

Mobilise end users to harness your last line of human defence with our **Cyber Awareness as a Service** offering



Reasons why it's **ESSENTIAL** to Cyber-Train your Staff ...

Why Hack when you can Con?

Social engineering is a far more efficient option for cyber criminals than attempting to hack into a well-protected corporate system.

Humans are the Weakest Link

Even with the most advanced defences, your security posture is severely weakened if just one employee can be tricked.

Anyone can be Phished

Cyber criminals troll companies for months to gather the necessary data to pull off a successful attack.

Phishing Emails can Bypass Filters

Malicious emails no longer have to contain harmful links or malware.

Harness your Human Firewall

Fully trained employees can help identify, report and stop attacks.

Create a Positive Security Culture

Promote healthy skepticism; incentivise and reward those who report suspicious activity; induct new staff as soon as they join.

What is Cyber Awareness as a Service (CAaaS)?

Hackers are evolving faster than security technology. Phishing is now the **biggest** attack vector. Ensuring your users present an effective last line of defence is paramount. **Cyber security is everyone's job!**

Cyber-Awareness Training is an essential element of your security posture, ensuring your employees know the most common threats and can identify them. Phishing emails are becoming tricky to spot, often appearing to originate from well-known credible websites.

Autodata provides a **comprehensively managed Cyber-Awareness Service** that will take your employees from cyber zero to Cyber Hero. Our objective is to significantly reduce your "phish-prone percentage" to evidence that your human firewall is intact.

Our CAaaS offering is priced per user per year and includes:

- 1. FULLY-MANAGED ONBOARDING** - delivered by our technical specialists
- 2. QUARTERLY MEETINGS** - face-to-face on-site/remote to discuss your campaign activity and output and plan together for the next quarter
- 3. MONTHLY PHISHING CAMPAIGNS** - expertly-run and carefully socially-engineered to mimic genuine phishing attacks; targeting options include C-Level/Management, specific departments or companywide
- 4. AUTOMATIC TRAINING FOR "CLICKERS"** - those falling prey to our phishing emails are your weakest link - so we retrain them immediately
- 5. MONTHLY TRAINING** - can be tailored to specific user groups as desired
COMPANYWIDE >>> Cyber/H & S/GDPR/Compliance etc.
DEPARTMENTAL >>> CEO Fraud (Finance)/GDPR (Marketing)/H & S (Ops)
- 6. ANALYTICS REPORTING** - pass/fail details from phishing emails; post-campaign training/retraining results
- 7. (OPTIONAL) PHISHING & USB DRIVE TESTS** - simulated attacks delivered via voicemail and USBs; **SMISHING & ADA** (AI-Driven Agent) targets users when they are deemed to be more susceptible
- 8. (OPTIONAL) SOCIAL ENGINEERING / SPEAR PHISHING** - additional services that are costed on a price per engagement basis