KnowBe4
Human error. Conquered.

Island
Bifurcation
Ridge ending
Pore
Crossover
The core of fingerprint pattern
Short Break
The delta is where the ridges divide

WHITEPAPER

How to Fortify Your Organization’s Last Layer of Security – Your Employees

Cyber security threats continue to proliferate and become more costly to businesses that suffer a data breach. One reason for that is that hackers have realized it’s easier to find someone who may be willing in a moment of weakness to open an attachment containing malicious content than to exploit technical vulnerabilities within computer software, according to Symantec.

When it comes to combatting these growing risks, most organizations continue to place more trust in technology-based solutions than on training their employees to be more aware of the threat landscape and able to recognize the red flags in cyber breach attempts. Organizations tend to see their employees as liabilities rather than as assets, who, when trained appropriately and incentivized, can be part of a more robust solution to many problems.

A report, “Magic Quadrant for Security Awareness Computer-Based Training,” by Gartner*, the leading computer trends analyst, evaluates a broad range of computer-based security training products on the market. “People impact security outcomes, much more than any technology, policy or process,” Gartner explains. “The market for security awareness computer-based training is driven by the recognition that, so long as technology-based security systems do not provide perfect protection, people play an undeniable role in an organization's overall security and risk posture. This role is defined by both inherent strengths and weaknesses: people's ability to learn and their capacity for error.”

> “...people play an undeniable role in an organization's overall security and risk posture.”
>
> - Gartner

*https://info.knowbe4.com/gartner-2017-magic-quadrant-security-awareness-cbt

There's a right way and a wrong way to train employees in cyber security awareness. The wrong way approaches training as a once-a-year or semi-annual exercise in which employees are gathered in the break room with snacks and subjected to a long, or sometimes too-brief, PowerPoint presentation. This method treats employees as a passive audience and inadequately engages them. Done wrong, security training feels more like punishment than an opportunity to teach and inspire employees to be active contributors to their organization's safety and well-being.

The wrong way also reflects a one-size-fits-all organizational mindset, which fails to take into account that people have various strengths and abilities, and respond differently to a range of methods by which training material is presented. They also have varying security awareness needs depending on their role and level of access to sensitive information within their organization. Another key flaw of the breakroom approach is that the impact of training gets measured in terms of attendance instead of content retention and behavior modification.

A 2016 study of the effectiveness of security awareness training by Enterprise Management Associates, a leading IT industry analyst, reported that nearly 60% of the companies that provide such training were using less effective methods such as the breakroom approach (23%) and the monthly security video approach (36%). As a result, organizations tend to be disappointed by statistically low levels of improvement in behavior. That is likely to cause senior executives to dismiss the whole field of security awareness training rather than question the methods by which it is delivered.

When it's done properly, security awareness training is parceled out in more digestible portions that expose employees to content with greater frequency and variety so it can have a deeper impact. This approach treats training more as a carrot than a stick and is interactive and role-based, making it feel more relevant and worthwhile to employees. And because it's more challenging, it engages the minds and memories of workers much more effectively than when they are forced to passively sit through a presentation once a year or even at more regular intervals.

Security awareness training never occurs in a cultural vacuum. So it's advisable that an organization's risk management department evaluate the organizational culture and adjust the messaging appropriately. For example, an authoritarian corporate environment in which employees are expected to simply follow instructions without questioning how a task fits into a broader context is likely to require more effort to modify an employee's behavior or default responses to things like phishing emails than a culture that promotes cooperation and critical thinking and recognizes the value of getting managerial and staff buy-in for new initiatives.

How to change employee behavior to be less susceptible to social engineering

The central goal of security education is to modify an employee's behavior so he or she doesn't fall for social engineering -- the art of manipulating, influencing or deceiving somebody to take an action that isn't in either his or his organization's best interests. The most common examples of social engineering are phishing and spear-phishing attacks, which use phone, email, postal services or direct contact to try to trick people into doing something harmful.

“Interactive computer-based training is a central component of a comprehensive security education and behavior management program,” according to Gartner. “It is a mechanism for the delivery of a learning experience through computing devices, such as laptop computers, tablets, smartphones and Internet of Things (IoT) devices. The focus and structure of the content delivered by CBT vary, as do the duration of individual CBT modules and the type of computing endpoints supported. Understanding the diversity of people in the organization is as important to security and risk management leaders as an understanding of how security fits into an organization's larger goals.”

