HOOK SECURITY

SECURITY AWARENESS TRAINING:

THE 2021 ULTIMATE GUIDE

Table of Contents

CHAPTER 1

WHAT IS SECURITY AWARENESS TRAINING?

What is Security Awareness Training?

Security Awareness Training is the most effective way to protect companies and their employees from social engineering phishing attacks.

But What is Security Awareness Training?

Hook Security defines it as an education program that teaches employees about security and phishing while creating best practices and good habits.Let's unpack that.

One of the biggest weaknesses in any cybersecurity system is the human factor. It doesn't matter whether your organization is using sophisticated passwords, multiple firewalls, anti-malware programs, etc. The human factor will always be an issue in keeping your company and yourself safe. At the end of the day, the employees are the ones who are most vulnerable and need the right tools. If an employee has not been effectively trained on cybersecurity awareness, the chances are high they will compromise a company through simple mistakes, negligence, or even apathy.

Cybercriminals know this. They know that hardware is incredibly difficult to get by but targeting a person or group gives them the best chance to attack. Using methods like phishing emails exploit human vulnerabilities. When successfully used, something as simple as a phishing email can compromise an entire organization and its network. **That's bad news.**

Security Awareness Training aims to resolve this by directly focusing on the human factor. At Hook Security we research and craft simulated phishing attempts (what we like to call "real fake emails,") based on the latest tactics that criminals are currently using.

Then, when employees fall prey to our trap, we give them a short, educational but entertaining video to train them on their mistakes.
The aim is to leave the employee not scared, but aware. Not afraid, but just a little bit paranoid about emails. Though small, the difference between those two is incredibly impactful.

The Emergence of Psychological Security

As the cyber threat landscape continues to grow, guarding our information systems becomes harder and harder. This is often because the focus, attention, and ultimately the blame are in the wrong places. We've started to see a need for companies beyond just information security, and the reason for this is right there in the name. Protecting a business's information by simply focusing on the information itself still leaves you vulnerable, as over 90% of breaches involve social engineering. As crazy as it may sound, we have to protect our minds, our intuitions, our dependence, and our trust. Enter the idea of Psychological Security.

Psychological Security is the practice of protecting humans from being manipulated and exploited by technology. From hyper-targeted ads to phishing attacks, technology and data are used to influence us every day. This is the reason that phishing is so successful. We've learned to trust and depend on the technology we use, the brands we buy, and the people we know. Add the fact of professional environment with bosses, deadlines, and raises, and the risk of manipulation skyrockets.

Will you fall for a Starbucks phishing email? Maybe. Will you download a mystery spreadsheet from your "boss" called "ChristmasBonuses2020.xlsx"? Definitely. This is the reason regular training is so important. To guard against phishing we have to train employees to recognize the risk and create pattern recognition over time.

Benefits of Security Awareness Training

Initiatives like cybersecurity awareness training force a company to examine its procedures, policies, and personnel. Inefficiencies and opportunities often come to light as a result of this, which may have nothing to do with security, but can still benefit a firm.

Training can help to reduce errors or help recognize the "bad guys'" tricks and trends.

Cybersecurity awareness training for employees can strengthen and enhance your company's security posture.

When your employees are educated and trained they are more compliant.

Training can keep your customer's reputation clean and clear of mishaps.

Education and training can bolster confidence and even help morale for your customers.

Money and time can be saved for your customer by having training.

Your customer can sleep at night knowing they are actively training to the latest threats through training.

Building a Culture of Security Awareness

A security awareness training program can act as a team-building and collaboration exercise. Because the nature of the goal is generally not to solve a problem where finger-pointing is common, it lends itself to improving relations among employees. A common enemy (cyber threats) often unites a group.

Hook Security's edutainment-based training content creates a fun, yet engaging experience for the workforce, and does not shame the employee for failing but provides a memorable training experience. We believe people shouldn't be afraid that their job is on the line with every email they get. When companies realize the importance of security awareness training and adopt our program, they increase productivity, boost creativity, and ultimately are much safer.

CHAPTER 2

WHY IS SECURITY AWARENESS TRAINING IMPORTANT?

Why is Security Awareness Training important?

Over 90% of cyber attacks include some sort of phishing or social engineering element. It shouldn't be a shock that reducing the risk of phishing attacks reduces the risk of a breach.

