A Comprehensive Guide to

Security Awareness Training

FROM THE MANAGED SERVICES EXPERTS AT TPX

Executive Summary

In recent years, businesses have been under the growing threat of financially devastating cyberattacks. To make matters worse, successful breaches are increasingly the result of human error.

This guide looks at error-induced cyberattacks and how organizations can prevent them using security awareness training.

Key Takeaways

- Ninety percent of all data breaches are the result of human error.
- Security awareness training programs can reduce phishing email click rates by 75 percent.
- Security awareness training solutions should follow NIST guidelines to ensure content relevancy.
- MSPs take on the burden of content creation for security awareness training programs.

Table of Contents

INTRODUCTION

Successful Cyberattacks Start with Employees

Human error is the No. 1 cause of data breaches, accounting for more than 90 percent of all breaches. Your employees are your most significant liability in avoiding cyberattacks.

Increase in Successful Human Error-Induced Cyberattacks

Instances of cybercrime are exploding. Since the onset of the COVID-19 pandemic, **the FBI has reported a 300 percent increase** in reported cybercrimes.

The increase in attacks is partly due to businesses lacking a consistent formal security awareness training program. Only 25 percent of organizations allocate "two or more hours" to formal training annually, **Proofpoint's 2022 State of the Phish report** shows.

What makes matters worse is that employers are "punishing" and "disciplining" employees for real and simulated attacks even though they don't receive adequate training.

What Primary Forms of Cyberattack Target Your Employees?

Hackers target your employees with various ploys designed to gain access to your systems, including:

Phishing

Phishing is a data breach through social engineering. It's the bad guys fooling your employees into admitting them into your network or otherwise helping them commit cybercrimes against your business. Typically, the hacker disguises its email, phone, or other means of communication to appear as if it's coming from a legitimate source. Your staff is tricked into divulging critical information such as passwords or other sensitive data. Phishing might result in identity theft or financial theft through fake invoices or payroll diversion fraud, among other crimes.

Ransomware

Ransomware is a type of malware that encrypts data, so the perpetrator can demand a ransom payment to decrypt the data and restore access. Ransomware remains the most common cyberthreat to small and medium businesses (SMBs), with **60 percent of managed services providers (MSPs) reporting that their SMB clients have been hit as of third quarter of 2020**, Datto reveals.

Domain Spoofing

Domain spoofing is a form of phishing wherein an attacker impersonates a known business or person with a fake website or email domain to fool people into trusting them. This can be done by sending emails with false domain names that appear legitimate or by creating websites with slightly altered characters inside the URL that appear at-a-glance to be correct. A spoof website or email mimic the logos, navigation menu layouts and visual design of a legitimate enterprise or business. Victims of these attacks typically will be prompted to enter financial information or other sensitive data under the false belief that they're being sent to the right place.

Drive-by Downloading

Drive-by download attacks occur when malicious programs install on your computer or mobile devices without your consent as an unintentional download. A drive-by download can take advantage of an application, operating system (OS) or web browser that contains security flaws due to failures to update. Unlike a majority of other types of cyberattacks, a drive-by doesn't rely on the user to do anything to activate the attack. Once on your system, a drive-by download will hijack your device to build a botnet, infect other machines, extract information, destroy data or disable your device.

PART 1

What is Security Awareness Training?

Security awareness training is a formal process for educating an organization's employees and relevant third parties with system access on how to protect that organization's computer systems, data, people and assets from internet-based cyberattacks and security breaches.

