HOXHUNT

How to create behavior change with security awareness training?

A practical guide

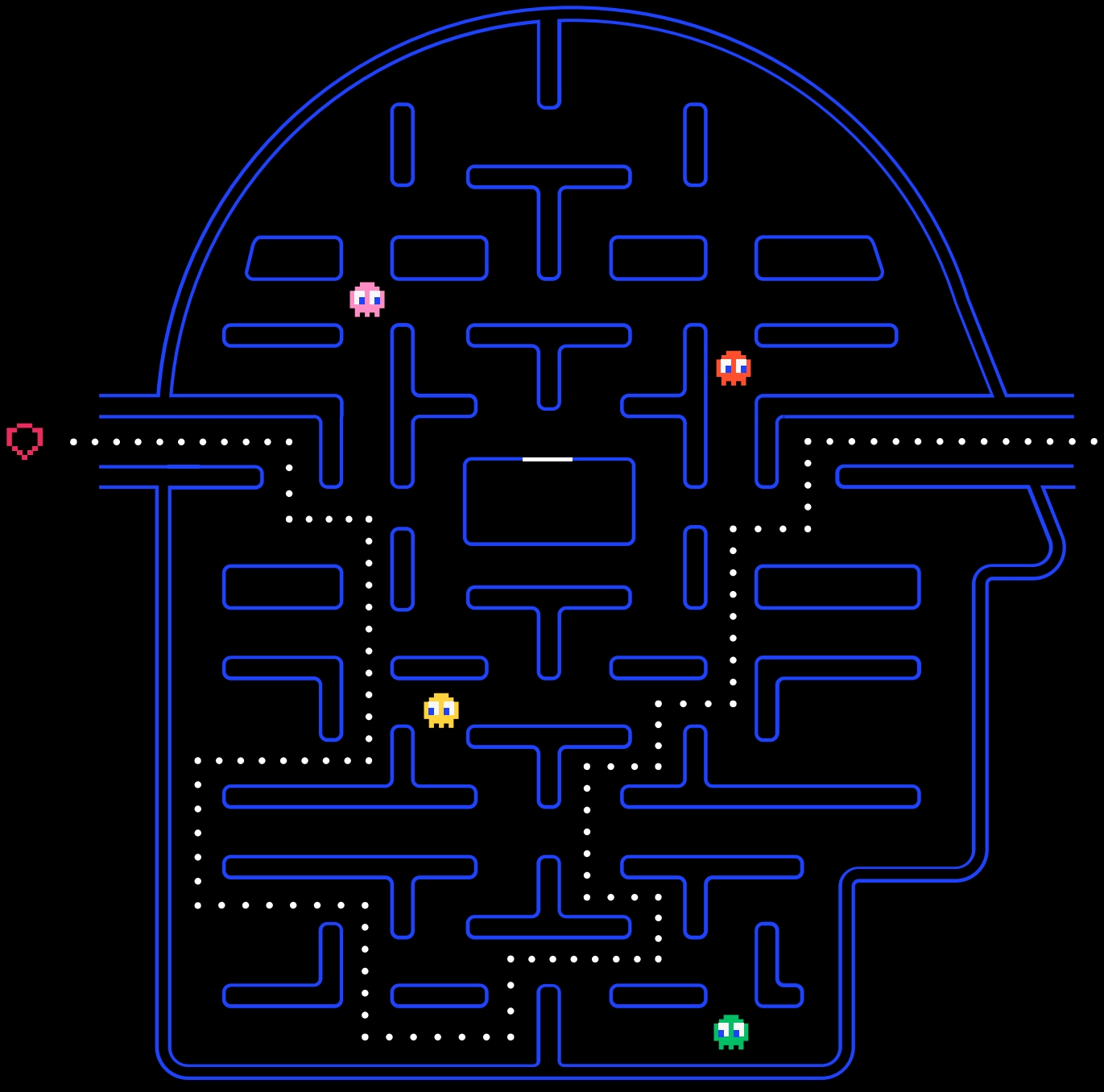

Table of Contents

Introduction

Conducting security awareness training is not enough for reducing risk. When people receive in-frequent, once a year or quarterly training, they get a lot of information at once on how to be responsible when they face online threats. Without frequent practice, they may not know what to do when they encounter an actual attack. It's not about negligence. It's about not providing people with the right training.

