PHISHING DEFENCE

Playbook for UK SMES 2026

How to defend against the #1 attack vector facing UK businesses today

A practical guide for IT leaders, business owners and operations directors

WHY PHISHING, AND WHY NOW

Phishing is the most reliable attack vector in cybercrime today. It is the way the majority of ransomware infections start. It is the way most credential thefts begin. It is the way Business Email Compromise scams open. And it is the way every successful Microsoft 365 takeover we have ever investigated began. Other attack types come and go with the technology of the day; phishing is the constant.

It is also the attack type where SMEs are most vulnerable, for a simple reason: phishing exploits people, and people are a part of every business that the security industry has spent the least effort defending. Firewalls have improved dramatically. Endpoint protection has improved dramatically. Identity controls have improved dramatically. Awareness training in most UK SMEs has not improved meaningfully since the days when phishing emails arrived in pidgin English from improbable Nigerian princes.

The technology will catch most of the phishing attempts. The few that get through are caught or not by your people. That last layer is the difference between an attempt and an incident.

- Recurring lesson from incident response engagements

Use this guide as

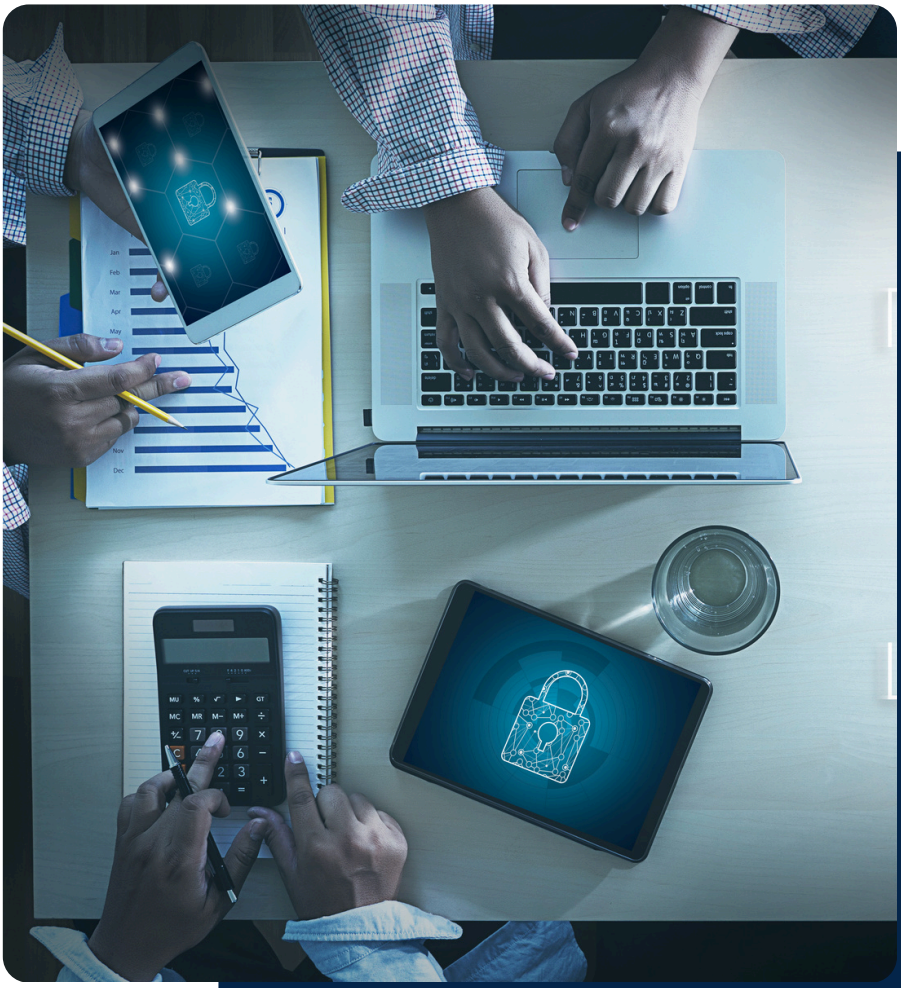
- A baseline for your phishing defence both technical and human.
- A briefing document for your leadership team, IT team, or MSP.
- A starting point for an awareness programme that goes beyond annual e-learning.
- A reference for what to do in the first hour after someone clicks.

