B SEARCH TERMS

Simulation, Alternatives to phishing provider, Awareness education material, awareness, Awareness campaign, awareness learning, awareness training, awareness, behaviour change cybersecurity, bekannte anbieter security awareness, customized security awareness, Cyber awareness training, cyber security, Cyber security awareness training, cyber security elearning for employees, cyber security training, cyber security training awareness, cyber security training for workforce, cybersecurity, Cybersecurity awareness, cybersecurity implementation training, Cybersecurity Training, Data Protection E-Learning, Educational material info sec, employee awareness program cyber security, Employee education information security, Employee training, employee trainings cyber security, Evidence-based, Forrester Security Awareness, gamification, Gartner security awareness, How do I make IT security transparent and understandable within large companies, Info sec Training catalogue, Info sec training games, Information security training and learning, information security training awareness ISO27001 awareness, it security awareness, IT Sicherheit menschliches Verhalten, IT Sicherheit Sensibilisierung Mitarbeiter, Knowhow in communication, Knowhow in cybercrime, Language skills, micro learnings, phishing campaign, phishing compliance, phishing simulation, Phishingsimulation, phishing training, Phishingtraining, Psychology, raise security awareness culture, Research, security, security and privacy awareness campaign, security awareness, Security awareness & training, Security awareness and phishing, Security awareness and training vendor, security awareness behavior change, Security awareness certification, Security awareness costs, security awareness elearning, Security Awareness e-learning, Security Awareness E-Learning, security awareness elearning erfahrung, security awareness elearning reviews, Security awareness feature matrix, Security awareness frameworks, Security awareness games, Security awareness gamification, Security awareness gamification and training, Security awareness innovation, Security Awareness leader, Security awareness platform, security awareness provider, Security awareness research, Security awareness sheet cheats, Security awareness target group, Security Awareness Training, Security awareness Training and phishing simulation, Security awareness trainings, Security awareness vendors, Security awareness white papers, Security awareness without phishing, Security awareness workshop, Security Awareness, Behaviour Change, measurement, Security behaviour change, security behaviour vendor, Security culture, Security culture training, Security culture within companies, Security education, security learning, Security E-Learning, Security mindset training, Security training platform, Security Training, Security trainings, Security trainings and workshops, simulated phishing training, Social Engineering Training, Studies in cybersecurity or IT, supplier cyber security awareness, supplier cyber security trainings, Teaching secure behaviours, training, Usable security.

C COMPLIANCE FRAMEWORKS

Vendors named the following compliance frameworks and regulations with the claim to help their customers fulfill the different requirements: CCPA, CMMC, CPRA, Cyber Essentials Certificate (UK Government), DORA, EU Laws and Regulations, FedRamp, FERPA, FISMA, GDPR, Gramm-Leach-Billey Act (GLBA), HIPPAA, HITRUST, ISO ISO/IEC 27001, ISO27001:2022, NERC CIP, NICE NIS2, NIST 800-16, NIST 800-50, NIST Cybersecurity Framework, NIST, OMB A-130, PCI DSS, PCI, SOC 2, SOC/SOC2, SOX, and US Federal Law

D CODE BOOK

Table 2: Our codebook (1/2).

Code	#	Description	Exemplary Quote
RQ1: Products	–		
Customizable	176	The SAT product can in look & feel, or in its content be adapted to the customers' demands.	*"Tailor presentations to address key concepts most relevant to your teams, business context, or compliance needs."* — [V4]
Behavioural Science	61	The product explicitly utilizes concepts from psychology (e.g. nudging) to engage end-users (employees) or to manipulate their behavior.	*"To change security behavior, we need to focus on nudging employees towards system 2 thinking"* — [V6]
Sophisticated Training Library	84	The training content/ library is big or has special content that other vendors might not have.	*"1,000+ customizable training modules"* — [V27]
Metrics	262	Any measurement or metric that is supposed to show the success of the vendors' SAT and is offered as part of the product.	*"Run phishing simulations that tell you what drives behaviors. Find out why people click on, engage with, and report phishing emails—or why they don't."* — [V11]
Content	270	Malware, password security, public wifi security, you name it. Every peace that tells us something about the topics that are covered within the SAT products.	*"Office hygiene, helping employees understand the best way to protect paper, desks, screens, and buildings."* — [V52]
Type	405	What SAT products are offered (type of training, or awareness raising measures)?	*"CyberEscape Online is an opportunity to get your team connected and engaged with security while having fun together!"* — [V51]
RQ2: Reasoning	–		
Better than Others	64	Bashing of other vendors, or other/older SAT methods.	*"Traditional training falling flat You've probably experienced this yourself. Once or twice a year, it's announced that all employees must complete the security awareness training program by a certain date in order for the company to remain in compliance with regulations."* — [V1]
Customer References	57	Whenever customers are publicly used as references on the websites or when there is an award for customer feedback.	
Science Claims	44	If science or links to reports/ white papers are directly used to back up product claims.	*"[our] techniques, scientifically proven, involve participants, increase the retention rate, and motivate behavior change. This explains why 68% of the brain is more involved when having fun."* — [V51]
Human Error Problem	57	if human error is displayed as the primary problem (e.g., "over 90%... with human error") and SAT is displayed as the solution to those problems.	*"After all, phishing attacks account for 90% of data breaches (CITE), and unfortunately attacks continue to evolve and grow in sophistication."* — [V44]
RO(S)I	27	Any explicit, or abstract calculation that should show that SAT is worth their costs.	*"The real question is whether you can afford not to implement phishing training for your employees? Especially when it has a robust ROI."* — [V43]
Success Proof	22	The vendor shows numbers that should prove that SAT has been successful before.	*"You can see that by the third phishing test, the users had over a 50% reduction in mistakes made, meaning that they were much less likely to fall for phishing emails."* — [V8]

Table 3: Our codebook (2/2).

Code	#	Description	Exemplary Quote
Management Satisfaction	25	The SAT product will help to satisfy management, the CISO, or other leading stakeholders.	*"With Executive Reports, give your C-suite the insight they need to maximize security awareness training ROI and track security compliance."* — [V24]
Low Effort	141	The SAT will be easy to integrate into the customer systems or will be easy to manage/operate so that SAMs have easy times.	*"1-Click Campaigns & Auto-Generated Content"* — [V22]
Compliance Fulfillment	97	The SAT will help to fulfill regulatory requirements.	*"Test learner knowledge and retention, and generate reports to demonstrate your compliance for auditing purposes."* — [V20]
Easy learning	117	The SAT will easily raise awareness.	
RQ3: Users	–		
Effort & Usable Security	78	The vendor is aware of the effort security takes from employees, or is advertising usable security concepts.	*"Attending security awareness training should be your top priority."* — [V47]
Time Effort	63	Any number (minutes, days, months) that indicates how much time employees should spend on training.	*"By comparison, modern security awareness training uses a blend of fresh training methods to engage people daily, prevent complacency, and make security a part of their daily routine."* — [V11]
Psychology	56	Explanations why employees fail (e. g., in detecting phishing emails, due to stress), or why they succeed, e.g., due to superiors being role models.	*"We evolved to see crocodiles in the river, not phishing attacks in our inbox."* — [V19]
Part of the Solution	79	Human Firewall, Well trained employees are good defenders, Last Line of Defence	*"Our employees are our first line of defense, and it is essential to empower them with the right security mindset."* — [V58]
Blaming	67	Weakest Link, Human make errors, is a problem	*"Information leaks by companies are often caused by a lack of employee literacy."* — [V25]