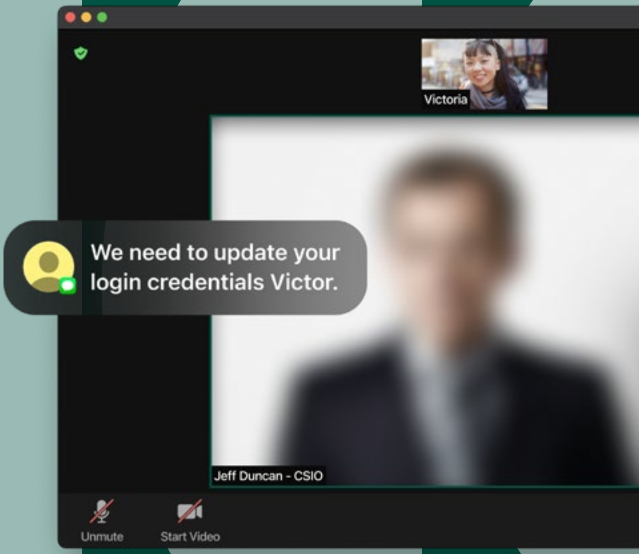
Adaptive

# Deepfake-Proofing Your Workforce

A Next-Gen Approach to Defending Against AI Phishing Attacks & Deepfakes

adaptivesecurity.com

# Traditional Security Awareness Training is Failing.



We need to update your login credentials Victor.

**In 2024, a multinational company fell victim to a sophisticated deepfake scam, resulting in a staggering $25 million loss.**[1] It occurred when a finance team employee, tricked by a video conference call featuring artificial intelligence (AI)-powered representations of the organization's chief financial officer and other team members, authorized a series of transactions to transfer funds from the company's account to the attackers without hesitation — all under the impression that they were, in fact, colleagues.

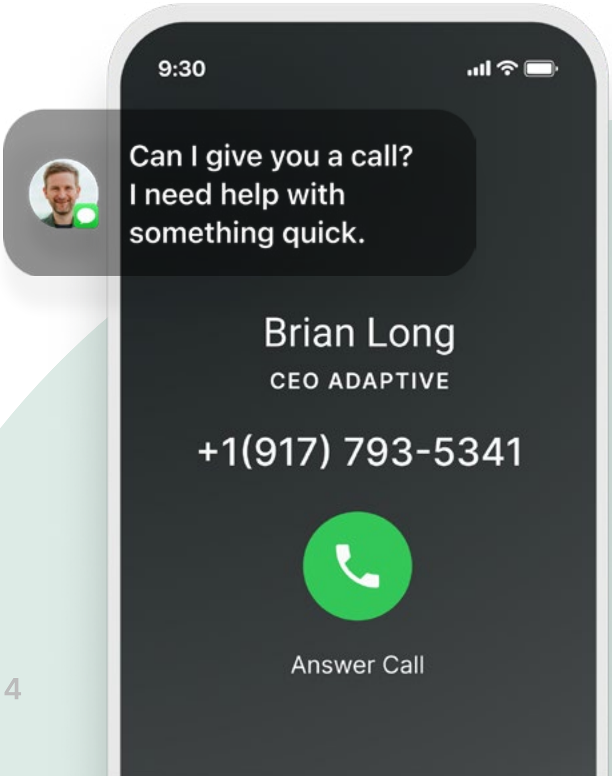
# What's Inside the Guide

**Employees are on the frontlines of a new, AI-powered battle as they face increasingly sophisticated attacks**, meticulously crafted to exploit human vulnerabilities. Deepfake voice and video scams, hyper-personalized phishing emails, and insidious social engineering tactics are becoming the norm, not the exception. The question is no longer if your organization will be targeted but when — and whether your workforce is prepared.

Traditional security awareness training, often characterized by infrequent, one-size-fits-all video modules and easily forgotten quizzes, fails to keep pace. It's like trying to fight a modern war with outdated weaponry.

A new approach is urgently needed: one that's adaptive, personalized, and purpose-built for the realities of the AI-powered threat landscape. It means moving beyond basic awareness and equipping your employees with the skills and knowledge they need to recognize and respond to evolving threats effectively.

In this guide, Adaptive Security helps you accomplish just that. We'll explore the changing threat landscape, expose the limitations of outdated security awareness training methods, and provide a clear, actionable roadmap for building a truly cyber-resilient workforce.



Can I give you a call? I need help with something quick.

Brian Long

CEO ADAPTIVE

+1(917) 793-5341

**92%**

**of companies have experienced financial loss due to a deepfake.**[2]

# The New Threat Landscape: Generative AI, Deepfakes, and Beyond

## Rising Threats: Understanding Generative AI-Powered Cyberattacks

Generative AI is rapidly transforming industries, creating unprecedented opportunities for innovation and efficiency. But this technology has a dark side, too.

In the hands of cybercriminals, AI is a formidable weapon that enables attacks with far more sophistication, personalization, and difficulty to detect than anything seen before. See, this isn't science fiction anymore. It's the new reality of cybersecurity.

To understand the evolving threats, understand the strategies and tools used. Let's break down areas where AI is revolutionizing cybercrime.

✉ **Email**

🎤 **Voice**

▶ **Video**

💬 **SMS**

## Generative AI Phishing: The Perfect Lure

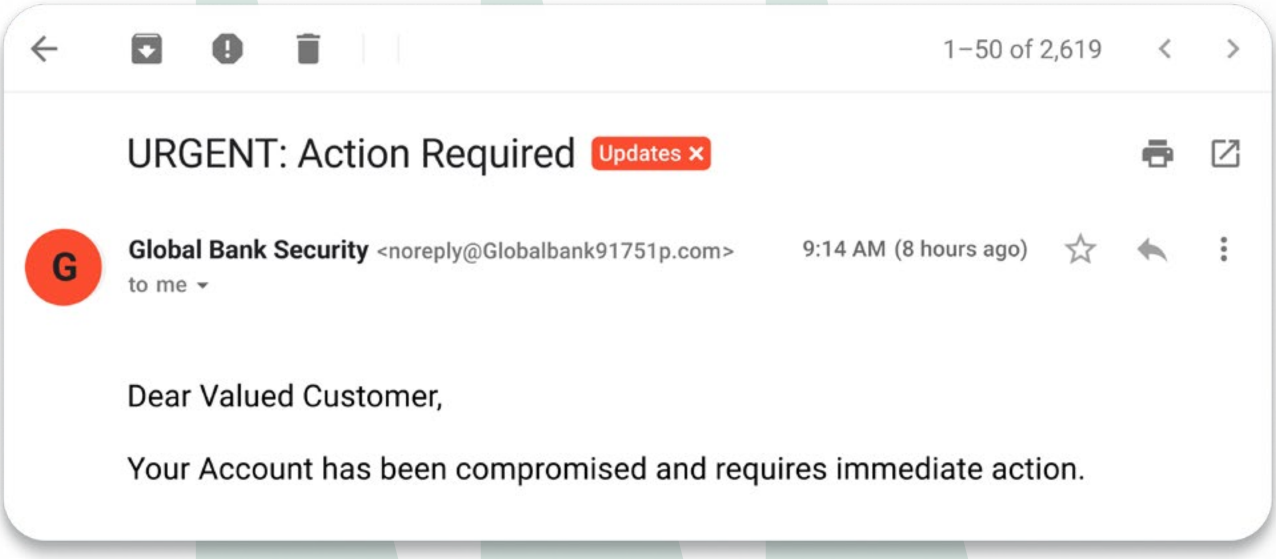
Traditional phishing emails often contain telltale signs, including grammatical errors, generic greetings, and suspicious links. Generative AI, however, is changing that.