Behavior change is the best way to mitigate the risk related to employees. To strengthen organizational security, people must receive training that results in behavior change, meaning that they know what to do when they see a threat.

Achieving behavior change takes time and practice. That's why quarterly phishing tests are insufficient. The more often the user can practice with real threats, the better they will be able to adopt the behavior of spotting dangers and reporting them.

As social engineering attacks become more sophisticated and increasingly target employees, people play an equally important role in your defense work as technology. With a people-first cybersecurity training approach, you will positively impact people's behavior and organizational risk.

This guide will explain why behavior change is relevant for cybersecurity, the applicable psychological mechanisms, tools, and theories to achieve behavior change, and how you can start to carry out training that truly reshapes people's behavior.

Why does awareness training not lead to behavior change?

Awareness training is not sufficient for creating behavior change. Cybercriminals know that people receive very high-level awareness training so a well-crafted attack can easily help them to achieve their goals. For cybercriminals, the easiest entrance to your assets and systems is to attack your employees and hope that they will fall for the bait.

What's the problem with awareness training?

The name says it all. It tends to focus solely on awareness instead of having a real impact on people's knowledge and skills. Awareness training uses policies and strict rules (many do's and don'ts), and it's typically infrequent, one-size-fits-all content, and lacks enough practice.

When there are too many rules, people can perceive cybersecurity as something negative. It's uninspiring, not motivating, and it fails to engage people.

Awareness does not focus on creating a new, correct habit. Developing a new habit takes time and practice. Without simulations, employees will make errors and easily fall victim to attacks. You can't blame them when they didn't receive good enough practical training to reinforce their skills and behavior.

Moving away from awareness

Awareness and knowledge are not enough. People need to be motivated and engage with practical exercises so that your training will result in behavior change.

Did you know?

Inefficient training leads to errors

Training that lacks frequent practice does not provide employees with enough knowledge and skills to do the right thing in a difficult situation. Even when people know the rules, they may not act accordingly. They can still make a skill-, decision-, or knowledge-based error.

Types of errors

A **skill-based error** occurs during highly routine activities when the individual's attention is diverted from the task because of his/her thoughts or external factors. When a skill-based error happens, people generally have the right skills to correctly perform the task, but they fail to do so.

Decision-based errors are also called mistakes. A decision-based error has two subtypes: a **knowledge-based error** and a rule-based error. A decision-based error occurs when we make the wrong judgment, but we believe that our call is the right action.

A **knowledge-based error** means that the person does not have sufficient or correct knowledge to perform the right action.

Mistakes can happen, but with the right amount of practical training, it's possible to minimize error occurrences.

Behavior change and reducing risk

Employees represent the biggest attack surface for your organization. The more employees you have, the bigger the risk is. An employee that does not receive continuous practical training or decides to ignore the learnings can become an enormous risk for the company.

To reduce risk, cybersecurity training must focus on the goal of behavior change.

Behavior change refers to any transformation or modification of human behavior. Behavior is a computed response to various stimuli, whether internal or external, conscious or subconscious, overt or covert, voluntary or involuntary.

The goals of behavior change in cybersecurity training are the following:

· **Employees must be able to identify threats online and understand that they must not interact with them.**

· **Employees must report potential threats or committed errors to your incident response team.**

When employees learn the correct behavior through frequent training, they are less likely to fall victim to targeted cyberattacks. Instead, they will have the right skills to spot an attack and report it to the security team.

