SECURITY AWARENESS TRAINING:
YOUR BEST INVESTMENT

ID AGENT
A Kaseya COMPANY

EMPOWERING EMPLOYEES WITH SECURITY SAVVY STOPS CYBERATTACKS AND SAVES MONEY

Employees are at the heart of their company's security. They are the last line of defense against cyberattacks and the first ones to notice when something unusual is happening at work. That makes them every organization's most valuable security asset.

However, they can also be a vulnerability. When an employee makes a mistake, like mishandling data, clicking on a malicious link or giving a cybercriminal their password, they are opening the doors to expensive compliance failures and security nightmares for their organizations.

The everyday choices employees make have a tremendous impact on their company's security as well as its success. That's why it is critical that every employee is educated about the risks they face as well as smart security behaviors that keep their companies compliant with laws and industry regulations and safe from threats like a cyberattack or a data breach.

Security awareness training is the answer. This powerful tool empowers employees to make smart decisions about security and compliance by arming them with the knowledge they need to avoid pitfalls – because a company is only secure when everyone knows they are part of the security team.

HOW DO EMPLOYEE CHOICES IMPACT SECURITY?

Every time someone logs on to the company's network, answers an email or takes work home, they're taking an action that could have security repercussions whether they mean to or not. The actions that employees take result in insider risk for their organizations.

As companies become increasingly dependent on technology to get the job done, employees have more opportunities to take actions that could be harmful. About 60% of organizations say employee-involved security incidents have become more frequent.

In a world of digital complexity, not everyone is going to be equipped to navigate the dangerous seas of cybercrime threats, making insider risk more complicated. Insider risk rose by more than 40% in 2021. While insider risk is not something that can be eliminated completely, it can be mitigated, and security awareness training is an affordable and effective way to do it.

> | *Human error is responsible for an estimated 90% of security breaches.*

EVERYONE NEEDS TO BE ON BOARD TO BUILD A STRONG SECURITY CULTURE

Companies with a strong security culture have a high level of security awareness — and that's a powerful asset. However, many IT professionals face challenges in getting everyone in their company on the same page about the vital role their security culture plays in both defense and compliance.

> 93% of cybersecurity experts agree *that organizations should focus on both humans and technology to detect and respond to cyberthreats.*

The SANS Managing Human Cyber Risk 2021 report cites strategic alignment as one of the three biggest blockers to managing risk. Less than half of the security professionals surveyed said they felt they had the support they needed from leadership to grow a strong security culture, and about 10% said they had no support at all.

> *Cautious leaders may be more supportive when they learn that companies that engage in regular security awareness training have 70% fewer security incidents.*

SECURITY AWARENESS TRAINING HAS CONCRETE BENEFITS

Taking a look at some concrete benefits of security awareness training shows exactly how valuable security awareness training is and why smart companies are making this small investment that gives them a big security advantage.

IMMEDIATELY EXPAND YOUR SECURITY TEAM WITHOUT ADDING HEADCOUNT

Worryingly, 45% of respondents in a HIPAA Journal survey said that they are not responsible for maintaining security because they don't work in the IT department. That's a disaster waiting to happen. Security awareness training changes this mindset. When employees gain security savvy, they realize that maintaining security to fight back against cybercrime is everyone's job.

CHOOSE A SMART IT INVESTMENT WITH HIGH ROI

Security awareness training is a powerhouse security investment that offers an excellent ROI.

Small and Midsize Businesses (SMBs) ..... **69% ROI**

Larger Organizations ..... **562% ROI**

MAINTAIN COMPLIANCE WITH NATIONAL, LOCAL, REGIONAL AND INDUSTRY-SPECIFIC REGULATIONS

Data privacy and cybersecurity regulations are tightening in many industries, and the price of a compliance failure is high. About 61% of organizations have experienced a compliance-related security failure, incurring expensive regulatory scrutiny. Security awareness training is also required under many data privacy and data handling statutes.

DRAMATICALLY REDUCE THE CHANCE OF A SECURITY BLUNDER

Researchers in a U.K. study discovered that the improvement in employee behavior that companies see when they engage in security awareness training around risks like phishing 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 the phishing messages**.*

| *Security awareness training improves password security* by an estimated 30% to 50%.

LOWER SECURITY EXPENSES, LIKE THE COST OF PHISHING

Phishing is expensive whether the attack is successful or not. If it hits, you've got a potentially devastating incident on your hands. If it doesn't, the matter still requires investigation. The cost of just dealing with the headache of phishing altogether for businesses has almost quadrupled over the past six years, with large U.S. companies losing an average of $14.8 million annually (or $1,500 per employee) to phishing. Security awareness training makes employees more resistant to phishing and reduces the cost of phishing by more than 50%.

LEADING COMPANIES RELY ON SECURITY AWARENESS TRAINING TO PREVENT CYBERATTACK DISASTERS

Security awareness training gives companies an edge against cyberattacks by boosting cyber resilience, making them less likely to be crippled by a cyberattack. About 84% of leading organizations in the IBM Cyber Resilient Organization Study 2021 cite security awareness training as a key building block of cyber resilience.

