SECURITY AWARENESS TRAINING
BUYER'S GUIDE FOR BUSINESSES

IDAGENT
A Kaseya COMPANY

Businesses are under siege by a never-ending barrage of cyberattacks, and the situation is only growing worse. They need all hands on deck to prevent expensive security disasters like a data breach or a ransomware incident. Unfortunately, many employees are unable to recognize security threats on their own, making security awareness training a necessity.

Security awareness training gives employers the opportunity to add more eyes to their security team by empowering employees to recognize and avoid the common threats that they face every day. It's a smart investment that provides a big security boost without a major upfront cost.

That empowerment pays off. From teaching data handling best practices to preventing an employee from downloading a ransomware-laden attachment, security awareness training is the key to building a strong defense against today's biggest cybersecurity threats.

WHY IS SECURITY AWARENESS TRAINING IMPORTANT?

Every organization is facing a rising tide of risk as cybercrime and its associated losses explode. The U.S. Federal Bureau of Investigation Internet Crime Complaint Center (FBI IC3) 2021 report offers an excellent snapshot of the danger that businesses face.

IC3 received a record 847,376 complaints from U.S. businesses impacted by cybercrime in 2021, a 7% increase over 2020. But the total amount of loss is the real stunner, at a new record high of $6.9 billion in 2021, a whopping 48% increase over 2020.

Drilling deeper, these statistics can give you a snapshot of the cyberattack risk that businesses face right now.

- 84% of businesses were the victims of a successful phishing attack in 2021, a 15% increase over the same 12-month period in 2020.
- The U.S. has incurred a 127% year-to-date increase in the number of ransomware attacks while the U.K. has seen a 233% surge in ransomware infections.
- The average cost of a breach is estimated at $4.2 million per incident, 10% higher than in 2020 and the highest recorded in the 17 years.

WHAT IS THE LEADING CAUSE OF A SECURITY BREACH?

The leading case of a security breach never changes: human beings. An estimated 90% of security breaches are caused by human error. Unless they receive the right training around common risks, employees are likely to make mistakes that have a potentially devastating impact on their organization's security.

EMPLOYEES WHO ARE UNEDUCATED ABOUT SECURITY ARE A DISASTER WAITING TO HAPPEN

Unfortunately, many employees don't have a clue about the importance of their behavior in maintaining security. An estimated 45% of respondents in a HIPAA Journal survey said that they don't need to worry about cybersecurity safeguards because they don't work in the IT department.

Without the knowledge that they need to identify security problems, untrained employees are a ticking time bomb.

- **Only an estimated 30%** of internet users know what ransomware or malware is
- **97% of employees** cannot spot a sophisticated phishing email
- Only **16% of employees** can recognize cyberthreats without security awareness training

EMPLOYEES WILL FALL FOR PHISHING

Phishing is the catalyst for many of today's nastiest cyber threats like business email compromise and ransomware. Unfortunately, many employees who do not receive proper training are more likely to fall for phishing tricks.

- **1 in 3** employees are likely to click the links in a phishing email
- **1 in 8** employees are likely to share information requested in a phishing email
- **60% of employees** interact with suspicious email messages

TRAINING TRANSFORMS EMPLOYEES INTO SECURITY ASSETS

Security awareness and phishing simulation training is an effective measure to mitigate the risks that employees encounter daily. The more training employees receive, the more adept they get at spotting and avoiding security risks.

Researchers in a U.K. study discovered that the improvement in employee behavior that companies see when they engage in security awareness training is stark.

At the beginning of the study, as many as 40% to 60% of the employees surveyed were likely to open malicious links or attachments.

After about six months of security awareness training, the percentage of employees who took the bait dropped to 20% to 25%.

When the employees completed three to six months more of security awareness training, only 10% to 18% of them fell for phishing messages.

Ongoing training is essential for organizations to receive benefits like these. According to Accenture, each employee should receive 11 sessions per year.

SECURITY AWARENESS TRAINING DELIVERS AN AMAZING ROI

No one's budget can support spending on a security measure that doesn't get the job done. But that's not something to worry about when it comes to security awareness training. It's one of the best IT investments an organization can make with an impressive ROI.

