HOXHUNT

The fundamentals of behavior-changing cybersecurity training content.

Table of Contents

This guide discusses which fundamental characteristics of training content facilitate behavior change, and how they differ from traditional approaches.

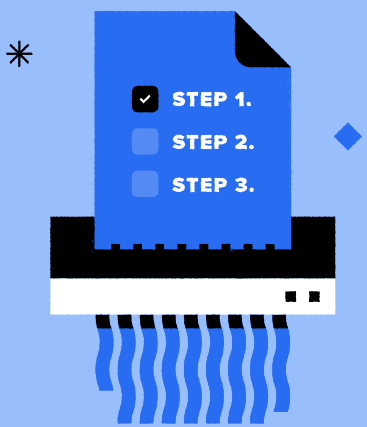
Why simulation training content is important

Security teams must address phishing and social engineering in cybersecurity training as they remain the number one cause for breaches. **According to reports by Verizon and Symantec, 70-90% of breaches derive from phishing or a form of social engineering attacks**. Social engineering is constantly on the rise and it is putting your employees and organization at great risk. Therefore, it is a prevalent danger, and cybersecurity training must address it to avoid negative consequences such as financial losses, stolen data, or brand damage.

There are a variety of attacks continuously putting your employees to the test: phishing through emails, SMS, spoofed websites, and phone scams, in many different forms. Some attacks can be difficult to spot for employees, and social engineers are continuously finding new ways to make them increasingly sophisticated.

The best way to train your employees to recognize attacks is to send attack simulations that replicate realistic threats. Once people start to learn with the help of simulated attacks, they will start recognizing malicious threats alike. As a result, it will become much more challenging for attackers to trick your employees into falling victim to their attacks. With successful training, you will create a strong human firewall, and that's one of the most impactful ways to lower organizational human risk.

Simply sending infrequent organization-wide simulations will not decrease human risk. To change how employees interact with real threats, you need to send frequent simulations with relevant, personalized content. This guide will explain why content is important for achieving behavior change and reducing risk. We will also examine the traditional content development methods that are often believed to be effective, to help you understand why frequent, individualized, and up-to-date content is vital for successful training.



Traditional training content and its shortcomings

Traditional approaches

There are two main traditional content approaches currently used by security teams to simulate threats.

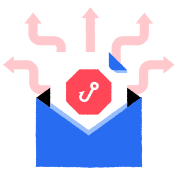
A manual content approach requires a series of steps to set up the simulation content before sending it out. This process is quite complicated and resource-consuming. First, you must set up domains both for the sender email address and the landing page. You also need to create the simulation content manually. To make the phishing emails look realistic, you often use an HTML template to do so. And to resemble real threats you should include simulated attachments. This requires extra work, especially when you want to track your employees' interactions.

With a **tool-based content approach**, you gain access to a library of simulation templates that you can send to your employees. Still, the security team needs to do a lot of manual work related to planning, setting up domains, analyses, personalization, training employees, establishing a process for employees to follow, setting up a threat reporting functionality, threat classification, and incident response. A tool-based content approach isn't scalable when you want to change the behavior of larger workforces with hundreds or thousands of people.

Shortcomings of traditional approaches

While using a manual or tool-based solution is a step in the right direction, both approaches have several shortcomings. Many companies use cybersecurity training to create awareness or remain compliant.

Compliance-based and awareness training is often based on a one-size-fits-all training like e-learning or infrequent phishing tests that won't engage employees because it's theoretical, impractical, and impersonal.



Lack of personalization

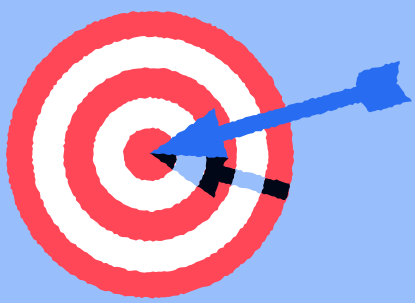
Awareness training doesn't consider the skill and knowledge level of an individual employee. The training could be either too easy or too difficult for the person, which won't engage or motivate them to participate. When the content isn't personalized or doesn't resonate with the employees on an individual level, you can't expect them to know what to do when they encounter real personalized threats like spear phishing.