Here's how generative AI-powered phishing works:

- **Hyper-Personalization**: AI algorithms analyze open-source intelligence (OSINT), publicly available data, from company websites, news articles, and social media profiles, to craft highly personalized phishing attacks tailored to the target's specific role and interests.

- **Perfect Grammar & Context Relevancy**: AI generates emails and other communications free of the errors that often give away traditional phishing attempts, mirroring the language and tone of legitimate communications and making them difficult to identify.

- **Automated & Dynamic to Scale**: AI generates and deploys thousands of personalized phishing attempts in moments, dramatically increasing reach while analyzing responses to improve success rates.



URGENT: Action Required

Global Bank Security <noreply@Globalbank91751p.com>
to me

9:14 AM (8 hours ago)

Dear Valued Customer,

Your Account has been compromised and requires immediate action.

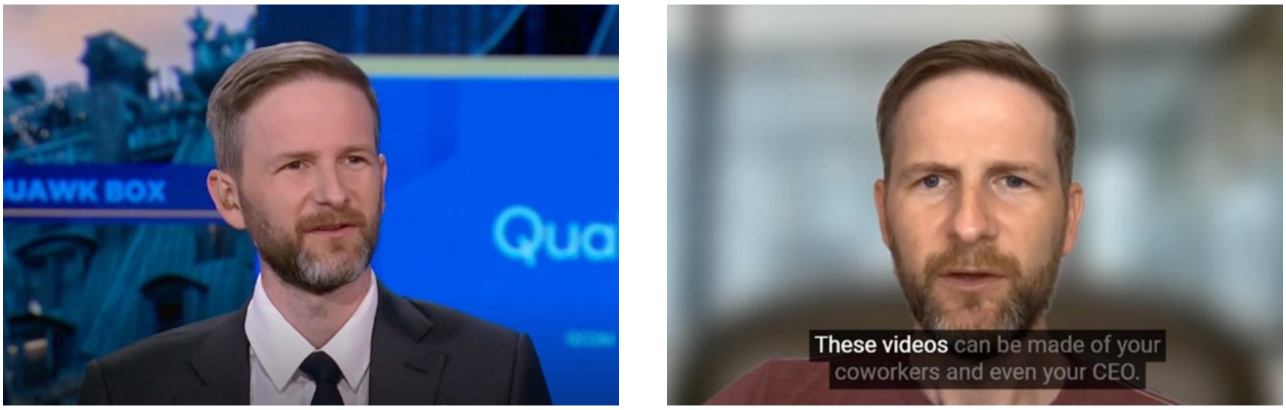
## Deepfakes: The Art of Deception in a Digital World

Deepfakes are images, videos, and audio recordings that have been digitally manipulated to convincingly depict someone saying or doing something they never actually did.

Think of a deepfake as an enhanced Photoshop powered by machine learning algorithms and applied to all media types.

Algorithms that generate deepfakes learn from vast amounts of data surrounding a target individual, analyzing their facial expressions, voice patterns, and mannerisms to then generate new content that mirrors their appearance and voice with astonishing accuracy.

**Left: Actual image, right: AI-gen deepfake of Adaptive CEO Brian Long**


UAWK BOX
Qua
These videos can be made of your coworkers and even your CEO.

The evolution of deepfakes is far from plateauing. Hyper-realistic rendering and real-time manipulation continue accelerating and will only grow more challenging to identify. It's also critical to realize that deepfakes aren't made by criminal enterprises alone.

With tools like ChatGPT, Gemini, and Deepseek widely available, the ability to generate sophisticated deepfakes is accessible to billions of people around the world.

### Video Manipulation

Through a video conference call or message from a trusted source, the other party looks and sounds like the colleague portrayed to deceive an individual or damage a company's reputation.

### AI Voice Cloning

An executive, senior leader, or colleague calls an employee via phone to make an urgent request, and their voice sounds natural and identical to the person portrayed.

### Disinformation Campaigns

Deepfakes can be used to spread false information and manipulate public opinion, causing social unrest that causes employees to question their decisions.

**4,151%**

**Increase in phishing attacks since the launch of OpenAI's ChatGPT.**[3]

## Smishing, Quishing, and Social Engineering: Exploiting Trust

Given the significant augmentation in AI's capabilities in recent years, smishing and quishing remain popular tactics for attackers seeking to obtain company and customer data.

Smishing, or SMS phishing, mirrors the tactics of traditional email phishing but utilizes text messages as the delivery mechanism to trick recipients into clicking a malicious link or revealing sensitive information. Text messages used for smishing typically appear to come from legitimate sources, such as banks, delivery services, or colleagues.

Generative AI plays a crucial role in enhancing smishing attacks by enabling the creation of personalized messages and continuing the conversation in real time, just as an actual person would.

Quishing, or QR code phishing, leverages the convenience of QR codes to direct victims to malicious websites or unwanted actions like downloading software. Attackers embed malicious URLs within QR codes, which, when scanned, redirect recipients without revealing the destination address until it's too late.

Here's how AI is transforming social engineering attacks, including smishing and quishing, from an art into a science for hackers:

- **Automated Reconnaissance:** AI algorithms scour vast amounts of online data, including public records, online forums, and social media profiles, to gather comprehensive information about potential targets. This allows attackers to identify interests, relationships, and vulnerabilities to craft personalized attacks.

- **Creating Fake Personas**: AI creates convincing fake personas with realistic online profiles and footprints. Typically, these personas infiltrate online communities, such as LinkedIn, to build trust and then exploit that trust for malicious purposes.

- **Chatbots for Deception**: AI-powered chatbots engage in natural and realistic conversations to gather information, build rapport, and subtly guide targets toward taking actions that compromise security.

- **Deepfake Technology**: AI generates realistic video or audio, known as a deepfake, of a trusted person to request sensitive information or demand money. Due to their realism, deepfakes can bypass even the most cautious employees, as seeing or hearing a trusted colleague is convincing.

**8.9-14.5%**

**Average SMS click-through rates.**

**433%**

**QR code scans are up 433% over the last four years.**

# Why Traditional Security Awareness Training is Falling Short

## The Training Gap: Your Current Program Leaves You Open to Attacks

Traditional security awareness programs fail to keep pace with the new threat landscape. The uncomfortable truth is that most traditional approaches aren't equipped to prepare employees for imminent, sophisticated threats.

For years, training against attacks has often been treated as a compliance-driven, check-the-box exercise. Employees sit through a yearly program, click through a few modules, and take a multiple-choice quiz. While this approach would've offered basic protection in the past, it's woefully inadequate in the face of today's threats.

## One-Size-Fits-All Doesn't Fit Anyone

Traditional training often delivers the same generic content to every employee, regardless of their role, technical expertise, or risk profile.