Employees receive phishing emails every day. And while most security tools do a great job of filtering out most phishing emails, hackers are changing their tactics every day, and some phishing emails ultimately land in an employee's inbox.

And the phishing attack is just the beginning. Phishing is the attack vector the hacker uses to get access to a company's system. Once an attacker has access, that's where they do their damage. Some examples of cyber attacks include malware, ransomware, business email compromise (BEC), and more.

Security Awareness Training aims to resolve this by directly focusing on humans and creating habits.

It's one thing to simply warn employees of the dangers of phishing, but if you can properly create habits and reach the primitive part of the brain that controls threat recognition and response, that's where you really start to see a reduction in phishing email clicks.

> **Over 90% of cyber attacks include some sort of phishing or social engineering element.**

Security Awareness Training Creates a Positive Security Culture

Security awareness training, when properly executed, contributes to your company's security culture, and ultimately your overall company culture.
First, you should understand that culture is not something you can command, direct, or mandate. Culture is not a policy. Policy is what employees are told to do. Culture is how they actually behave.
How do you influence culture?

At Hook Security we say there are four main things you can do to contribute to a healthy security culture:

- **Train Everyone -** Culture comes from the top down. If top-level employees aren't being trained, or see themselves as "above training", it completely dilutes its importance and other employees will not take security seriously.
- **Expect Mistakes -** They are inevitable. How you react to them is everything. When you roll out security awareness training to employees, you will see people click. But that's okay. The goal is to reduce risk. It's virtually impossible to eliminate the risk of phishing attacks. Just be glad the phishing email they clicked on was a phishing test, and not the real thing.
- **Set Goals -** Encourage your employees and track progress. If you're creating a healthy, positive culture around cybersecurity, employees will want to know how they're doing. Encourage them by letting them know when they pass or fail phishing tests.
- **Don't Punish Mistakes -** This is the number one pitfall of many companies trying to have a security awareness program. If you truly want to have a positive security culture, treat mistakes as an opportunity for growth. After all, would you report a phishing email if you thought you could be fired?

By offering security awareness training to your employees and following these guidelines, you will attain a positive security-aware culture that is FAR more effective than using fear, uncertainty, and doubt.

Security Awareness Training Helps with Compliance

Compliance is a nice by-product of security awareness training, but to do it successfully, you shouldn't make compliance the reason for offering training. This approach can lead to poor performance and results.

However, more and more industries, regulators, and compliance programs are starting to include having a security awareness program. Some compliance regulations that already require security awareness training include:

- PCI DSS
- HIPAA
- ISO/IEC 27001 and 27002
- FISMA
- GDPR
- Many State privacy laws

If these areas of compliance affect your company or companies you offer IT services to, you should offer security awareness training for compliance.

Security Awareness Training Helps Avoid Downtime

Similar to point number one above, security awareness training significantly reduces your risk of company downtime, for two reasons:

First, the biggest cause of downtime is when your company is hit with a cyber attack. If you are hit with something like ransomware, your files will be completely encrypted, and many business functions will be shut down completely.
There are other, less obvious forms of downtime related to cyber attacks such as loss of business, PR issues, employee morale, time to fix, and more.

Simply put, phishing attacks are bad for business.

