FREE GUIDE - CYBERSECURITY

Phishing Attack Prevention Guide

A practical, plain-English guide to recognising and avoiding phishing emails, SMS scams, and fake websites - with a team checklist included.

Published by Vanguardis - vanguardisltd.com - Beginner Level

What Is Phishing?

Phishing is a type of cyber attack where criminals impersonate trusted organisations - banks, government agencies, tech companies, or even your employer - to trick you into revealing sensitive information such as passwords, bank details, or personal data.

Phishing attacks arrive via email, text message (smishing), phone calls (vishing), and fake websites. They are the most common form of cyber attack worldwide, and they work because they exploit human psychology rather than technical vulnerabilities.

DID YOU KNOW?
Over 90% of successful data breaches begin with a phishing email. No organisation is too small to be targeted.

How to Recognise a Phishing Attempt

1. Suspicious Sender Address

Always check the full email address, not just the display name. Attackers often use addresses like support@paypa1.com (note the number 1 instead of l) or noreply@amazon-security-alert.net.

2. Urgency and Pressure Tactics

Phishing messages create a false sense of urgency: Your account will be suspended in 24 hours, Immediate action required. Legitimate organisations rarely demand instant action via email.

3. Generic Greetings

Messages that begin with Dear Customer or Dear User rather than your actual name are a red flag. Your bank knows your name.

4. Suspicious Links

Hover over any link before clicking. The URL should match the real domain. Watch for slight misspellings: secure-login.barclays-bank.com is not a Barclays website.

5. Unexpected Attachments

Be extremely cautious with unexpected attachments, especially .zip, .exe, .docm, or .xlsm files. These can install malware on your device when opened.

6. Requests for Sensitive Information

No legitimate organisation will ask for your password, full bank card number, or PIN via email or text message. Ever.

RED FLAGS AT A GLANCE
Urgent language - Mismatched sender address - Generic greeting - Suspicious link - Unexpected attachment - Request for personal data

SMS Scams (Smishing)

Text message phishing follows the same patterns as email phishing. Common examples include:

- Fake parcel delivery notifications asking you to pay a small fee

- Fake HMRC or tax authority messages claiming a refund or fine
- Fake bank fraud alerts asking you to verify your account
- Fake prize or lottery win notifications

If you receive an unexpected text with a link, do not click it. Go directly to the official website by typing the address yourself.

Fake Websites

Phishing websites are designed to look identical to legitimate sites. Before entering any login credentials or payment information:

- Check the URL carefully - look for misspellings or extra characters
- Look for the padlock icon (HTTPS) - but note that HTTPS alone does not guarantee a site is legitimate
- If you arrived via a link in an email or text, close the tab and navigate to the site directly
- Use a password manager - it will not autofill credentials on a fake site

What To Do If You Suspect a Phishing Attempt

1. Do not click any links or open attachments.
2. Report the email to your IT or security team if you are at work.
3. Forward suspicious emails to your email provider abuse address (e.g. report@phishing.gov.uk in the UK).
4. Delete the message.
5. If you think you may have already clicked a link or entered details, change your passwords immediately and contact your bank if financial information was involved.

GOOD HABIT
Enable two-factor authentication (2FA) on all important accounts. Even if a phisher obtains your password, they cannot access your account without the second factor.

Team Phishing Awareness Checklist

Print this checklist and share it with your team. Tick each item to confirm your organisation is protected.

- [ ] All staff have received basic phishing awareness training in the last 12 months
- [ ] Two-factor authentication is enabled on all business email accounts
- [ ] Staff know how to report a suspicious email internally
- [ ] Email filtering and anti-spam tools are in place
- [ ] A password manager is in use across the organisation
- [ ] Staff are reminded never to share passwords via email or chat
- [ ] An incident response process exists for suspected phishing attacks
- [ ] Software and operating systems are kept up to date
- [ ] Simulated phishing exercises are conducted at least annually
- [ ] Leadership has reviewed and approved the cybersecurity policy

Further Resources

- NCSC Cyber Aware (UK): cyberaware.gov.uk
- Action Fraud (UK): actionfraud.police.uk
- CISA (US): cisa.gov/phishing
- Have I Been Pwned: haveibeenpwned.com
- Vanguardis Cybersecurity Training: vanguardisltd.com/events