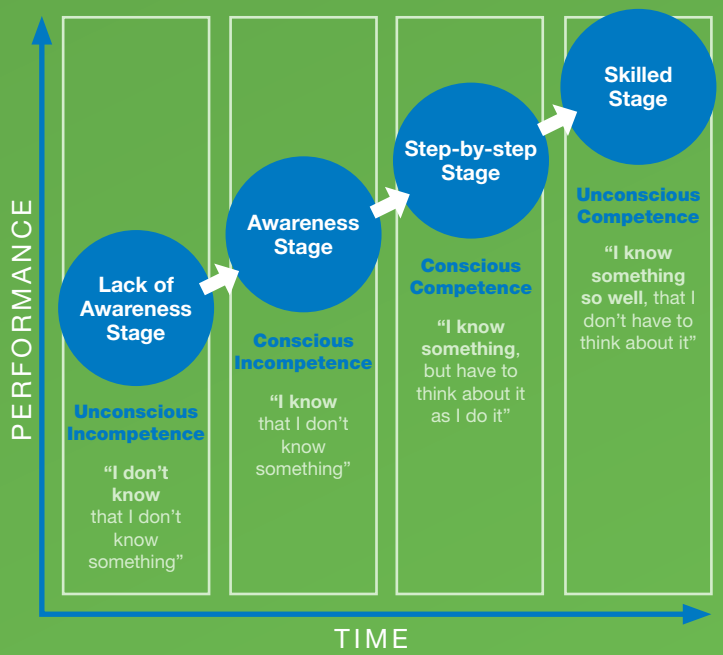
How Does Security Awareness Training Work?

The goal of security awareness training is to change user behavior.

The "Conscious Competence Ladder" developed by Noel Burch in the 1970s shows us how people progress through behavior change.

They start in the "lack of Awareness" stage and the goal is to get them to the "skilled" stage – where they can recognize and avoid cyberattacks without thinking about it.

It's at that point where you have success and genuinely changed behavior.

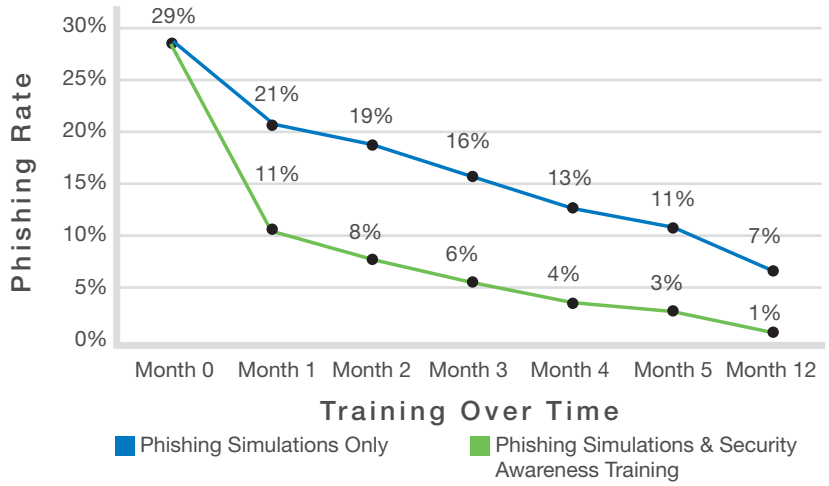


Noel Burch, Gordon Training International, Conscious Competence Lader, 1970s

How Does Your Business Achieve Security Behavior Change?

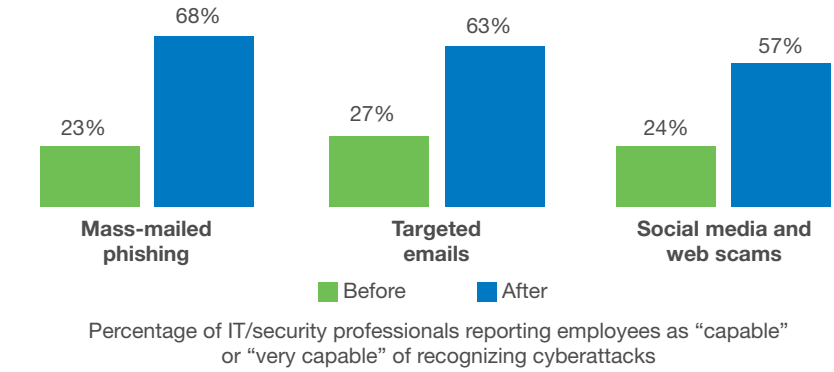
Combining phishing simulations with security awareness training coursework is a significant factor in your program's success.

Research from InfoSec Institute shows the combination not only results in a lower phishing rate over time, but leads to faster success – with lower rates happening sooner in the process.



Source: InfoSec Institute

Data from Osterman Research tells us that people are far more capable of recognizing cyberattacks after training. Organizations want to make sure to combine both phishing simulations and training in their security awareness program.



Source: Osterman Research, Inc.

What Elements Are Included in Security Awareness Training?