IT SECURITY COSTS BEFORE & AFTER TRAINING

	Before training 50 – 999 employees	Before training 1000+ employees	After training 50 – 999 employees	After training 1000+ employees
Annual IT payroll hours spent disinfecting workstations, networks	$760.00	$137.30	**$565.50**	**$120.50**
Annual misc. incident remediation cost per email user	$29.23	$5.28	**$21.75**	**$4.63**
Annual IT security costs per email user	$7.51	$28.11	**$0.75**	**$2.81**
Cost of employee time spent in SAT	$0	$0	**$21.11**	**$27.83**
Estimated annual costs per email user (including IT payroll costs)	$249.39	$455.41	**$24.94**	**$45.54**

Source: Osterman Research, The ROI of Security Awareness Training

TOTAL ROI FOR SECURITY AWARENESS TRAINING

Small and midsize businesses (SMB, 50 to 999 employees) ..... **69% ROI**

Large businesses (1,000+ employees) ..... **562% ROI**

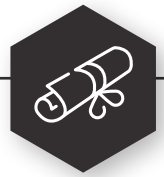
Source: Osterman Research, The ROI of Security Awareness Training

SECURITY AWARENESS TRAINING OPTIONS LANDSCAPE

Determining what category of training (or combination of training categories) best serves your users and your organization is a core part of building a security awareness training program. The U.S. National Institute for Standards and Technology (NIST) breaks employee training around security into three knowledge categories based on what the training is set to accomplish.

Awareness – the ability of the user to recognize or avoid behaviors that would compromise cybersecurity

Training – the action provided to a user in the acquisition of security knowledge, skills and competencies



Education – knowledge or skill obtained or developed by the learning process

WHICH TYPE OF TRAINING DELIVERY IS RIGHT FOR YOUR ORGANIZATION?

THERE ARE TWO MAIN TYPES OF TRAINING FROM WHICH TO CHOOSE: ONLINE OR IN-PERSON

The preferred style for your organization will be influenced by a number of factors including support for remote workers, geography and language options.

Online training is the most common style companies use because of its flexibility and ease of program administration. An estimated 90% of companies use eLearning for employee training. Online training is also extremely cost-effective. Microsoft discovered that when it switched its employees from in-person to eLearning for training, their training costs plummeted, going from $320/hour to just $17/hour, a savings of almost 95%.

COMMON TRAINING FORMATS

After determining how you'll deliver training, you'll need to consider the format of the training. A combination of formats may be the winner for you.

VIDEO: Teach employees about security and compliance using short educational videos that are often accompanied by quizzes to measure retention. This is a universally preferred option: 83% of learners prefer video content.

INTERACTIVE/GAMES: Use interactive exercises or gamification tools to deliver knowledge and awareness.

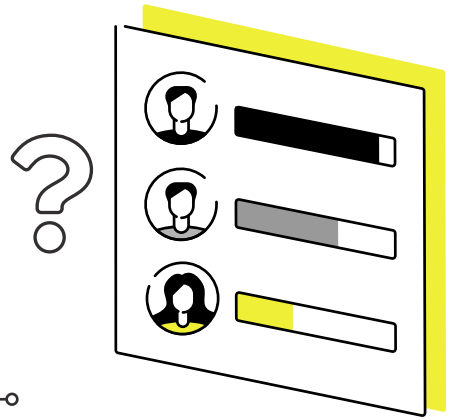
EMAIL/NEWSLETTER: Publish on a schedule an internal roundup of important security policies as well as security and compliance tips.

IN-OFFICE VISUALS: Posters, flyers, signs and similar tools outlining security policies, procedures and tips around the office or in areas where employees congregate.

THE IN-HOUSE VS. OUTSOURCING DILEMMA

It's important to decide whether your training will be developed and delivered by in-house IT personnel or if you'll be utilizing a training solution. The answers to these questions might provide clarity.

- **Who has the skills to architect and guide the program?**
- **Who has the bandwidth to handle this project?**
- **How will implementation work?**
- **How much funding do you have for the program?**



WHAT TO LOOK FOR WHEN YOU'RE EVALUATING SOLUTIONS

When you're evaluating training solutions, the answers to these questions should be the deciding factor to help you find the perfect fit.

DOES IT PROVIDE SECURITY AWARENESS TRAINING, PHISHING SIMULATION TRAINING, OR BOTH?

Make sure the solution that you choose can really get the job done by ensuring it offers the training that you need.

Security training – Lessons about the major security threats and security-related topics your users are likely to face.

Compliance training – Lessons about the compliance requirements employees must meet to comply with relevant policies and regulations.

