WELCOME TO THE SECURITY AWARENESS PROGRAM PLAYBOOK!

Your job is to create, launch, and manage your organization’s security awareness program. Where do you even start? It’s a daunting challenge that leaves many people with more questions than answers. That’s why we’ve put together this guide with some tips and tricks to help you create an awesome DIY awareness program!

The following pages are full of information that will aid you in the initial planning stages. At the end of this guide, there is a worksheet that will help you begin laying out your in-house security awareness program. To get you started, here are some other resources to assist you along the way.

RESOURCES FROM THE SECURITY AWARENESS COMPANY

FREE CONTENT ARCHIVE · free.thesecurityawarenesscompany.com
We’ve revamped our freebie archive, so check it out to download FREE awareness materials! Newsletters, posters, videos, and more. We update it every month, so bookmark it and come back later. Yes, it’s all really free. No strings!

TWITTER · twitter.com/secawareco
By following the right accounts, your newsfeed can be full of infosec news, tips, and tricks. Follow us for access to FBI-issued security alerts and important stories posted around the industry.

BLOG · thesecurityawarenesscompany.com/blog
We post a wide range of articles that you can use in email blasts to your employees. Look through our archives for tons of advice on running successful awareness campaigns, as well as simple tips that appeal to the average user.

YOUTUBE · youtube.com/user/thesacompany
Our channel is full of videos that you can use to supplement existing materials and/or to teach key concepts in short, easy-to-understand snippets. Be sure to check out our music videos as well!

PAPER.LI · paper.li/secawareco
This service keeps you up-to-date with our daily newspaper, which aggregates all the top stories from our Twitter feed, our partners, and other social media outlets. A new edition is available every morning!

Some final words before moving forward...

You can’t change users’ behavior without changing their mindset, so we believe in approaching security awareness from an advertising and marketing standpoint. We find inspiration in the same places all the top advertising firms find theirs, and we take cues from pop culture and web trends as well as eLearning giants and industry experts. Think about your awareness program as a messaging campaign. Focus on regularity, frequency, and relatable content. By making awareness content personal, it will resonate with your users much more than if you just focus on policies and compliance. By using regular and frequent messaging—such as posters, short videos, or games—you will reinforce your messages much better than by relying on once-a-year training. Make awareness part of your company culture and it will become part of your users’ mindsets. Then you’ll start to see a shift in behavior and a shift towards more security.
Every path to success begins with a well-planned strategy. Follow our Circle of Awareness to help you build and manage an awesome security awareness program. These eight steps will help you get on the right track towards shifting your users’ mindsets and changing behavior. Pretty soon you’ll have a whole team of human firewalls!

**CIRCLE OF AWARENESS**

**ONE**

What are your goals? What compliance guidelines affect your organization? How many users? Do you need to train contractors and remote workers? Do you have a global presence and need for translated materials? Do you need an LMS (learning management system) or hosting solution?

**TWO**

Does your company culture encourage humor, games, contests, or other fun learning methods? Do you have strict brand guidelines that must be followed internally? Does your company already encourage professional development for employees or will there be pushback for more training?

**THREE**

What are you trying to accomplish? What would you like to improve? Do you want to create a company culture of awareness? Do you have a specific measurable goal of reducing calls to the help desk by 15%? Do you want to just meet compliance regulations or actually educate your users? Make sure everyone is on the same page regarding the goals of the program.

**FOUR**

This is often the trickiest part. How much money are you allowed to spend to make this program amazing? Does the budget cover the cost of the training materials and maybe additional staff to help manage the program? Does the budget include a hosting solution? Enough licenses for all your users around the world? Do you need translations?

**FIVE**

Your plan is set, you’ve created or purchased materials, and you’re ready to launch! Make it fun, shout it from the rooftops, use email and the company intranet, and posters around the office. Hang art in the restrooms and public areas. Get creative! Make a big deal about it.

**SIX**

Do you have a launch date? Take time to plan! You can’t do it all at once. Create a content calendar, a release schedule, and an assessment plan. Predetermine how you will host the training, what types of training you’ll use, how much of it will be mandatory, what you’ll give your users in exchange for completing it, etc.

**SEVEN**

Your plan is set, you’ve created or purchased materials, and you’re ready to launch! Make it fun, shout it from the rooftops, use email and the company intranet, and posters around the office. Hang art in the restrooms and public areas. Get creative! Make a big deal about it.

**EIGHT**

Using the metrics you’ve collected, see where you’re improving and where your users still need help. Do you need to make more of the training mandatory? Are the assessments too hard or too easy? Would your users react more favorably to games or animated videos? Get feedback, tweak the system, and go forth.
GETTING FUNDED

How to Convince Your Boss to Let You Spend Money on a Security Awareness Program

One of the biggest hurdles a security team has to jump is getting a budget that meets their needs. Often, they’re asked to accomplish a mile-long to-do list with shoestring resources and little support from management. But what happens when a data breach occurs? The organization faces tough monetary losses and blame trickles down to the security team, whose underfunded, patched together awareness program failed.