High-quality security awareness training programs typically include these key components:

Automated Reporting

Weekly reports are provided to managers and administrators to help your company track your progress toward meeting your security goals.

Scheduled Training Courses

Each month, existing learners will automatically be enrolled and invited via email to participate in that month's class. Monthly classes are online and self-paced. Courses follow the National Institute of Standards and Technology (NIST) curriculum guidelines.

Phishing Simulations

Enrolled learners will receive phishing simulation emails each month. Email templates and delivery times are randomized to improve their effectiveness.

PART 2

Why Should Businesses Invest in Security Awareness Training?

Security awareness training programs protect businesses from cyberattacks on their digital systems or attempted data breaches. Depending on the severity of a given incident, successful cyberattacks can be both crippling financially and damaging to the brand reputation, as the compromised company is viewed as a security risk.

Security awareness training helps everyone in an organization understand their role in helping combat information security breaches. When done effectively, security awareness training helps employees understand proper cyberhygiene, the security risks associated with their actions and ways to identify cyberattacks they may encounter via email and the web.

Cyberattacks Can Be Prevented by Security Awareness Training Programs

Security awareness training is proven effective. Seventy-seven percent of U.S. companies report that employee training has reduced cyberattack incidents, according to a **2017 Hiscox Cyber Readiness Report**.

Security awareness training programs enable your business to:

Expand Awareness to Reduce Cyberthreats

Proactive training helps your users learn how to recognize and avoid cyberattacks, which can significantly reduce the threat to your company.

Reduce Costs and Liabilities

Cyberattacks are expensive. A recent IBM study showed the average cost per data breach is $3.86 million.

Minimize Successful Phishing Attacks

Phishing is the top cyberattack method used by cybercriminals. According to InfoSec Institute, the right security awareness training program can reduce phishing email click rates by 75 percent.

PART 3

What Should Businesses Look for in Security Awareness Training?

Security awareness training is not a “check the box” solution, as the program’s quality is critical in rolling out an effective initiative at your company.

What Are Key Considerations in Selecting a Security Awareness Training Solution?

Businesses should look for the following components as part of their security awareness training solution:

1. Curated content following NIST guidelines to ensure the right topics are being taught
2. Short pieces of training at regular intervals
3. Engaging and relevant content
4. Randomized phishing email templates in simulated phishing emails
5. Automated tracking and metrics

What Are Common Mistakes Made in Selecting a Security Awareness Training Solution?

When selecting a security awareness training solution, businesses tend to make these mistakes:

Mistake 1

Focusing on flashy content instead of educating staff

Mistake 2

Only purchasing security awareness training or simulated phishing, rather than both solutions, which reinforces what employees have learned

Mistake 3

Keeping the same curriculum year to year, not updating for current tactics

Mistake 4

Not including assessments with educational videos to ensure understanding

Mistake 5

Longer training at irregular intervals

PART 4

Should Businesses Insource or Outsource Security Awareness Training?

Companies have two ways to address their security awareness training needs: they can take it on themselves or outsource it to a third-party, such as a qualified managed services provider (MSP).

Why Should Businesses Outsource Security Awareness Training?

Organizations like yours outsource their security awareness training instead of handling it in-house for these key reasons:

1. **Lack of Expertise –** The breadth and depth of knowledge demanded by IT teams today is vast and spans not only cybersecurity expertise but data storage, data integrity insight, software development, information technology infrastructure library (ITIL) knowledge, database design and management, network services, cloud computing, data analysis, troubleshooting and more. Security is a unique and complex discipline in itself.

2. **Lack of Time –** Due to the interconnected nature of integrated applications, devices and other technologies, IT departments are stretched thin, putting out fires. Many teams don't have the time to handle creating an effective security awareness training program.

3. **Lack of Talent –** The IT skills gap is a well-known challenge for businesses, especially SMBs that cannot typically pay for hard-to-source expertise. This skills gap is prominent in the hyper-specialized realm of cybersecurity and ransomware protection.

4. **Lack of Content Creation Resources –** A security awareness training program involves ongoing animated video scripting and production, automated if/then email sequence development and deployment, quiz/test creation and more. An in-house IT team would need to engage their in-house marketing resources or third-party marketing agencies to create content for their organization.

