ASSURED DIGITAL

Phishing Defence Toolkit

5 Practical Steps to Stop Email-Based Attacks

A Customer Advisory from Assured Digital

ASSURED DIGITAL

The Threat: Phishing Is Surging

84% of UK businesses reported phishing attempts last year." - CyberSmart

Phishing is still the #1 way attackers get in. But the emails are smarter, and so are the tactics. Think urgent payment requests. Fake login pages, QR codes, and urgent payment requests designed to fool even savviest technical teams.

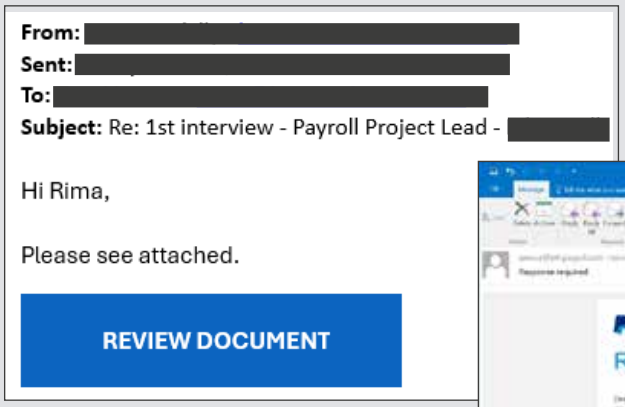
Examples we're seeing across client networks

- Spoofed Microsoft Teams invites and SharePoint links
- Fake invoice emails from real-looking suppliers
- QR-code phishing targeting mobile staff
- Outlook rules that hide replies from IT or finance

"Nearly 3 in 4 breaches involve human error." - *Verizon DBIR 2023*

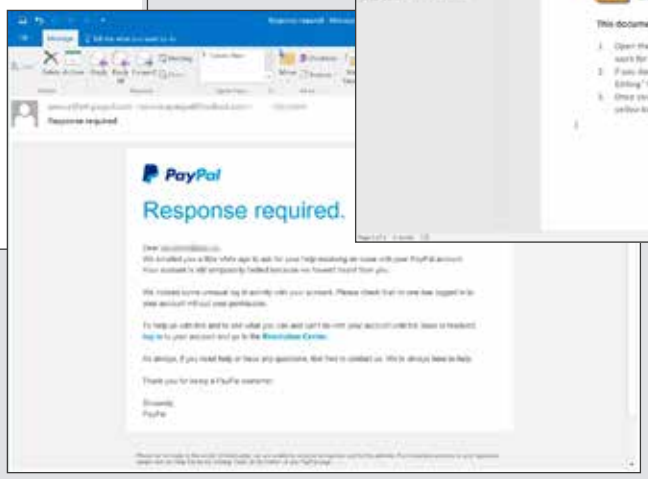
What We're Seeing in the Wild

Phishing isn't always obvious. In 2025, it looks like this:

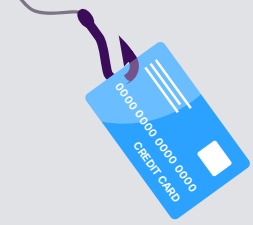


Fake job interview response with a "Review Document" link that installs malware

Malicious Word doc disguised as HR or invoice file prompts users to enable macros



Spoofed PayPal alert using urgency to trick users into clicking



ASSURED DIGITAL

How They Bypass Filters and What to Do About It

Modern phishing evades basic defences. *Here's how:*

- Phishing emails land during low-focus times: Friday afternoons, lunch breaks, internal change windows
- Attackers exploit inbox rules that hide replies or auto-mark messages as read
- They adapt to filtering tools, standard spam filters aren't enough

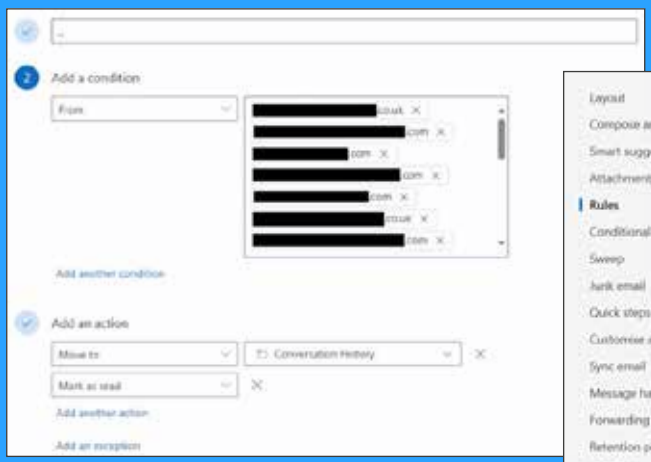
Why do people still fall for phishing attacks?

- **They feel familiar.** Attackers impersonate suppliers, recruiters, Microsoft, even your colleagues.
- **They create urgency.** "Your account will be locked." "Invoice overdue." "Action required."
- **They appear safe.** Domain names look legit, branding is copied, and links are shortened.