Employees are seen as a security burden

Traditional approaches see the users as a security burden.
At Hoxhunt, we like to see them as an opportunity. You can't blame an employee for failing a simulation or causing a breach when they haven't received frequent practical training with personalized content. Achieving behavior change takes time and practice. That's why quarterly phishing tests are insufficient. The more often the user can practice with simulated threats, the better they will become at protecting your organization.

Awareness training does not focus on behavior change

It's also challenging to measure the effectiveness of compliance-based and awareness training and whether these help with lowering human risk. The typical awareness training KPIs don't help with quantifying the risk related to employees. Traditional training metrics and KPIs mostly focus on pass rate (whether the employee passed the training) and failure rate (the employee clicked something). Instead, you need to consider if they are proactively engaged in training and whether employees start reporting real threats as a result. When they report both simulations and real threats it indicates that the training is working and impacting their behavior.



Fundamentals for training content to facilitate behavior change

Since manual- and tool-based approaches can't facilitate behavior change training on a large scale, you will need to consider a scalable, continuous, and personalized approach to achieve behavior change.

The need for behavior change

Your training's goal must be to teach your employees to behave the right way when they encounter threats. That's the only way you can truly decrease your human risk profile. To do so, you must improve your employees' internal pattern recognition.
By providing your employees with personalized training content that has identical patterns to real threats, you'll teach them how they can recognize real attacks. Do so repeatedly and it will become second nature for people to recognize and report threats.

The right training content can also help positively improve the employees' perception of cybersecurity training. You can engage employees to keep participating in the training by making content relevant rather than uninspiring and impersonalized

Content characteristics for behavior-changing training

Content is the foundation of behavior-changing training.
If the training content does not have the right characteristics, it will be hard to facilitate the correct behavior. Let's look at the most important aspects of behavior-changing training content.

Variety of content

Your employees can face a variety of threats, whether personalized or not, that aim to trick them into taking the wrong action for your organization. Some threats are far more sophisticated than others. They can look very realistic like common emails from service providers, or even impersonation of managers and co-workers. In short, it is crucial to prepare your employees for every type of threat out there at any difficulty level.

Most traditional tools offer outdated training content that is not relevant anymore. Attackers are innovating constantly to find new ways to trick your employees. Your training must reflect the most up-to-date and innovative techniques. Our users from different organizations report hundreds of real threats daily. We use that information amongst others to develop training content that mimics the most current attack types.

These are the wide range of themes we like to train our users on with simulation examples that are included in each theme:

THEME NAME	EXAMPLES
Online services	Service invitation New feature,new login Account expiration, account security compromise Online service activation External services, popular services New service activation Login credentials Inter-org. systems Inter-org. mentions (e.g., yammer)
Packet delivery notifications	Localized postal notifications
Personal	Direct messages: casual messages from coworkers Other messages just for you, Social media (mentions, etc.)
Authority impersonation	Authority (external) Authority (CXO)
Dangerous files	PDFs, macros, installables, attachments, file sharing
Temporal attacks	Trending attack (actual, current, trending) Events (Olympics, war, Covid-19, Christmas)
IT admin (Inter org)	Admin (IT) Security (MFA, compliance etc.) Policy update (IT) Internal guidelines / guidance (IT) Service / tool in use

THEME NAME	EXAMPLES
Inter org communications	Admin (general) HR communications Internal guidelines / guidance (general) Voice message / request to call (interorg)
Email	Spam filter Encrypted email Fake error Failure to load
Invoice scam	Fake invoice
Industry	Maritime Banking Logistics, etc.
Sensitive information gathering	Where the failure mechanism is you inputting data somewhere: surveys, sending reply
Profession	Relating to personal work (e.g., Salesforce for sales people)

Difficulty level

Traditional training content is produced for the masses although the knowledge and skill levels of employees differ. Instead, you must send different types of content at different difficulty levels to everyone. You don't want to make it too easy for more advanced learners and vice versa because that can be very demotivating from the start. Over time, our automated content engine gradually advances in each of the difficulty levels. So that your employees end up recognizing the most sophisticated threats. The difficulty depends on previous user data as well as other factors related to content varieties. The right amount of difficulty along each employee's personalized learning path will keep them engaged, interested, and will challenge and activate them to think critically.

