2025

New Hires Phishing Susceptibility Report:

Human Cyber Risk During Onboarding

keepnet

www.keepnetlabs.com

Executive Summary

New hires are 44% more likely to fall victim to phishing and social engineering attacks during their first 90 days. This increased risk arises from unfamiliarity with corporate culture, cybersecurity processes, eagerness to comply, and limited cybersecurity training—factors that can lead to significant security breaches if left unaddressed.

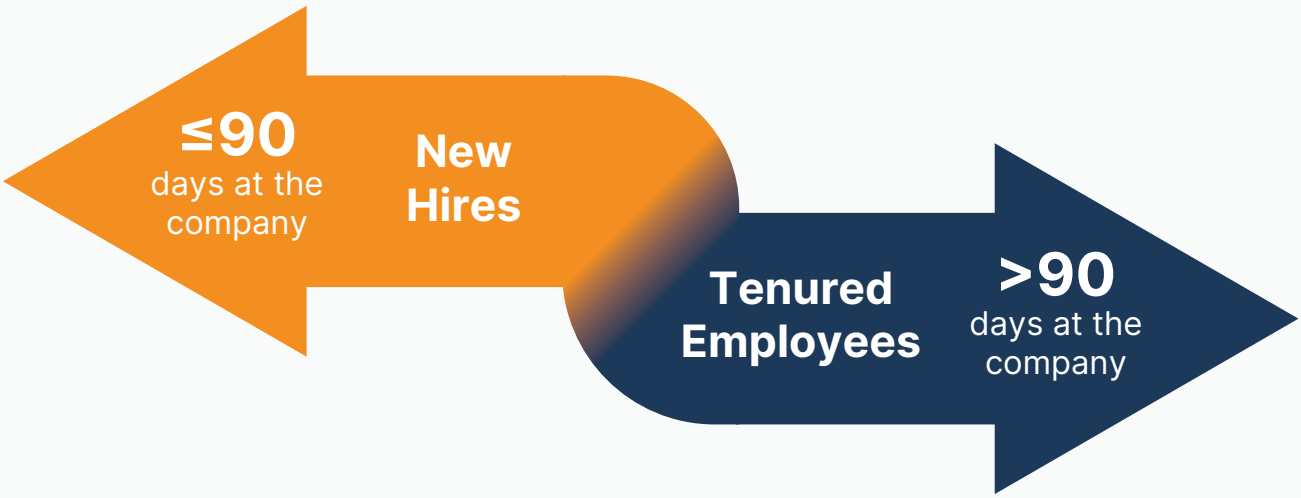
Implementing Keepnet's **security behavior and culture program** during onboarding can reduce this risk by **30%**, improving employee preparedness and organizational resilience. Organizations should use AI-driven phishing simulations, adaptive cybersecurity awareness, and incident response tools to reduce onboarding cyber risks. Key strategies include automated employee segmentation, hyper-personalized training, gamification, and real-time behavior analytics.

Keepnet helps organizations of all sizes reduce new hires' susceptibility to phishing, preventing potential data breaches and ransomware incidents. Its human-centric security platform, which embeds strategies like adaptive training and real-time analytics, embeds secure behaviors and continuously improves organizational resilience.

Methodology

Sampling Base:	Organizations Involved:	Sector Diversity:	Sampling Methodology:
From a total of 5,000 organizations	237 selected randomly	Covered multiple industries	Randomized, cross-sector representation

New Hires vs. Tenured Employees



For details, visit our Research Methodology.

The Challenges with New Hires

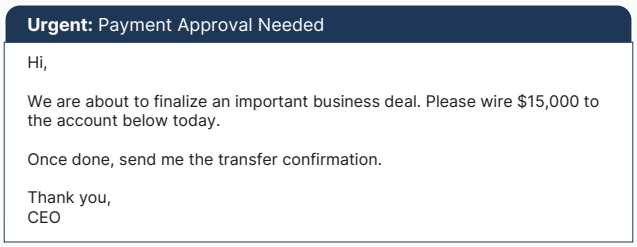
New hires are, on average, more susceptible to phishing attacks and social engineering attempts than tenured employees (Williams, E. J., et al., 2018). Recognizing and segmenting risky groups like new hires is key; Keepnet conducted this research to identify risky groups and reduce employee-driven cybersecurity risks.