People-centered training that uses behavior science to prevent people from falling victim to social engineering is the best solution for risk reduction. It's a measurable way to show progress and put risk into context. When people report threats, you know that they are learning and acting according to the expectations. You can draw a correlation between people's behavior development and the reduction of organizational risk. Learning by doing will also increase the feeling of personal responsibility for security at work.

Did you know?

Behavior change to fight against social engineering techniques

It's not a surprise that people make errors and fall victim to phishing. Social engineering attacks are sophisticated, and hackers utilize human psychology for crafting their campaigns.

They use persuasion techniques in their campaigns. Their operations rely on using techniques such as fear, trust (higher authority – one of the biggest human drivers – even more effective than greed), desire, greed, curiosity, and urgency. With these, attackers want to establish credibility and trust to persuade people to take action – like giving away passwords, downloading malware, or making a bank transfer.

When people are not conscious of social engineering techniques, it's easy to fall for phishing and other online attacks. That's why we need to teach people to identify online dangers and act the right way to protect the company's assets from attackers' manipulation.

Behavior change psychology and tools

To successfully implement a program that results in behavior change, it’s essential to understand how people behave, what motivates them, or how to influence them.

Psychological influencing strategies integrated into awareness training will teach employees the right behavior online and diminishes high-risk behavior.

The wheel of behavior change

To achieve behavior change, you need to include the three key elements in your training: personalization, shaping through practice, and positive reinforcement.

Training and persuasion techniques: influencing and shaping

Persuasion is the attempt to change attitudes or behaviors or both without using coercion or deception. The two main persuasion techniques for behavior change are influencing and shaping.

How to influence employee behavior?

Using influencing as a persuasion strategy for behavior is challenging. Even when the advice comes from an expert or an authority, people may not follow the rules and processes.

Influencing can work in training, but only when it uses positive emotions. Cybersecurity playbooks often use fear as a primary influencing technique. Fear is a negative emotion, and it likely creates resistance. Other persuasion techniques, such as humor, expertise, repetition, intensity, and scientific evidence are more useful in influencing people.

To successfully change people's behavior, training should influence them. When developing a behavior-changing security awareness training approach, consider incorporating the following 9 influencing factors:

1. The messenger

Who communicates the information? Typically, the information is well received when it comes from an authority.

2. Incentives

People respond to incentives. Could you incentivize them to be more motivated to perform a specific task?

3. Norms

What do other people do or think? How the environment of the employee perceives the training matters – positivity is key!

4. Defaults

We follow pre-set options and rules. Make sure that the rules and the processes are clear and easy to follow.

5. Salience

Is it relevant for us? When training is personalized and relevant it can boost engagement.

6. Priming

Subconscious cues often influence our acts. When people act in a subconscious manner, they don't think about why they do it, they just do it automatically.

7. Affect

Emotions can powerfully influence our actions. When people feel negative about training, it's less likely that they would want to engage with the practices.

8. Commitments

We seek to be consistent with our public promises and reciprocal acts. When people promise to do something, they will be more likely to actually do what they promised.

9. Ego

We act in ways that make us feel better about ourselves. People want to gain something for their benefit. This is why recognition can work well in training.

Using these influencing mechanisms in training can stimulate people so that they will apply the learnings in real-life situations. All these elements need to be seamlessly integrated into your program. Besides these, the training needs to consider the effects of motivation, individualism, and culture on engaging people with the training so that they can adopt the correct cybersecurity behavior.

Individualism and behavior

Employees have different levels of knowledge, skills, and understanding of cybersecurity. They may have previous experiences or perceptions about information security from another workplace. It is challenging, yet necessary, to personalize the training to be suitable for different backgrounds.

To influence people with various backgrounds, focus on personal motivation and personal ability. To form new habits, people first need to overcome negative feelings about security training, measures, and policies. Training that considers people's knowledge, level of skills, language, territory, department, role, co-workers, and more can provide an outstanding personalized training experience.