Headline numbers

- Phishing is the initial attack vector in over 90% of ransomware incidents affecting UK SMEs.
- An employee at a business with no awareness programme has roughly a 30% chance of clicking a phishing link in any given simulation. With a properly run programme, that number drops below 5%.
- AI-augmented phishing has eliminated the traditional "bad spelling" tells. Modern phishing reads like a legitimate corporate email—and is increasingly personalised.
- Business Email Compromise phishing's most expensive variant costs UK businesses an average of £125,000 per incident. Most incidents are not insured for the full loss.

Want to know how your team would actually do?
We offer a free Phishing Vulnerability Assessment a controlled, ethical phishing simulation against your team, with detailed results and a benchmarked report. No naming, no shaming. Just an honest baseline of your current human-layer risk, completed within five working days.

- Request your free Phishing Vulnerability Assessment at systemforce.co.uk



KNOW YOUR ENEMY: TEN TYPES OF PHISHING

"Phishing" is not a single attack it is a family of related techniques, each with distinct tells, technical countermeasures, and impacts when they succeed. Effective defence starts with knowing which variants are likely to land in your business and why.

Type	What it looks like	Typical target
Bulk phishing	High-volume, low-effort emails, fake bank, courier, HMRC, Microsoft notices.	Anyone who opens an email
Spear phishing	Personalised email referencing real colleagues, projects, or pending work.	Specific named staff
Whaling / CEO fraud	Impersonation of a senior leader requesting urgent action, wire transfer, credential reset.	Finance, executive assistants
Business Email Compromise (BEC)	Compromised supplier or partner mailbox sends "updated bank details" mid-transaction.	Anyone paying invoices
Smishing	Phishing by SMS, fake delivery, banking or 2FA prompts targeting mobile devices.	All mobile-using staff
Vishing	Phone-based phishing, often following up on an email "This is IT, we need your password to fix it".	Front-line, helpdesk, finance
Quishing	QR codes in emails or print materials linking to credential-harvesting sites.	Hybrid/mobile workers
MFA fatigue	Repeated push-notification spam until the user accepts to make it stop.	Anyone using MFA push
Adversary-in-the-middle	Real-time proxy of the login flow captures credentials AND the MFA token.	M365 users (specifically)
Consent phishing	Asks the user to grant a malicious OAuth app access to their mailbox or files.	M365 / Google Workspace users

What's changed in 2026: the lower half of this table adversary-in-the-middle attacks, MFA fatigue, consent phishing, and Business Email Compromise, accounts for the bulk of incidents we now see in UK SMEs. These are the attacks that bypass MFA, target the cloud workspaces businesses depend on, and cause the highest-value losses. Bulk phishing is still the most common, but it's no longer the most dangerous.

THE THREE-LAYER DEFENCE MODEL

Effective phishing defence is built in three layers each catches what the previous one missed. No single layer is sufficient. Together, they reduce successful phishing from a near-certainty to a manageable, low-frequency event.

Layer 1: Technical controls

The first layer stops as much phishing as possible from ever reaching the user. Modern email security platforms Microsoft Defender for Office 365, Proofpoint, Mimecast and others typically block 95–99% of inbound phishing before it reaches a mailbox. This is the cheapest, most consistent layer and the one every UK SME should have in place at full strength.

Inbound email controls

- Anti-phishing engine (Defender for Office 365, Mimecast, Proofpoint, etc.) not just basic Exchange Online Protection.
- Safe Links rewrites URLs in email so they're checked at click time, not just at delivery.
- Safe Attachments sandboxes inbound files in a virtual environment before delivery.
- Impersonation protection trained on your VIPs, your domain, your suppliers.
- Anti-spoofing, DMARC at p=reject, SPF and DKIM correctly configured.

Identity controls (defence-in-depth for what gets through)

- MFA enforced via Conditional Access on every account, every application.
- Phishing-resistant MFA (FIDO2 keys) for administrators.
- Conditional Access blocking risky sign-ins, legacy authentication, and untrusted devices.
- Token-binding policies that resist adversary-in-the-middle attacks.

Endpoint controls (for when something actually lands and runs)

- EDR deployed on every endpoint, not legacy antivirus.
- Application control or attack-surface-reduction rules limiting macros, scripts, and dual-use binaries.
- Web filtering blocks known malicious or newly registered domains.

