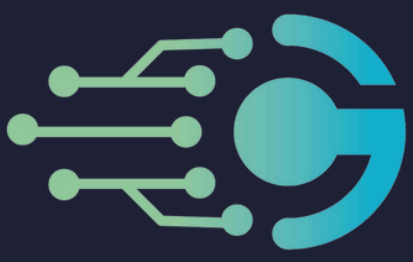
GUIDE

How to Train Your Team to Spot Phishing Emails

A Guide for Financial Services Firms



Chapman Technology Partners

Phishing emails remain one of the most common and damaging cyber threats to financial services firms. With sensitive client data, regulatory responsibilities, and reputations on the line, it's critical that every member of your team becomes a line of defence against phishing attacks.

This guide outlines a practical, structured approach to training your team to recognise and respond to phishing emails, helping protect your firm from fraud, data breaches and compliance failures.

Why Phishing Training Matters

Financial services firms are prime targets for phishing attacks due to the high-value information they hold.

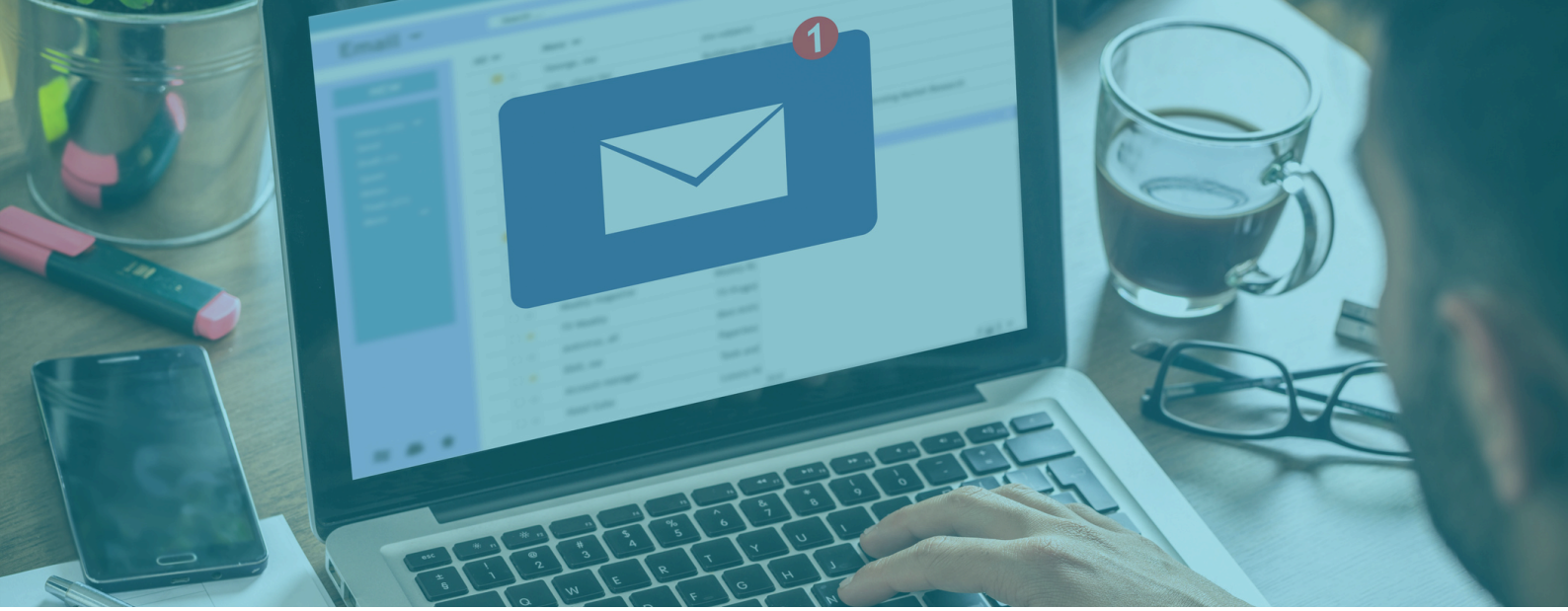
A successful phishing email can:

- Trick staff into transferring money or revealing login credentials
- Lead to ransomware attacks or data breaches
- Result in FCA compliance violations and financial penalties
- Damage client trust and professional reputation

The good news is that phishing awareness training is highly effective. When delivered correctly, it empowers employees to become your first and most reliable security filter.

Phishing remains the leading cause of data breaches, with 91% of successful attacks starting from a malicious email.

