OXFORD COLLEGE SCIENTIFIC JOURNAL
Volume 1, Issue 1 (2026) · Open access

REVIEW ARTICLE · INFORMATION TECHNOLOGY

Cybersecurity Awareness Training in Organisations: What Makes It Effective?

Oxford College Research Office
Oxford College, London, United Kingdom

Published 24 November 2026 · Volume 1, Issue 1 (2026)

ABSTRACT

Most security incidents involve a human element, such as a mistaken click, a reused password or a misdirected file. Organisations therefore invest in security awareness training, yet its effect on behaviour is often limited. This review examines what distinguishes effective programmes from routine compliance exercises. Drawing on established guidance for security awareness programmes, international information-security standards and the theory of planned behaviour, it identifies six characteristics of effective training: role-based content, short and repeated learning, realistic practice, positive reporting culture, visible leadership support and measurement of behaviour rather than attendance. The article argues that awareness training works best as one part of a wider security culture in which systems are designed to make the safe action the easy action, and in which employees are treated as partners in defence rather than as the weakest link.

Keywords: cybersecurity awareness; security training; human factors; phishing; security culture

1. Introduction

Technical controls — firewalls, encryption, multi-factor authentication — have become steadily stronger, and attackers have adapted by targeting people. Phishing emails, fraudulent payment requests and social-engineering telephone calls exploit trust, routine and time pressure. Annual industry analyses of security breaches, such as the Verizon Data Breach Investigations Report (Verizon, 2024), consistently describe the human element as a factor in a large share of incidents.

Security awareness training is the most common organisational response. Almost every organisation of meaningful size now requires employees to complete some form of training. Yet practitioners frequently observe that people complete the modules, pass the quiz, and continue to behave as before. This review asks what makes the difference between training that changes behaviour and training that merely records attendance.

2. Awareness, training and education

Guidance from the United States National Institute of Standards and Technology distinguishes three levels (NIST, 2003). **Awareness** focuses attention on security and is aimed at everyone. **Training** builds specific skills needed for particular roles. **Education** develops deeper expertise for security specialists. Many programmes stop at the first level. Awareness is necessary, but knowing that phishing exists is different from reliably recognising a well-crafted fraudulent message on a busy afternoon.

International standards reinforce the point. ISO/IEC 27001:2022 requires organisations to ensure that people are competent, aware of the information-security policy and of their own contribution, and aware of the implications of not conforming. Competence implies capability in practice, not only completion of a course.

3. Why knowledge does not automatically change behaviour

The theory of planned behaviour (Ajzen, 1991) offers a useful explanation. Behaviour follows intention, and intention is shaped by three factors: attitudes towards the behaviour, perceived social norms, and perceived behavioural control. Traditional training addresses mainly knowledge, which influences attitudes only partly. It often neglects norms (Do my colleagues and managers actually behave securely?) and control (Is it easy for me to do the right thing, such as reporting a suspicious email?).

Security behaviour is also subject to fatigue. Employees who receive frequent warnings, complex password rules and alerts that are mostly false alarms may begin to ignore them. Effective programmes therefore reduce unnecessary friction while focusing attention on the actions that matter most.

4. Characteristics of effective programmes

Six characteristics recur in practitioner guidance and in the behavioural literature.

4.1 Role-based content

A finance officer who approves payments faces different threats from a software developer or a receptionist. Content that reflects the real risks of each role — invoice fraud for finance, credential theft for administrators, tailgating for front-desk staff — is more relevant and more likely to be applied.

4.2 Short and repeated learning

Annual one-hour sessions are easily forgotten. Short modules of a few minutes, delivered regularly and linked to current threats, support retention and keep security visible without overwhelming people.

4.3 Realistic practice

Simulated phishing exercises, when used carefully, allow people to practise recognition in a realistic setting. Their purpose should be learning: immediate, constructive feedback is more useful than public lists of who "failed". Exercises that humiliate employees damage trust and can reduce reporting.

4.4 A positive reporting culture

The single most valuable behaviour is often reporting — of a suspicious message, a lost device or a mistake. People report when reporting is easy (for example a single button in the email client), when they receive a quick and appreciative response, and when they are confident that honest mistakes will not be punished.

4.5 Visible leadership support

Norms are shaped by what leaders do. When senior managers complete the same training, follow the same rules and talk about security as part of quality and customer trust, employees perceive

security as a shared responsibility rather than an IT requirement.

4.6 Measuring behaviour, not attendance

Completion rates show who has clicked through a module, not who behaves securely. More meaningful indicators include reporting rates and reporting speed for simulated and real phishing, the proportion of accounts with multi-factor authentication, and the number of incidents traced to avoidable human error. These measures allow programmes to be adjusted over time.

5. Designing for secure behaviour

Training cannot compensate for systems that make secure behaviour difficult. Password managers, single sign-on, multi-factor authentication that is quick to use, clear labelling of external emails and simple procedures for verifying payment changes all make the secure action the easy action. A useful principle is to ask, for every rule: what would make it easier for a busy, well-intentioned employee to comply?

6. Implications for organisations

Organisations can strengthen their programmes by mapping role-specific risks, replacing long annual courses with short regular content, introducing an easy reporting mechanism, using simulations for learning rather than blame, involving leaders visibly, and reporting behavioural indicators to management. For small organisations without a security team, even a few of these steps — particularly easy reporting and multi-factor authentication — can reduce risk considerably.

7. Limitations and future directions

This review synthesises established guidance and theory rather than presenting new data. The effects of awareness programmes are difficult to measure, because successful prevention is invisible and threat levels change. Further research comparing programme designs over longer periods, and examining the role of organisational culture, would strengthen the evidence base.

8. Conclusion

Awareness training is most effective when it moves beyond information to practice, culture and design. Treating employees as capable partners, making secure behaviour easy, and measuring what people actually do allow organisations to turn awareness into lasting protection.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO.

National Institute of Standards and Technology. (2003). *Building an information technology security awareness and training program* (NIST Special Publication 800-50). NIST.

Verizon. (2024). *2024 Data breach investigations report.* Verizon Business.

Article information. This review article was prepared by the Oxford College Research Office with the assistance of generative AI tools, and was reviewed and approved by the editorial office of the Oxford College Scientific Journal. It synthesises published literature and does not report new empirical data.

How to cite. Oxford College Research Office (2026). Cybersecurity Awareness Training in Organisations: What Makes It Effective?. *Oxford College Scientific Journal*, 1(1).

Licence. © 2026 Oxford College. Published open access by Oxford College.