SFIT observation: the technical layer is the cheapest single uplift in most SME phishing programmes. Many tenants are licensed for Defender for Office 365 (included in Microsoft 365 Business Premium) but have never enabled the default security policies. The licence cost is sunk; the configuration is free; the protection difference is dramatic. Start here.

Layer 2: The human layer

Whatever the technology blocks, a percentage of phishing emails will still reach their targets. That's where the human layer takes over. Trained staff who recognise phishing, know what to do about it, and feel safe reporting it are the second line of defence. Untrained staff are the second line of attack.

The human layer is built from three components: education (the training programme), simulation (the practice), and culture (the safety to ask, report, and admit clicks). All three matter.

Programmes that focus only on education produce theory without instinct; programmes that focus only on simulation produce fear without understanding; programmes that lack a positive reporting culture produce silence and silence is what attackers count on.

What good awareness training looks like

- Bite-size 5–10 minute modules, monthly cadence, not 60-minute annual marathons.
- Scenario-based built around realistic situations the staff actually face.
- Role-targeted finance sees invoice scams, executives see whaling, IT see vendor spoofs.
- Up-to-date refreshed quarterly to cover new techniques (AI-augmented, smishing, quishing, MFA fatigue).
- Constructive focused on "how to spot it next time", not "why you got it wrong this time".
- Measured completion rates, comprehension scores, and behavioural change tracked over time.

What a good simulation looks like

- Realistic, uses the same tactics, brands and pretexts attackers actually use.
- Frequent, at least monthly, varied across email, SMS, and (for higher maturity) voice.
- Differentiated, different scenarios for finance, sales, IT, and executives.
- Coupled with training, staff who click are taken straight to a brief lesson, not punished.
- Tracked, click rate, report rate, repeat-clicker tracking over time.
- Internally communicated, successes celebrated, learnings shared, the programme visible.

What a good reporting culture looks like

- A clear, low-friction reporting channel one-click report button in Outlook is ideal.
- "It's better to over-report" messaging from leadership, repeated and meant.
- Genuine appreciation for reports including for the false positives, especially for the false positives.
- No blame for clicks staff who admit clicking are part of the solution; staff who hide clicks are part of the problem.
- Visible feedback loop "Sarah reported this email last Tuesday, and we blocked the sender well spotted, Sarah"

SFIT observation: the single highest-impact metric in phishing defence is not click rate. It is the report rate. A team where 50% of staff actively report suspicious emails has functional immunity to the attacks the technology missed; a team where 5% report even if their click rate looks similar does not. Build for reports first, and click rate falls naturally as a side effect.

Layer 3: Detection and response

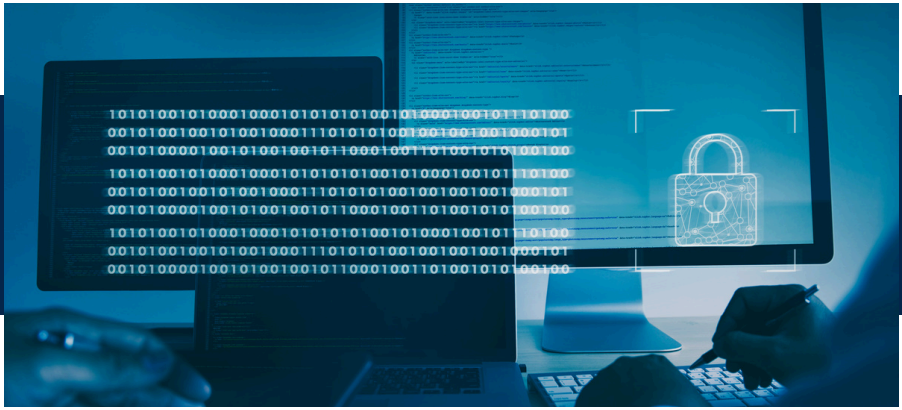
However good Layers 1 and 2 are, some phishing will succeed. Layer 3 is what determines whether the successful phish becomes a contained inconvenience or a major incident. The hours immediately after a click are the most expensive in cyber security because what you do (or fail to do) in them defines everything that follows.