So how can you convince your boss to provide a big enough budget that will allow you to do your job?

The answer comes down to motivation. Humans are motivated primarily in two ways, both of which can help you convince your boss to increase spending and provide you with the appropriate amount of resources.

Fear and desire: these are the reasons we do anything. They are the motivating factors behind every decision people make hundreds of times every day. If you’re worried you’ll be late to work, you leave the house a little early. Worry is a form of fear. Wanting to impress the boss with your hard work ethic, you show up to the office before others. Want is just another word for desire.

Most organizations are scared to death of data breaches. What would happen if your organization got breached? The average global cost of a data breach is estimated to be hundreds of dollars per compromised record. Beyond monetary concerns, organizations face damaging their reputation and losing the confidence of clients. The fear of financial loss, data loss, or reputational damage is what leads to most organizations realizing they need security awareness training. The trouble is if the fear isn’t strong enough, the security awareness program won’t receive the level of priority it truly deserves.

And therefore, it is your job to scare the living daylights out of the right people.

**FIRST:** Figure out what your organization is most afraid of—losing money, data, clients, or reputation.

**SECOND:** Learn which language to use when talking to decision makers. Do they speak dollars, identity theft, followers...?

**THIRD:** Do some research. Find stats to scare your bosses. Find the companies that you don’t want to emulate and use them to your advantage.

It will probably take more than one conversation. Much like awareness training itself, this is not a one-and-done situation. It might take teaming up to some other departments that will back you up, and it might take putting your research on display more than just once. Think about the scary research out there about tobacco; we know it causes cancer. Often, people are not truly motivated by the fear until they see it first hand, or until they’ve seen the consequences. Get ready to act like a broken record so you can train your users and secure your organization!

People are often more motivated by desire than by fear. Many people exercise not because they’re scared of heart disease or osteoporosis, but because they want to look good and feel good. Many people work hard and long hours not because they are worried they will be passed over for a promotion, but because they desire to earn more money.

While some organizations fear data breaches and public humiliation, other companies want to be a step ahead of the curve. Their executives want to be on the forefront of progress, with secure employees who make smart decisions not out of fear of losing their jobs but because they are cyber savvy users. Some organizations are not concerned about meeting compliance mandates but actually want an educated army of security aware individuals working the front lines of defense. If you proactively train users instead of reactively, results will skyrocket.

Strong leadership means encouraging a healthy, happy, secure work environment that promotes professional educational development. They want to impress your clientele with your users’ security awareness. Your bosses just want a safer internet for everyone and know that educating users is the place to start.

The Final Word

We all know that effective security awareness training can secure an organization from the inside out, but sometimes it will take a little extra coercion to get the C-levels to sign off on the money required to do so. It’s up to you to figure out what motivates your upper levels and then use research to help you exploit that motivation to everyone’s advantage.

Most organizations are scared to death of data breaches. What would happen if your organization got breached? The average global cost of a data breach is estimated to be hundreds of dollars per compromised record. Beyond monetary concerns, organizations face damaging their reputation and losing the confidence of clients. The fear of financial loss, data loss, or reputational damage is what leads to most organizations realizing they need security awareness training. The trouble is if the fear isn’t strong enough, the security awareness program won’t receive the level of priority it truly deserves.

And therefore, it is your job to scare the living daylights out of the right people.

**FIRST:** Figure out what your organization is most afraid of—losing money, data, clients, or reputation.

**SECOND:** Learn which language to use when talking to decision makers. Do they speak dollars, identity theft, followers...?

**THIRD:** Do some research. Find stats to scare your bosses. Find the companies that you don’t want to emulate and use them to your advantage.

It will probably take more than one conversation. Much like awareness training itself, this is not a one-and-done situation. It might take teaming up to some other departments that will back you up, and it might take putting your research on display more than just once. Think about the scary research out there about tobacco; we know it causes cancer. Often, people are not truly motivated by the fear until they see it first hand, or until they’ve seen the consequences. Get ready to act like a broken record so you can train your users and secure your organization!

People are often more motivated by desire than by fear. Many people exercise not because they’re scared of heart disease or osteoporosis, but because they want to look good and feel good. Many people work hard and long hours not because they are worried they will be passed over for a promotion, but because they desire to earn more money.

While some organizations fear data breaches and public humiliation, other companies want to be a step ahead of the curve. Their executives want to be on the forefront of progress, with secure employees who make smart decisions not out of fear of losing their jobs but because they are cyber savvy users. Some organizations are not concerned about meeting compliance mandates but actually want an educated army of security aware individuals working the front lines of defense. If you proactively train users instead of reactively, results will skyrocket.

