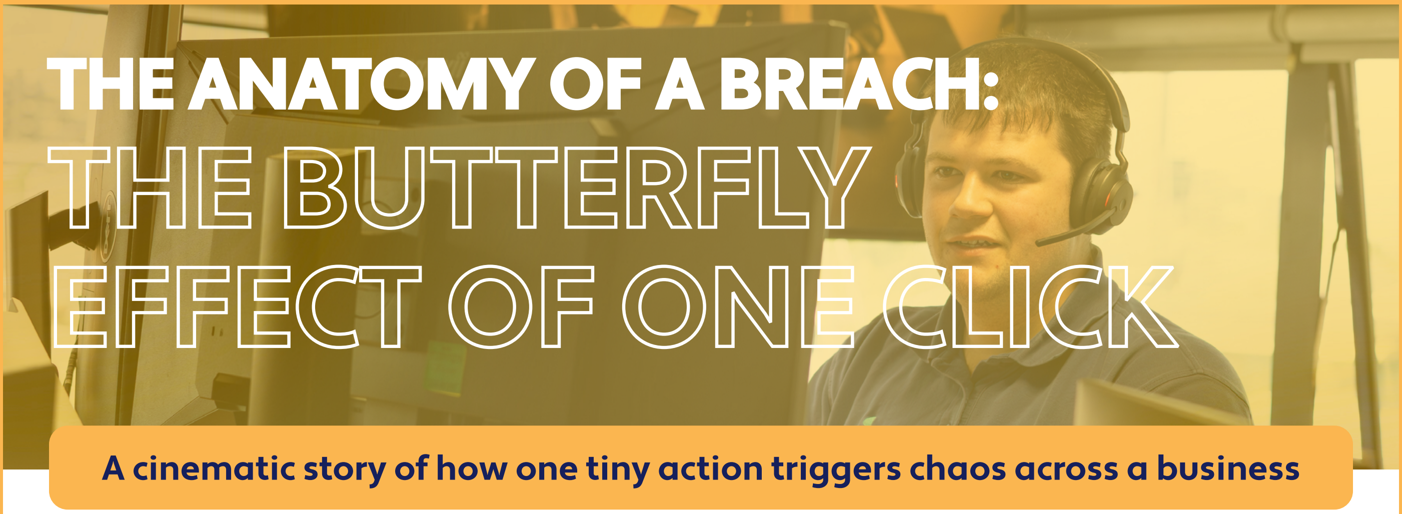
For businesses contemplating the adoption of the Apex Cyber Security Sphere, my advice is straightforward: Go for it. In today's intricate digital landscape, cybersecurity is not just an option but a necessity. And while understanding its complexities is essential, managing it in-house can be a daunting task, especially for companies that don't have the bandwidth or resources to maintain a dedicated cybersecurity team. The Sphere addresses this challenge head-on, offering expertise and state-of-the-art protection. By opting for the Sphere, you're essentially entrusting this critical aspect of your business to seasoned professionals, ensuring your digital assets are safeguarded by the best in the field. So, rather than navigating the murky waters of cybersecurity alone, leverage the prowess of experts and let the Apex Cyber Security Sphere fortify your defences.

How would you describe the overall experience of working with Apex Computing Services during the implementation and ongoing use of the Apex Cyber Security Sphere?

Working with Apex Computing Services during the implementation and ongoing use of the Apex Cyber Security Sphere has been an exemplary experience. Their team exuded professionalism from the onset, ensuring the entire process was seamless.

Is there anything else you would like to share about your journey with the Apex Cyber Security Sphere?

In summary, the Apex Cyber Security Sphere has become both a critical and essential cornerstone of our business's cybersecurity resilience. It acts as our digital shield, ensuring that our assets, data, and operations remain uncompromised in the face of ever-evolving cyber threats. Its presence has fortified our defences, elevating our cybersecurity posture and instilling a renewed sense of confidence in our ability to safeguard our business and client interests. In essence, the Sphere has transitioned from being a mere tool to an indispensable ally in our quest for digital security.



