wizer
wizer-training.com

How to Build a Security Awareness Training Program?

This is a comprehensive guide on how to build a successful Security Awareness Training Program for your company. If you are interested in learning how to get your employees engaged, what learning materials work best, and how to develop a positive security culture - then You're in the right place!

Contents

1 Security Awareness Training Essentials

2 What Topics Should Security Awareness Include?

3 How to Engage Your Employees?

4 How to Get Executive Support for Security Awareness?

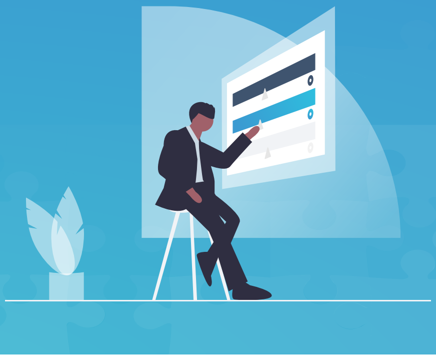
5 Quick Guide for Setting Up an Ambassador Program

6 Measure the Effectiveness of the Security Awareness Program

web.wizer-training.com/how-to-build-security-awareness-training

1.Security Awareness Training Essentials

Here we’re going to discuss the most important things you can do right away to secure your company without big budget. Start simple and build a foundation.



It All Starts With Onboarding...

It’s crucial to instill the importance of security from the very beginning. New hires are often targeted by cyber criminals because they don’t know many co-workers and are more likely to follow direction from someone who pretends to be an executive.

What's in It for Me?

yber criminals are indiscriminate and often use the same methods to hack organizations and individuals. People are more accepting of learning when it’s personal. So make training personal and teach employees how to protect themselves at home, they will soon apply the same behavior at the workplace.

Stay Away From Just Ticking the Compliance Box

After all, we just want our employees to learn something and change their behavior, so take the time to explain why you are implementing the program. If they don't understand the importance of security, then they won't take it seriously. And don’t make it a once a year thing, it should be a continuous effort all year long.

Get the Boss (Or leadership) to Buy-In

Show how security training aligns with organizational goals and specific targets. Remind them that they have a huge target on their back because they have access to valuable and sensitive information. This is also where compliance can help.

How to Convince Your Boss to Invest in Security Awareness

Getting the Employee to Buy-In

Employees will probably complete training if they are forced to, however it is much better to get their buy-in. Establish a supportive presence by creating a circle of influencers that will act as ambassadors of the training program

Your Ambassador Program

Keep It Simple and Real

Don’t assume employees have a technical background, so use simple terms and real life examples they can relate with. And don’t make it childish, adults don’t appreciate content appearing like it was taken from a kids TV show like “Dora the Explorer”.

Make It Easy to Consume

After all, we just want employees to learn something and change their behavior, so take the time to explain why you are implementing the program. If they don't understand the importance of security, then they won't take it seriously. And don’t make it a once a year thing, it should be a continuous effort all year long.

2. What Topics Should Security Awareness Include?

So, how do you decide what topics to include in your security awareness training. There is no one-size-fits-all answer, however to increase engagement you will first need to grab their attention.

Start With Showing Them Personal Benefit

For example, teach them how to secure their social accounts, photos, bank, and how to ensure their kids stay safe online. Then show how the same principles are applied at work.

The key is to blend personal benefit with work related training. This can be done by splitting training into 3 categories:

Protect Yourself

Protect Your Devices

Protect Your Data

When taking this approach, it will be easier to refresh content every year. Instead of replace one phishing video with another, you can include new threats that involve phishing, such as COVID-19 related scams.

How to Protect Yourself?

Personal

- Identity Theft
- Social Media Safety
- Common Scams (Job Scam, Fake Check Scam, Shopping Scam, Covid-19...)

Business

- Phishing, Smishing, Vishing
- Wire Fraud
- Work Related Scams like HR Scam
- Work From Home
- Insider Threat
- Public Wifi

How to Protect Devices?