This heightened risk is driven by several key factors that make new employees particularly vulnerable during their initial 90 days:

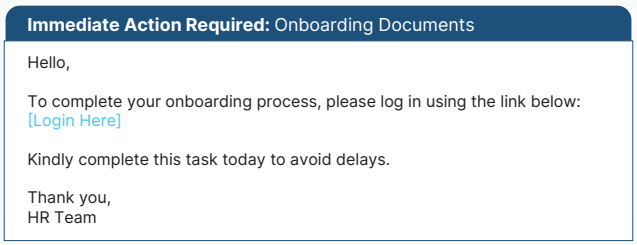
- **Unfamiliarity with Cybersecurity Protocols:** New hires often lack an understanding of standard workflows and may misinterpret phishing attempts as legitimate requests.
- **Information Overload:** The volume of information presented during onboarding can create a mental burden, making it easy for new employees to overlook critical cybersecurity practices.
- **Eagerness to Comply:** New employees are typically eager to please and may comply with unusual requests, increasing their susceptibility to authority-based phishing scams.
- **Lack of Cybersecurity Awareness:** Initial security training is often delayed or insufficient, leaving new hires underprepared for sophisticated threats.

Examples of Phishing Scenarios for New Hires:

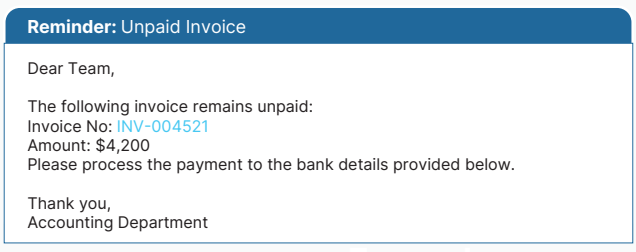
- **CEO Impersonation:**
  A new hire receives an urgent email from a sender appearing to be the CEO requesting a wire transfer or sensitive internal data. They may comply without question because they are unfamiliar with internal communication norms.



- **Credential Harvesting via Fake HR Portal:**
  An attacker sends a phishing email disguised as an HR announcement, prompting new hires to log in to a fake portal to access onboarding documents. This technique exploits new employees' eagerness to complete onboarding tasks.



- **Vendor Invoice Scam:**
  A phishing email claims to be from a recognized vendor requesting payment for a **"Unpaid invoice."** New hires in finance or procurement roles who are unfamiliar with standard vendor interactions might approve such payments.