An employee on the finance team, for example, needs in-depth training on recognizing deepfake voice scams and sophisticated phishing attempts targeting financial transactions. An employee in human resources, on the other hand, needs to focus on protecting employee privacy, understanding data protection regulations (like GDPR), and recognizing social engineering tactics aimed at obtaining personal information. Generic training fails to address these distinctions and leaves significant gaps in your company's defenses.

## Outdated Content Against Moving Targets

With the cybersecurity landscape in constant flux, new threats emerge daily, and attackers continuously refine their techniques. Traditional training programs, often updated infrequently (if at all), quickly become obsolete.

Imagine a training module from 2020 trying to prepare employees for a deepfake CEO voice scam or an AI-generated phishing email that mimics a colleague's writing style. It wouldn't be relevant due to the increased sophistication and realism, and employees would be left vulnerable to attacks they haven't been trained to recognize.

## Missing or Half-Baked Simulations

Legacy solutions used for security awareness training struggle to offer multi-channel phishing simulations because they're unable to offer them at all, or the simulations they can offer lack any customization to put employees' knowledge to the test.

## Lack of Engagement

Everyone agrees that training programs, in their current state, feel boring. Long, dry presentations and quizzes filled with technical jargon and abstract concepts are unlikely to capture employees' attention or lead to lasting behavioral change.

Passive learning and lack of interactivity lead to low engagement and poor knowledge retention, which means employees won't be able to apply information when it matters most: in the face of an actual attack.

## Infrequent Training: The Forgetting Curve

Even if your training program today is somewhat engaging, the 'forgetting curve' is a powerful force. Studies have shown that people rapidly forget information they've learned if it's not regularly reinforced.[4]

Annual training sessions, the standard in many organizations, aren't frequent enough to maintain a high level of security awareness. It leaves employees vulnerable between training sessions, creating massive windows of opportunity for attackers.

## Limited Focus on Social Engineering

Traditional training focuses heavily on technical aspects of security, such as passwords and software updates, while neglecting the human element. Social engineering attacks, which exploit human psychology to trick people into making mistakes, are a major threat vector, and their effectiveness is amplified by AI.

An employee might have a strong password and keep their software up to date but still fall victim to a cleverly crafted phishing email or a deepfake voice scam that plays on their emotions or sense of urgency.

## Missing Measurement & Personalization

Many traditional programs for security awareness training lack robust capabilities for tracking employee progress, identifying areas of weakness, and tailoring training to individual needs. Without data-driven insights, it's impossible to know whether your training is actually effective or in need of targeted improvements.

You're essentially flying blind, with no way to measure the return on investment (ROI) of your training program or to identify and address specific vulnerabilities within your workforce.

## Consequences of Inadequate Security Awareness Training

### Financial Losses

Data breaches, ransomware attacks, and fraud cost companies millions of dollars in direct losses, recovery expenses, and legal fees.

### Reputational Damage

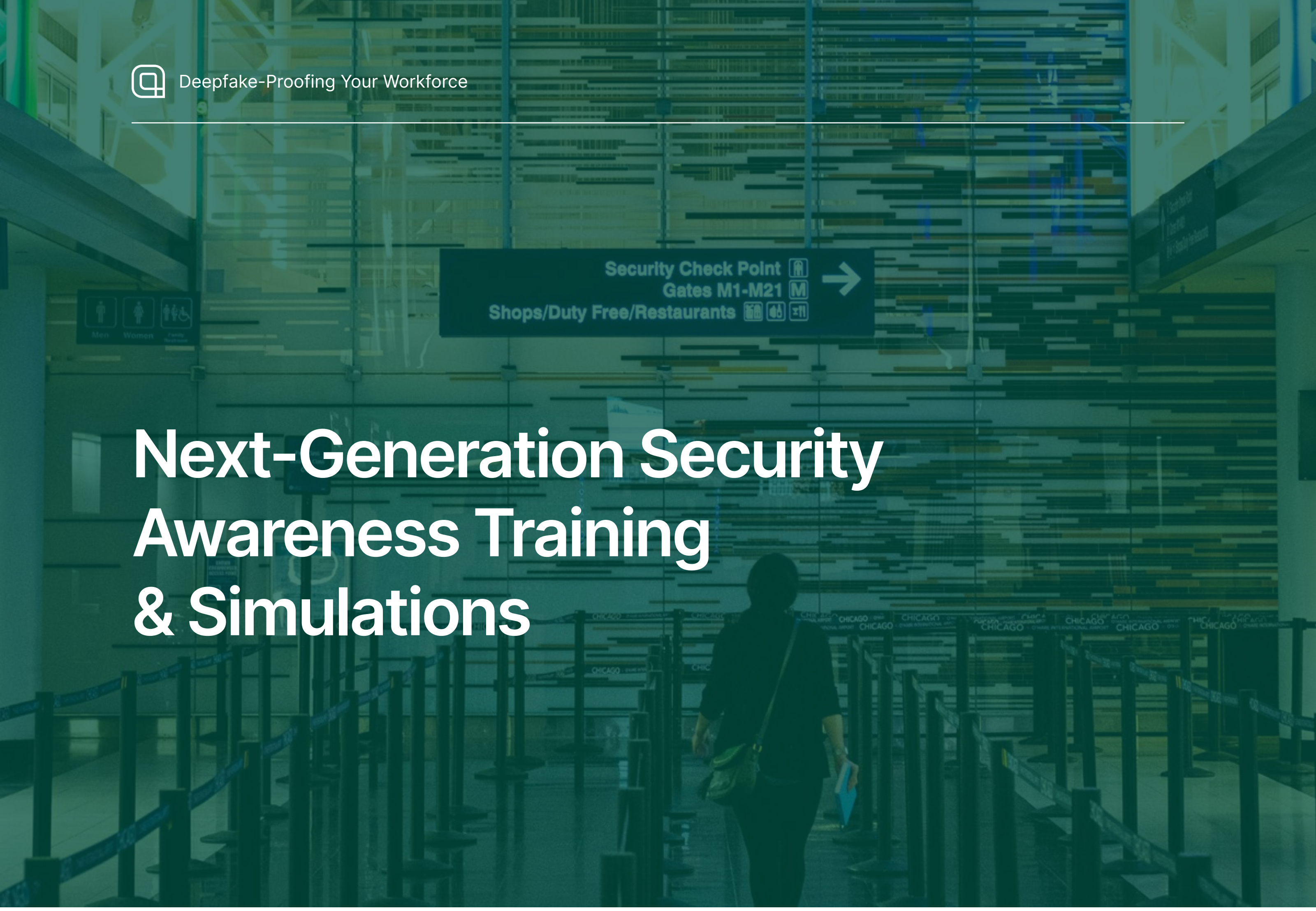
A successful cyberattack erodes customer trust, damages your brand, and leads to long-term business consequences.

### Legal & Regulatory Issues

Sensitive customer data, intellectual property, and financial information can be stolen and exposed, leading to liabilities and fines.

### Operational Disruptions

Security incidents shut down critical systems and processes, disrupt business operations for several weeks, and lead to lost productivity.



# Next-Generation Security Awareness Training & Simulations

## Building a Resilient Workforce: A New Approach to Security Awareness

Protecting your organization and its workforce from the evolving landscape of AI-powered cyber threats demands a fundamental shift in how you approach security awareness training, and it all starts with a platform like Adaptive Security — highly personalized to your company with custom deepfakes, role-based content, and infinite customization in an always-growing content studio.