THE ANATOMY OF A BREACH: THE BUTTERFLY EFFECT OF ONE CLICK

A cinematic story of how one tiny action triggers chaos across a business

1 Scene 1: Monday, 09:17 - The Click Heard Round the Office

A finance assistant named Sarah gets an email from "Accounts Payable". It looks urgent. She clicks the link.

A blue login box flashes. She signs in.

That's it. The domino falls.

2 Scene 2: Monday, 09:19 - The Infiltration Begins

Her credentials are already being sold on the Dark Web.

Within minutes, an AI-driven bot logs into the company's Microsoft 365 environment from Eastern Europe.

3 Scene 3: Monday, 10:43 - The Phantom Employee

The attacker creates a new mailbox rule: **All emails with "invoice", "bank", or "payment" are auto-forwarded.**

No one notices. Business continues as normal.

4 Scene 4: Wednesday, 08:02 - Detonation

Encrypted files. Locked screens. A ransom note that simply reads: ***"Your data is ours. £10,000 to get it back."***

Where Could This Have Been Stopped?

1. Multi-Factor Authentication - credentials useless
2. Staff trained to spot fake domains
3. Threat monitoring to catch the anomaly
4. Offline backups - business continuity saved

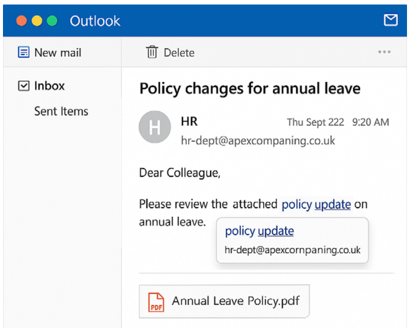
QUIZ:

CAN YOU SPOT THE PHISH?

ANSWERS REVEALED

FAKE!

01 | HR UPDATE



Policy changes for annual leave

HR Thu Sept 222 9:20 AM
hr-dept@apexcompaning.co.uk

Dear Colleague,

Please review the attached policy update on annual leave.

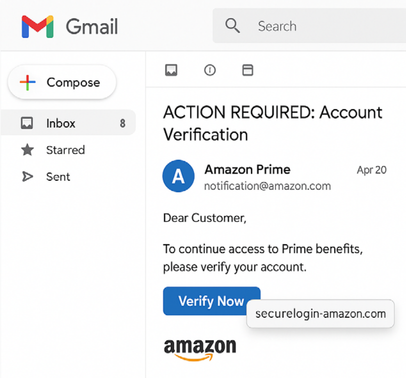
policy update
hr-dept@apexcornpaning.co.uk

Annual Leave Policy.pdf

Did you notice the spelling error in the domain? Instead of @apexcomputing.co.uk they threat actors have used @apexcompaning.co.uk.

FAKE!

02 | VERIFICATION



ACTION REQUIRED: Account Verification

Amazon Prime Apr 20
notification@amazon.com

Dear Customer,

To continue access to Prime benefits, please verify your account.

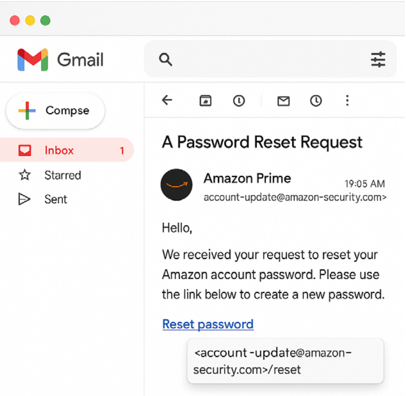
Verify Now
securelogin-amazon.com

amazon

Did you notice the unusual domain and the urgency of the email? www.securelogin-amazon.com is not a legitimate Amazon domain, and the email is suggesting that the "customer" is missing out on Prime benefits by not verifying their account.