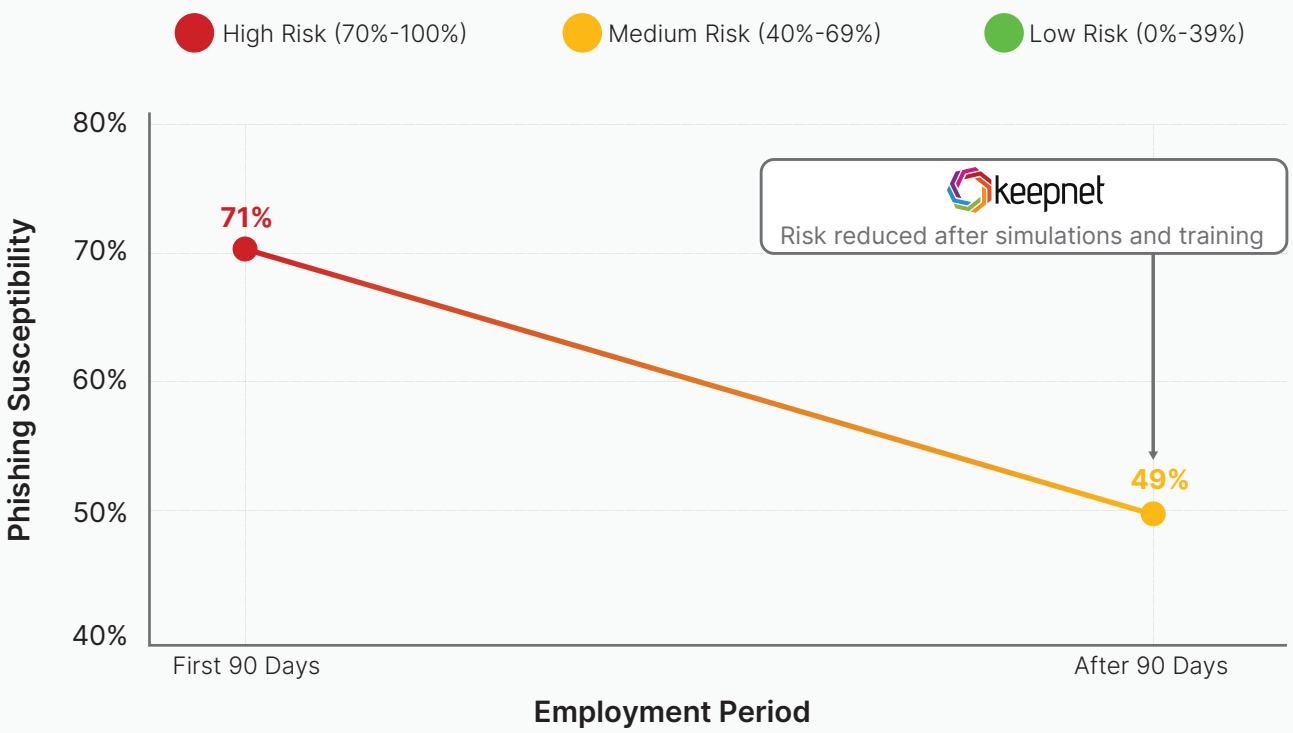


Example

Findings

New hires pose a high cybersecurity risk during onboarding due to their lack of familiarity with cybersecurity processes and limited cybersecurity training, increasing their phishing susceptibility to social engineering attacks (see calculation details in footer 1).

Research conducted by Keepnet in 2025 highlights the following key findings:



1. **71%[1] Phishing Susceptibility in the First 90 Days:** New hires, during their onboarding, have an average Phishing Susceptibility of 71%, indicating significant exposure to cyber threats (see calculation details in footer 1). In contrast, tenured employees benefit from prolonged cybersecurity training and greater familiarity with processes, demonstrating much lower susceptibility to such attacks.

2. **44%[2] More Susceptible to Phishing:** New hires are 44% more likely to fall for phishing and social engineering attacks than tenured employees. This figure is based on data analysis and comparative studies (see details in footer 2). This heightened risk reflects their limited familiarity with organizational processes and insufficient exposure to security training during onboarding.

[1] To see how Phishing Susceptibility is calculated, refer to our guide here https://doc.keepnetlabs.com/next-generation-product/platform/reports#how-is-the-phishing-susceptibility-calculated

[2] The 44% increased susceptibility for new hires compared to settled staff is calculated using the formula:
- (New Hire Risk - Settled Staff Risk) / Settled Staff Risk × 100
- Substituting the values from Keepnet's data: (71 - 49) / 49 × 100 = 44%

This demonstrates that new hires are approximately 44% more susceptible to phishing and social engineering attacks compared to settled employees.

Findings

A 2024 study by Baltuttis D. et al. further supports these findings, revealing that new hires are 36% more likely to fall for phishing attacks than settled employees. This aligns with Keepnet's analysis, reinforcing the need for targeted cybersecurity training during onboarding.

3. **30%[3] Phishing Risk Reduction After 90 Days:** Organizations implementing Keepnet's adaptive phishing simulations and ongoing cybersecurity awareness training achieved an average 30% reduction in phishing risk for new hires after their first 90 days (see details in footer 3).

New hires are nearly **45%** more susceptible to CEO Impersonation phishing attempts than settled employees.[4]

New Hires

New employees are more vulnerable to CEO impersonation attacks.

%71

Tenured Employees

Established employees are less susceptible to CEO impersonation attacks.

%49

[3] The 30% decrease in new hires' average phishing susceptibility is calculated using the formula:

- (New Hire Risk - Settled Staff Risk) / Settled Staff Risk) × 100
- Substituting the values: (71 - 49) / 71 × 100 = 30%

This demonstrates that the risk score dropped by approximately 30% after the first 90 days of employment.