The aim of most social engineering schemes is to get somebody to click on a hyperlink or open an attachment sent in an email that will then give the bad guys access to the user’s computer. Showing a trainee how to recognize that out of nearly 20 types of files an email attachment could come in, the only one that is absolutely safe to open is a file ending in .txt can be a security game changer. Providing short, three- or four-question quizzes at regular intervals during a training module helps employees review and reinforce their understanding of particular training elements and can increase their trust in the impact the course is having and motivate them to complete it, thanks to congratulatory messages after each quiz.

Human beings can become an organization’s last layer of defense only when security awareness training demonstrates to them how susceptible they are to social engineering, which is considered to be the single greatest security risk in the coming decade, much more than electronic hacking. The FBI has reported a 2,370 percent increase in exposed losses between January 2015 and December 2016 from social engineering schemes such as CEO fraud, also known as Business Email Compromise (BEC). A total of more than $5 billion has been stolen from businesses through cyber theft from October 2013 through December 2016, with an average loss per incident of $100,000 and are projected to top $9 billion in 2018.

Training exercises that tell a compelling story and put the trainee in the position of somebody who has been targeted, such as a company’s controller, engage all the senses by making the trainee choose the best course of action in response to a suspicious email. When he has the opportunity to select the wrong response to an attack, “that employee definitely has an ‘Aha!’ moment because a big screw-up caused major problems” for his

> “Interactive computer-based training (CBT) is a central component of a comprehensive security education and behavior management program.”
>
> - Gartner

organization, says Kevin Mitnick, chief hacking officer for IT security company KnowBe4, provider of new-school security awareness training.

These exercises teach employees to carefully check all the details in an email for telltale signs of potentially malicious content: a “From” address with a misspelling, a hyperlink that when you pass your cursor over it reveals the actual URL destination you will be taken to (and that will infect your computer), and the suggestion of negative consequences if an action isn’t taken quickly and before confirming the email’s veracity.

Learning that dangerous emails often appear to come from reputable organizations or from someone you know and trust within your own organization drives home the lesson: **think before you click.** Making training interactive ensures it takes deeper root in an employee’s mind.

The ultimate goal of simulated phishing attacks is to train people’s reflexes so they learn the optimal response to such emails. “This is like learning how to catch a ball or to do any complex move that the human body might want to do, but this is doing it mentally,” says Perry Carpenter, chief evangelist and strategy officer at KnowBe4. “That means putting somebody in the situation where they’re having to make that decision and use that behavior that we actually want somebody to have embedded over and over again so it becomes something that doesn’t feel uncommon or different from their normal decision-making, but is integrated with and will just naturally become their pattern of habit.”

Security education should start with phishing emails that use a method that is very easy to detect, and then gradually escalate to more challenging simulated attacks in order to fully inoculate employees against all kinds of phishing attacks. This will help them understand how persistent bad guys are in sending increasingly sophisticated attacks until they can trick somebody.

The idea is to repeat variations of the exercise continuously so a trainee has a chance to fail in a safe environment and be redirected to a form of corrective behavior, Carpenter says. “Even more important is to have multiple successes, multiple times to show themselves that they know how to detect a phish and report it so they have that behavior ingrained within the way that they do business every day.”

How to change organizational culture

Changes in behavior cannot be sustained by an organization’s culture without continuous reinforcement. For example, you can reduce the rate at which an employee clicks on a phishing email link to the low single digits from an initial 27% average percent level after training and repeated testing. However, “if you just leave that alone and never train them again, you’re going to see it creep back up for a couple reasons,” Carpenter warns.

First, the stimulus for reinforced behavioral patterns disappears once you take away the immediate feedback an employee gets when s/he successfully recognizes a simulated phishing attack. Second, on the organizational level, the natural churn of personnel as some people leave the organization while others join it translates to a smaller percentage of employees who have been trained rigorously in security awareness.

Then there is behavioral drift over time because nothing is being done to help employees sustain new habits they have learned regarding an approach to emails they receive. Think of seasonal circumstances that can push against an employee's heightened security awareness and his resulting behavior.

For example, "I'm in retail. It's the holiday season. I'm getting 300 more emails a day than I naturally would get, and I'm just trying to knock stuff out, so I'm naturally going to get a little more careless," Carpenter says. In the retail world, holiday season lasts at least two months, from early November until New Year's Day.

