Jericho Security

Jericho VS Traditional

In today's digital landscape, the threat of phishing attacks is ever-present and constantly evolving. As organizations seek to protect themselves from these threats, the importance of effective phishing training cannot be overstated. However, traditional phishing training vendors often fail to provide comprehensive and innovative solutions to keep pace with modern cybercriminals.

The comparison chart focuses on key factors (categorized below) differentiating Jericho Security from traditional phishing training vendors like KnowBe4, InfoSec, and ISSP:

Reporting

Customization

User experience

Innovation

Jericho Security

The comparison chart visually represents the phishing training landscape and highlights the areas where Jericho Security outperforms its competitors.

	Traditional	Jericho Security
Dynamic, generative AI-based	✕ Template-based phishing simulations that send the same message to different users, reducing the accuracy of real-world phishing tactics and emails being sent out today.	✓ Hyper personalized AI-powered spearphishing simulations that incorporate dark web data and real-world phishing examples to increase realism and accuracy.
Customization	✕ Outdated or one-size-fits-all training content that struggles to keep up with the rapidly evolving tactics used by cybercriminals or with urgent, time-sensitive issues (e.g., a breach occurs in the company, a geo-political event occurring in the area). *Customization is available, but it takes weeks to months to deliver	✓ Training content can be 100% customizable to address unique audiences, needs, and risks with a variety of use cases, from AI governance to HR training, leading to higher-impact training. AI engine utilization quickly generates customer training content within 24 hours.
Native, Custom Language Support	✕ Lack of support for certain languages in phishing templates Lack of quick multi-language support and solutions for training videos. *Can develop custom content but requires weeks to develop.	✓ Multilingual phishing simulations with a click of a button, supporting native languages such as Japanese and Korean . Generated multi-language training videos with a quick turnaround .

Jericho Security

Jericho Security

	Traditional	Jericho Security
Intuitive User Experience	✕ Unintuitive user experience leads to frustration and increased time spent to deploy and fine-tune the solution.	✓ User experience optimized to ensure ease of use and ease of integrations for onboarding and deployment, drastically reducing time to value.
Real-Time Reporting and Analytics	✕ Limited reporting that lacks granularity or that requires additional data massaging to get the necessary analysis. Difficulty in demonstrating impact on business goals.	✓ Executive-level reporting, with a focus on board reporting, including monthly campaign reports and quarterly executive summaries The ability to track performance and progress in granular detail, identifying key trends and high-risk activity across individuals, groups, and roles.
Continuous Innovation	✕ Slow to adopt new technologies, approaches limiting the ability to provide cutting-edge phishing defense solutions.	✓ Commitment to continuous improvement with rapid adaptation to emerging threats and trends Investment in the latest cybersecurity research and technologies to fine-tune product roadmap.

Level up your phishing defense

As organizations seek to protect themselves from the growing threat of phishing attacks, it is essential to recognize the limitations of traditional phishing training vendors. By understanding these limitations, organizations can make informed decisions and select the phishing training solutions that best meet their unique needs and risks.