Individual point of view

Spear phishing is a highly personalized type of threat that is hard for anyone to spot. It causes about 65% of company breaches according to Symantec. For your employees to recognize such threats you must personalize your simulated training content. Hoxhunt automatically includes roles, departments, localization, names, colleagues' names, managers, logos, collaborators, service-providers, and context in the training content. With Hoxhunt, every employee receives a personalized simulation. This makes it challenging, but once your employees start recognizing this type of threat, they will become very effective in defending your organization.

Bob Beginner

LOCATION:	LANGUAGE:	DEPARTMENT:
Germany	German	Finance

Bob is new to the organization and just got enrolled to Hoxhunt. Bob is a beginner in recognizing and reporting phishing threats. Bob is part of the finance team based in Germany. An advanced simulation for Bob would be hard to spot or could raise fear or doubt, especially when failing it while starting out. Therefore, we warm Bob up with simulations based on his skill level. The simulations will always be relevant to Bob, they can include his colleagues' names or department related matters. Bob selected that he wants to receive his simulations in German. So, we localize the simulations for Bob to reflect the language and cultural context.

Jane Advanced

LOCATION:	LANGUAGE:	DEPARTMENT:
USA	English	Marketing

Jane has been enrolled in the Hoxhunt training for a while now. Jane is part of the marketing team in the USA. Over the past few months, she managed to recognize and report several simulations and threats. Jane needs more challenging simulations because she has become really good at spotting them. Our game engine recognizes Jane's previous performance and sends simulation that are tailored to her skill level and role in the organization not to make it too easy for her. Else Jane may lose interest in reporting threats and participating in the training. Jane receives simulations in English, and they reflect the American culture. For instance, where Bob receives a notification from Deutsche Post as a simulation, Jane will receive a notification from FedEx.

Timing and cadence

Infrequent phishing tests are not sufficient to facilitate the correct security behavior. Neither are mass simulations that reach all your employees at the same time. Instead, send personalized training to everyone at different times so that the simulation comes as a surprise. When employees receive a simulation in the middle of something stressful or when they least expect it, their guards are down. And you want your employees to recognize threats even during those moments, because that's when attackers can succeed too.

Each simulation that is sent is based on the user's previous performance. As a rule of thumb, we send a simulation to each individual 14 days apart at the very most. Especially in the beginning, people start forgetting about the right behavior after twenty days. When employees get used to receiving attacks frequently, the issue will stay at the top of their minds. Repeating this over a longer period will shape new cautious habits among your employees.

Skills

Employees will only start behaving correctly when they possess the right skills to do so. The most straightforward skill for employees to learn is to click a reporting plugin whenever they see something suspicious. Once the reporting button is in place and your employees understand the need to report suspicious emails, you can begin the simulated training content. Their skills will develop when you continuously send them simulated content with the earlier mentioned characteristics. Over time, they will know how to recognize a real threat and that they must report it through the plugin.

With our variety in content at different difficulty levels, we train our users to recognize and report threats like dynamic category based threats based on employee roles, online services, packet delivery notifications, personal emotional subjects, authority impersonation, dangerous files, temporal attacks, sensitive information gathering, IT admin messages, regular emails, invoice scams, inter-org. communications, and threats based on industry. Typically this has spill-over effects into other categories of threats additionally.

We recognize that employees have varying levels of skills. It's necessary to adapt simulations and training moments to correspond to each person's individual skills. Based on their previous data, whether failing, missing or passing a specific simulation or training moment, our engine will develop the next simulation and training moment to fill the skill gap of the employee. This differs for every individual.