FAKE!

03 | PASSWORDS



A Password Reset Request

Amazon Prime 19:05 AM
account-update@amazon-security.com>

Hello,

We received your request to reset your Amazon account password. Please use the link below to create a new password.

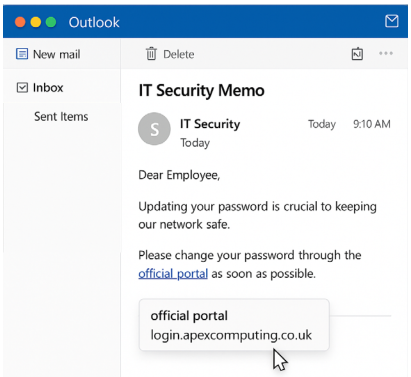
Reset password

<account-update@amazon-security.com>/reset

Did you notice the fake email address? @amazon-security.com is not a real email address. The urgency of the email and scare tactics used make the user think someone is hacking into their account by requesting a new password and to reset it to stop someone malicious changing it first.

FAKE!

04 | UPDATE DETAILS



IT Security Memo

IT Security Today 9:10 AM
Today

Dear Employee,

Updating your password is crucial to keeping our network safe.

Please change your password through the official portal as soon as possible.

official portal
login.apexcorrputing.co.uk

Did you notice any errors? How about the 'r' added to 'computing'? It's really difficult to see but it's there! Always be vigilant.

SCORE YOURSELF:

4/4 - Cyber Ninja!

3/4 - Phish Whispered

2/3 - Training Needed!

<2/4 - Call Apex Immediately!

Employee Spotlight

MEET ROSS ANSELL

We're speaking to one of our T3 Engineers, Ross, who has been with Apex since February 2024!

How did you get into the IT/MSP world?

I first started working in IT at one of the UK's largest construction companies, but when my friend invited me to join his Managed Service Provider business, it opened my eyes to a whole other side of the industry. One that was fast-paced, varied, and constantly evolving. I joined Apex in February 2024 and this is where I truly discovered the unique appeal of the MSP world. No two days are ever the same here, with new challenges, technologies and opportunities to make a real difference for our clients.

You've just won the lottery - what do you do?

If I won the lottery, I'd jet off on a once-in-a-lifetime trip around the world. Top of the list would absolutely be seeing all Seven Wonders of the World, followed by going on a mission to visit every Disney theme park across the globe. Disney World Florida is already on my list for this year! I'd love to experience the nostalgia and joy all the parks across the world offer. I'd love the blend of adventure, imagination, and magic exploring the Wonders of the World and Disney parks would give me.

What's one thing you wish more people understood about your job?

Everyone thinks IT is just "turning it off and on again", and while that does work for some things, T3 is where the real magic happens. It's deep-diving into technical knowledge, advanced troubleshooting, and staying ahead in a constantly evolving industry. I always have to think outside the box to find creative and unexpected solutions to problems that aren't responding to usual fixes.

Are there any upcoming technologies or trends you're excited about?

I'm really excited how AI has been transforming IT support. While it's opened people up to things like advances in cyber security threats, it's also creating more predictive maintenance, faster resolutions, and smarter automations. It's giving us the tools to be more proactive, efficient, and secure for ourselves and our customers, while freeing us up to focus on complex problem-solving and innovation.

Born and bred in Manchester or moved here?

I moved to Manchester 10 years ago from a small town in Lancashire. The city was the perfect place for me to have better job prospects, especially in IT, and have better social offerings.

What's your favourite hidden gem in Greater Manchester?

You definitely have to visit the Vimto Statue near Sackville Street. It's a wooden sculpture of a giant Vimto bottle surrounded by carved fruits celebrating the drink created in Manchester back in 1908. It's unexpected, fun and a sweet nod to local history. Plus who doesn't love an ice-cold Vimto?