Personal

- Mobile Safety
- Internet of Things Safety

Business

- USB Safety
- Laptop Safety
- Physical Security

How to Protect Your Data?

Personal

- Strong Password
- Multi-Factor Authentication
- Protecting Your Privacy

Business

- Preventing Data Leaks
- Avoiding Ransomware

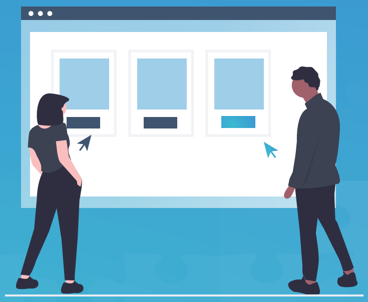
Next, you will need to address the different regulations you need to comply with, such as PCI, GDPR, HIPAA etc…

Now You Can Start Plugging in Training Videos Similar to This

You can find videos on Wizer Platform

3.How to Engage Your Employees?

Security Awareness is about changing people's behavior, therefore the focus should be on them, and what's better than showing what's in it for them?



Quit That Bullshit

Use conversational language to explain things and skip the technology jargon, instead use relatable terms. For example, most people have never experienced a "Data Breach" in their personal lives, but they probably know someone who was “scammed” or “hacked”. We created a quick dictionary to explain simple technology terms.

Wizernary (Geek to English)

Do not baffle with bullshit or blind with science... This is NOT a slightly off-kilter tribute to W.C Fields, but a reminder that, as an industry, we HAVE spent TOO many years trying to baffle people, outsmart them or simply tell they don't understand

Chris Roberts
Wizer's Hacker

Get to The Point Because Our Attention Span is Short!

Let's face it, security awareness training isn't everyone's favorite video genre. Many feel they barely have time to do the work they're paid for, let alone with the same 45-minute video from last year. So if you want people to remember anything, keep it short and to the point. Yeah this is can be done, all of Wizer's videos are 1-minute long, and many are free.

Make It Relevant

Keep content fresh and relevant, nobody wants to watch the same exact video over and over again… and make it personal. For example, for Valentine's day we created a video "Nobody Loves you on the internet" and a "work from home" video during COVID-19. You can check out our [awareness calendar here]

Create Easy to Consume Content

Create content that is frictionless to consume! Follow patterns people use to consume content to increase engagement. For example, almost everyone today uses their mobile devices to watch videos, so go mobile! Make sure employees can do the same with your content. Secondly, set up a one-stop shop for everything security related and make sure they know how to access it. Lastly, use single sign-on or something similar, because you don't want your employees prevented from accessing this knowledge base just because they forgot their password.

Make It Personal

Most scams that target individuals like the “Job Scam”, “Fake Check Scam” and many of the social media scams (more scams), follow the same attack patterns that target companies. The main difference is in the context, so instead of impersonating your boss, the scammer will impersonate a buyer who wants to buy your iPhone or a recruiter with a once in a lifetime job offer. Once people learn how to protect themselves and their families, they will soon apply the same behavior at the workplace.

In this guide you will learn all about the internet threats for your kids, how to teach your children to stay safe and what to do in case it happened!

READ MORE

Scammers are getting smarter so we need to stay up to date and protect ourselves from potential threats

READ MORE

4.How to Get Executive Support for Security Awareness?

Help Make Money

Security is like car brakes. They were invented as a solution for going fast. It's the ability to stop quickly that allows us to travel fast. Without brakes we would all be driving very slowly. Security is about creating a safe environment for the company to grow fast without crashing. We need to align security with the business goals. Once we know the business goal, we can then create a safe environment for the business to grow fast. For example, if the business wants to improve collaboration with partners, the security team should offer to set up a secure collaboration and security training for them. Instead of a general statement that “security is important”, focus on security that is aligned with the business objectives.

Save Money

Many compliance regulations require employees to complete annual security awareness training. So this is an easy one, it is basically a “must do” type of activity. However instead of just ticking a checkbox, conduct security awareness the right way to act as a force multiplier for the security team. Training employees will result in less fraud, compliance fines, data breaches, money loss, etc.