Positive reinforcement and feedback

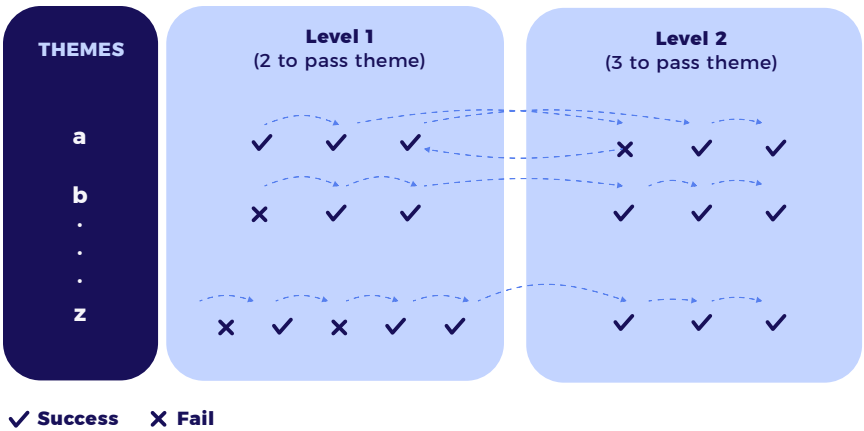
Simultaneously, you may wonder how to keep your employees engaged with the training. That's where the Hoxhunt stimuli play an important role. Positive reinforcement is key. Positive reinforcement helps you to truly engage your employees and removes any negative feelings towards cybersecurity training. When training is positive, your employees will be more eager to participate in developing their skills and reporting threats, and they want to keep coming back for more.

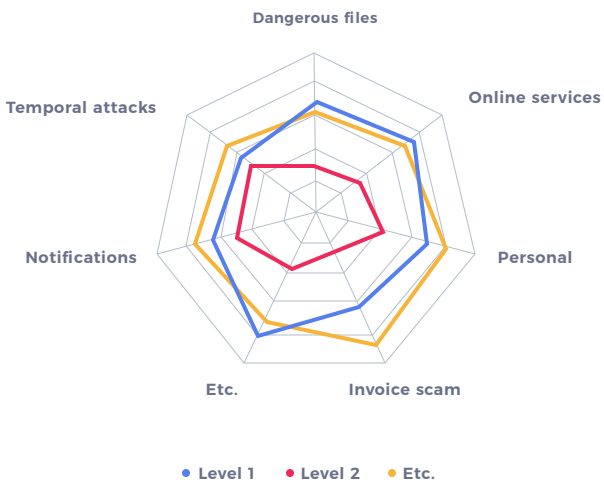
Feedback and recognition are important for positive reinforcement. Whenever someone reports a simulated threat, they will receive points and stars, allowing them to level up on a company leaderboard. No matter whether they failed or succeeded in a simulation, the employees receive extra points and stars when they go through micro-learning moments related to the email they reported or failed. The micro-learning moments take around one or two minutes altogether so that it doesn't bore or disrupt the employees. By finishing the micro training and tips, employees receive the skills needed to prepare themselves for the next possible simulation or threat. This loop repeats itself consistently and becomes increasingly advanced.
As a result, employees learn to recognize the most sophisticated threats after a few months.

Bringing it all together

About every ten days, our algorithm decides which personalized attack simulation to send to each individual in the organization based on all the elements we have discussed earlier. Our threat engine always aims to fill the knowledge gap based on previous performance, which changes after each simulation. This way it ascertains that every employee is trained to recognize every type of threat.

Each simulation is followed by a gamified training experience that takes one or two minutes to complete. Our users develop new behavioral patterns over time as a result of the holistic user training experience.





04

Conclusion

To change employee behavior and to reduce human risk, you must deliver people-first cybersecurity training. You simply cannot do that with manual or tool-based solutions, especially when you want to send personalized content to hundreds or thousands of employees.

Even if you have just started to explore the solutions for awareness training, you can easily begin your journey with behavior-changing training. Ultimately, you want to develop your employees' skills by training them with a variety of content that is personalized and frequent enough. Once threat reporting becomes a natural habit for your employees, they will actively fend off threats, and your security team will gain insights into the reported threats that get through the email filters.


HOXHUNT