Let's dig into what a next-generation platform for security awareness training and simulations looks like so you can empower your employees as a human firewall and the first line of defense, not your weakest link.

**Continuous, Adaptive Learning**

**Personalized Training Paths**

**Generative AI-Powered Simulations**

**Multi-Channel Training**

**Automated Reporting & Compliance**

**Measurable Results & ROI**

## Continuous, Adaptive Learning

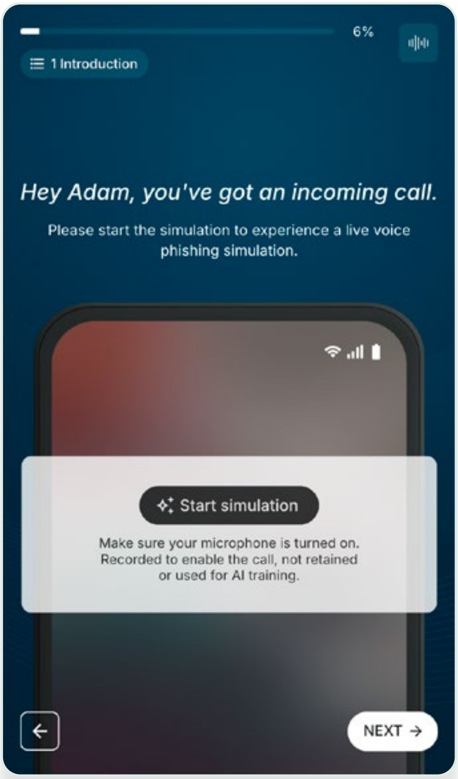
Being that the cybersecurity landscape isn't a static entity, new threats emerge daily, attacker tactics evolve rapidly, and vulnerabilities are discovered and exploited with alarming speed. To keep pace, training must be continuous, not a once-a-year event or a sporadic, reactive response in the aftermath of incidents.

Here's what that means with Adaptive Security's platform:

**Automated Content Updates:** Your training and simulation platform should automatically update its content to reflect the latest threats, vulnerabilities, and best practices. This ensures that employees always learn about the most relevant risks, keeping their knowledge fresh and applicable. This is pivotal in the age of AI-powered attacks, where new techniques are constantly developing.

**Microlearning:** Break down complex topics into short, digestible modules such as 3-5 minute videos, interactive exercises, and quick quizzes. Known as microlearning, this approach offers several advantages:

- **Improved Knowledge Retention:** Shorter bursts of information are easier to absorb and remember than lengthy lectures.
- **Increased Engagement:** Employees are more likely to engage with short, focused content that fits easily into their busy schedules.
- **Flexibility:** Microlearning modules can be accessed anytime, anywhere, and on any device to make training more convenient.



*Hey Adam, you've got an incoming call.*

Please start the simulation to experience a live voice phishing simulation.

Make sure your microphone is turned on. Recorded to enable the call, not retained or used for AI training.

In-module simulations provide employees with a continous, adaptive learning experience.

**Regular Refreshers:** Implement short quizzes, simulated phishing tests, or security reminders at regular intervals. This keeps security top-of-mind and reinforces learning over time, and the ongoing reinforcement helps combat the 'forgetting curve' and builds lasting behavioral change. It also allows for the continuous assessment of employee knowledge and identification of areas needing further attention.

**Adaptive Learning Paths:** The platform should learn, too. Based on assessment results, refresher exercises, and simulation data, your platform needs to provide materials that target areas where specific teams and employees display weakness.

The inherent ability to update content, deliver microlearning experiences, and tailor refreshers demonstrates the adaptive nature of a next-generation platform, responding to both external threats faced by an organization and its internal learning needs.

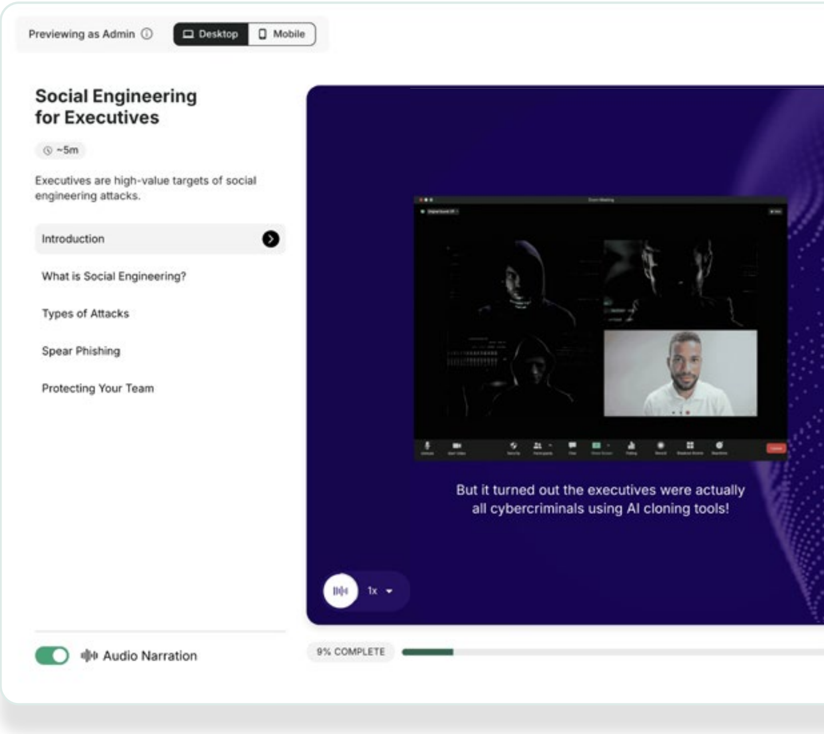
## Personalized Training Paths

Every employee is different, from their roles and levels of technical expertise to their learning styles and levels of exposure to risk. A one-size-fits-all approach to training inevitably leaves gaps, creating vulnerabilities that attackers deliberately exploit. Personalized, role-based training addresses this by tailoring the learning experience to the individual.

**Risk Assessments:** A next-generation training and simulation platform begins by assessing each employee's individual vulnerabilities and risk profile. This might involve analyzing their role, team, access levels, past performance in simulated phishing tests, and self-reported security habits.

**Role-Based Training:** Tailor training content to the specific responsibilities and potential threats faced by different teams and roles within the organization. For example:

- **Executives:** Specialized training on deepfake voice scams, spear phishing attacks targeting high-value individuals, and business email compromise (BEC).
- **Finance Team:** In-depth training on recognizing fraudulent invoices, verifying wire transfer requests, and identifying social engineering attempts targeting financial transactions.
- **Customer Service Representatives:** Focused training on identifying and reporting suspicious emails, handling sensitive customer data securely, and recognizing social engineering attempts through phone calls or online chats.



Social Engineering for Executives

~5m

Executives are high-value targets of social engineering attacks.

But it turned out the executives were actually all cybercriminals using AI cloning tools!

**From the front lines to the C-suite, every employee needs role-based, personalized training.**

- **IT Staff:** Requires advanced training on technical security topics, vulnerability management, incident response, and the latest attack techniques.

**Learning Styles:** Offer training in various formats, including text, video, interactive exercises, and gamified modules, to accommodate different learning styles and preferences. Some employees learn best by watching, others by reading, and others by doing. Providing options increases engagement and knowledge retention.

