INFOSEC IQ

Security awareness & phishing simulator buyer's guide

Despite even the best firewalls, spam filters and cybersecurity software, attack vectors can and will reach your employees.

Educating your entire workforce to identify and report cyber threats they encounter might sound daunting. However, cybersecurity education companies like Infosec have helped millions of employees in virtually every industry stay cybersecure. With the right security awareness and anti-phishing training solution, you can turn your workforce into one of your greatest cybersecurity assets.

How should you use this buyer's guide?

This buyer's guide will help you establish security awareness and training goals, prioritize your organization's needs and establish the features and training content you require to run a successful security awareness and training program. You can also use the vendor scorecard to compare solutions and ensure you make the best vendor selection for your organization.

Who should use this buyer's guide?

This buyer's guide is useful for anyone evaluating security awareness training and anti-phishing solutions. While this often includes members of the security or IT department, it may also include your employee training team, corporate communications department, human resources or even the executive team.

Start Your Vendor Evaluation

Table of contents

Setting goals

Selecting the right security awareness and training solution starts with setting objectives. Security awareness might sound like an abstract goal, but training completion rates, employee lesson retention, organization susceptibility and more can all be measured — and improved upon — with the right tools.

Outline your security awareness goals and aspirations to help guide your vendor evaluation process and select the best solution.

What are your goals?

- [ ] Build your organization's first security awareness and training program
- [ ] Mature and scale an existing security awareness and training program
- [ ] Remain compliant
- [ ] Reduce your organization's number of security incidents
- [ ] Reduce your organization's phishing risk
- [ ] Increase employee reported emails
- [ ] Inspire employee behavior change and good security habits
- [ ] Streamline security policy distribution and acknowledgement
- [ ] Improve application security
- [ ] Use data to inform your security awareness and training curriculum
- [ ] Identify and educate at-risk employees
- [ ] Launch a security champions program

Prioritizing needs

In addition to the unique cybersecurity challenges your organization faces, your ability to address those challenges is dependent on your time constraints, the size of your team, your experience running a security awareness program and even support from stakeholders and the executive team.

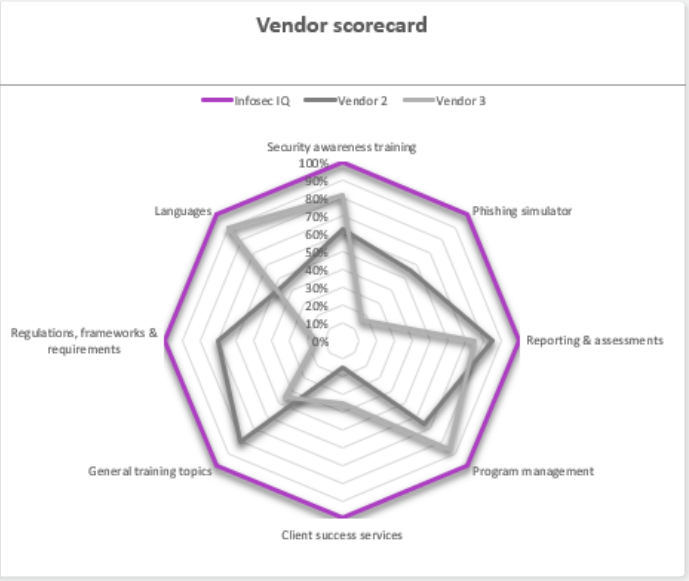
With a wide range of security awareness and training solutions on the market, it can be hard to focus on the features and training resources that matter most to your organization. That's why it's important to start with a set of decision criteria. You can use this criteria to evenly evaluate multiple vendors and select the solution that best fits your needs and will help you achieve your goals.

Evaluating solutions

Our vendor scorecard contains feature and training checklists to help you score the vendors you evaluate based on the platform toolset and training content coverage. As you evaluate solutions, you rate each vendor against your most important decision criteria. You can even customize the feature and training checklists and weigh the importance of each item based on your goals and needs. Once complete, the scorecard automatically rates each vendor across eight categories to help you identify the best fit.

INFOSEC IQ **Vendor scorecard**

	Infosec IQ	Vendor 2	Vendor 3
Feature evaluation			
Security awareness training	100%	63%	82%
Phishing simulator	100%	55%	16%
Reporting & assessments	100%	85%	75%
Program management	100%	66%	86%
Client success services	100%	15%	35%
Feature evaluation score	100%	57%	59%
Training content evaluation			
General training topics	100%	81%	45%
Regulations, frameworks & requirements	100%	70%	15%
Languages	100%	45%	90%
Training content evaluation score	100%	65%	50%
	Infosec IQ	**Vendor 2**	**Vendor 3**
Vendor total score	100%	61%	55%



Download Vendor Scorecard

INFOSEC IQ

Security awareness training & phishing simulator

Infosec IQ awareness and training empowers your employees with the knowledge and skills to stay cybersecure at work and home. With over 2,000 awareness and training resources, you'll have everything you need to prepare employees to detect, report and defeat cybercrime. Every aspect of the platform can be customized and personalized to match your organization's culture and employees' learning styles.

"Infosec IQ plays a big part in **helping our clients** fulfill and document HIPAA compliance."

— Kevin Patterson
Technical Financial Solutions

"**We haven't experienced any ransomware attacks** since deploying Infosec IQ."

— Pete Just
Metropolitan School District of Wayne Township

"We've noticed a huge increase in the amount of suspicious emails reported to the security department. **People are definitely a lot more aware.**"

— Marc Puhala
Penn National Gaming

About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We provide the best certification and skills development training for IT and security professionals, as well as employee security awareness training and phishing simulations. Learn more at infosecinstitute.com.

INFOSEC