Strong leadership means encouraging a healthy, happy, secure work environment that promotes professional educational development. They want to impress your clientele with your users’ security awareness. Your bosses just want a safer internet for everyone and know that educating users is the place to start.

The Final Word

We all know that effective security awareness training can secure an organization from the inside out, but sometimes it will take a little extra coercion to get the C-levels to sign off on the money required to do so. It’s up to you to figure out what motivates your upper levels and then use research to help you exploit that motivation to everyone’s advantage.
WHICH IS BETTER: PROACTIVE USER TRAINING OR REACTIVE USER TRAINING?

With security awareness, the answer is BOTH!

Many clients come to us in crisis: “Help! Too many of our employees are falling for phishing scams!” or “Help! We got breached last year!” or “Help! We didn’t pass compliance and need to train our users!” They reach out to us, panic in their voices and desperation in their eyes because they see dollar signs and lost trust from their own customers. To them, they’re in a sinking boat full of holes and need us to help them fill those holes with plugs as fast as we can.

We also have a lot of clients come to us because their peers have been breached. They are on a tight schedule, sometimes trying to get in under a deadline to impress an exec or beat a compliance deadline, but they haven’t been hit yet and want to keep it that way.

Ideally, we should try to prevent situations from arising by teaching users how to create strong passwords, how to recognize social engineering attacks, how to prevent personal identity theft, and why data classification is so important. But if something bad in the cyber world does happen, we should also react with training, not as a punishment but rather to reinforce lessons we’re already teaching, and to correct unsecure and careless behavior.

BOTH WAYS—REACTIVE AND PROACTIVE—RESULT IN AWARENESS PROGRAMS. BUT WHICH WAY IS BETTER?

TIPS & TRICKS

USE MINOR MISTAKES AS LEARNING OPPORTUNITIES

If someone forgets their badge, can’t remember their password, or neglects to lock their desktop screen before getting up, these are not huge infractions but can be a good opportunity for you to remind them of policy.

MAKE IT PERSONAL

People care way more about themselves than they ever will about the organization they work for. Give them some useful information about securing their own lives & protecting their own privacy. At the end, just be sure to say, “Hey, by the way, all this stuff we’re teaching you? Do it here at work, too.”

REQUIRE TRAINING FOR THE WHOLE GROUP

If something bad happens and everyone knows about it (an insider gone bad, a data breach, an outside attack, etc.), let the employees know that’s the reason for the training. One bad apple does spoil it for the whole bunch. No one wants to be the bad apple.

NEW HIRE TRAINING IS SUPER IMPORTANT

“Start ‘em while they’re young,” is something we’ve all heard about teaching kids whatever particular subject matter is at hand. Don’t wait until employees have been there six months. Catch them while they’re new. Hit them with awareness training from the get-go to ingrain it into their work behavior.

PHISH YOUR EMPLOYEES

You should also require additional training for anyone who fails. This is an immediate reactionary, defensive form of training since the person who falls for the phishing email will receive an immediate learning opportunity and see what they did wrong.

ONCE-A-YEAR WON’T CUT IT

For employees who have been there more than a few months, don’t just rely on a yearly compliance review. Remind them regularly of policies, best practices, and why security awareness should be at the forefront of their minds in everything they do.
CREATING YOUR OWN SAP

So you’ve been tasked with building a security awareness program? It’s a tough job. You’ve got to figure out how to tell people about the program, teach them the security lessons that are most important to your organization, and stay within a tiny budget.

What’s even tougher is figuring out which lessons to teach, which messages to focus on, and what kinds of materials work best for your organization. Do you need to use an LMS to track user data? Will your users prefer watching one short video every month, or one long video every quarter? Should you offer incentives for the employees who finish the training?

Every organization is different, and we can’t tell you how to run your security awareness program. But what we can do is offer you some free resources, tips, and helpful hints to make the process a lot easier.

FIND INSPIRATION: The internet is full of awesome stuff but sometimes the sheer amount of information can be overwhelming. Follow some infosec people and companies on Pinterest to find useful infographics, posters, quotes, and blog posts you can send to your users or use as inspiration for making your own materials!

MAKE IT PERSONAL: In order to change behavior, you’ve got to change their mindsets. And the only way to change the way they think is to get them to CARE. If you get them to care about protecting their family and teach them how they can be safer online and at home, then it’s easy to slide in that organizational reminder. “Oh, by the way, all that stuff we taught you about protecting your family? Do it here at work, too!”

