◆ SANTRE IT · HANDBOOK V1.0

Security Awareness Handbook

◇ INTRODUCTION

Why this matters

Most successful cyberattacks don't start with a clever piece of malware — they start with a person. An employee clicks a link, reuses a password, or wires money on the strength of a convincing email. The attackers know this, so they invest in the human side of the attack, not the technical one.

Roughly nine out of ten breaches involve some form of phishing or social engineering. Antivirus, firewalls, and MFA all help, but the single most effective control is a team that can spot the signs and push back. That's what this handbook is for.

Read the three lessons below. At the end of each, you'll find a short self-check. If you can answer those, you're already ahead of most attackers' primary target.

◇ LESSON 1 OF 3

Phishing

What is phishing?

Phishing is when an attacker impersonates someone you trust — a bank, a supplier, your CEO, a delivery company — to trick you into handing over sensitive information, clicking a malicious link, or downloading a file you shouldn't. It almost always arrives as an email, but the same tricks show up in text messages (*smishing*), voice calls (*vishing*), and chat platforms.

The goal is to bypass your critical thinking. Attackers rely on instinct, urgency, and authority to push you into a click before you've had time to check.

The six classic red flags

- **Urgent or threatening language.** "Act now or your account will be closed." Legitimate organisations rarely impose 24-hour deadlines via email.
- **Suspicious sender address.** Check the domain carefully. `security@paypa1.com` (with a numeral "1") and `support@bankofamerica.com` (with a Cyrillic "c") are not real.
- **Generic greetings.** "Dear Customer" or "Dear User" from an organisation that should know your name.
- **Spelling and grammar mistakes.** Real companies proofread. A polished brand with broken English is a tell.
- **Suspicious links.** Hover over a link (don't click) — the real destination appears at the bottom of the screen. If it doesn't match the text, that's your answer.
- **Unexpected attachments.** Especially `.exe`, `.zip`, or files with double extensions like `invoice.pdf.exe`.

A worked example

From: `security-alert@bankofamerica.com`
Subject: URGENT — Verify Your Account Within 24 Hours

"Dear Valued Customer, We have detected unusual activity on your account. Click here to verify: `http://bankofamerica-secure-login.tk/verify`. If you do not verify within 24 hours your account will be permanently suspended."

What's wrong: the "a" in "america" is a Cyrillic lookalike, the deadline is manufactured urgency, the greeting is generic, and the link is a free `.tk` domain pretending to be the bank. No real bank asks you to verify via an emailed link.

What to do when something smells off

1. **Don't click.** Don't tap links, don't open attachments, don't reply.
2. **Verify out-of-band.** If the email claims to be from your bank, log into the bank's website directly (type the URL yourself). If it claims to be from a colleague, call or message them via a channel you already trust.
3. **Report it.** Forward to your IT/security team before deleting — they use these reports to warn everyone else.
4. **If you clicked already:** change the affected password immediately, enable or verify MFA, and tell IT. The faster you raise the alarm, the smaller the damage.

Self-check

1. An email says your account will be closed in 24 hours unless you "verify" via the link. What's the right response? *(Answer: don't click — report it and, if needed, log into the service directly.)*
2. Which is a red flag — professional formatting, a personalised greeting, or a threat about account closure? *(Answer: the threat.)*
3. Before clicking any link, you should… *(Answer: hover to reveal the real destination.)*

◇ LESSON 2 OF 3

Password Security

Why passwords still matter

Weak and reused passwords remain the number-one cause of account takeovers. Every time a website is breached, attackers add the leaked usernames and passwords to a dictionary and try them against every other service they can think of — email, banking, Microsoft 365, everything. If you've reused a password, one breach becomes many.

What makes a password strong

- **Length beats complexity.** Aim for **12–16 characters or more**. Four random words strung together (`purple-battery-carpet-saturn`) is stronger than a shorter password full of symbols.
- **Mix character types** — upper, lower, numbers, symbols — but only if it doesn't cost you length.
- **Avoid predictable patterns.** No "Password123", no keyboard walks like "qwerty", no "Winter2024!".
- **No personal information.** Birthdays, kids' names, pet names, street names — all guessable from social media.
- **Unique per account.** If you reuse one password and any site it's on gets breached, every account with that password is exposed.

Use a password manager

Nobody can remember thirty unique 16-character passwords. A password manager remembers them for you — you only need to remember *one* strong master password. It also generates strong passwords, warns you about reuse, and auto-fills logins so you spend less time typing.

Popular choices: **1Password**, **Bitwarden**, **Dashlane**, **KeePass**. Most have a free tier. Pick one and use it.

Turn on two-factor authentication

2FA (also called MFA) requires a second proof of identity beyond your password — usually a code from an authenticator app, a tap on your phone, or a hardware key. Even if your password is stolen, the attacker can't log in without that second factor.

