End User Security Awareness Training: what the regulators say

National Cyber Security Centre
a part of GCHQ

10 Steps: User Education and Awareness

“

Users have a critical role to play in their organisation's security. All users should receive regular training on the security risks to the organisation. Establish mechanisms to test the effectiveness and value of the security training provided to all users.”

ISO 27001

Annex A.7.

“

All employees and relevant contractors must receive appropriate security awareness education and training to do their job well and securely.

It is common for the information security team to partner with HR or a Learning & Development team to carry out skills, knowledge, competence and awareness assessments and to plan and implement a programme of awareness, education and training throughout the employment lifecycle (not just at induction). You need to be able to demonstrate that training and compliance to auditors. Also carefully consider how the training and awareness is delivered to give the staff and contractor resource the best chance of understanding and following it – this means careful attention to content and medium for delivery.”

CIS
Center for Internet Security®

Control 17 – Implement a Security Awareness Program

“

Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.

An effective cyber defense training program is more than an annual event; it is an ongoing process improvement. The training is repeated periodically, measured and tested for effectiveness, and updated regularly.”

Gartner

“People influence security more than technology or policy, and cybercriminals know how to exploit human behaviors. Security and risk management leaders must invest in tools that increase awareness and influence behavior that supports security business objectives through computer-based training.”

“There is an increasing recognition that relying on technology alone to secure an organization’s critical assets is not enough, and, therefore, educating employees on the various techniques used by bad actors can improve the overall security posture and reduce risks.

The combination of increased risks and a lack of internal expertise pushes many CISOs to seek solutions in the market that are capable of producing measurable improvements in employee security behavior. In order to support security objectives, employees need skills, knowledge and motivation. Security education focuses on developing secure employees who, in turn, enable security performance, follow internal policies and procedures, and adhere to regulatory compliance.”

GDPR

Article 39 and Article 47

“Article 39 requires that “the data protection officer shall … monitor compliance with this Regulation … [through] awareness-raising and training of staff involved in processing operations.”

Article 47 requires “the appropriate data protection training [for] personnel having permanent or regular access to personal data”.

About Purplephish

Looking to quickly and easily empower your employees to prevent cyber attacks? Purplephish’s security awareness and real-world phishing simulation solution is proven to reduce user susceptibility to today’s biggest threats.

Demonstrate the reduction in risk across your organisation via our industry-leading suite of dashboards as your users undertake a regular, ongoing training program, encompassing tried-and-tested methods guaranteed to ensure key security knowledge is forefront of mind should they come under attack.