If you weren't in IT, what would you be doing?

I'd be in Texas, living the dream as a BBQ Pit Master. There's just something about slow-smoked brisket, open flames, and crafting the perfect rub and sauce that speaks to me. I'd trade servers for smokers any day! BBQ is a massive passion of mine.

What's one common cyber security myth you'd love to bust?

One myth I'd love to bust is that cyber security is "just an IT problem". It's everyone's responsibility. The strongest firewall or latest security tool can be undermined by a single weak password or clicking the wrong link. Technology is vital, but people and good habits are the first line of defence.

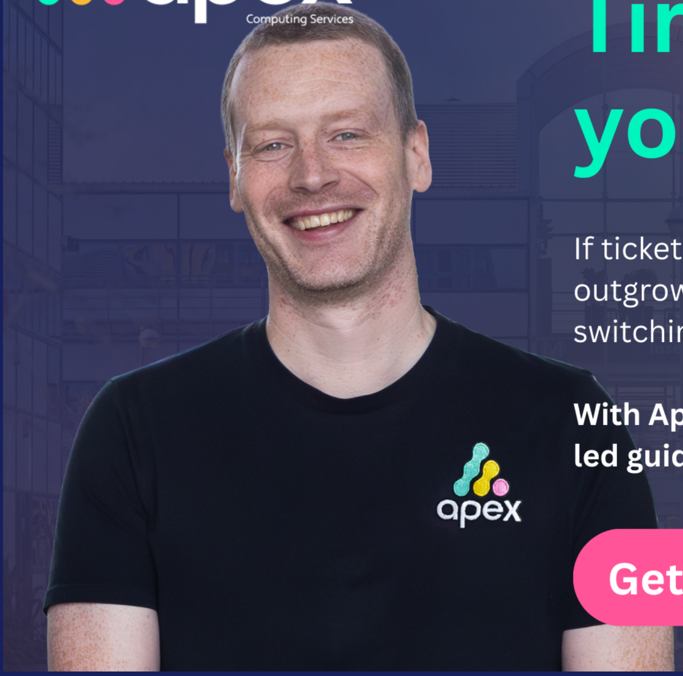
What's your favourite part about working at Apex?

My favourite part about working at Apex is the people. I'm lucky to work with a talented, supportive team of people that make even the busiest days enjoyable. I also love our monthly Culture Club events where we get to spend time with colleagues outside of work and have some fun together. It gives us a really strong sense of team.

What's one thing that makes the Apex team stand out from others you've worked with?

Apex is truly like a family. Whenever anyone has an issue, everyone is ready to jump in and help, no matter what their role. It's created a great place to work that's customer-focused, solves problems fast, and delivers the best possible service together.

apex
Computing Services



Tired of chasing your IT provider?

If tickets drag on, security feels shaky, or you've outgrown your current IT support partner, switching doesn't have to be painful.

With Apex Computing, you get seamless, expert-led guidance - and 24/7/365 support you can trust.

Get Started ➤

Watch: Hear from our Onboarding Manager, Daryl, on the process of switching to Apex as your IT partner here >

Switching IT Providers Doesn't Have to Be Hard

Our **Switching Made Simple Guide** shows you how to move on from poor IT support without downtime, data loss, or stress.

- Spot the red flags
- Follow our 4-step switch plan
- See what life looks like after the move

Download your free guide today
and discover just how easy switching can be.

Download your guide here

apex
Computing Services
make IT simple

Switching Made Simple

Your friendly guide to breaking up with your IT provider (without the drama)

apex
Computing Services

Contact us

Want to get started?

Apex is ready to assess your business and provide you with a tailored IT Solution package. For a free IT consultation - please feel free to get in touch:

Laser House, Media Village, Waterfront Quay, Salford Quays, M50 3XW.
WhatThreeWords: blur.beside.spoken

☎ 0161 233 0099 ✉ enquiries@apexcomputing.co.uk

Contact us