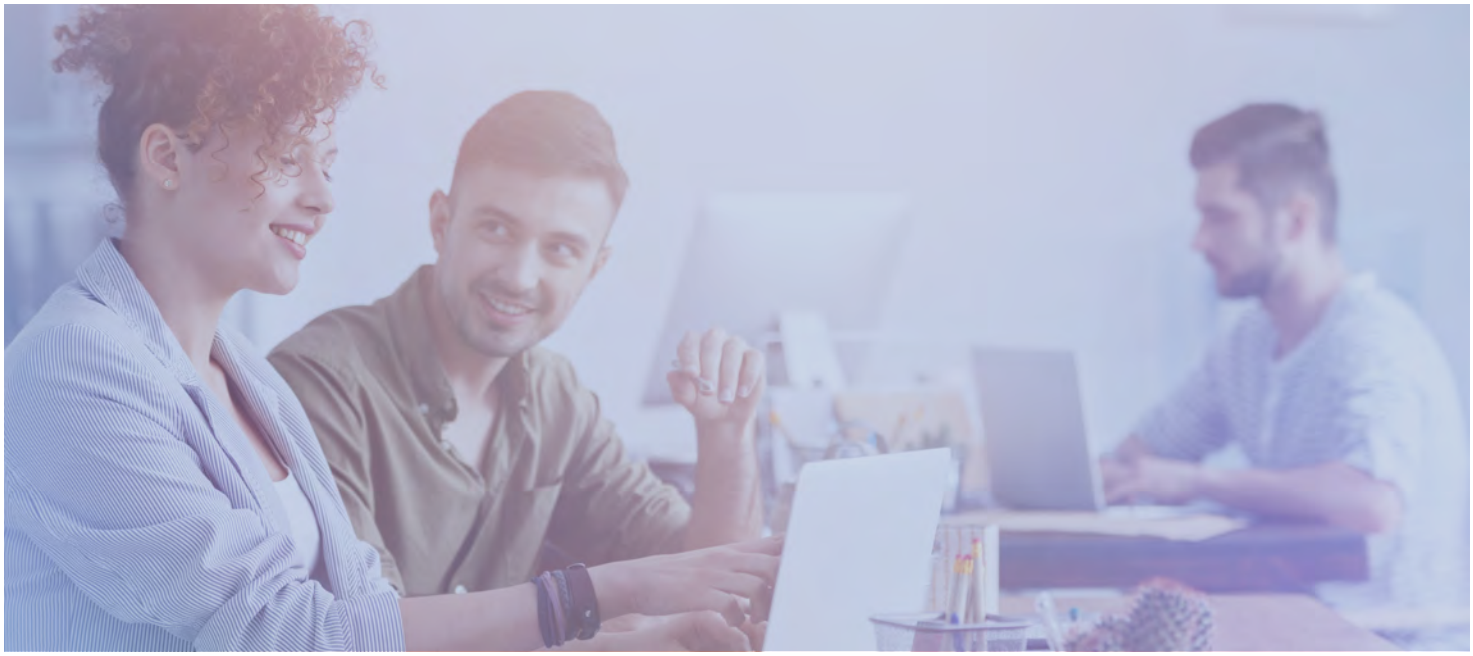
Second, when you roll out something like our Psychological Security Awareness Training, the training is short, doesn't take time out of an employee's day, and boosts morale rather than hurt it.

How does this work?

At Hook Security, we research and craft simulated phishing attempts based on the latest tactics that criminals are currently using. We send these simulated phishing emails to employees every month.

Then, when employees fall prey to our trap, we give them a short, educational but entertaining video to train them on their mistakes. The whole experience from clicking the email to receiving training is less than 5 minutes.
The traditional form of training involved hours-long training in a conference room, or long, drawn-out computer-based training. This approach kills productivity. And we like productivity.

By training your employees at the moment they clicked (we call this the point-of-infraction), they quickly learn from their mistakes, have a laugh, and move on with their day.



Your Employees Are Your Greatest Asset.

Many security providers and companies say that employees are your biggest weakness when it comes to cybersecurity, and to be honest we've said the same in the past.

And while there may be some truth in the statement, it does very little to accomplish our goals in security awareness.

Your tools can not be security-aware. Your computers can not be security-aware (well….not yet….oh god I'm so scared for the future). We have found that the number one way to create security rockstars out of your employees is to treat them like your greatest asset, not your biggest weakness.

Your employees are the number one keeping your company going. And yes, they are also the people clicking on phishing emails, but you should see them as an opportunity versus a threat. This will have a great impact on the effectiveness of security awareness training.

Why is it Important to Offer Security Awareness Training?

If you are an MSP, MSSP, VAR, or any kind of IT services provider, you may or not already offer security awareness training to your customers. But should you?