Source: UK National Cyber Security Centre (NCSC)



1. Start with the Basics: What Is Phishing?

Begin by ensuring all staff understand what phishing is and how it works.

Phishing is a form of cyber attack where criminals pose as trusted contacts to trick individuals into disclosing sensitive information or clicking malicious links.

Explain the different types of phishing relevant to your team:

- Email phishing – The most common, often appearing as messages from banks, HMRC, Microsoft, or internal departments.
- Spear phishing – Targeted attacks that use personal or company-specific details.
- Business Email Compromise (BEC) – Where attackers impersonate senior executives or suppliers to request urgent payments.
- Smishing and vishing – Phishing via SMS (smishing) or voice calls (vishing).

---

2. Teach Them the Red Flags of a Phishing Email

Equip staff with a mental checklist of warning signs to look out for. Focus on practical, memorable indicators:

- Spelling or grammar mistakes – These are often a telltale sign of a scam. However, with the rise of AI tools, cyber criminals are getting better at avoiding these errors.
- Unusual sender addresses – Look for subtle changes like info@rnicrosoft.com instead of info@microsoft.com
- Generic greetings – “Dear customer” instead of using a real name
- Unexpected attachments or links – Especially those urging urgent action
- Urgency or pressure tactics – “You must act now” or “Your account will be closed”
- Requests for sensitive data – No reputable company will ask for passwords via email

3. Use Real-World Examples (and Create Your Own)

Show real phishing examples and dissect them as a team. Better yet, create custom mock phishing emails that reflect your firm's branding, supplier relationships, and client communication style.

This makes the training more engaging and context-specific. For instance, simulate a fake message from a CRM provider or a financial platform your team uses regularly.

---

4. Make It Routine: Run Simulated Phishing Campaigns

Regular phishing simulations are proven to improve vigilance. Use cyber security tools or managed service providers to send mock phishing emails and monitor who clicks.

- Don't shame staff – Use mistakes as coaching opportunities
- Track progress over time – See who's improving and where further support is needed
- Reward positive behaviour – Recognise team members who report suspicious emails

---

5. Reinforce Best Practices with Policy and Process

Training must be backed by clear procedures. Establish and document the right actions staff should take when they receive a suspicious email:

- Don't click any links or open attachments
- Don't reply to the email
- Report it to the IT team or use the "Report Phishing" button if available
- Delete the email once reported

Ensure everyone knows who to contact and what to do in the event of a suspected phishing attack.

---

6. Keep Training Fresh and Relevant

Cyber threats evolve quickly. Keep your team's awareness sharp with:

- Quarterly refresher sessions – Include any new tactics you're seeing
- Updates on real attacks – Share anonymised stories from within your industry
- Short reminders – Posters, screensavers or intranet banners with key tips
- Ongoing communication – Use team meetings or newsletters to share quick wins and reinforce habits

7. Involve Leadership

When directors and senior advisers take phishing training seriously, it sends a strong cultural signal.

Ensure leadership participate in training, support simulations, and encourage a "report-it-first" mindset, especially in client-facing teams.

---

8. Partner with a Cybersecurity-Focused IT Provider

Even with excellent training, mistakes happen. That's why layered security is essential. Working with an IT provider who understands the financial sector ensures you have the right technical controls in place, including:

- Advanced email filtering
- Multi-factor authentication (MFA)
- Endpoint detection and response (EDR)
- User activity monitoring

They can also run phishing simulation campaigns, provide tailored training, and support your incident response plan.

Final Thought

Training your team to spot phishing emails isn't a one-off exercise, it's a long-term investment in your firm's security culture.

In a sector where trust is paramount and the stakes are high, arming your people with the knowledge and confidence to recognise threats is one of the smartest moves you can make.

Only 27% of UK employees feel confident identifying phishing emails

A recent YouGov survey found that less than a third of UK employees are confident in spotting phishing attempts - highlighting the need for better training across industries.

Source: YouGov Cyber Security Perception Survey, UK, 2024)

Need support delivering phishing training tailored to financial services?

Book your free 15 minute intro call here and let's discuss how we can help your team become your strongest line of defence.

www.chapmantechnologypartners.co.uk

Chapman Technology Partners

Strategic IT, Cyber Security & AI Solutions
for Regulated Industries

Strawberry Fields Digital Hub,
Chorley, PR7 1PS

enquiries@ctpartners.co.uk
01257 542388

CYBER ESSENTIALS
CERTIFIED