SafeDaTech

Security awareness

Ten security habits for every staff member

A printable poster of ten everyday habits that stop most phishing, account takeover and data loss incidents.

Most security incidents start with an everyday mistake, not a sophisticated attack. These ten habits stop most of them.

Ten habits

1. **Pause before you click.** Urgent emails, texts and WhatsApp messages asking you to log in, pay or download are the most common attack.
2. **Check the sender.** Look at the full email address and the link destination, not just the display name.
3. **Confirm payment changes by phone.** Call a known number before changing bank details or approving an urgent payment.
4. **Use a different password everywhere.** A password manager makes this easy.
5. **Turn on multi factor authentication** for email, banking, social media and work systems.
6. **Lock your screen** whenever you step away, and never share your login.
7. **Update your devices** when prompted. Updates close security holes.
8. **Keep work data in work systems.** Not in personal email, personal cloud storage or messaging groups.
9. **Be careful on public Wi-Fi.** Avoid logging in to sensitive systems, or use the organisation's VPN.
0. **Report quickly.** If you clicked something suspicious or lost a device, tell [IT contact] at once. Fast reporting limits the damage.

Report incidents to

[Name] · [Phone] · [Email]

General guidance only, not legal advice. Adapt it to your organisation. © 2026 EDAN Development & Consulting Ltd.