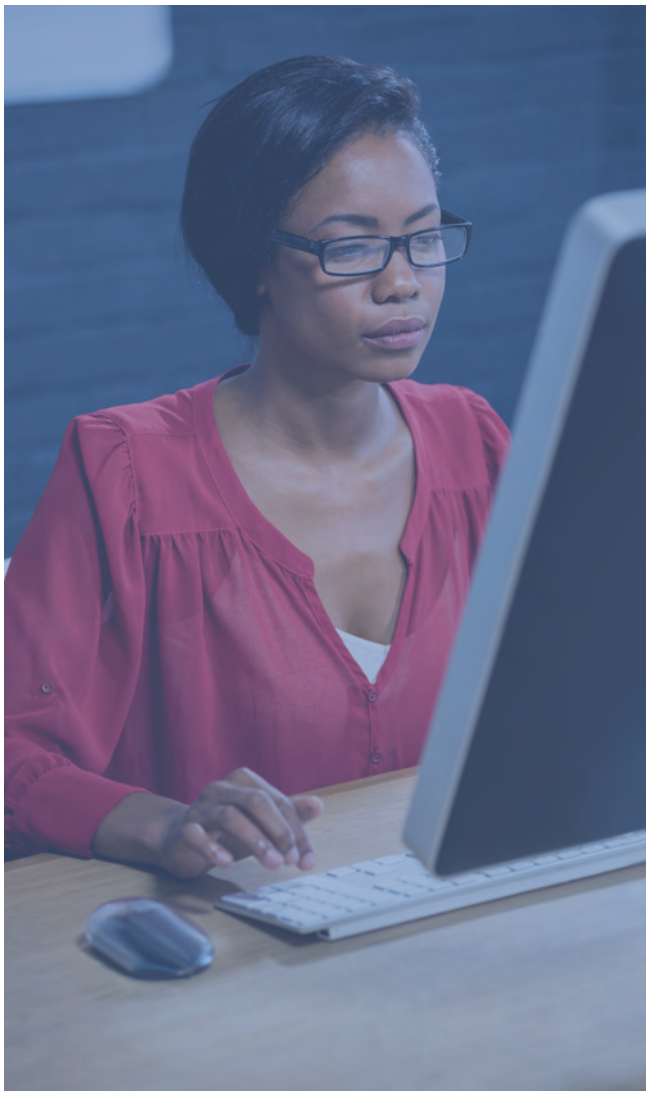
Well, we may be biased but we think so.
But so do other MSPs.

In Datto's 2020 State of the MSP Report, they showed that 60% of MSPs consider security awareness training a critical service to provide for their customers, while slightly less than 60% reported they actually offer it currently.

The cold, hard truth is that if you aren't offering security awareness training and other emerging services as part of your managed offerings, you could be in danger of losing customers. Because as company adoption of awareness training increases, companies will look for and ultimately go with providers that offer it.

CHAPTER 3

HOW TO CREATE EFFECTIVE SECURITY AWARENESS TRAINING



How to Create Effective Security Awareness Training

Security Awareness Training for employees is more crucial than ever. One could even argue that security "awareness" is just the first step in a company's security culture and that employees should be educated, motivated, and empowered to keep a company safe. In a world where the majority of cyber-attacks involve human error, employees need to know that they are the last line of defense, and that they are capable of stopping cyber attacks.

Gone are the days that your security awareness program is a box you check a few times a year. With the emergence of new compliance programs like CMMC, you'll need to show that your security posture is maturing over time, educating employees monthly. Here are a few things you can do to run an effective security awareness program.

Clearly communicate the purpose of security awareness training

It's clear that delivering security awareness training individually to employees is more effective than, say, a group presentation or conference room meeting. Plus, in this current mostly remote world, group training is near impossible. But before your employees start receiving phishing testing and taking online security awareness training courses, you need to provide some context to them for they might see in their inbox. That isn't to say, ruin the surprise of a phishing test, but employees should:

1. Understand the "why" behind security awareness training and phishing testing

2. Know that this isn't a "big brother" punitive measure, but a positive thing

Along with proper context behind the reason for security awareness training, the training itself should be relatable and should connect with the employee. It should feel as though the training was written for them, not other security professionals, other groups, etc.

Find Security Champions Within Your Organization

One of the best ways to grow your security culture is to have champions and supporters coming from places outside IT. It may seem frustrating at first, but employees are more

likely to take the advice seriously when it comes from their peers, not IT. Learn to use that to your advantage.

Find those whose communication skills penetrate across departments and ask them to send out notices regarding training. Additionally, enlist help from communications teams like HR to simplify your messaging in a clear, concise way. After all, getting company-wide buy-in to a cause is a human issue, not a technology one.

Phish Your Employees

There are two major keys to training success that we at Hook Security recommend - Regularly identifying risk, and training the employee at the time they're most likely to retain the information. Phishing testing accomplishes both of these.