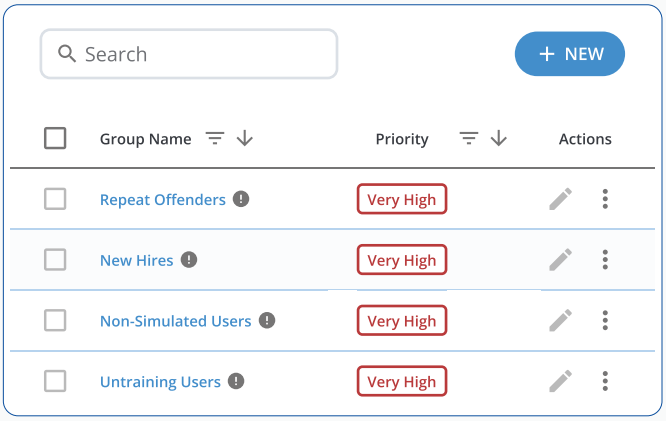
[4] (71 - 49) / 71 × 100 = 30%

Tackling New Hire Risk with Keepnet

Keepnet helps prevent up to 92% of data breaches and ransomware attacks by reducing human-related cyber risks through AI-powered phishing simulations, adaptive training, and advanced phishing response. Its scalable solutions enable organizations to manage employee-driven threats effectively.

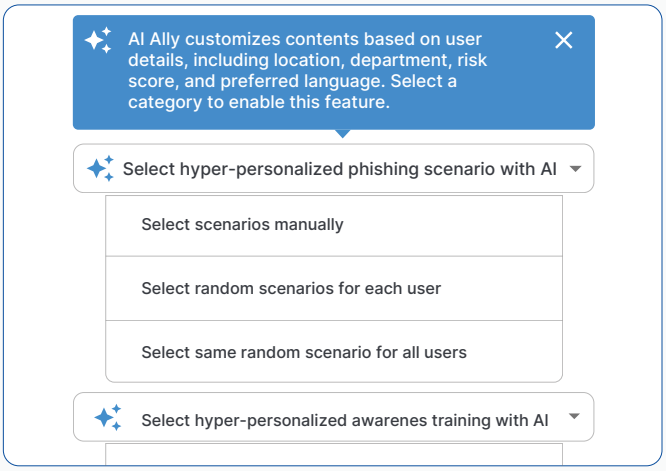
1. Automated Segmentation

Keepnet's platform automatically groups employees based on risk profiles, roles, and behaviors. This segmentation enables focused training for high-risk users, new hires, and specific departments, ensuring efficient resource allocation.



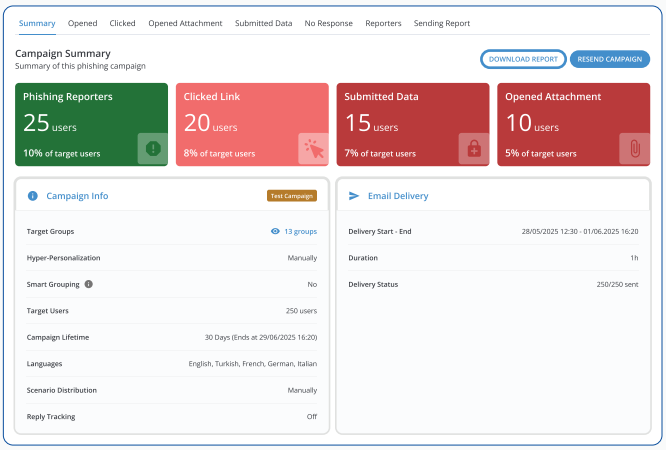
2. AI-Driven Simulations and Adaptive Training Programs

Use AI-powered tools to deliver hyper-personalized phishing simulations and adaptive training programs. These solutions dynamically adjust to employees' roles, risk profiles, and behavior patterns, ensuring relevance and scalability.