"Science says it takes 66 days to formulate a behavior or to change a behavior, so that two-month period I'm pushing on basically creating an entirely new habit," he explains. "When January comes around after holiday season, my behavior has shifted to whatever the new norm was unless I was constantly training. And now this person is not thinking again as they open and answer emails."

Security education is also an opportunity to strengthen communications within an organization so that employees become less susceptible to social engineering attacks. For example, if the HR and IT departments start to issue advance warnings about changes to email or other systems that are coming down the pike and what to expect in terms of updating login credentials, staff members will grow more suspicious of unexpected emails posing as such updates and trying to trick them into sharing personal information. Establishing clear procedures for things like suspicious emails such as reporting it immediately to the IT department, also helps recondition employee behavior.

Given that the ultimate aim is to retrain employees' reflexes regarding online behavior, it's imperative that managers respond to training results in a constructive, nurturing way instead of a punishing one.

"If somebody fails one or even a few times, that shouldn't mean that we come down on them and we shake our finger in their face and tell them how bad they are," says Carpenter. "They're failing because they're human, and we're putting them in a situation that tests their humanity in a lot of ways. And we're putting them in that [situation] because we know that this is the natural default behavior that people have and we're trying to shift it."

Mitnick agrees it's better to take a carrot approach to encourage people to take security as self-interest in what they're doing. "People don't really care about security unless it's in their self-interest. They could be worried about their job or about protecting their own data. They could just want to do the right thing for the company because obviously they don't want the company victimized." The key is to turn an employee's mistakes into teachable moments that further strengthen an organization last layer of defense.

Recommended Action Items

1. Be realistic about what is achievable in the short term and optimistic about the long-term payoff.
If your goal is behavior change, focus on 2 to 3 behaviors for 12 to 18 months at a time. You can't effectively train on everything.

2. Plan like a marketer, and test like an attacker.
Starting with communications such as executive messages and videos, department manager

messages and security town halls, conduct phishing and social engineering testing through LMS modules, and reinforce through regular newsletters and digital signage.

3. View Awareness through the vision of organizational culture.
Focus on understanding the different personalities, drivers and learning styles within your organization. Complete a list of recommended tasks that are designed based on feedback in your company's staff questionnaire. This will let you personalize your approach and get the most out of your Security Awareness Program. Tasks may include engaging your organization's stakeholders, creating and completing a baseline phishing campaign, communicating the Security Awareness Program to your employees, reviewing and selecting a primary training module, and creating training campaigns for your quarterly training modules.

4. Leverage behavior management principles to help shape good security hygiene.
Embrace best practices such as (a) formulating goals before starting, (b) getting the executive team involved, (c) prioritizing and making your messages and training relevant, (d) phishing frequently, at a minimum of once a month and (e) testing frequently to build security reflexes.

5. Have a vision of what "good" looks like for your organization.
Build a network of "security champions" inclusive of all roles and geographic regions across the enterprise. Present to candidates the role of a champion as a developmental opportunity and integrate it into performance and career development plans.

Changing employee behavior to be less susceptible to social engineering requires a consistent and repeatable approach to security education. Security awareness training done right engages users and moves their natural "reflexes" from being unaware to being proactive and competent in identifying potentially hazardous social engineering tactics. Successful behavioral change starts with clear communication to employees on why security education is important that also aligns with an organization's unique culture and workplace dynamics. Rolling out a realistic security awareness training program will empower users to protect themselves and be part of the solution in fortifying an organization's last layer of security.

Ready to Get Started?

Build your own customized program using KnowBe4's free Automated Security Awareness Program tool which will show you all the steps needed to create a fully mature training program in just a few minutes!

https://www.knowbe4.com/automated-security-awareness-program

*Gartner, "Magic Quadrant for Security Awareness Computer-Based Training," Joanna G. Huisman, 26 October 2017.

Gartner Disclaimer
Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Additional Resources

Free Phishing Security Test
Find out what percentage of your users are Phish-prone.

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do.

Free Domain Spoof Test
Find out if hackers can spoof an email adress of your own domain.

Free Phish Alert Button
Your emloyees now have a safe way to report phishing attacks with one click.

Mailserver Security Assessment
Find out if the bad guys can penetrate your email filters with our free test.

Ransomware Hostage Rescue Manual
Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

To learn more about our additional resources, please visit www.KnowBe4.com/resources

About KnowBe4

KnowBe4 is the world's largest integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line

of defense and enable them to make better security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com