Phishing testing allows you to send simulated phishing emails to your employees to test their ability to spot a phish in their inbox. Paired with good reporting, this allows you to identify risk in your organization and track success over time. Additionally, we provide "point of infraction" training - Training at the moment they clicked on a phishing test. This gives you the ability to do two things:

- Train the employee at the exact same time they're realizing the mistake they made, making the training incredibly relatable

- Train the employee quickly and efficiently, allowing them to get back to doing their job

Tracking phishing test failures against those who actually reported the suspicious email gives you a great understanding of where you're at on your risk reduction journey. Phishing testing is an important way to show progress in a security awareness program, as the alternative phishing-related KPI to track would be in terms of things not happening (i.e. data breach, phishing attack) versus actual track-able results.

Make it Personal

We as security professionals are both experts and passionate about cybersecurity. Your employees are neither, and this is an important point to keep in mind when training. If you assume employees will care about security by default, you're wrong. You need to make it personal.

Here's how to go about doing that.

When delivering security awareness training, you have to operate under the default assumption that nobody cares. This allows you to meet the employee where they are in their security journey and make them care.

Additionally, the whole security awareness program should be positioned as a positive experience. Like I mentioned earlier, help them understand the reason behind the training, and that this is not a punishment-based experience. Employees should be hesitant to click on suspicious emails not for fear of firing, but for motivation to keep everyone secure.

Make it Engaging

To make training relatable to your employees, your security awareness training should be engaging, non-patronizing, and often humorous. You can relate to employees by comparing complex security topics to everyday situations. Reference well-known news stories of breaches and explain how they happened, or, the most effective tactic, give your employees tips for personal security.

Employees are much more likely to take security seriously when they understand how it affects their personal lives as well. Show employees how to practice good password safety, change their wifi passwords, and update software on personal devices.

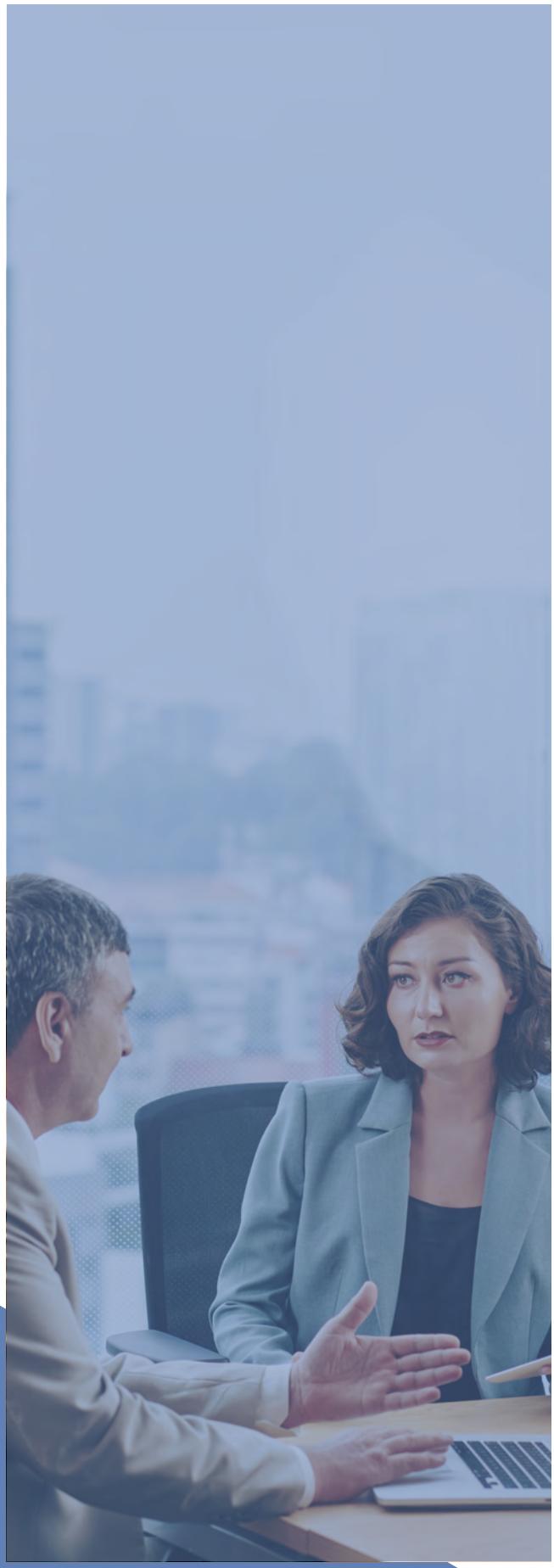
Finally, one of the pillars of psychological security is to tell stories. Narrative storytelling blows a PowerPoint presentation out of the water. People don't remember facts and tips nearly as well as they remember stories and feelings.

