

# Security Awareness

# 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 security culture. This document was designed to help you set up an ambassador program.

## What's Your Story?

Yeah, brand identity for the security awareness program is really important. Pick a cool mascot and logo, and include it everywhere. Make your program recognizable with appealing brand awareness that shines. Reach out to your marketing team, communication team, and HR for assistance and get them onboard as program stakeholders.

## Now Let's Choose the Ambassadors

It's best to let the business help select the ambassadors. Here are a few tips on how to accomplish that:

- **Ask executives from different departments to nominate candidates from their teams.** This will help create a group that has a diversity of thoughts.
- **Make sure you have ambassadors at every level/rank of the organization including the executive team.** When one of their own is working with them the message is delivered better and it creates an environment that is more open for feedback.
- **Choose ambassadors that are not technical.** They should know the business, how data is consumed by their team, and the pain points. Their role is to serve as a bridge between the business and the security team.

- **Pick people that are approachable, outgoing, and good at presenting**, after all, they will be the go-to people for their teams.
- **You don't need one ambassador for every department.** Think about the functional distribution of ambassadors to people, for example, one ambassador can serve several departments if these departments regularly meet or collaborate.
- **Make sure the ambassadors have 3- 4 hours a month set aside for this role.**

## Train Them

Train the ambassadors and make it a fun and interesting experience. To get their buy-in, treat security as a life skill and make it personal. For example, bring speakers that can teach them how to keep their kids and family safe. If possible bring doughnuts :). Another idea is to show them Defcon videos, YouTube, or Wizer videos...

## Set Expectations

Because the ambassadors are not technical, make sure they understand that you are not expecting them to know everything... Obviously they won't become security experts just because they are ambassadors. Their goal is to be the eyes and ears on the ground and act as a focal point and a bridge between the teams and the security awareness program.

## One Stop Shop

Create a hub or portal where ambassadors can easily obtain information to support their teams. This portal will include videos, news, announcements, and basically everything cyber security related you want them to share with their teams. As a one stop shop, take advantage of integrating your ticketing

system or creating google forms to make it easy for them to report incidents or ask questions. Having materials in a central location will take the pressure off the ambassadors because they will know there are resources there to help them when they get stuck.

## **Give Them a Voice**

Engagement starts with giving people a voice... so set up a workplace where they can share their own views and converse. It can be over Slack, Teams, Sharepoint, or whatever makes it easy for them. Encourage them to share security and privacy related news items they find online. Once a month create a company wide newsletter and include insights from the things they share and don't forget to give them credit.

## **Always Give Feedback!**

Feedback shows you care! This is core to building relationships with employees. If you don't show that you care they won't care either. For example, when someone reports a phishing email, phone scam, or any unusual activity, get back to them. Let them know if that was a real threat or just a marketing email that they can unsubscribe from. Responding shows that someone is reading their email and that their feedback is appreciated, and will also encourage employees to actively report things they see.

## **Clear Objectives**

First of all, don't forget to give them a budget for doughnuts (or something special), otherwise, no one will come to their meetings :). But more importantly, the ambassadors need to understand what is expected of them.

For example:

Hold monthly meetings with their team and share emerging threats. Train the team on how to transfer files securely. Find out about new or ongoing projects and advise if they need to talk to the security team about it. Also, encourage team members to report phishing emails, phone scams, or anything unusual.

Pick one small topic every month or two, make it simple and get the ambassadors to teach their teams on it. Over time, you will raise the bar across the organization.

## Make it Simple

Lastly, if you want people to remember anything, then make it simple. You may have a 100 page security policy that explains everything, however, it's more effective to distill it into key components. It's better that people remember these key points than nothing... Here's an example.

### Top 5 points you want to teach:

- **Think before you click**
- **Think before you send**
- **Be respectful online**
- **Keep files and devices secure**
- **Report anything unusual**

## It's not Forever...

You will be surprised but many will want to volunteer! Consider ways you can share the role or have multiple ambassadors in a team participate if they are interested. Ideally, the ambassadors are there for an ongoing role, but you could also have them share or rotate after a period of 12 months. Do it in a way that fits the culture of your organization, but be as inclusive as possible.

## Resourcing...

Ensure you have adequate resources engaged in the security team to run the program on an ongoing basis. This will include ongoing training, personnel to manage ambassadors as they join and leave the organization, creating materials, and answering questions. This is an ideal activity to give to a more junior member(s) of a security team such as grads/interns to manage under the direction of a leader as they will be able to demonstrate creativity and engagement across the organization.

It is critical that resourcing is continual, without management the program will be unsuccessful to sustain.

## Make it Fun...

**Don't forget to keep it light hearted and as fun as possible.** Try to gamify things as much as possible. Hold phishing competitions between ambassador teams to see whose team have the lowest click rates, hand out goofy phishing trophies, awards, etc. The more fun and engaging you can make it, the more successful it will be!