Culture and behavior

Consider the cultural and environmental factors to shape people's behavior successfully. The communication and the training content must be culturally relevant for the employees. Culture has a powerful effect on how people respond to training and how they behave. People are social creatures and tend to comply with the rules to meet the expectations of co-workers, the environment, or society.

Motivation and behavior

Motivated behaviors always derive from individuals. Motivation is born when people enjoy engaging in an activity, feel satisfied, or attach other positive feelings toward a task. Earning a reward or avoiding punishment can also be drivers for motivation.

People can be motivated to follow the rules they've learned. But when the rules hinder their work, they could start to ignore them.

Do not only incentivize the right behavior but also remove these barriers of motivation, such as:

- **Complicated rules**
- **Heavy reading materials**
- **Unengaging classes and e-learning**
- **Training that's not suitable for the employee's level (either it's too difficult or too easy)**
- **Security obstacles that prevent people from effectively performing their work**

All these blockers could result in negative feelings, also called "security fatigue" and that's when people stop caring about security.

How to shape employee behavior?

To change behavior, it's not necessary to change people's thinking. The shaping technique can have the most significant impact on the actions employees take in security training.

Shaping uses a series of small steps and actions to modify the learner's behavior. The goal is that people would know how to perform a particular action by following specific processes. Shaping is a subtle way of creating a new habit.

Why does shaping work in cybersecurity?

To reduce the organization's human risk, you need to teach employees the correct security behavior through frequent practice.

Personalized training can activate people's critical thinking about email and online dangers. When the reporting process is simple enough, people can effortlessly report threats. When the behavior of reporting is repeated continuously, it can become second nature for the learner.

How to use positive reinforcement for behavior change?

Positive reinforcement is pivotal to the shaping technique. It refers to the introduction of a desirable stimulus after a behavior to make it more likely that the behavior will reoccur. Shaping works best in training when employees receive recognition and feedback for their work as part of positive reinforcement.

For positive reinforcement, stimuli can include awards, rewards, scores, competition, leaderboard, recognition, or feedback. You can get creative and think about what fits your organizational culture the most in terms of motivation.

Feedback plays a vital role in positive reinforcement. People can learn from additional training moments about what they did right and what the clues were. They will then be motivated to report a threat the next time. Feedback and interactive training can trigger that response.

Positive reinforcement is powerful and effective in the long-term. It’s easier to remember learnings and required actions when people relate them to positive feelings.

Avoid negativity and punishment

Removing negativity can seem difficult when you're dealing with a sensitive topic such as reporting threats or the employee's own failure (e.g., clicking on a link or downloading malware). Still, using positive reinforcement will have an encouraging effect on the security culture and people's willingness to cooperate.

Avoid punishment for the wrong behavior. Punishment never helps with correcting behavior, people can become defensive, secretive, or uncooperative. When people don't dare to come forward, you won't have the right information to discover security incidents as quickly as possible.

Let your employees know it's safe to come forward when they've made an error. Positivity is the key here: believe that people try their best to practice safe online habits and enable them to do so.

How to create behavior change with training?

By now you understand that behavior change is critical to risk reduction. You are perhaps wondering how to achieve behavior change. We'll show you how to reshape security awareness training in a way that can truly result in employees adopting the habit of threat reporting.

Pursuing behavior change

Is behavior change for your company? It can work for any company that wants to have a real impact on its human risk profile.

If you already have awareness training and compliance-based training, you should go beyond that. Add a layer of continuous practical training that is impactful both in terms of behavior change and minimizing risk.

If you don’t yet have cybersecurity training, the following Hoxhunt method is something you can easily start doing. You will start to reap the benefits of behavior-changing training almost immediately.

Training for behavior change

To successfully change people's behavior, they need to understand why their support and participation are essential. While behavior-changing training is a must, communication plays a critical role in guiding employees toward safe online practices.

The following elements that are also deeply incorporated into Hoxhunt's people-first cybersecurity training are necessary for behavior change.