3. Phishing Reporting, Analysis, and Response

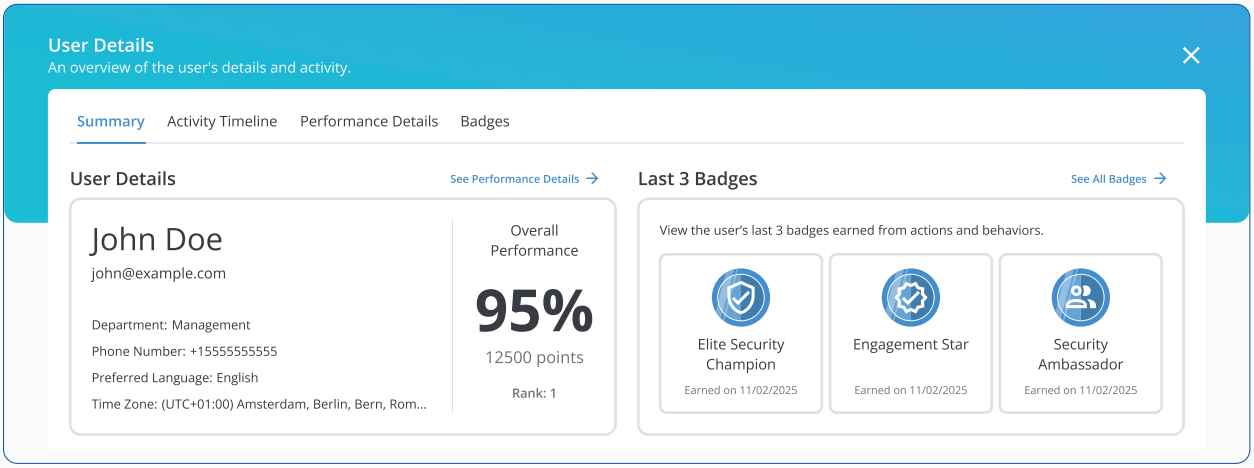
Keepnet enables employees to report phishing attempts easily while providing organizations with automated analysis and rapid response tools. This human-centric cybersecurity approach ensures quick threat detection and mitigation.



Tackling New Hire Risk with Keepnet

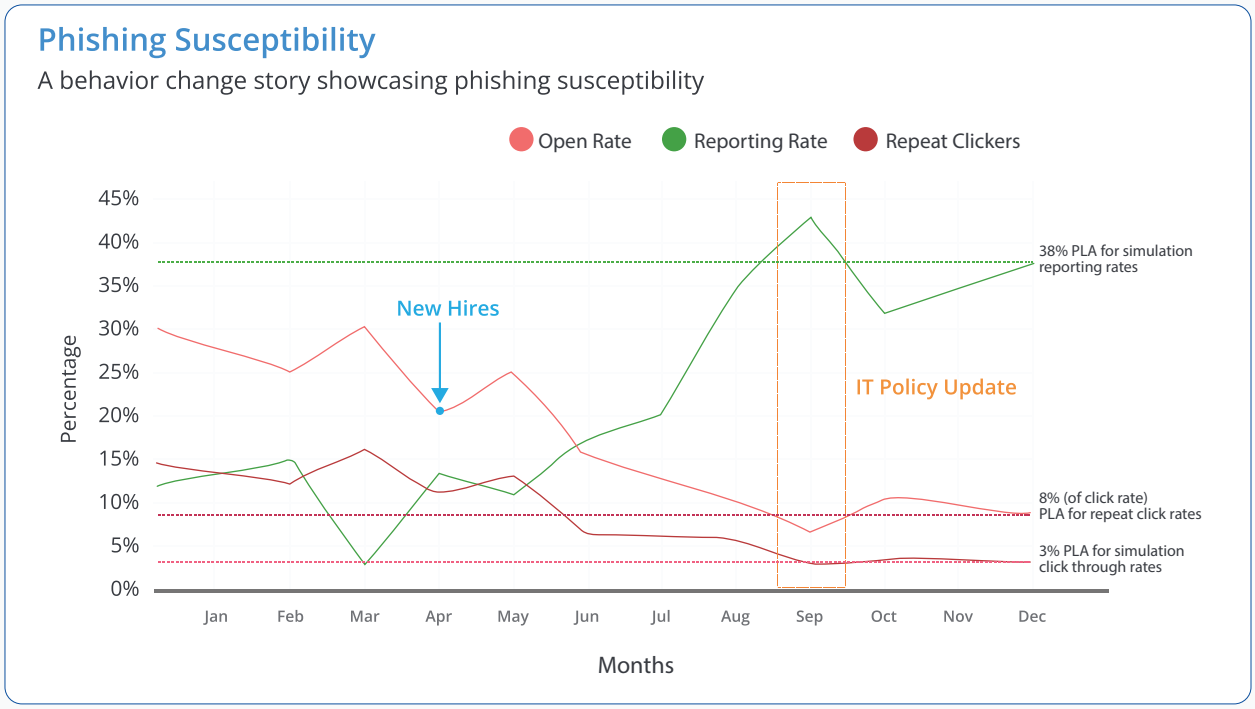
4. Gamification

Keepnet incorporates gamification features like leaderboards, badges, and points to drive employee participation in training and phishing simulations. These elements are grounded in Behavioural Science principles, using nudges to subtly guide users toward secure behavior choices.



