HOXHUNT

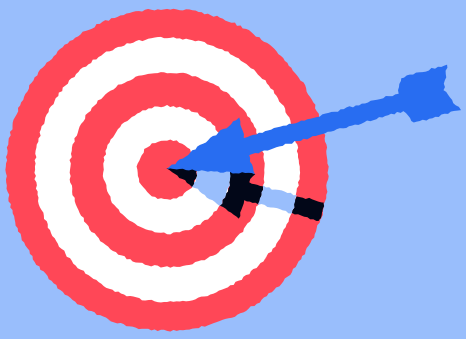
The risk of new employees for your security team and how to tackle it

Table of Contents

Introduction

Starting a new job can be a stressful time for most of us. Even though the interview process has probably taught you a lot about the organization, and the organization about you, there is still a great deal of unfamiliarity. In the first weeks, you discover new things about processes, colleagues, tools and software, activities, communication channels, and much more. This can be very overwhelming, and unless you work with cybersecurity or for a cybersecurity company, it often goes at the expense of secure behavior. Simultaneously, a report by Dell showed that more than 50% of companies believe security training for new employees should be a top priority.

Human risk is generally already very high, but according to our user statistics, the vulnerability spikes to 40% during the onboarding of new employees. Therefore, this is something you want to tackle with your security team from the get-go. As if it wasn't hard enough already to onboard new employees, the hybrid or remote working environment has also come with its challenges. Attackers exploit this transition in the way we work with targeted attacks aimed at new employees.



New employees are an opportunity for attackers and a weakness for cybersecurity teams

New employees still need to get acquainted with the communication style and tools that you use, leaving them exposed to attackers. Especially at the beginning, it's challenging for your new employees to tell which notifications are real, which services they'll use, and which of those services require a login. An opportunistic attacker can utilize any of these factors with a well-timed attack. If successful, your employees might give away their credentials without being aware of it. One way social engineers can easily craft such personalized attacks is by checking people's social media accounts, on which they often update their networks on job updates.

Another attack method that leaves your employees vulnerable, especially during their onboarding, is vishing, or voice phishing. A good example of this is when you receive a phone call from an attacker who is pretending to be part of your IT department. It's fairly easy to fall for this as the context feels right for newer employees: They just started working, so the IT department gets in touch to discuss something related to their computer. It makes sense, right? It does, especially more so in a remote working environment when we haven't met our colleagues in person or we don't even know what our colleagues sound like.

Never assume that new employees have followed cybersecurity training before. It could be someone's first job after graduating. Even if you hire someone more experienced who has followed actual cybersecurity training, it doesn't guarantee that they can identify malicious threats. Most training programs are created to check the compliance regulations box by sending easy, identifiable threats to reach the failure rate threshold that is required. As you can imagine, one slightly more personalized threat can easily throw these employees off and cause major harm to your organization.

What do you do to prevent new employees from falling for attacks?

Communicate your intentions

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.

Different skill levels

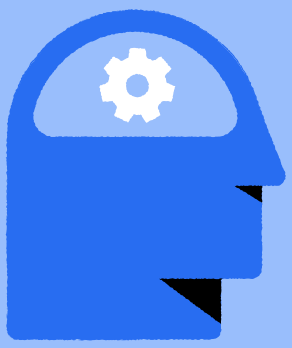
Every new employee has a different skill level depending on their background. Your training should consider that. Employees become uninterested if the training is either too easy or too difficult. Quickly test your new employees by simulating different threats, and build a risk profile based on their performance. After that, every time an employee receives a simulation or training, keeping engagement to a maximum should be relevant. You should always aim to gradually fill knowledge gaps to enable employees to protect the organization from any type of incoming threat.

Positive reinforcement is key

Use positive reinforcement. Imagine starting a new job and getting punished for failing a training or test. That not only puts the security team in a bad light, harming your cybersecurity culture, it can also demotivate new employees throughout their first weeks. To avoid this, you should use positive reinforcement even when employees fail tests. Focus on what they can improve on rather than what they've done wrong.

Integrate bite-sized learning into the employee's workflow

Make the training short so that it doesn't disrupt the onboarding process of your new employee. In general, people tend to lose interest when training is too long and dreadful. We've seen higher effectiveness and engagement rates when training is short (around 1 or 2 minutes) and relevant. You can train your employees more frequently as a result so that it stays at the front of their minds.



Conclusion

In the end, you want to enable your new employees to fight threats with you and give them a sense of belonging in the cybersecurity team's mission. Collectively, you can make an impact.


HOXHUNT