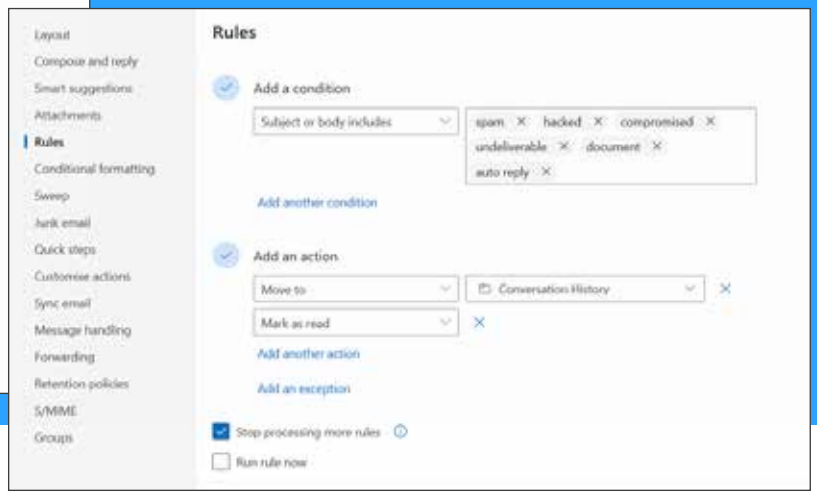
"47% of users admit to clicking a phishing link while distracted." - Guardz, 2024

Proactive Rules You Can Set Today

Email Rule to Flag High-Risk External Senders

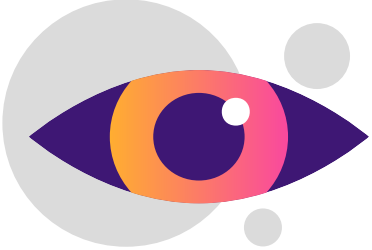


Email Rule to Auto-Surface Suspicious Language



Quick Wins. Big Impact.

- **Tag external senders + block risky attachments** | *Quick wins that reduce what gets through in the first place.*
- **Focus on high-risk roles (e.g. finance, execs)** | *Target training where attacks land most often.*
- **Review security quarterly, not yearly** | *Threats change fast. So should your defences.*
- **Normalise near-misses** | *Create a culture where reporting "almost clicked" is the norm, not embarrassing.*



Want to know your weak spots?
Try our free 2-Minute Cyber Health Check or speak with our security team.

The Quorum, Bond Street, Bristol, BS1 3AE
enquiries@assureddigitaltech.com

ASSURED DIGITAL

What Happens in a Breach

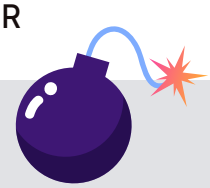
"One phishing email exposed 79,000 patient records. The ICO issued a £3M fine." - ICO Enforcement, 2025

One click is just the beginning. *Here's what usually happens next:*

- Attacker logs in and sets up their own MFA, locking you out
- Outlook rules silently hide alerts and replies
- The attacker emails your clients and suppliers using your identity
- They access Teams, SharePoint, and OneDrive - often unnoticed

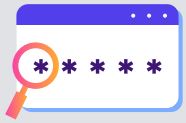
Consequences for your business

- **Ransomware may follow,** encrypting data and locking you out of systems
- **Operations can grind to a halt** until payment is made or recovery is complete
- **Client and supplier data may be accessed or leaked**, leading to reputational damage
- **Microsoft may block outbound emails for 24+ hours**, disrupting communication and delivery
- **Sensitive documents, chat logs, and contracts can be compromised**
- **Fines and legal costs can be severe,** up to £17.5M or 4% of turnover under UK GDPR



What To Do If You Suspect a Breach

Step 1: Lock It Down



- Change your password
- Remove unknown MFA devices
- Disconnect from the network

Step 2: Alert Your IT Team or Assured Digital

- Pause before deleting emails, evidence matters.
- Send suspicious emails to ADT for investigation.

Step 3: Clean Up the Mailbox

- Remove inbox rules and filters
- Recheck shared mailboxes for visibility and threats

Step 4: Understand the Spread

- Review M365 logs, check if files or clients were affected.
- We'll guide response, clean-up, and comms.

Step 5: Strengthen Defences

- Audit/ reinforce your MFA setup
- Launch phishing simulations
- Harden your filtering and monitoring

Even if you're not sure...
Ask us to check.
It's what we're here for.

The Quorum, Bond Street, Bristol, BS1 3AE
0330 055 2678

ASSURED DIGITAL

5 Fixes to Stop Phishing in Its Tracks

Simple fixes. Major protection.

Most breaches start with a single click. The steps below are high-impact changes you can make today to harden your business against phishing, without adding friction for your team.

Step	Why It Matters	What to Do
Turn On MFA Everywhere	*Think of MFA like a deadbolt on every digital door. Even if attackers get a password, MFA stops them using it.*	• Roll out Microsoft Authenticator or Duo • Apply MFA to Microsoft 365, finance apps, CRMs, remote access tools
Lock Down Email Entry Points	*Unconfigured inbox rules often hide phishing attacks. Hackers know it, and use it.*	• Tag all external senders • Block risky attachments (.exe, .iso, .js) • Audit mailbox rules every 90 days
Back Up & Test Recovery	*Most ransomware attacks target your backups. If you haven't tested a restore, you're exposed.*	• Back up to cloud or secure offsite locations daily • Test restores quarterly • Use immutable backup options that can't be tampered with
Train Your Team Little and Often	*"47% of users admit they've clicked phishing links when distracted."* - Guardz, 2024	• Run short, monthly simulations • Share 1-minute micro-lessons in team meetings or ovefr email
Always Verify Money Requests	*Business Email Compromise (BEC) costs UK firms ££ millions annually. Most start with urgent payment emails that look legit.*	• Never rely on email alone to approve payments • Call or text known contacts to confirm large or unusual requests

Think You're Covered? Let's Find Out.

Most breaches start with one click. Let's make sure your team isn't vulnerable.

- *Run our free 2-minute Cyber Health Check*
- *Get instant insight into your biggest risks*

How We Can Help

- Run phishing simulations & awareness campaigns
- Harden Microsoft 365 & breach response
- Test and improve recovery plans
- Tighten MFA and access control

Start your free check now, or reach out for more info

Scan the QR code
Or visit our website
assureddigitaltech.com

enquiries@assureddigitaltech.com

0330 055 2678