5. Outcome-Driven Metrics

Executive reporting connects cybersecurity metrics to business outcomes, helping leadership align cybersecurity initiatives with organizational goals. Reports highlight reduced incidents, improved operational efficiency, and strategic alignment backed by actionable data and business-centric narratives.



Tackling New Hire Risk with Keepnet

6. Security Behavior & Culture Program

The program provides real-time insights into metrics like Phishing Susceptibility, Phishing Dwell Time, and Repeat Offenders. It empowers organizations to monitor progress, prioritize interventions, and track cultural engagement.

Security Behavior & Culture Program

This sample program below delivers actionable insights into employee behavior, security culture maturity, and compliance alignment. It helps organizations assess progress, detect high-risk trends, and drive meaningful behavioral change.

Area	KPI	Change	Q1–Q4 2025 Movement	Current Status	Suggested Actions
User Behavior	Phishing Click Rate	↓ 12%	Declined from 30% to 18%	Improving	Deploy focused anti-phishing simulations & follow-up training
	Reporting Accuracy	↑ 15%	Grew from 60% to 75%	Improving	Launch weekly "report phishing" gamification contests
	Leaked Password Events	↓ 8%	Dropped from 50 to 35 cases	Improving	Enforce 2FA, block reused credentials, and conduct refresher workshops
	Lost Device Reports	— No Change	— Stable at 0–12 per quarter	Monitor Closely	Initiate quarterly asset inventory & awareness drives
Security Culture	Participation in Engagement Events	— No Change	— Consistent at 50–55 entries	Holding Steady	Promote events with prizes or recognition
	Cybersecurity Feedback Sessions	↓ 5%	Down from 40% to 35% participation	Needs Push	Offer incentives and simplify feedback processes
Governance Alignment	Acceptable Use Violations	↑ 20%	Rose from 30 to 36 incidents	Urgent Attention	Schedule targeted policy reminders and reinforcement sessions
	Sensitive Data Mishandling	↑ 25%	Jumped from 8 to 10 incidents	Urgent Attention	Apply DLP policies, simulate mishandling scenarios, and coach high-risk teams
Compliance & Learning	Training Completion Rate	↑ 98%	Up from 85% to 98%	On Track	Celebrate milestones and provide team-based completion dashboards
	Risk-Based Training Delivery	↑ 10%	From 70% to 80% deployment	Improving	Add content tailored to deepfake, MFA fatigue, and QR code threats

Implementation of Keepnet Solutions & Business Value

Keepnet is a SaaS platform that seamlessly integrates into an organization's workflows. It empowers customers with scalable solutions that are easy to implement and maintain, ensuring minimal disruption to daily operations.

Integration with Existing Tools

Keepnet integrates with HR, IT, and security systems, including SSO, email platforms, and APIs, for a seamless experience. Learn more at our Keepnet API Documentation.

Seamless Onboarding and Rapid Value Delivery

Keepnet onboard customers within a day integrates fully in 2-4 days, and provides continuous support for long-term security success.

Ongoing Support and Customization

Keepnet provides 24/7 support, tailored training, and data-driven insights to optimize security performance worldwide. For more details, visit our Support & Help Desk.

Scalability for Organizations of All Sizes

Keepnet scales seamlessly for SMBs, enterprises, and MSPs with flexible, cost-effective subscription plans to fit any need. Learn more at our MSSP Partners page.

Business Value Story of an Effective SBCP (Security Behavior & Culture Program)

Keepnet reduces human-driven cyber risks, strengthens security, and protects revenue. The table below highlights its key benefits:

Business Benefit	Cybersecurity Benefits
Met Compliance Requirements	100% completion rate on core securit awareness training
Improved enterprise risk posture	80% reduced likelihood of phishing attacks resulting in material disruption or notifiable data breach
Reduced avoidable costs incurred	85% reduction in security incidents related to targeted behaviors, potentially avoiding an average of $1 million annually.
Reduced unwanted media attention	Minimizes security incidents that could lead to negative PR and reputational damage.
Improved employee productivity	Reduces downtime caused by security incidents through adaptive training that improves your employees' productivity
Improved revenue stream resiliency	Strengthens security culture, preventing disruptions to business operations.
Client-centered targets safeguarded	Protects customer data by training employees to recognize and prevent cyber threats.

Industry Insight

Keepnet minimizes human-driven cyber risks while fundamentally strengthening organizational security culture.