HOW OFTEN SHOULD COMPANIES RUN SECURITY AWARENESS TRAINING?

The cadence of security awareness training matters. In a report from consulting giant Accenture detailing the characteristics of a cyber-resilient organization, researchers placed the ideal number of training courses for employees each year at 11, or just a little under one per month.

That's because the benefits that employees gain from security awareness training diminish over time. Researchers tested subjects four, six, eight, 10 and 12 months after they completed a security awareness training course. Once the subjects passed the four-month mark, their retention dropped — and their performance at 10 months was the same as it was when they started the study.

ABOUT 62% OF COMPANIES DO NOT DO ENOUGH SECURITY AWARENESS TRAINING TO RECEIVE FULL SECURITY BENEFITS.

TRAIN EMPLOYEES TO RESIST YOUR TOP DATA SECURITY THREAT: PHISHING

The biggest security risk that any organization faces today is phishing. It is the number one cause of a data breach. Phishing is also the risk that employees encounter the most — and fail to detect the most as well — often opening their organization up to dangerous cyberattacks like ransomware.

EMPLOYEES AND PHISHING ARE A DISASTROUS COMBINATION

1 IN 3 EMPLOYEES ARE LIKELY TO CLICK THE LINKS IN PHISHING EMAILS.

30% OF PHISHING MESSAGES GET OPENED BY TARGETED USERS.

1 IN 8 EMPLOYEES ARE LIKELY TO SHARE INFORMATION REQUESTED IN A PHISHING EMAIL.

Cybercriminals are adept at using hard-to-detect ways, like impersonating a well-known brand, to fool their targets into falling for a phishing message — and they're very good at it. So good that 97% of employees are unable to spot a sophisticated phishing email without training.

HELP EMPLOYEES AVOID MALICIOUS ATTACHMENTS

Almost 30% of untrained users in a social engineering study fell for phishing lures that enticed them to click on malicious links, download suspicious files and email attachments, enter their credentials at a fake site and even correspond with cybercriminals.

That's a huge problem for businesses. Almost 50% of all malicious files attached to emails are in one of the MS Office formats. Security awareness training teaches employees how to identify suspicious attachments carrying malware that masquerade as routine files.

An estimated 34% of business IT leaders say that a simple lack of employee understanding of today's sophisticated phishing threats is their biggest security problem.

EMPOWERED EMPLOYEES PROTECT COMPANIES FROM TODAY'S MOST DANGEROUS THREATS

A new cyberattack is launched every 39 seconds. That's bad news for organizations that aren't prepared because only 16% of employees are able to recognize sophisticated threats without security awareness training.

RANSOMWARE & MALWARE

Ransomware attacks climbed 134% in 2021 over the prior year's total. However, ransomware isn't the only malicious software on the block. Payment skimmers, cryptominers, Trojans and other nasty malware types can also cause devastating damage. No business is too small to be at risk — a shocking 50% of malware attacks, including ransomware, are aimed at SMBs every year.

How security awareness training helps prevent this

Employees encounter these threats every day but are unlikely to detect them without training — only an estimated 30% of internet users even know what ransomware or malware is, let alone how it is transmitted.

ACCOUNT TAKEOVER

A bad actor taking over a user account is a nightmare for every IT professional, especially if the bad guys hijack an account that belongs to a privileged user like an IT administrator or executive. Account takeover (ATO) fraud takes a number of forms, including phishing attacks, phone scams or credential compromise. In fact, ATO attacks have become much more frequent — up 671% in 2021 over the prior year.

How security awareness training helps prevent this

Effective training keeps users abreast of the signs of an ATO as well as the dangers of ATO risks, like phishing and credential compromise, and prevents these attacks from landing.

BUSINESS EMAIL COMPROMISE

In a common business email compromise (BEC) scenario, bad actors target a victim and pose as a company the victim's organization would do business with to fraudulently obtain money or sensitive data. The U.S. Federal Bureau of Investigation (FBI) categorizes BEC as an attack that is 64 times more revenue damaging than ransomware. But the costs don't stop there. BEC also endangers a company's reputation and relationships, with employees encountering this hazard daily.

How security awareness training helps prevent this

Employees who have strong cybersecurity awareness are more likely to be suspicious when they experience unusual behavior when communicating with third-party service providers or suppliers.

BRAND IMPERSONATION & SPOOFING

Bad actors will often use cloned or "spoofed" legitimate email messages from a well-known company like Microsoft to send phishing messages that trick unwary readers into taking an action to do things like correct a problem, collect a prize or snag a deal. Employees confront this threat frequently — 25% of all branded emails that companies receive are fake.

How security awareness training helps prevent this

When employees know what to look for, fraudulent-branded messages will be less attractive. But if they don't, 50% of users will click on a link without concern that it may be unsafe.

DATA BREACH

A stunning 90% of incidents that end in a data breach start with a phishing email, and employees are bombarded with malicious messages daily. However, getting tricked by a phishing email isn't the only way employees can cause a data breach. Errors like sending someone the wrong file and other data handling mistakes are just as dangerous.