By tailoring the learning experience to the individual, the training becomes adaptive, focusing resources where they're most needed and maximizing the effectiveness of the security awareness training program. It's about delivering the right training to the right person at the right time.

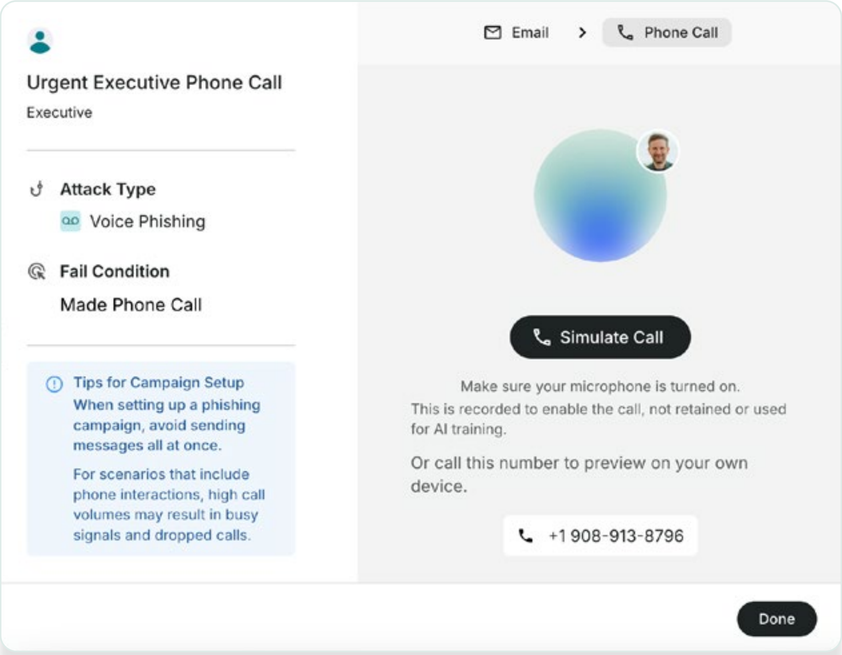
## Generative AI-Powered Simulations

Experiencing real-world attacks is the most effective way to prepare employees for, well, real-world attacks. But that's simply unrealistic to consider, so realistic simulations in a safe, controlled environment become crucial.

Simulations bridge the gap between theory and practice, allowing employees to apply their knowledge and develop critical thinking skills in a risk-free setting:

**Deepfake Simulations:** Expose employees to realistic deepfake video and audio scenarios, teaching them to identify subtle clues (such as unnatural lip movements, inconsistencies in video or audio quality, or illogical context) and to question specific requests, even if they appear to come from a trusted source. These simulations should be varied and challenging, reflecting the sophistication of generative AI.

**Phishing Email Simulations:** Send simulated phishing emails that mimic the latest attack techniques, including AI-generated content and personalized lures. Track click rates, provide immediate feedback to those who fall for the simulation (explaining why it was a phishing email), and offer targeted remediation training to reinforce learning.



Urgent Executive Phone Call

Executive

Attack Type

Voice Phishing

Fail Condition

Made Phone Call

Tips for Campaign Setup

When setting up a phishing campaign, avoid sending messages all at once.

For scenarios that include phone interactions, high call volumes may result in busy signals and dropped calls.

Make sure your microphone is turned on.

This is recorded to enable the call, not retained or used for AI training.

Or call this number to preview on your own device.

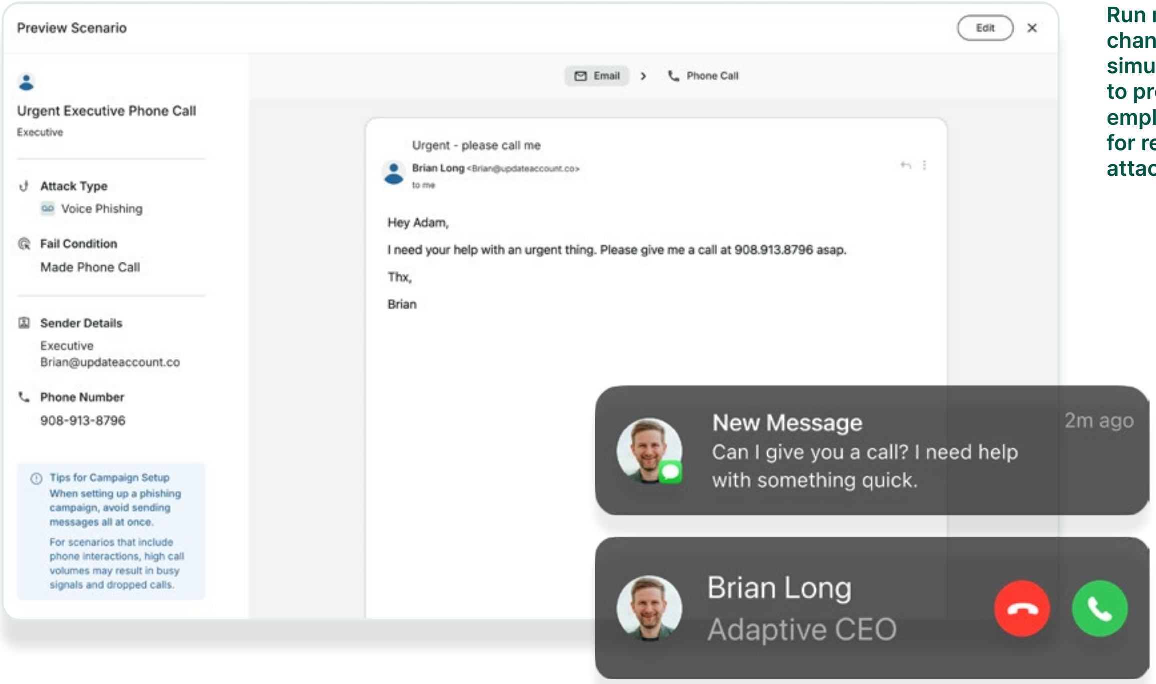
+1 908-913-8796

**Prepare employees with real-world phishing simulations.**

**Smishing & Social Engineering Simulations:** Extend simulations beyond email to cover other attack vectors, such as SMS messages ('smishing'). This prepares employees for a wider variety of threats and reinforces the importance of vigilance across all channels. For example, a simulated phishing attack might involve a text message claiming to be a bank, urging the recipient to click a link to resolve an urgent account issue.

The use of generative AI in simulations allows for a level of realism that was previously impossible for security awareness training, and it creates a dynamic and adaptive testing environment that reflects the rapid evolution of real-world attacks.

Simulations through Adaptive Security, for example, can be automatically adjusted based on real-world data, courtesy of open-source intelligence, and employee performance, providing more challenging scenarios for those who excel and more support for those who struggle.



Urgent Executive Phone Call
Executive

Attack Type
Voice Phishing

Fail Condition
Made Phone Call

Sender Details
Executive
Brian@updateaccount.co

Phone Number
908-913-8796

Tips for Campaign Setup
When setting up a phishing campaign, avoid sending messages all at once.
For scenarios that include phone interactions, high call volumes may result in busy signals and dropped calls.

Urgent - please call me
Brian Long <Brian@updateaccount.co>
to me

Hey Adam,

I need your help with an urgent thing. Please give me a call at 908.913.8796 asap.

