nowSecure TRAIN

Four new best practice actions for stronger cyber security.

People are now the key vulnerability.

The 2022 infosec environment is even harder to defend. Cyber attacks are on the rise, and staff are more vulnerable to phishing and social engineering tricks as remote working becomes increasingly prevalent.

There is a science to behaviour change and this is the key ingredient that's often missing from organisational attempts to change how people approach cyber-security.

Psychology and the behavioural sciences bring us over 40 years of research on what works in changing behaviour — and why.

We've used this to develop four best practice actions that leverage behavioural science principles and turn cyber-security from a "boxticking exercise" into a process where users become invested in using and propagating good cyber-security practices.

→ Cyber-attack facts

2021 Gallagher survey: 60% of data breaches were inadvertent

Key vulnerability:	People (especially remote workers)
Key target:	C-suite executives
Key vector:	Phishing emails
Key tactic:	Psychological and social engineering

Four new best practice actions

ACTION 1.
Raise awareness
Integrate psychology and behavioural science principles into user education

ACTION 2.
Simulate attacks
Embed security and data protection activities as part of every user's daily experience

ACTION 3.
Measure to improve
Use data analysis to identify new threats and mitigate individual and organisational vulnerabilities

ACTION 4.
Support your people
Establish processes to let the organisation benefit from user insights

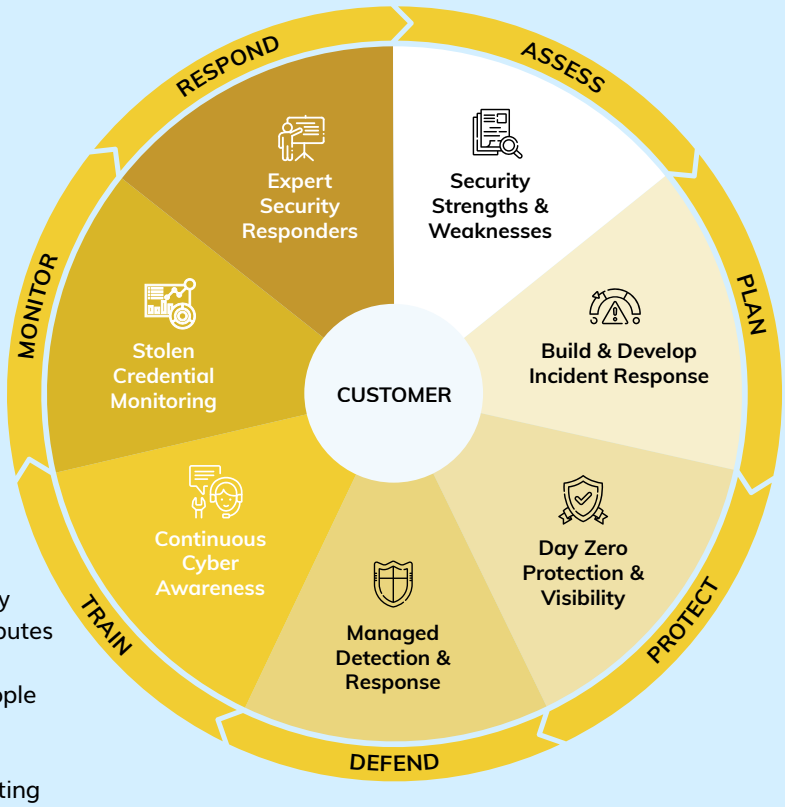
nowcomm nowsecure@nowcomm.com nowcomm.com 0300 3031200

nowSecure TRAIN

A cloud-based unified cyber awareness platform

A unified cyber security awareness platform focused on the human aspect of cyber security and data protection.

Designed in collaboration with psychologists and behavioural scientists it helps drive better security behaviours (not just security awareness) through making best practice an instinctive response for users.



Underpinned by evidence-based theory from the fields of psychology and behavioural science and contributes to ongoing academic research and development which will benefit people and businesses around the world.

Applies advanced cognitive computing technology to deliver autonomous evolving intelligent software that delivers threat-based, context-specific content to users in real-time.

Uses advanced data analysis to deliver a clear visualisation of human cyber risk and vulnerability at organisational and individual level.

Delivers GCHQ-accredited content that is relevant, timely and accessible to all users.

Enables organisations to benefit from insights and understanding from across the user community.

Uses data and analysis to produce insight that enables a greater understanding and more effective mitigation of human cyber risk.

Is easy to implement, integrating seamlessly into the most popular SSO, LMS and GRC solutions used by businesses of all sizes.

Delivers an advanced, integrated and constantly optimising user experience in which users are engaged, motivated and encouraged to embed good cyber and data protection practice into their day-to-day lives.

Demonstrably reduces human cyber-risk

CREDIT SUISSE

- 81% have a more positive attitude towards security
- 92% now consider themselves more responsible for security
- Average confidence in cyber security has increased

CANARY WHARF GROUP

- Only 1% of passphrases now considered low strength
- No high-risk phishing events since change
- 100% of all users served a phishing intervention no longer exhibit risk

Try **nowSecure Train** for 30 days. Fully managed trial. No obligation. →

CISCO Partner
Gold Provider
Advanced Security Architecture Specialized
Customer Experience Specialized

CYBER ESSENTIALS PLUS
Cyber Eseesntial Plus re-certified in 2021

QMS ISO 27001 : 2013 REGISTERED
Certificate No:374862021
ISO 27001 and 9001 Certified in 2021

nowcomm
nowsecure@nowcomm.com nowcomm.com 0300 3031200