1. Practical training

Without practice, employees won't be confident with spotting and reporting threats that get through email filters. Using simulations that mimic real threats can prepare people for facing actual attacks. We truly believe that the only way to secure behavior is by learning by doing it. So don't skip the practice!

2. Continuous and frequent practice

A few simulations a year won't make a difference in how people retain learnings. Infrequent tests certainly won't shape the adoption of the right cybersecurity habit of staying alert and reporting anything suspicious.

People need to receive simulations frequently. At Hoxhunt, we aim to send users at least 36 simulations a year. That's one every ten days. Building the habit with shaping takes time so that's why frequent simulations are essential.

3. Positive reinforcement

Integrating positive reinforcement into the training may not seem like a priority, but it can truly have a meaningful effect on people's emotions and motivation toward the training.

Small steps such as adding recognition (for example, using gamification like collecting stars, points, and showing leaderboards), feedback, and micro-learning mechanisms can motivate people to participate in the training continuously.

Hoxhunt fuses all these positive reinforcement tools into the training so that people keep coming back for further training and learning.

4. Up to date attack simulations

Attackers keep coming up with new attack types all the time. The attacks tend to be well-crafted and hard to spot. New phishing emails could also be referring to recent events. Typically, attacks are preying on people's emotions to harvest their reactions.

Make sure that people are up to date with the latest attack types. They will understand that new phishing emails can be hard to identify. This will help to keep people informed and more determined to spot and report an actual attack.

5. Personalized and relevant content

To make sure that people care about the training, it must be personalized and relevant to fit the needs, skills, and knowledge of the individuals. In addition to personal skill and knowledge level, other factors such as language, geography, culture, department, role in the organization, time spent in the organization, or even teams, collaborators, and tools used should be considered to make the experience as engaging and realistic as possible.

6. Integrated into the employee's workflow

Employees often feel frustrated that security measures interfere with their workflow. It doesn't need to be like that. When people check their emails, they can spot the simulation in seconds – just like they would spot real threats – and report it with a click of the Hoxhunt plugin.

7. Simple reporting process

The reporting process must be easy and effortless. Even when people know they should report a threat, they may not do it if the process is as complicated as calling the Service Desk.

With Hoxhunt, people can use the reporting plugin for reporting simulations and actual phishing emails. It's just a click of a button and only takes a few seconds. And it works on all devices.

Putting risk measurement into context

In another guide, we've written about the metrics to measure behavior change. You can measure how people are progressing in the training and the effect of frequent simulations on how they behave. You can take a look at reporting rates – both reporting simulations and real threats – and the failure rates.

With reporting, your goal should be to engage most of the population so that you know they are developing their skills by recognizing and reporting threats. When training is done right, people keep participating in the training continuously. While failure rates are indicative of people's learning, it's also important that if they fail, they fail in a safe environment so that they can learn from their mistakes.
In addition to measuring the success of the training, the number of reported threats is also a good indicator of behavior change.

Data on the development of behavior change can help to put risk into context. You should be able to quantify the positive impact of training on your risk profile and score.

Defend your organization together with your employees

Behavior changing training is in the toolbox of every forward-thinking CISO. They know that this is the only feasible way to truly lower human risk.

By providing frequent practical training to your employees, you are giving them tangible skills to defend your organization – as well as their own assets in their daily lives.

Is it difficult to adapt this methodology for behavior change? To be fair, doing it manually is almost impossible – especially when you have thousands of employees. It's time-consuming and labor-intensive. If you are trying to keep up with attack trends and create personalized learning tracks for each employee, you must automate the process. Luckily, there are automated solutions on the market such as Hoxhunt.

To successfully decrease human risk, you shouldn't start training from the basics, like awareness posters, videos, or quizzes. Instead, with Hoxhunt you can rapidly start sending simulations to all your employees. When you provide them with positive and engaging training experiences, they can confidently support your defense work. In a company, where people and security teams cooperate for a strong and positive cybersecurity culture, cybercriminals will have a much harder time to find an open door to your assets.


HOXHUNT