What needs to be in place before the click

- Unified audit logging enabled and retained without it, post-incident investigation is largely guesswork.
- Alerts configured for high-risk events: mailbox forwarding rules, OAuth grants, MFA changes, mass downloads.
- EDR feeding into a SOC or central monitoring service with someone watching, not just dashboards updating.
- Documented incident response plan with named owners, escalation paths, and decision authority.
- Clear staff guidance: who to tell, how, and what to do until told otherwise ("don't try to hide it, don't try to fix it yourself").

What a good response looks like in the first hour

When a credential is phished, attackers are sometimes inside the mailbox within minutes. Speed is the difference between containment and breach. The 10-step response workflow later in this document gives the structured sequence but the principle is simple: deactivate the account first, investigate second.



THE AWARENESS PROGRAMME MATURITY LADDER

Most UK SMEs sit at Level 0 or Level 1 of the maturity ladder below. Movement up the ladder takes deliberate investment but produces measurable, reproducible results. The metrics shown are typical industry figures your starting point and target should be agreed with your leadership team and reviewed quarterly.

Level	Training	Simulation	Target metric
0 NONE	Induction-only or nothing.	None.	30%+ click rate
1 BASIC	Annual e-learning module.	Quarterly basic email.	15–25% click rate
2 ACTIVE	Bite-sized monthly training; targeted follow-up after misses.	Monthly varied scenarios.	5–10% click rate
3 EMBEDDED	Continuous, role-based, scenario-driven content.	Ongoing, multi-channel (email, SMS, voice).	<5% click; >50% report rate

How to use the ladder: honestly self-assess your current level, then aim for one level up over the next 12 months. Most businesses can move from Level 0 to Level 2 inside a year with modest investment (typically £2–£5 per user per month for a managed awareness platform). Level 3 Embedded, is the destination of mature programmes, usually requiring 18–24 months of sustained effort.

What's behind the metrics

Click rate measures the percentage of recipients who click a simulated phishing link. Lower is better, but it has a floor even mature programmes plateau around 3–5%, because perfectly designed phishing is genuinely hard to spot. Report rate measures the percentage of recipients who actively report a suspicious email. Higher is better. A high report rate indicates that staff are engaged, that reporting is friction-free, and that the culture supports speaking up. It is the leading indicator of a healthy programme and the metric that most reliably predicts response capability when a real incident lands.

SFIT observation: we typically see SMEs make rapid progress in the first six months moving from "never simulated" to "running monthly" is the largest single gain. Plateau usually hits around month nine. Continued progress beyond that requires varying scenarios, introducing role-targeting, and bringing in non-email channels (SMS, voice). Programmes that don't evolve eventually stagnate and click rates drift back up.

DESIGNING A PHISHING SIMULATION PROGRAMME

Running phishing simulations is straightforward to start and easy to do badly. The principles below distinguish a programme that builds defence from one that breeds resentment, gameable behaviour, or both.

Cadence

- Monthly minimum quarterly is too infrequent for muscle memory; weekly is exhausting and gameable.
- Random within the month predictable timing breeds predictable looking-out.
- Avoid genuinely sensitive periods, bereavements, redundancies, real incidents in progress.

Scenario design

- Vary across the recognised types, credential harvest, attachment-based, link-based, BEC, QR codes.
- Reflect topics actually arriving in inboxes, couriers, M365 notifications, supplier invoices, internal HR comms.
- Tier difficulty, start with obvious tells, progress to current attacker tradecraft.
- Calibrate to roles, finance see different scenarios from sales, executives different again.
- Update at least quarterly, yesterday's scenarios get spotted, harming the data.

Response to clicks

- Immediate just-in-time training the click leads to a 60-second lesson, not a punishment screen.
- No public naming, no public shaming the only person who needs to know about an individual click is that individual.
- Repeat-clicker tracking, privately, with structured follow-up after multiple misses.
- Aggregate statistics shared with the team "as a team, our click rate this quarter was 8%" encourages collective improvement.

What to avoid

- Naming and shaming, produces fear and silence, not learning.
- Making the simulation a disciplinary instrument turns staff against the programme.
- Using genuinely cruel pretexts fake redundancy notices, fake bereavement notifications. Effective and unforgivable.
- Running it as a one-off "campaign" instead of a continuous programme.
- Measuring only click rate hiding the much more important reporting metric.
- Letting the programme become predictable same day every month, same style every time.