Get Top-Down Support

This is imperative to really any company wide initiative, but even more important for security awareness training. Get buy-in and support from the top executives in your company. This is very important for two reasons:

If they don't take it seriously, the rest of the company won't either. Executives should receive phishing simulations as they are the biggest targets and often the most impersonated people in the company by hackers.

Culture is created at the top. Encourage your executives to validate your program and practice positive security behaviors. Other employees will see that security awareness is to be praised and will follow.



CHAPTER 4

HOW TO CREATE A SECURITY-AWARE CULTURE

How to Create a Security-Aware Culture

We all know security is important. If you ask any employee of a company, they would most likely agree that keeping their company safe is important.

But how deep does that opinion go? Is it important to them? Do their subconscious actions reflect that?

When it comes to a company's cybersecurity, we often start with tools, processes, and policies. Once we realize our people are the largest security vulnerability, we start to look toward training and security awareness. This is great! But what we often leave on the table is how to make "security awareness" actually take effect, and move the company forward. We fail to tie awareness to culture and habits. For example, I'm aware that a yellow traffic light means "slow down" but my habit is quite the opposite. I'm making that light.

Weird metaphors aside, hope is not lost for your company! While security awareness culture is paramount to avoiding a major breach, it's quite attainable! Here's how:

First, you should understand that culture is not something you can command, direct, or mandate. Culture is not a policy.

Policy - What employees are told to do

Culture - How they actually behave

A cultural change happens on a subconscious level. If you can reach people's subconscious, you can change their behavior. This is why security awareness for employees is important.

Let's zoom out a bit.

Policy vs. Culture

Policy

What employees are told to do

Culture

How employees actually behave

Why are humans often the largest weakness in security?

Because **people aren't hardwired to recognize threats**

Even if they want to keep their company safe,

What is Phishing?

A cyber-attack that covers ANY attempt to collect sensitive information in which the perpetrator disguises their identity.

Hackers are often after:

everyone is vulnerable to phishing attacks, social engineering, and manipulation by technology.
This is scary, and the natural tendency is to teach by exposing employees to the fear of phishing, but this approach is one of negativity.

Why The Old Training Model Doesn't Work Anymore

The old way of training just doesn't cut it these days. The threat landscape moves faster than ever before, and people learn, think and act differently now because of technology.
The Old Training Model:

- Covers too much at once
- Takes too long
- It's disruptive
- Misaligned with cognitive recognition

This takes many forms, not just the classic hour-long training in the conference room.
If training is intrusive, instills fear, or tries to solve everything at once, it does not contribute to a positive security culture.

If training is intrusive, instills fear, or tries to solve everything at once, it does not contribute to a positive security culture.

How to Instill a Positive Security Culture in your Organization

Positivity is the number one approach we've discovered that contributes to culture. Scaring someone into a habit is an ounce as effective as encouraging and motivating someone to do the same.

There are four things you can do to accomplish this:

- **Train Everyone -** Culture comes from the top down
- **Expect Mistakes -** They are inevitable. How you react to them is everything
- **Set Goals -** Encourage employees and track progress
- **Don't Punish Mistakes -** would you report a phishing email if you thought you could be fired?

Now that we have the foundation of a positive security culture, how do we change the way we train?

The New Training Model: Psychological Security Training

- **1-2 Key Takeaways:** Rather than pack everything into one video or training experience, we focus on 1-2 things the employee can walk away fully understanding and caring about.
- **Train Regularly:** Keep the training short. Our target length for a training video is less than two minutes, preferably 90 seconds. If you have 1 key takeaway, it should take that long to make it resonate.
- **Train in a Familiar Environment:** Employees should be able to complete the training quickly and in their normal work environment. Training should contribute to productivity, not kill it.
- **Tell Stories and Use Humor:** This is our bread and butter. We use "edutainment" videos to train. Before the teaching moment occurs, employees get to have a laugh, get grossed out, or get entertained. Psychologically, this opens the brain up to be receptive to the information.