REMEMBER USERS FREQUENTLY: We live in an ADHD world. No one has the attention span to read a policy book front to back (did you?). But people are used to watching short, 3-minutes-or-less YouTube clips, and reading quick 1-page-or-less blurbs in magazines. Every month, pick a topic (phishing, social engineering, passwords, backup) and create short newsletters and/or videos on that topic, distributing them at the same time every month. The regular (but not annoyingly frequent) reminder will bring security to the forefront of everyone’s minds.

KEEP IT SIMPLE: Most users don’t need to become experts or even need much technical know-how in order to be security aware, so don’t try to overload them with technical jargon, complex diagrams, or intimidating cyber speak. Keep things simple by teaching the basics in easy-to-understand language. Not everyone understands what ‘social engineering’ is but everyone understands what a con artist is. So teach about the dangers of social engineers by making real world comparisons to con artists and scammers to drive the point home.

DON’T DO IT ALL AT ONCE: Start slow. Build momentum. Don’t start with everything all at once. Unless you have a huge dedicated staff, you’re not going to have the time, manpower, or mental bandwidth to handle all things all at once. This means instead of doing a really awesome job and rolling out an eye-catching, engaging, and effective awareness program, you’re going to end up with something poorly developed and haphazard. It’s not going to be successful, and you’ll be frustrated. So don’t try rolling out a program that includes training modules, videos, posters, newsletters, and interactive games, and a gamified LMS all in the same month or quarter—and certainly don’t just dump all of your awareness materials on an intranet and hope people will click on them.

ESTABLISH WHO’S BOSS: Too many cooks in the kitchen will ruin your program. Find out who has to be involved in the decision process, then streamline as much as you can. One person should be the single point of responsibility for the entire program.

USE A SPOONFUL OF SUGAR: Humor is an effective learning tool. Put a smile on your users’ face, and they will be more likely to remember the lesson than if you go at it with cut-and-dried policy language. Use graphics and videos, use some pop culture examples, use cats. Do whatever you need to make them take their security awareness medicine, so to speak.

BRAND YOUR PROGRAM: A recognizable brand and theme helps users identify anything you present and drives the message home. Mascots and character development assist in teaching awareness.

RINSE & REPEAT: Security Awareness is like advertising. In order for the message to stick and for the user to take action, it’s got to be in front of them multiple times during a year. Once-a-year training is not enough. Quarterly training is okay but monthly and/or weekly reinforcement is even better. Treat your SA program like a marketing campaign using monthly newsletters, screensavers, posters, weekly email tips, videos, quizzes, and games to engage and educate your user population. The more they see the message, the longer it will stay in the forefront of their minds and the better their behavior will be.

AVOID DEATH BY POWERPOINT: Don’t waste your time creating long presentations that will bore your audience. You want them paying attention, not playing Candy Crush while you drone on about security policies. If you have to use a PowerPoint presentation, use funny photos and avoid a lot of text on the screen. Use videos on YouTube to get your point across. Entertain your users into actually learning something.
## SECURITY AWARENESS PROGRAM PLANNING WORKSHEET

<table>
<thead>
<tr>
<th>AWARENESS CAMPAIGN NAME:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAD CAMPAIGN MANAGER:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAMPAIGN TEAMMATES:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOES YOUR PROGRAM AND/OR DEPARTMENT HAVE A BRAND? (Colors, logos, mascot, etc.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CREATE PROGRAM GOALS.
(Enter one to three goals and how you plan to tackle each goal. Example goal: create on-boarding security training for new employees. Example plan: create short presentation, create quiz, print notes.)

<table>
<thead>
<tr>
<th>GOAL ONE:</th>
<th>GOAL TWO:</th>
<th>GOAL THREE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WE WILL TACKLE THIS GOAL BY:</td>
<td>WE WILL TACKLE THIS GOAL BY:</td>
<td>WE WILL TACKLE THIS GOAL BY:</td>
</tr>
</tbody>
</table>

### CIRCLE THE THREE SUBJECT AREAS MANAGEMENT IS MOST CONCERNS ABOUT AND WILL BEST HELP YOU MEET YOUR GOALS.
(For example, if your goal is to reduce the number of users who click on phishing links, you might want to focus on Phishing and Social Engineering.)

- General Security Awareness
- Social Engineering
- Executive Awareness
- Compliance Regulations
- Safe Surfing
- Acceptable Use
- Physical & Non-Technical
- Company Policy
- Mobile & the Cloud
- Security Phishing
- Data Classification
- Passwords

### WHAT KIND OF CONTENT WILL YOU START WITH?
(Enter Emails, PDF newsletters, posters, screensavers, eLearning modules, videos, animations, in-person training, games, etc.)

### HOW WILL YOU DELIVER CONTENT?
(LMS, intranet, email blasts, etc.)

<table>
<thead>
<tr>
<th>CAMPAIGN START DATE:</th>
<th>FIRST ASSESSMENT DATE:</th>
</tr>
</thead>
</table>