5. **Lack of a Learning Management System (LMS) –** To successfully track the effectiveness of a security awareness training program, the courses themselves have to operate on a system with the same functionality and capabilities as a full-blown LMS. Most organizations don’t have the technical expertise or resources required to develop an LMS to deliver the curriculum in the training program.

What Are the Benefits of Outsourcing Security Awareness Training?

Outsourcing security awareness training provides businesses with:

✓ Instant Access to Expertise

Outsourcing to an MSP delivers instant access to teams of trained personnel that are experts in protecting your business from cybercrime.

✓ Reduced Overhead

You won't need to hire, retain or train cybersecurity specialists in-house since the MSP takes care of that process and expense for you.

✓ Affordable, Predictable & Scalable Plans

Outsourcing security awareness training can be significantly less expensive than developing and deploying a sophisticated program internally. MSP solutions are scalable and offer predictable pricing, giving you control over your IT budget.

✓ The Ability to Focus on Your Business

Cybersecurity is a complicated undertaking and an entire business unto itself. By outsourcing, you can focus on managing and growing your core business.

✓ Subscription Consistency

The MSP has created ongoing content to deliver a consistent service with unique monthly programming for hundreds of clients. Your in-house IT department won't have to be concerned about gaps in programming, which is possible if taken on internally.

✓ LMS Investment Lies with MSP

The security awareness training program requires a full-scale learning management system (LMS) to facilitate the courses. The investment in creating this expensive resource is on the shoulders of the MSP, not an in-house IT team.

PART 5

Why Select an MSP for Your Security Awareness Training?

MSPs can provide reliable and consistent security awareness programs with security awareness training courses and email phishing simulations.

What Are Key Considerations in Selecting an MSP for Your Security Awareness Training?

Key considerations in deciding to use an MSP to manage your security awareness training include:

- Reducing IT overhead for managing and administering new courses
- Receiving expert guidance on what courses best fit your organizational needs
- Complementing your existing security resources, augment your efforts and increase your security posture
- Delivering a cost-effective solution with solid ROI

PART 6

What is TPx's Security Awareness Training Solution?

TPx's security awareness training solution empowers employees to be crucial to your defense against cyberattacks.

Key Features of TPx Security Awareness Training

Phishing Simulations

- Randomized phishing simulation emails are sent to all enrolled users on a regular basis
- Phishing users are automatically directed to customized training content
- Weekly tracking reports delivered via email

Awareness Training

- Monthly training courses sent automatically to each user and online dashboard to access courses
- Many courses available in multiple languages, user selected
- Weekly tracking reports delivered via email

Topics covered include:

- Phishing
- Password security
- Safe web browsing
- Social engineering
- Malware
- Mobile security
- Physical security
- Removable media
- Working remotely
- Vertical-specific training depending on the company (HIPAA, PCI, GDPR, etc.)

Key Benefits of TPx Security Awareness Training

- Educate employees on potential threats.
- Reinforce good cybersecurity habits.
- Incorporate employees into your security strategy.
- Outsource all setup and support to reduce management costs.
- Follow NIST guidelines to ensure topic relevance and accuracy.
- Improve retention and change behavior with short training delivered at regular intervals.
- Engage users with relevant content to keep them interested and focused on learning.
- Provide a cost-effective solution with a strong ROI.

PART 7

Why Choose TPx?

Running a business is challenging enough. You don't also need to worry about data breaches and the potentially catastrophic impact of cyberattacks on customer relations, operations, workflow and your bottom line. At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.

Security Awareness Training Services: What will TPx Do?

When businesses outsource security awareness training to TPx, we handle these key elements:

Onboard

TPx handles setup to reduce your management costs. We'll configure training with custom content following NIST guidelines. We'll program phishing simulations for your departments at pre-determined cadences.

Run

Once we have you onboard, we'll run random phishing simulation emails three times every month for each user and provide monthly training classes and assessments.

Support

TPx provides technical support, user management and campaign assistance as needed.

Report

We configure and send weekly user audits, phishing and training reports.

Security Awareness Training Services: What Won't TPx Customers Have to Do?

TPx's security awareness training clients can offload:

- Identifying & Creating Courses
- Configuring Simulated Phishing Campaigns
- Adding & Removing Users
- Testing Allow Listing

Why Choose TPx?