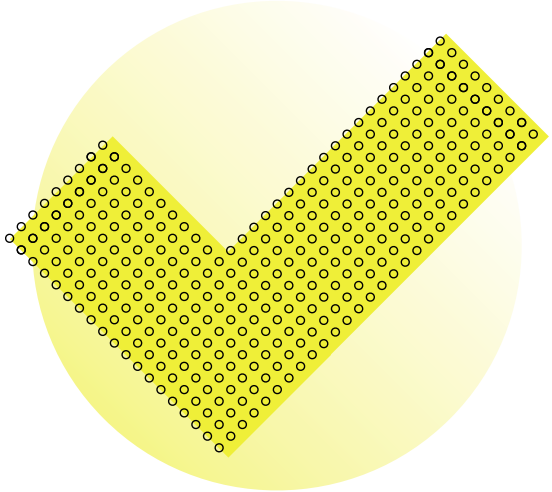
Phishing simulations – Exercises in which simulated phishing messages are sent to employees and their actions around those messages are measured to determine what tricks employees are likely to fall for as well as who need education about phishing. Employees who train using simulations retain 11% more knowledge.

IS THE CONTENT HIGH QUALITY AND TIMELY?

A good solution offers trustworthy, well-made and relevant content. If your organization is multinational, it's also important to find a solution with options for training in multiple languages.

It's essential that a solution's content library is updated regularly to ensure that users are getting the training they need. A well-stocked training library will feature a wide variety of topics including these must-haves:

- **Password safety**
- **Phishing**
- **Ransomware**
- **Regulatory compliance**
- **Data handling best practices**



WHAT PHISHING SIMULATION CUSTOMIZATION OPTIONS DOES THE SOLUTION OFFER?

Customization is a valuable feature in phishing simulations because it enables you to do two important things: **1) improve the effectiveness of training with phishing simulations that reflect the unique threats employees in your organization face**, and **2) increase the believability of your fake phishing messages by making them appear to come from a trusted source**.

When assessing a solution's customization options, be sure that it offers:

- **The ability to modify current phishing simulation emails to tweak them to your needs**
- **A blank template to create custom phishing emails from scratch**
- **The option to use your organization's domain to send out simulated phishing messages**

DOES THE SOLUTION OFFER FLEXIBILITY IN TRAINING CAMPAIGN SETUP?

Training isn't a one-size-fits-all proposition, and a comprehensive security and compliance awareness training solution is designed with that in mind. A truly flexible solution will offer you the ability to:

- **Create custom employee training groups and assign different training paths to each group based on their needs and the threats they're most likely to encounter**
- **Stagger phishing simulation emails to be sent at random times to prevent employees from alerting each other**
- **Schedule training session invitations to be sent automatically weeks or months in advance**
- **Clone, copy or modify previous campaigns to avoid creating new ones from scratch.**

CAN THE SOLUTION ALSO SERVE AS A LEARNING MANAGEMENT PLATFORM FOR OTHER TYPES OF TRAINING YOUR ORGANIZATION NEEDS?

Security and compliance education isn't the only training employees need. Look for a training solution that can be used in multiple ways for maximum value. If a solution can also be used for other training that you upload, like new employee onboarding, sexual harassment training or business process education, it's a winner.

IS THE SOLUTION CONVENIENT FOR EMPLOYEES AND IT PERSONNEL TO USE?

Training that is a hassle isn't beneficial to anyone. Make the training process a snap for employees by choosing a solution that delivers each employee's training through a personalized portal accessible anytime, anywhere. That makes it easy for employees to access the training they've been assigned and keep track of the courses they've completed.

Don't forget about productivity features that will make training less burdensome for the IT team, too. Choose a solution that auto-syncs with your employee directory to make setting up training groups easy and eliminates manual updates when staff changes occur.

DOES THE SOLUTION TEST EMPLOYEE KNOWLEDGE RETENTION AFTER TAKING TRAINING?

For a training program to be effective you need performance data. A testing feature is essential in a training solution. A post-training online test that's instantly scored is ideal. Employees who take quizzes after their training sessions retain 26% more knowledge than employees who do not take a test.

Make sure the testing feature includes the ability to set parameters like the passing score for each lesson and the number of times an employee can attempt to pass the test before they fail the course.

DOES THE SOLUTION PROVIDE AN ABILITY TO TRACK TRAINING RESULTS, BOTH IN-PROGRESS AND FINAL?