Thx,

Brian

New Message 2m ago
Can I give you a call? I need help with something quick.

Brian Long
Adaptive CEO

**Run multi-channel simulations to prepare employees for real-world attacks.**

## Multi-Channel Training

Attackers don't limit themselves to one channel, so your security awareness training program shouldn't either. A comprehensive program covers all relevant attack vectors and provides a holistic approach to security awareness.

**Comprehensive Coverage:** Address threats across email, SMS, social media, phone calls, and physical security. This ensures that employees are prepared for attacks from any direction.

**Integrated Approach:** Ensure training across channels reinforces the same core security principles, creating a consistent and cohesive learning experience.

Multi-channel training also provides an opportunity to use varied approaches in an adaptive manner. The training isn't just delivered over multiple channels; instead, it's integrated so that the channel matches the message.

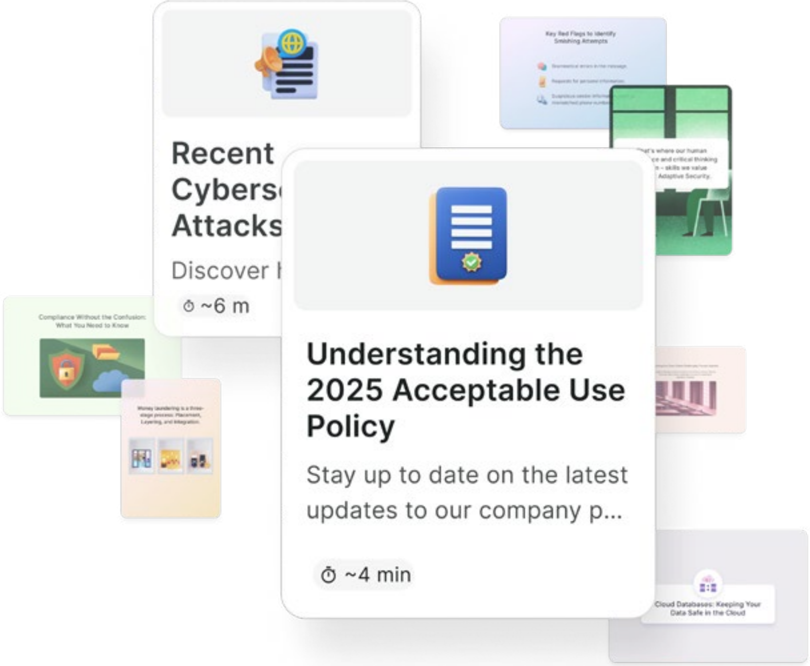
**60%** **of data breaches occur with human involvement, underscoring the human firewall's importance to a strong security posture.**

## Automated Reporting & Compliance

Launching an impactful training program is an achievement, but sustained effectiveness demands continuous monitoring and adaptation. Beyond the initial rollout, ensure your program thrives over time.

In addition, navigating the complexities of regulatory compliance is non-negotiable. Organizations across all industries face requirements — HIPAA, GDPR, PCI DSS, CCPA, and more — each carrying the potential for substantial penalties in the event of a data breach. With this in mind, a training program should educate employees and demonstrate adherence.

A next-generation training platform like Adaptive Security empowers you to streamline reporting and compliance, transforming the potential burden into a strategic advantage.


Recent
Cybers
Attacks
Discover
~6 m
Understanding the 2025 Acceptable Use Policy
Stay up to date on the latest updates to our company p...
~4 min
Key Red Flags to Identify Smishing Attempts
Compliance Without the Confusion: What You Need to Know
Money laundering is a three-stage process: Placement, Layering, and Integration.
Cloud Databases: Keeping Your Data Safe in the Cloud

**Real-Time Performance Analytics:** Move beyond basic tracking. Gain instant insights into employee engagement, completion rates, and proficiency through interactive dashboards. Ultimately, this allows you to identify knowledge gaps and tailor future training for maximum impact.

**Automated Compliance Documentation:** Generate comprehensive, board-ready reports that prove employee understanding of best practices, internal policies, and relevant regulations.

**Audit Trails:** Maintain a secure, detailed record of all training activities by capturing every interaction, from module completion to quiz scores, and providing a transparent and verifiable history of your program's effectiveness.

**Proactive Risk Mitigation:** Leverage data-driven insights to identify potential compliance vulnerabilities and pinpoint areas where employees may be struggling and implement targeted interventions to prevent breaches and avoid costly fines.

The transition to automated reporting and compliance is transformative, eliminating time-consuming administrative tasks and unlocking a holistic, data-driven view of your organization's security posture.

With a seamless data flow, you can provide stakeholders with board-ready reports that demonstrate the program's effectiveness and ongoing relevance.

## Measurable Results & ROI

You need to know if your training program is actually working and demonstrate its value to stakeholders, including executive leadership. This requires clear metrics and reporting that legacy solutions aren't designed to uncover in any meaningful capacity.

**Key Performance Indicators (KPIs):**

- **Phishing Click Rates:** The percentage of employees who click on malicious links in simulated phishing emails or text messages. A decreasing click rate over time indicates improved awareness and behavioral change.

- **Incident Reports:** The number of security incidents reported by employees. Increased reporting could indicate improved vigilance and a willingness to report any suspicious activity.

- **Employee Knowledge Scores:** Assess employee understanding of security concepts through quizzes and assessments, both before and after training.

- **Completion Rates:** Track the percentage of employees who complete required training modules.

- **Remediation Completion Rates:** For employees who fail simulations, track if they take and complete additional training.

**Reporting & Analytics:** Provide dashboards and reports that visualize training effectiveness, identify areas of weakness within the organization or specific teams, and track progress over time. These reports should be easily customizable and accessible to relevant stakeholders.

**Demonstrate ROI:** Show how the training program is reducing risk, preventing costly incidents, and contributing to the organization's bottom line.

- **Estimate the potential** impact of a data breach and compare it to the cost of security awareness training.

- **Quantify the reduction** in phishing click rates and correlate it to a decrease in the likelihood of a successful phishing attack.

- **Highlight improvements** in employee security behavior and the overall security posture of the organization.

A data-driven approach with continuous monitoring and reporting allows for an adaptive strategy that enables you to fine-tune your training program based on real-world performance and emerging threats. You can identify areas where employees are struggling, adjust the training program accordingly, and continuously improve the program's effectiveness.

# Implementing a Next-Generation Training Program: A Step-by-Step Guide

## Putting It Into Practice: A Roadmap to Resiliency

You understand the threats. You recognize the limitations of traditional training. Now, it's time to take action.

Implementing a program for next-generation security awareness training and simulations doesn't need to feel daunting. By following a structured approach, you'll build a robust and effective program that empowers employees and strengthens your organization's defenses.

**Step 1: Assess Your Current Security Training Needs**

**Step 2: Define Clear Goals & Objectives**

**Step 3: Choose the Right Training Platform (& Partner)**

**Step 4: Develop a Comprehensive Training Curriculum**

**Step 5: Launch & Promote Your Training Program**

**Step 6: Monitor, Measure, and Iterate**

## Step 1: Assess Your Current Security Posture & Training Needs

Before you build or overhaul your training program, understand your starting point. Conduct a thorough assessment of your current security posture and a clear identification of training needs.