How security awareness training helps prevent this

Security awareness training arms employees with knowledge that helps them resist threats like phishing while making them more thoughtful in general about how their actions and behaviors impact security.

REMOTE AND HYBRID WORKERS

Remote workers add unique security challenges. One in three employees think they can get away with risky behavior like writing down passwords or opening suspicious emails when working remotely. Plus, cybercriminals know that remote workers are more likely to fall for phishing tricks and less likely to report a problem or ask for help if they don't even know who to ask.

How security awareness training helps prevent this

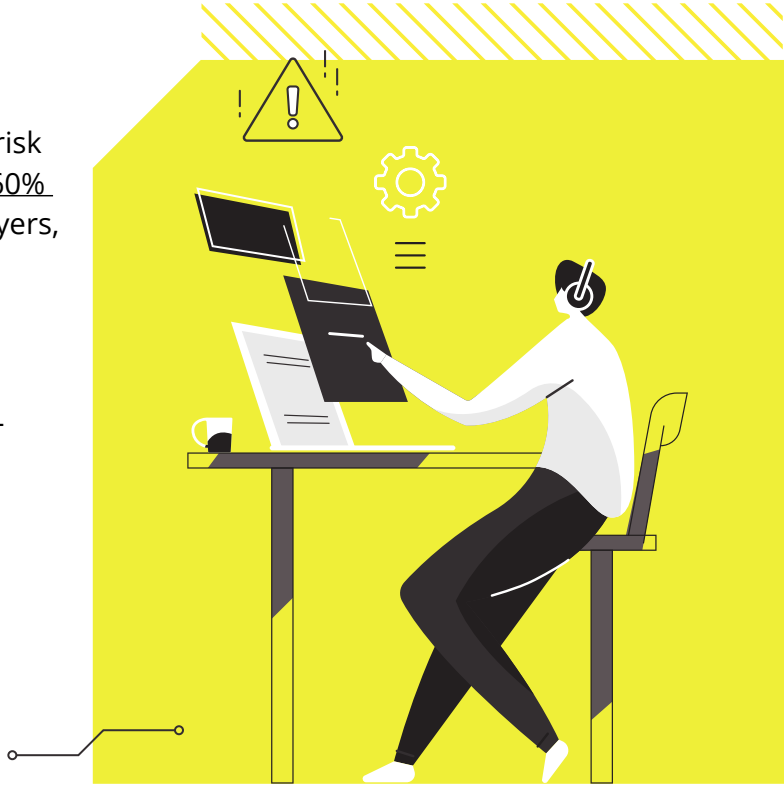
An estimated 40% of remote workers have caused cybersecurity repercussions for their company. Security awareness training makes them more cognizant of why maintaining security matters regardless of where they are and teaches them what to do if there is a problem.

INSIDER RISK

Every employee is an insider, and every employee brings a certain degree of risk to the table whether they intend to or not. Negligent employees create over 60% of security incidents. However, some employees are out to harm their employers, and they're responsible for an estimated 25% of confirmed data breaches.

How security awareness training helps prevent this

A strong security culture is a major determinant in a company's overall risk, and security awareness is the foundation on which it is built. If security is top-of-mind for everyone, employees make fewer mistakes and notice suspicious behavior faster.



SECURITY AWARENESS TRAINING IS EASY AND AFFORDABLE WITH BULLPHISH ID

Are you ready to put the power of security awareness training to work for your company? We're ready to help you get the job done.

BullPhish ID is the ideal solution to use for ongoing security awareness and phishing resistance training. Conduct efficient, effective training around compliance education as well as a variety of risks, including phishing and ransomware, all in one place for less money than competing solutions. **You'll love:**

- ✔ **Fully customizable phishing simulation kits, including messages, landing pages and attachments.**
- ✔ **Plug-and-play phishing kits that make running training on the latest threats a snap.**
- ✔ **Engaging video lessons accompanied by short quizzes that cover threats employees may face, compliance requirements and cybersecurity best practices.**
- ✔ **Frequently updated compliance training for PCI-DSS, HIPAA, GDPR, PIPEDA, CMMC and more.**
- ✔ **Simple, clear progress reports delivered automatically that demonstrate the value of training and show who needs more help at a glance.**
- ✔ **Easy administration and a painless training experience for everyone, with courses delivered automatically through a personalized end user portal.**
- ✔ **Content in eight languages including English, Dutch, French, German, Italian, Portuguese, Spanish (Iberian/European) and Spanish (Latin).**

START A SECURITY AWARENESS TRAINING PROGRAM AND REAP IMMEDIATE BENEFITS

Don't wait! Security awareness training is just what the doctor ordered to reduce risk and keep businesses safe in today's volatile threat landscape.

Call Computer Zone Today!

IDAGENT
A Kaseya COMPANY

Computer Zone
888-895-5173
www.computerzone.net/

ID AGENT
A Kaseya COMPANY