We solve the biggest IT issues – cybersecurity, connectivity and collaboration – under one umbrella.

Our buying power enables us to customize your solutions for maximum effectiveness within your budget.

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC and more.

We have the IT solutions, staff and experience you need for effective results within your budget.

We provide enterprise-class and 24/7 support for ongoing, proactive support tailored to your business.

We mix and match solutions and deliver a variety of service levels customized to meet your needs, including managed and co-managed options.

We modernize your IT, connectivity and communications while minimizing your risk from cyberthreats.

With 18,000 clients in 49,000+ locations, we're big enough to get the job done and small enough to be agile.

TPx is Your One-Stop Shop for Managed Security Services

Security Awareness Training

Users are your last line of defense. The more they know, the less prone they are to be victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and security awareness training courses with automated reporting to track your results.

Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your business from Internet-based threats. Next-generation firewalls block today's advanced threats while providing secure access, visibility and control to help your business be more productive.

Endpoint Management and Security

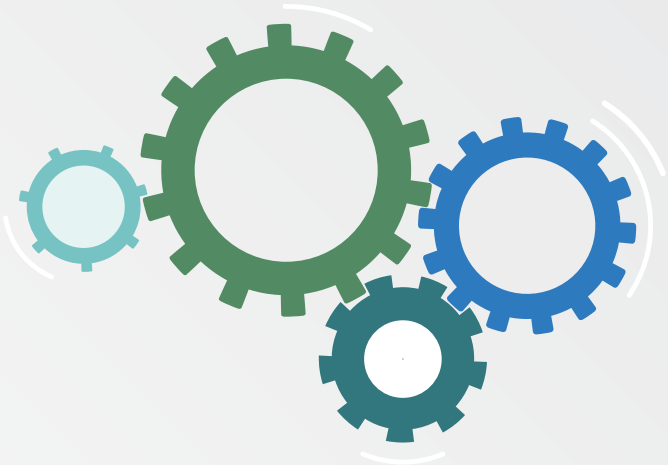
TPx helps keep your servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an "always on," best-in-class, 24/7/365 service.

Managed Detection and Response (MDR)

Discover, prevent and recover from cyberthreats faster. TPx's MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.



Email Security

Protecting your email communications is an important part of any security strategy. Whether it's protecting against email-based cyberattacks like phishing or ensuring that sensitive information doesn't fall into the wrong hands, we can help you navigate the email security challenge.

DNS Protection

We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless, and non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Backup and Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives.

Ransomware Detection

All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems as if it never happened.

Security Advisory Services

TPx advisory services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services comprise a cybersecurity gap assessment, network vulnerability and penetration scanning, network security assessment, wireless security assessment and ransomware readiness assessment.

PART 6

Glossary

Below are definitions of cybersecurity terms featured in this guide:

Phishing - Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person.

Spear Phishing - Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack.

Vishing - Short for “voice phishing,” vishing is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative.

Email Phishing - Email phishing is a scam wherein the attacker sends an email that looks legitimate and is designed to trick the recipient into entering information in reply or on a site the hacker can use to steal or sell their data.

HTTPs Phishing - This type of attack is carried out by sending the victim an email with a link to a fake website (see spoofing). The site may then be used to fool the victim into entering their private information.

Pharming - With pharming, malicious code is installed on the victim’s computer that sends the victim to a fake website designed to gather their login credentials.

Whaling - Whaling is a phishing attack that targets a senior executive who has deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.

Social Engineering - Social engineering uses psychological manipulation in an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Smishing - Smishing is phishing through some form of text message or SMS.

Spoofing - Spoofing is faking the sending address of transmission to gain illegal entry into a secure system or to induce a user or resource to take incorrect action.

Simulated Phishing - Simulated phishing is a campaign comprised of deceptive emails, similar to malicious or legitimate phishing emails, that are sent by an organization to their internal staff to gauge their response to email-based cybersecurity attacks. These emails are used to reinforce best security practices instilled through security awareness training.

Security Awareness Training - Security awareness training explains the proper rules of behavior for the use of information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed.

NIST - NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage and reduce their cybersecurity risk in an effort to protect their networks and data.

Ready to Take Charge of Your Security Awareness Training?

CONTACT US TODAY