The expert insights below make one thing clear: security awareness isn't optional—it's urgent. New hires often face confusion and uncertainty, creating risk. Even seasoned staff must stay alert, especially as scams and AI threats evolve. As these experts pointed out, proactive training that builds knowledge, sharpens instincts, and creates a shared culture of vigilance is key to staying secure.

> *New hires bring fresh energy and ideas, but they also come with a steep learning curve when it comes to cybersecurity. Policies can be overwhelming, and a lot of knowledge is assumed. As an employer, it's easy to forget how much of your security setup feels obvious. Put yourself in their shoes for just a minute, and you'll see how unfamiliar and confusing it can be.*
>
> *That early period is critical. Mistakes often happen not from carelessness, but from uncertainty. If we don't clearly explain how things work, why they matter, and where to go for help, we leave new starters to figure it out on their own. That's not just unfair, it's risky.*

Ant Davis
Tesco

> *As much as good security awareness involves being familiar with your company's policies and the latest scams, it's equally about taking your time and trusting your instincts. As criminals (and AI) continue to advance, taking an extra few seconds to review a message and paying attention to your gut—if anything feels even slightly off—can make the difference between catching a phish and causing an incident.*

Michelle Brown
Staples

> *New employees will have different backgrounds and the biases about information security that come from them. The planned, specific, and effective delivery of awareness of a company's policies, risks, and culture are imperative to bring personnel to a functionally secure level for the company's continued success.*

Mike Gorman
NetFoundry

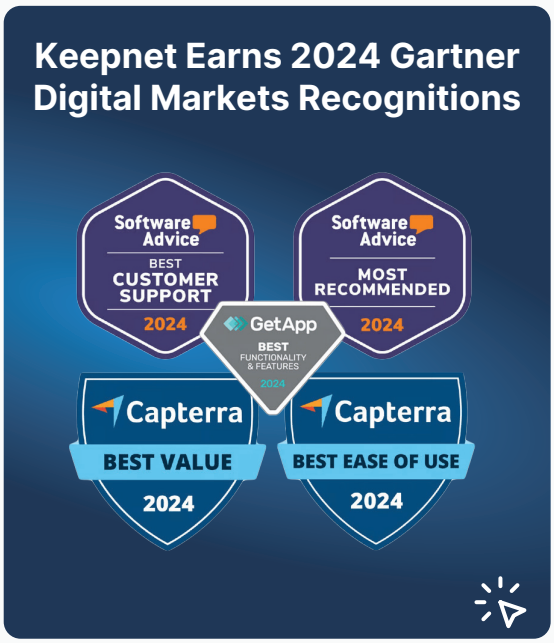
Global Recognition and Impact

Keepnet is recognized as a Strong Performer in Gartner's Voice of the Customer in 2023 and 2024, underscoring its commitment to delivering exceptional solutions for human risk management.

Learn more:

Additionally, Keepnet's Cybersecurity Awareness Training has been awarded Best Value by Capterra, Software Advice, and GetApp in 2024 and 2025, further solidifying its reputation as a trusted leader in the industry.

Learn more:



Keepnet has offices in the UK and the US. It is supported by a global, multi-cultural, and diverse team that drives innovation and delivers impactful cybersecurity solutions worldwide. Trusted by finance, healthcare, and technology organizations, Keepnet served the top global enterprises like Coca-Cola, Merck, and MSSPs to deliver enterprise-level security to SMEs. The team ensures organizations can connect cybersecurity benefits to business outcomes by leveraging outcome-driven metrics.

Vision for the Future

Keepnet's vision is to transform how businesses protect their human layer from social engineering threats, creating a safer and more resilient digital world.

Our Values

- **Collaboration:** We value diverse perspectives and foster teamwork to achieve shared goals.
- **Customer-Centricity:** We are dedicated to understanding and addressing our customers' unique needs, challenges, and objectives.
- **Agility:** We embrace change and adapt swiftly to evolving challenges and opportunities.
- **Integrity:** We uphold ethical standards and take responsibility for our actions in everything we do.

Resources

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1-13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. Computers & Security, 140, 103741. https://doi.org/10.1016/j.cose.2024.103741

Keshvadi, S. (2023). Enhancing Western organizational cybersecurity resilience through tailored education for non-technical employees. 2023 IEEE International Humanitarian Technology Conference (IHTC), 1–6. https://doi.org/10.1109/IHTC58960.2023.10508824

Contact Us