**Conduct a Risk Assessment**
Identify your organization's most critical assets and the threats they face.

- **Penetration Testing:** Simulate real-world attacks to identify weaknesses in defenses.

- **Threat Modeling:** Analyze potential attack scenarios and pinpoint likely threats to your organization.

- **Data Inventory:** Classify the sensitive company, employee, and customer data you hold and assess the risks associated with its compromise.

**Evaluate Existing Training (If Any)**
Review your current training program to protect against cybersecurity threats (if you have one) and ask yourself a series of questions.

- **What topics are covered?**
- **How is the training delivered? What formats are offered?**
- **How frequently is training conducted?**
- **How is the effectiveness of training measured (if at all)?**
- **What feedback have you received from employees about the training?**

**Identify Training Gaps**
Based on your risk assessment and evaluation of existing training, identify the areas where your employees are most vulnerable and where training is most needed.

**Consider Industry-Specific Regulations**
Consult with your organization's legal counsel to understand any specific regulatory requirements you must comply with, like HIPAA for healthcare, GDPR for data privacy, and PCI DSS for payment card security.

**~2X** **Medusa attacks observed in January and February 2025 as in the first two months of 2024.**

## Step 2: Define Clear Goals & Objectives

What do you want to achieve with your training program? Setting clear, measurable goals is essential for success as it determines the approach you'll take.

**Be Specific & Measurable**
Don't just say, "We want to improve security awareness." Instead, set specific, measurable, achievable, relevant, and time-bound (SMART) goals.

Here are a few examples:

- ✓ **Reduce phishing click rates by 50% within six months.**
- ✓ **Achieve 100% employee participation in mandatory training modules within three months.**
- ✓ **Increase employee reporting of suspicious emails by 25% within one year.**
- ✓ **Improve average employee scores on security knowledge assessments by 20% within six months.**

**Align with Business Goals**
Ensure that training objectives support your overall business goals and risk management strategy.

**Prioritize**
Focus on the most critical threats and vulnerabilities first. As your training program gets off the ground and you're finding success, expand to a broader array of incidents you want employees to prepare for.

## Step 3: Choose the Right Training Platform (& Partner)

Selecting the right platform for next-generation security awareness training and simulations is the difference between preparing your workforce to shield against all threats and falling victim to a devastating attack.

| | | Legacy Solutions | Adaptive |
|---|---|---|---|
| **AI Phishing Simulations with OSINT** | Deploy realistic simulations of sophisticated threat vectors including deepfake video, AI voice cloning, and traditional phishing through email and texting | ✗ | ✓ |
| **Limitless Customization** | Customize training modules and simulations specifically for your brand from an enormous library of content | ✗ | ✓ |
| **Personalized Learning Paths** | Tailor training content to individual roles, risk profiles, and learning styles | ✗ | ✓ |
| **Automated Content Updates** | Receive regularly updated content library to reflect the latest threats and best practices | ✗ | ✓ |
| **Multi-Channel Delivery** | Deliver training across all channels where employees experience threats | ✗ | ✓ |
| **Robust Reporting & Analytics** | Comprehensive dashboards and reports to track progress, measure effectiveness, and demonstrate ROI | ✗ | ✓ |
| **Ease of Use & Administration** | Navigate an intuitive user interface for both administrators and employees | ✗ | ✓ |
| **Integration with Existing Systems** | Integrate with existing people management and security infrastructure | ✗ | ✓ |
| **Scalability** | Handle present needs and quickly scale with future growth | ✗ | ✓ |

## Step 4: Develop a Comprehensive Training Curriculum

With a platform selected, it's time to develop the content of your training program.

**Cover Core Security Topics**
Employees, regardless of role or team, should be familiar with core security topics:

- **Phishing and smishing, with an emphasis on AI-generated threats**
- **Deepfake recognition and response**
- **Social engineering tactics and prevention**
- **Password security best practices**
- **Data privacy and protection, including relevant regulations**
- **Incident reporting procedures**
- **Safe web browsing and email habits**
- **Mobile device security**
- **Physical security awareness**

Remember that you'll adapt which topics to go deeper or pull back on, so it may be unnecessary to cover each with equal depth. It's still essential to cover all of the core topics in some capacity, however.

**Tailor Content to Roles**
Customize the training content for different roles within your organization. Between different and within the same teams, roles take on unique responsibilities with access to sensitive data; therefore, training needs to be tailored with role-specific content to maintain relevancy.

**Use a Variety of Formats**
Diversify the content types to keep employees engaged, including:

- **Short videos**
- **Interactive exercises**
- **Simulated phishing tests**
- **Quizzes and assessments**
- **Gamified modules**
- **Infographics and checklists**

**Keep Content Concise & Engaging**
Avoid overwhelming employees with too much information at once. Instead, focus on delivering clear, concise, and actionable advice throughout the training program.

## Step 5: Launch & Promote Your Training Program

A well-designed training program is useless if employees don’t participate. Effective communication and promotion are key to getting the program off the ground and on a continued path to success.

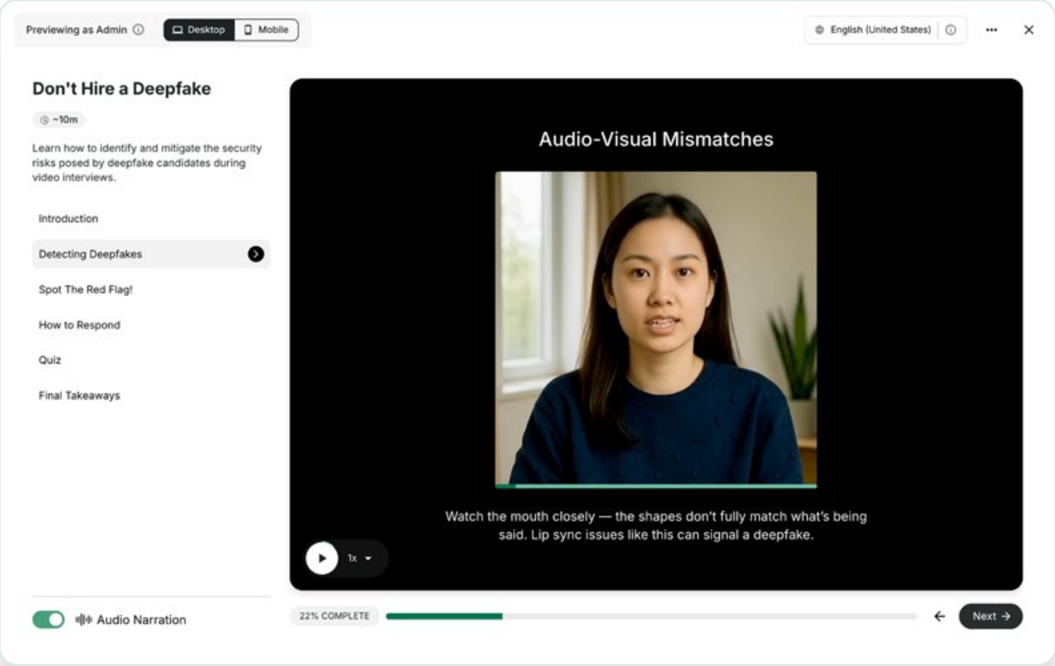
**Executive Sponsorship**
Secure buy-in and support from senior leadership. This demonstrates the importance of the program and encourages employee participation.