This approach is such a monumental shift from the old way of delivering security awareness training. From the phishing testing, to the training environment, to the training material itself, we've departed from old ways of thinking that protect the status quo.

This focus on people vs. information has led us to uncover what we think will become an entirely new vertical: Psychological Security.

By pioneering this new mind shift we were able to build our training experience from the ground up with people and their brains in mind.

This is the key to changing culture. Change minds.

Your employees CAN be trained to avoid manipulation by technology. Not only will employees naturally keep the company safe because of pattern recognition of phishing attacks, but they'll be excited to keep you safe because of the positivity, entertainment value, and humor that your new security-aware culture provides.

People become excited to spot and report real phishing emails.

CHAPTER 5

THE BEST WAY TO DELIVER SECURITY AWARENESS TRAINING

The Best Way to Deliver Security Awareness Training

Security awareness training isn't one size fits all. Delivering the training effectively is just as important as the training itself. Like we mentioned before, for years the training model has looked like this:

- Covers too much at once
- Takes too long
- It's disruptive
- Misaligned with cognitive recognition

Annual Training is Not Enough

Because of most compliance standards, training is often done to check the box of an annual requirement. So traditional training is done once a year, all at once.

But spending hours in a conference room or zoom is not an effective way to train.
Employees often check out, and frankly, it is unrealistic to expect an employee to remember everything thrown at them. And rather than internalizing a few key takeaways, they just shut off.

The way we deliver employee training is evolving, and for the better. Security Awareness Training has to be a regular occasion in order for it to be effective.

How to deliver Security Awareness Training

Train in a familiar environment
Employees should be able to complete the training quickly and in their normal work environment. Training should contribute to productivity, not kill it.

Use Relevant Content
If the training content doesn't feel like it's "for" the user that's watching, they are less likely to accept and retain the information. Avoid using terms and ideas that are too technical, and tread lightly with cartoons and animations. Use real-life examples and talk to the user like they're a human being.

Train Regularly
Between phishing tests and training courses, you should interact with your users at least monthly, if not multiple times a month. Habits are formed by pattern recognition over. If you want to train effectively, train regularly.

Dive Deep
Some of the most important security topics are the hardest to grasp, like ransomware, phishing, and other malware. Break this material down into examples and comparisons your employees will understand.

Lean on Video and Interactive Experiences
Odds are, your employees don't want to listen to you talk for hours on end about security. Using video training and interactive content is a great way to connect with employees on their terms, and quizzes and assessments help with retention as well as tracking

Measure and Report
In order to maximize the effectiveness of an awareness training program, its important to track your progress over time. You can track your program with reporting and dashboards. You can measure your employees by continuing to send phishing tests and monitor their progress.

CHAPTER 6

SECURITY AWARENESS AT HOME

Security Awareness At Home

The COVID-19 pandemic has changed the way that most companies work. Millions of people are working from home for the first time, and companies are struggling to adapt quickly.

Working from home brings all sorts of new work challenges: Watching the kids, avoiding distractions, staying in touch with coworkers, and figuring out new technologies just to name a few.

However, cybercriminals didn't quit when we all went home. In fact, they upped their game. In all the hustle and bustle of figuring out how to work remote, security has not been high on the priority list of many companies making the shift. Even for simple technology tasks like resetting passwords and troubleshooting WiFi, employees no longer have an IT person for which they can easily ask for help.

