



TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Security Awareness

Part of Wingman Human Risk

Are your users still clicking phishing links? Are they still opening attachments from unknown senders? The strongest cyber security defence you can provide to your organisation is educating your employees. Researchers from Stanford University and a top cyber security organisation (Tessian) found that approximately 88% of all data breaches are caused by an employee mistake*. Human error is still the driving force behind an overwhelming majority of cyber security problems.

With Wingman Security Awareness, you can provide on-demand, interactive and engaging training to your end users, and then test them on their learning. By testing through simulated phishing campaigns and then analysing the results, you can strengthen your team to ensure that your weakest link becomes your strongest asset.





Managed deployment

From completing the deployment to running customised campaigns. Wingman Security Awareness is there to support you in completing security training for your employees.

Progress tracking

Find the areas of your company that could do with additional support and see how your security posture increases, and security risk decreases over time with regular reporting as well as reporting as and when you need it.

Testing beyond e-mail campaigns

Test beyond phishing e-mails. With the ability to test user behaviour with the use of USB sticks and QR codes and how your staff members will interact with them, it's important to educate that security doesn't start and stop at the inbox.

Flexible testing schedules

After completing a Security Awareness Proficiency Assessment (SAPA) create testing schedules to track your security improvements and find the gaps in which you

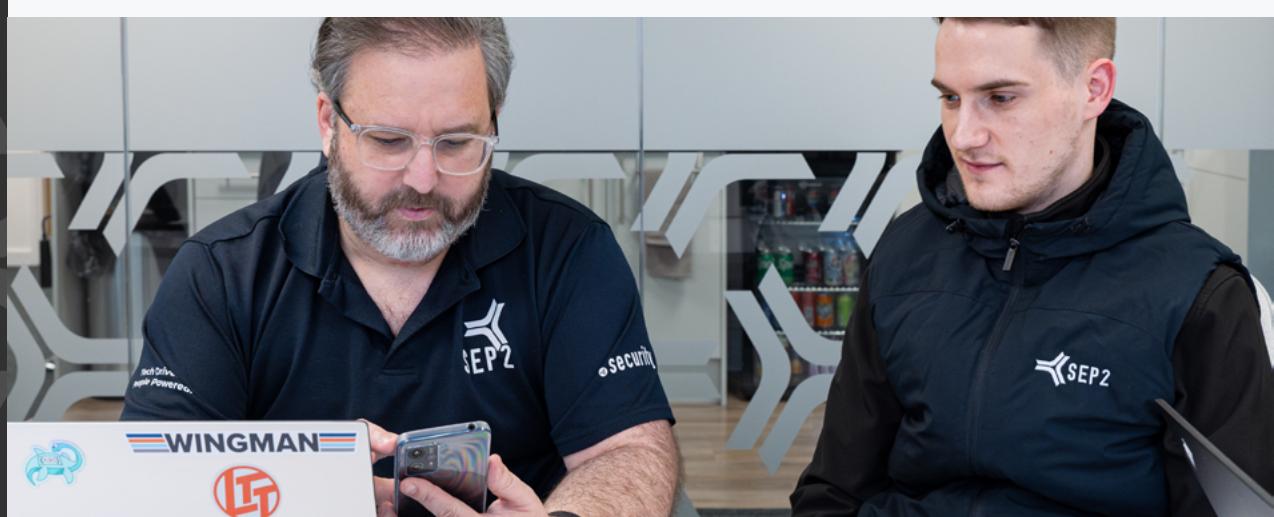
need to focus on. From weekly, monthly, quarterly, annual or ad-hoc testing, SEP2 will work with you to ensure that your employees are tested with a schedule that suits your organisation.

Customisable to target your employees

Change your campaign difficulty from 1* Basic up to 5* Advanced to ensure that your employees are being tested at the appropriate level and use a wide variety of different topics to make sure that employees are getting targeted with relevant testing.

Engaging security content

Sitting through a presentation may deliver on providing the material to access, but it doesn't always resonate with the target audience. Through storytelling using real life examples and building rapport with the characters and situations they are facing, you'll find that completing, understanding and engaging with the security training to your employees is no longer a burden that they must endure.





Wingman Security Awareness

- SEP2 Leeds ISO27001 SOC
- 8am to 6pm business days as standard
- SAPA baseline testing
- Arranging phishing simulations

- Distributing security awareness training
- Feeding reports back on results and completed training
- Managed phishing campaigns
- Tailored training for employees
- Reports created from results

FEATURES	BASIC	STANDARD	ENHANCED
UNLIMITED PHISHING SECURITY TESTS	Y	Y	Y
AUTOMATED TRAINING CAMPAIGNS	Y	Y	Y
PHISH ALERT BUTTON	Y	Y	Y
PHISHING REPLY TRACKING	Y	Y	Y
USER PROVISIONING - AD OR SCIM INTEGRATION	Y	Y	Y
SSO/SAML INTEGRATION	Y	Y	Y
MONTHLY EMAIL EXPOSURE CHECK	Y	Y	Y
OPTIONAL - KNOWBE4 STUDENT EDITION	Y	Y	Y
REPORTING, USER EVENT AND WEBHOOK APIs		Y	Y
SOCIAL ENGINEERING INDICATORS (SEI)		Y	Y
USB DRIVE TEST		Y	Y
SMART GROUPS		Y	Y
AI-DRIVEN PHISHING			Y
PASSWORDIQ* CHECK REUSED & WEAK PASSWORDS			Y
CALLBACK PHISHING			Y

*ONLY AVAILABLE FOR THOSE USING ACTIVE DIRECTORY

If you would like to discuss our Wingman Security Awareness please get in touch at info@sep2.security