Protect Brand Reputation

Brand reputation is more important than ever. Many companies have dedicated people monitoring social media for any mentions of the company and respond immediately. If employees are not training on how to be respectful on social media or how to represent the brand, it could be very costly to the brand reputation. Also, privacy is a big issue today. If customer data is leaked the resulting damage to the brand can be significantly higher than the compliance fines.

5. Quick Guide for Setting Up an Ambassador Program

What is the Ambassador Program?

Employees will probably complete security awareness training if they are forced to, however, it is much better to get their buy-in by engaging them on an ongoing basis. A good way to do this is to establish a group of influencers that will act as ambassadors of the security team to help create a positive security culture.

What's Included in the Ambassador Program?

- How to Identify Your Brand & Choose Ambassadors
- Train, Set Expectations, & Create a Hub for Communication
- Give Them a Voice and Provide Feedback
- How to Make Everything Simple and Fun!

Ambassador Program Guide

Visit the Ambassador Program Page

6. Measure the Effectiveness of the Security Awareness Program

So how can we measure the effectiveness of a security awareness program beyond the compliance reports that show us how many employees completed training and other criteria?

The key to measuring the effectiveness of a security awareness program is to test specific segments vs the entire program. One way is using A/B testing. So let's say we want to test the hypothesis - **Having an "external email" warning will help employees detect phishing emails**. Send a simulated phishing email to employees, half with the warning and half without, and analyze the results. In this case, the result is that an "external email" warning does help to reduce phishing clicks.

However, what about the hypothesis that - **extra training for those who failed the phishing test will help them avoid failing future tests**.

We should always be testing in order to validate that our initiatives are effective. Now let's review some of the indicators that show us that the employees' awareness is improving.

Are People Participating in Non-Mandatory Training?

When people proactively consume your content it is a great indicator they are interested and engaged. So offer optional training like "Online Family Safety" or lunch and learn sessions, and track how many people signed up or took the training.

How Deep Do They Go?

If you have analytic tools you can measure how deep people dig into your content, similar to how it's done with your website. For example, how many pages did they view, how much time did they spend consuming your content, etc. The more content they consume the more engaged they are, but this also requires high quality content.

How Many Requests for New Technologies?

Prior to training people, they may have used unauthorized apps to bypass security controls - commonly referred to as "Shadow IT". If people are now asking for permission to use new technologies, it is a sign they understand the risk and wish to mitigate it. This also shows healthy collaboration with the security team where people are not afraid to ask for assistance.

Is the Security Team Involved in More Projects?

Measure how often people are proactively coming to the security team for help to ensure new projects are 'secure by design'?

How Many People Reported Phishing, Loss Devices, or Other Incidents?

When security awareness is going up, you'd expect to see an increase (at least initially) in the accurate number of reports coming into InfoSec.

Is There a Decrease in the Amount of Clicks From Phishing Tests?

Phish testing puts the effectiveness of security awareness training to the test by reinforcing what has been presented. Results of the testing are evidence of effectiveness, or not. Monthly reporting can allow you to focus on the greatest areas of risk and provide a course of action for improvement, whether it's customized training or modifications to security policies.

Is There a Decline in the Amount of Confirmed Incidents?

When your security awareness training is effective, you would expect to see an overall decline in the amount of incidents year over year.

Are the Number of Policy Violations Going Down?

Adhering to security policies shows maturity in the security culture. It is usually a result of understanding why we implemented these controls and an open door to the security team. Instead of bypassing these controls, people feel comfortable reaching out to the security team

Do Employees Ask Questions?

A great way to measure engagement is to track how often employees ask questions. This could be through a ticketing system, google forms, or just in person.

Observe People's Behavior

Similar to how we observe our kids behavior when displaying respect for others, we can also do the same simply by walking around the office. You can observe people's behavior, for example how often sensitive information is laying around or do people still use sticky notes with their passwords. Some examples are do people check badges of others they don't know, has tailgating increased, are assets left unsecured, or are doors closing completely.