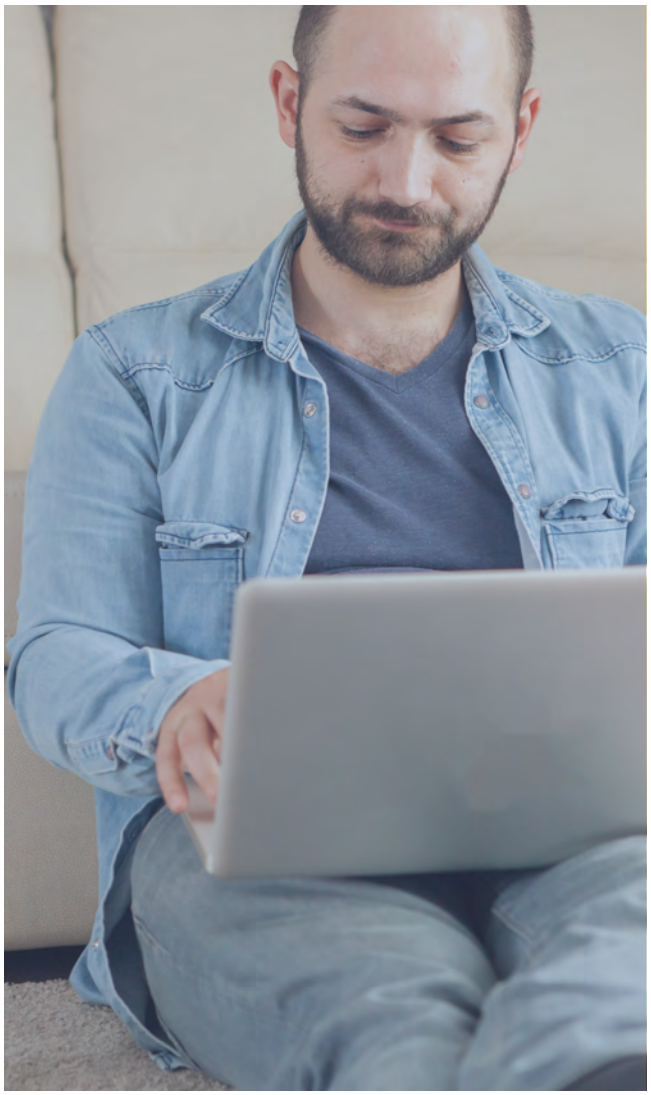
So, where does that leave us for security awareness?

Well, not in a very good place. People's guards are down more than ever as they struggle through remote working.

But while we can't always be there in person for every tech issue an employee has, we can equip them with some new knowledge to navigate this time.

In addition to regular security awareness training, provide education around some of the day-to-day IT tasks the employee needs to be able to accomplish, like updating firmware and properly locking devices.

This training can come in the form of new video training, a quick zoom call, or even a checklist the employee can follow.



As new threats evolve, continue to test your end users every month. Follow up with struggling employees, letting them know how they protect themselves against phishing and other cyber threats.

Finally, share tips for personal security with your employees. Share tips around public wifi, credit card skimmers, their bank password, and more. When employees understand that security affects their personal lives, they are much more likely to take that information and apply it to their *work lives.*

CHAPTER 7

SECURITY AWARENESS TOPICS TO COVER

Security Topics to Cover

Phishing
Learn how to spot and avoid cyber attacks via email.

Ransomware
Learn the effects that ransomware and other malware can have in your company.

Malware
Learn about malicious software and how to keep it out of your system.

Removable Media
How to correctly use removable media to avoid data theft/loss.

Social Engineering
How hackers use manipulation and trickery for fraudulent purposes.

Incident Response
learn how and when to report suspicious activity.

Mobile Security
How to keep your phones and other mobile devices safe and secure.

Physical Security
How to keep your office, desk, and other physical items secure.

Vishing & Scams
How to realize when a phone call is actually a scammer or hacker.

Passwords
Learn about what makes a strong password and how to use passwords correctly.

Safe Web Browsing
How to use the internet safely while protecting your sensitive data.

Working Remotely
Learn how working remotely introduces new risks and how to adapt to remote work safely.

CHAPTER 8

GETTING STARTED

Getting Started

Identify Risk. Create Awareness. Secure Your Business.

Launch, measure, and automate your phishing testing and security awareness training program with our easy to use platform.

Start your free 14-Day Free Trial to gain access to:

+ **Security Awareness Training**

  Equip your employees with a solid understanding of phishing, scams, malware, social engineering, physical security and more while giving them the ability to recognize and respond to cyber threats in the workplace.

+ **Automated Phishing Testing**

  We create new phishing tests every month and pair it with contextual training videos that match the phishing testing for the month.

+ **Psychological Security**

  Psychological Security, or PsySec, uses humor, repetition, a positive approach, and the latest research in neuroscience to train the part of the brain that houses threat recognition and response.

+ **Reporting With Actionable Insights**

  We provide more reporting data than anyone else on the market, which allows you to facilitate positive security discussions between you and your employees.

Get Started for Free