It's impossible to demonstrate the value of training without the right tools to measure performance. Look for a solution that offers a robust array of tools to track, measure and report on your training program's accomplishments including:

- **A dashboard to track progress in real time**
- **Customizable reporting**
- **Visually engaging, easy to understand reports to share with the stakeholders**
- **The ability to automate report generation and delivery to stakeholders**
- **Summary reports at the end of every campaign that show training course results, such as who didn't take the training, who started but didn't complete the training, who completed the training and how employees scored on tests**
- **Phishing simulation results including which simulated malicious messages were most effective, who didn't take any action, who opened the email, who clicked on the link in the email and who submitted their credentials on the fake phishing landing page**

LOOK FOR ROBUST SUPPORT AND INNOVATION

Thoughtful development and design can make all the difference in a solution's suitability for your organization as well as your satisfaction. Look for these green flags that indicate a high level of both support and innovation.

- Onboarding to get you up and running with the platform
- Helpful how-to video tutorials inside the product to help administrators become power users and make the most out of the platform
- Detailed guides, FAQs and articles to help you along the way, like a whitelisting guide to ensure the delivery of phishing simulation emails
- Constant evolution to improve performance and UI, with new features and enhancements introduced often
- Communication that ensures you are kept informed about new features, offerings and innovation via email, customer newsletter or regular webinars
- An online community of customers to exchange ideas and best practices with
- A place to submit product improvement ideas and provide feedback

DON'T SPEND MORE THAN NECESSARY

Yes, you can find a security and compliance awareness training solution that includes everything you need to succeed without blowing up your budget. Keep these considerations in mind when looking at the value and feasibility of a solution for you.

Do you really need all the bells and whistles you're paying for? If you don't need an option like training content in multiple languages, don't pay for it!

Learn the nuances of the seat purchasing requirements up front to ensure that you have room to maneuver if your organization's needs change. Does the initial seat minimum you have to purchase fit your needs? When you grow and need to add seats, will you be forced to add them in large increments and pay for the seats you don't need?

Are there hidden charges for must-have features and add-ons that inflate the low advertised price? Be sure to ask for a detailed quote that covers everything you're looking for and every add-on or option you're buying. Take time to understand what is and isn't included and avoid unpleasant surprises later.

CHOOSE THE TRAINING SOLUTION THAT CHECKS ALL OF YOUR BOXES

The right solution for your organization is here. BullPhish ID is the innovative, affordable, customizable solution that you're looking for to conduct successful security awareness and compliance training. **With BullPhish ID you can:**

- ✔ Gain access to a large library of training videos to educate employees on how to avoid cyberthreats like phishing and ransomware.
- ✔ Simplify compliance training with video lessons that make complex requirements easy to understand.
- ✔ Train your way and on your schedule with plug-and-play phishing simulation kits or customizable content that can be tailored to fit your industry's unique threats.
- ✔ Be confident that you're educating employees about the latest threats or compliance requirements, with at least four new training videos and fresh phishing kits added every month.
- ✔ Educate a geographically dispersed user base with training videos available in eight languages: English, Dutch, French, German, Italian, Portuguese, Spanish (Iberian/European) and Spanish (Latin).
- ✔ Leverage in-lesson quizzes and simple, easy-to-read reports to see the value of training, and know who needs additional support.
- ✔ Simplify the training process and make it convenient for every employee with a personalized user portal.
- ✔ Automatically generate and send reports to stakeholders.

Want to learn more about security awareness and compliance training with BullPhish ID?

Explore the features and benefits today. Or,

BOOK A DEMO AND SEE BULLPHISH ID IN ACTION!

BULLPHISH ID

ID AGENT
A Kaseya COMPANY

ABOUT ID AGENT

ID Agent, a Kaseya company, provides the leading Dark Web monitoring, security awareness training and identity & access management solutions worldwide. Its flagship product, Dark Web ID™, delivers validated intelligence to identify, analyze and monitor for compromised or stolen employee and customer data. The company's BullPhish ID™ product provides cybersecurity awareness training and phishing simulation geared to the non-technical end user, to enhance a company's overall cybersecurity and further safeguard corporate systems. Passly™ delivers comprehensive identity & access management to secure remote workforces and protects organizations from risk of exposure. To learn more, visit www.idagent.com.

IDAGENT
A Kaseya COMPANY