Most common mistake: running the programme without leadership having agreed in advance how repeat clickers will be handled. The team finds out the rules retrospectively, which is the worst time to find out. Decide the policy first, communicate it second, run the programme third.

INCIDENT RESPONSE: THE FIRST HOUR AFTER A CLICK

Phishing incidents move fast. Stolen credentials are sold or used within minutes. Mailbox-rule changes can occur within hours. By the time an incident is "obvious", the damage is already largely done. Speed in the first hour is everything but speed without structure produces missed steps. The 10-stage workflow below is the structured sequence to follow.

#	Phase	Action	Owner
1	Detect	User reports the email; or SOC/EDR/email security alert fires.	Any staff / system
2	Triage	Confirm phishing; assess what was clicked, entered, downloaded.	IT / SOC
3	Contain	Disable the affected account immediately. Revoke active sessions and tokens.	IT / SOC
4	Hunt	Check for inbox forwarding rules, mailbox delegation, MFA changes, OAuth grants.	IT / SOC
5	Investigate	Review sign-in logs, IP origins, device IDs, recent file access.	IT / SOC
6	Eradicate	Remove malicious rules, revoke OAuth grants, reset passwords, re-enrol MFA.	IT / SOC
7	Notify	Inform affected staff, suppliers, customers as required.	IT lead / business lead
8	Report	ICO breach notification (within 72 hours if data involved); insurer; regulators.	Business lead
9	Recover	Restore data from backup if needed; restore service; communicate "all clear".	IT
10	Review	Post-incident review what worked, what to improve, controls to strengthen.	All stakeholders

Critical principle: containment comes before investigation. The temptation to "have a look first" before disabling the account costs businesses material time. If a credential has been entered into a phishing site, treat it as compromised until proven otherwise. Disable the account, then investigate. Re-enabling later is cheap; not disabling early is expensive.

Don't wait until you're learning this in real time

We help UK SMEs design, deploy and operate phishing defence programmes technical controls, awareness platform, simulation cadence, and 24/7 incident response. Most of our clients move from Level 0 or 1 to Level 2 inside six months, with measurable click-rate reduction and a documented response capability. The programme pays for itself if it prevents a single BEC incident.

- Book a phishing defence consultation at systemforce.co.uk

COMMON FAILURES IN SME PHISHING DEFENCE

These are the patterns we see in the SMEs whose phishing defence programmes either fail to materially reduce risk, or fail outright when tested. Each is fixable; together they account for the bulk of preventable phishing incidents.

- Annual e-learning treated as the entire awareness programme staff forget within weeks.
- No phishing simulations "we tell them not to click" is not a programme.
- Defender for Office 365 licensed but never configured preset security policies untouched.
- DMARC at p=none spoofed emails using your domain land in customer inboxes today.
- MFA on email but not Conditional Access, adversary-in-the-middle tools bypass it.
- No "report phishing" button staff don't know what to do with suspicious mail.
- Reports go to a generic shared mailbox no one watches the only thing worse than not reporting.
- Staff who report get no acknowledgement and stop reporting.
- Click-only metrics programme appears to be improving while reporting stays at zero.
- No incident response plan IT ad-libs the first hour during a real incident.
- OAuth consent grants unmonitored malicious apps with mailbox access living quietly in the tenant.
- Untrained executives and finance the highest-value targets, with the least preparation.

If five or more apply to your business, your phishing defence is functionally weak, and AI-augmented phishing in 2026 is materially harder to spot than the phishing of three years ago. The gap is widening, not narrowing.

YOUR 90-DAY PHISHING DEFENCE PLAN

If everything in this playbook feels like a lot to take on at once, you are not alone most UK SMEs reach a mature programme over years, not weeks. Below is a realistic 90-day plan to move from "largely unprotected" to "materially defended" and to have measurable evidence of progress at each stage.

Days 1–30 Foundations

- Run a baseline phishing simulation establish your starting click rate honestly.
- Apply Defender for Office 365 preset security policies (Standard or Strict).
- Enable Safe Links and Safe Attachments tenant-wide.
- Configure impersonation protection for VIPs and your own domain.
- Publish DMARC record at p=none and start collecting reports.
- Confirm MFA enforced via Conditional Access for every account.
- Deploy a one-click "Report Phishing" button in Outlook.