Rule of thumb: turn on 2FA for email, banking, work accounts, and anything that can reset other passwords. Prefer an authenticator app (Google Authenticator, Microsoft Authenticator, 1Password) or a hardware key over SMS — SMS can be intercepted via SIM swapping.

Self-check

1. What's the minimum recommended password length? *(Answer: 12–16 characters.)*
2. Which is the strongest of these: `password123`, `MyBirthday1990!`, `Tr0ub4dor&3`, or `correct-horse-battery-staple-2024!`? *(Answer: the last — length plus unpredictability.)*
3. What's the main benefit of two-factor authentication? *(Answer: it combines something you know with something you have, so a stolen password alone isn't enough.)*

◇ LESSON 3 OF 3

Social Engineering

Manipulating people, not computers

Social engineering is the art of convincing a human being to do something that compromises security — hand over a password, hold a door open, wire money, install software. It exploits psychology rather than technology, which is why firewalls don't help.

The six tactics to recognise

- **Pretexting.** Inventing a believable story — "I'm from IT, we're doing a security audit" — to justify an unusual request.
- **Baiting.** Offering something tempting (a free USB drive, a gift card, exclusive content) in exchange for access or information.
- **Tailgating.** Physically following an authorised person through a locked door — often carrying a box or pretending to be on a call so nobody challenges them.
- **Quid pro quo.** "I'll fix your laptop if you give me your login" — swapping a small favour for a dangerous one.
- **Authority.** Impersonating a CEO, a regulator, a police officer — anyone whose status discourages questioning.
- **Urgency.** Manufactured time pressure. "I need this transfer processed in the next thirty minutes." Urgency short-circuits careful thinking.

Real-world example: vendor banking fraud

Your accounts payable team gets an email from a long-standing supplier saying their banking details have changed — please use the new account for the next invoice payment. The signature, the logo, the tone all look right, so a $42,000 transfer goes out on Friday.

On Monday the real supplier calls asking where their money is. The "update" email came from a lookalike domain sent by an attacker who had quietly monitored the real supplier's mailbox for weeks and struck at the perfect moment.

The fix is procedural, not technical. Any change to banking or payment details must be verified by phone, using a number from your existing vendor records — never a number or link from the suspicious email. One callback would have saved $42,000.

Defending yourself — and the team

1. **Verify identities out-of-band.** If someone on the phone or in an email claims to be from IT, the bank, or a vendor, end the conversation and call back on a number you found yourself.
2. **Question unusual requests** — especially ones involving money, credentials, or access. "Urgent" is not a reason to skip your normal checks; it's a reason to apply them.
3. **Follow the process.** Don't let someone's seniority or insistence pressure you into bypassing policy. Real leaders respect procedures that protect the company.
4. **Report suspicious behaviour.** If someone's trying to tailgate, probing for info, or asking you to break a rule — tell security. Attackers often try the same trick on multiple people.
5. **Secure physical access.** Don't hold secure doors for people you don't recognise, even if they have their hands full. Politely direct them to reception.

Self-check

1. Someone calls claiming to be from IT and asks for your password. What do you do? *(Answer: hang up and call IT back on the official number. Real IT never asks for your password.)*
2. What is "tailgating"? *(Answer: following an authorised person into a secure area without proper credentials.)*
3. Why do attackers use urgency? *(Answer: to pressure you into acting before you think.)*

◇ QUICK REFERENCE

Red flags at a glance

Print this page and stick it near your monitor. If you spot any of these, pause before acting.

- **Urgency or threats** in the email ("Act now or your account is locked!").
- **Lookalike sender domains** — swapped letters, extra hyphens, unusual TLDs like `.tk` or `.xyz`.
- **Generic greeting** where a personal one should appear.
- **Links that don't match** what they claim — always hover before clicking.
- **Unexpected attachments** — double extensions (`.pdf.exe`), executables, zipped archives.
- **Payment or banking changes** — always verify by phone using your own records.
- **Password, MFA code, or remote-access requests** — IT will never ask.
- **Out-of-character requests from senior staff** — gift cards, wire transfers, urgent secrecy.
- **Pressure to skip a process** — "just this once, we don't have time."

If you think you clicked or replied

1. Disconnect the device from the network if you downloaded something.
2. Change the password on the affected account — and any other account sharing that password.
3. Enable or check MFA on that account.
4. Contact IT/security immediately with what happened and when.
5. Watch for unusual activity on related accounts over the next few days.

> **Speed matters more than embarrassment.** A report in the first ten minutes is dramatically better than one the next day. Nobody gets in trouble for reporting fast — they get thanked.

— The Santre IT team