Days 31–60 Programme launch

- Select and deploy a managed awareness training platform (KnowBe4, Hoxhunt, or equivalent).
- Begin monthly simulation cadence start with general scenarios, plan for role-targeting from month 4.
- Roll out bite-size training modules 5–10 minutes each, tied to recent simulation results.
- Document incident response plan with named owners and escalation paths.
- Brief leadership and managers particularly on reporting culture and repeat-clicker handling.
- Move DMARC from p=none to p=quarantine.

Days 61–90 Hardening and evidence

- Run incident response tabletop exercise phishing scenario, full leadership team.
- Audit OAuth grants in Entra ID, revoke anything unrecognised or excessive.
- Configure alerts for high-risk events, forwarding rules, OAuth grants, MFA changes.
- Move DMARC to p=reject domain-spoofing protection complete.
- Run a follow-up phishing simulation measure click rate and report rate against baseline.
- Document programme metrics; set 6- and 12-month targets.
- Plan year-two evolution non-email channels, role-targeting, scenario refresh.

Realistic outcome: an SME starting at Level 0 (no programme, ~30% click rate) typically reaches Level 2 (active programme, 5–10% click rate, 20%+ report rate) within 90 days of structured execution. The technology changes alone are usually responsible for blocking a 5–10× increase in inbound phishing volume; the cultural changes drive the residual risk reduction.

HOW SYSTEM FORCE IT CAN HELP

Phishing defence is not a product you buy. It is a programme you run combining technical controls, awareness training, simulation, and incident response into a sustained operational discipline. Most SMEs lack the time, resources or specialist knowledge to do it themselves, and most generic IT providers focus on the technology and ignore the people side entirely.

System Force IT delivers:

- Phishing Vulnerability Assessments, controlled simulation against your team with a benchmarked report.
- Microsoft 365 email security configuration, Defender for Office 365 hardening, DMARC progression, anti-impersonation.
- Managed awareness training programmes, bite-size, monthly, role-targeted, measurable.
- Phishing simulation as a service, varied, realistic, with just-in-time training and reporting analytics.
- Incident response retainer 24/7 coverage with documented playbooks and rehearsed response.
- Strategic phishing defence reviews, programme design, maturity assessment, budget guidance.

Book a free Phishing Defence Review

One of our security specialists will assess your current phishing defence, technical controls, awareness programme, simulation maturity, response capability and give you a benchmarked report against the maturity ladder in this document, with a costed remediation plan. Free of charge, completed within five working days. The report is yours to keep regardless of whether you choose to engage further.

- Book your free Phishing Defence Review at systemforce.co.uk

Or call us directly: 01452 701355 We're based in Gloucestershire and protect UK SMEs against the attacks most likely to land tomorrow.

Authoritative sources and further reading

- NCSC Phishing guidance: ncsc.gov.uk/guidance/phishing
- NCSC Mitigating phishing attacks: ncsc.gov.uk
- UK Cyber Security Breaches Survey: gov.uk/government/statistics/cyber-security-breaches-survey
- Microsoft Defender for Office 365 documentation: learn.microsoft.com
- Action Fraud UK reporting line for cyber crime: actionfraud.police.uk
- ICO Breach notification guidance: ico.org.uk

This document is provided for general guidance only. Statistics and percentages cited are typical industry ranges from UK SME engagements; outcomes vary significantly by organisation, sector and starting maturity. Phishing techniques evolve continuously; verify current best practice against authoritative sources before acting on time-sensitive decisions.

System Force I.T.
Secure IT Simplified

Want a free Phishing defence assessment with System Force IT?

We run free, no-obligation reviews for UK SMEs.
Written report in 7 working days.
No sales pitch, no follow-up unless you ask for one.

Book at systemforce.co.uk
Or call us directly: 01452 701355

System Force IT | supporting UK businesses since 2006.

UKAS ISO/IEC 27001: 2022 Certified | Microsoft Solutions Partner | Certified 3CX Partner | Cyber Essentials Practitioners | RIPE NCC Member

Next Step:

Book your free PHISHING DEFENCE Playbook for UK SMEs.

01452701355

www.systemforce.co.uk

sales@systemforce.co.uk