**Internal Communication Campaign**
Use various channels — like email, direct messaging, intranet, and team meetings — to announce the program’s launch, explain its benefits, and encourage employees to participate.

**Make Participation Mandatory**
For critical security topics or areas that involve regulatory requirements, make training mandatory for employees.

**Gamification & Incentives**
Consider incorporating elements of game design, such as points, badgers, and leaderboards, or small incentives to boost engagement and motivation.

**Regular Communication**
Keep security top-of-mind by sending regular reminders, updates, and security tips.



Don't Hire a Deepfake

~10m

Learn how to identify and mitigate the security risks posed by deepfake candidates during video interviews.

Audio-Visual Mismatches

Watch the mouth closely — the shapes don't fully match what's being said. Lip sync issues like this can signal a deepfake.

Deepfakes are one of the fastest-growing types of attacks facing organizations and their employees today.

## Step 6: Monitor, Measure, and Iterate

Training in today's cybersecurity environment is not a one-time event: it's an ongoing process. Continuous monitoring, measurement, and iteration ensure the program's long-term effectiveness.

### Track Key Metrics

Use the reporting and analytics features of your training platform to track KPIs.

### Analyze Results

Regularly review the data to identify areas where employees are struggling, where the training is most effective, and where improvements are necessary.

### Gather Employee Feedback

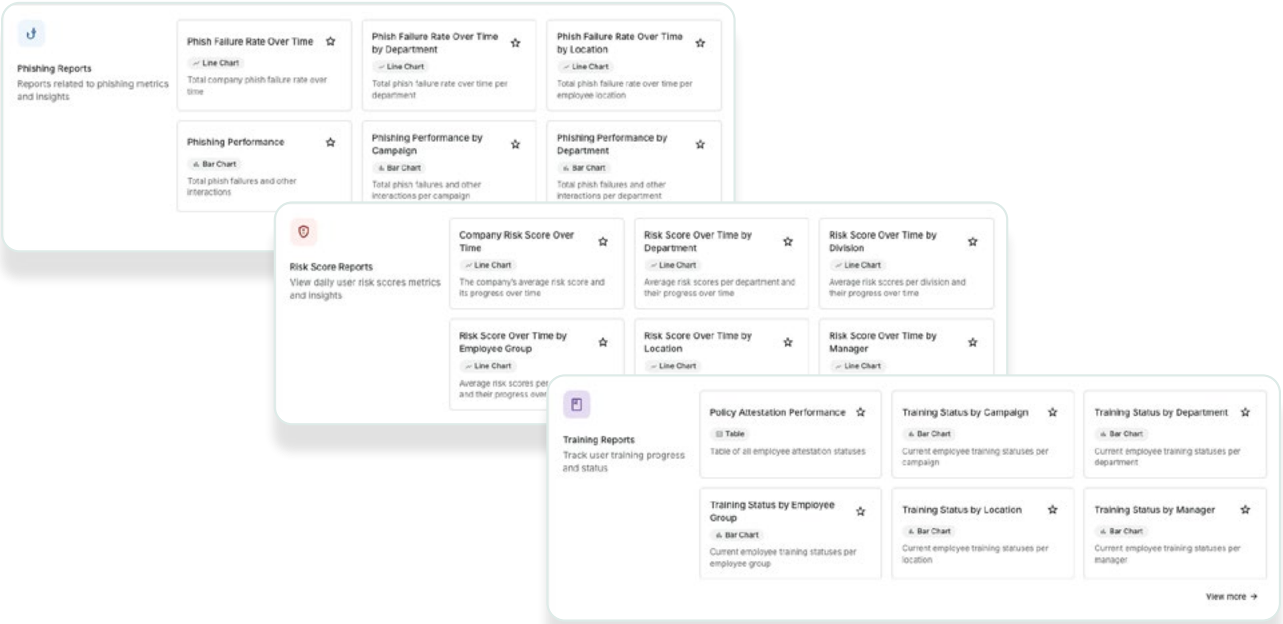
Collect feedback from employees through surveys, focus groups, or informal conversations. Ask employees what they found helpful, what was confusing, and what they'd like to see more of.

### Update Content Regularly

Keep the training content fresh and relevant by incorporating the latest threat intelligence, updating simulations, and adding new modules as needed. Much of this is done automatically through the training platform implemented, but you'll still want to make specific adjustments to customize messaging specifically for your organization.

### Refine Your Program

Based on the data and feedback collected, make adjustments to your security awareness training program — modify content, adjust the frequency of training and simulations, or target specific groups of employees with additional training.



**Phishing Reports**
Reports related to phishing metrics and insights

Phish Failure Rate Over Time ☆
Line Chart
Total company phish failure rate over time

Phish Failure Rate Over Time by Department ☆
Line Chart
Total phish failure rate over time per department

Phish Failure Rate Over Time by Location ☆
Line Chart
Total phish failure rate over time per employee location

Phishing Performance ☆
Bar Chart
Total phish failures and other interactions

Phishing Performance by Campaign ☆
Bar Chart
Total phish failures and other interactions per campaign

Phishing Performance by Department ☆
Bar Chart
Total phish failures and other interactions per department

**Risk Score Reports**
View daily user risk scores metrics and insights

Company Risk Score Over Time ☆
Line Chart
The company's average risk score and its progress over time

Risk Score Over Time by Department ☆
Line Chart
Average risk scores per department and their progress over time

Risk Score Over Time by Division ☆
Line Chart
Average risk scores per division and their progress over time

Risk Score Over Time by Employee Group ☆
Line Chart
Average risk scores per
and their progress over

Risk Score Over Time by Location ☆
Line Chart

Risk Score Over Time by Manager ☆
Line Chart

**Training Reports**
Track user training progress and status

Policy Attestation Performance ☆
Table
Table of all employee attestation statuses

Training Status by Campaign ☆
Bar Chart
Current employee training statuses per campaign

Training Status by Department ☆
Bar Chart
Current employee training statuses per department

Training Status by Employee Group ☆
Bar Chart
Current employee training statuses per employee group

Training Status by Location ☆
Bar Chart
Current employee training statuses per location

Training Status by Manager ☆
Bar Chart
Current employee training statuses per manager

# Secure Your Future: Take the Next Step in Security Awareness Training & Simulations

## The Urgency of Now

Organizations of every size are dealing with the rise of AI-powered attacks, from sophisticated deepfakes to hyper-personalized phishing campaigns. It's a new level of threat that demands a new level of preparedness.

Traditional, one-size-fits-all training programs aren't enough anymore. Powered by legacy solutions, they leave your organization vulnerable to financial losses, reputational damage, data breaches, and legal liabilities. The stakes are too high to rely on outdated methods and technologies.

Throughout this guide, we've explored the evolving threat landscape, exposed the critical flaws in conventional cybersecurity training, and presented a clear roadmap for building a resilient workforce. In addition, we've shown that next-generation training, characterized by continuous learning, personalized paths, realistic simulations, multi-channel delivery, automated compliance, and measurable results, is a must-have in today's environment.

## Key Takeaways for IT & Security Teams

Here are key takeaways to remember as you move forward:

**AI is a Game-Changer:** AI is being weaponized by cybercriminals, creating attacks that are more sophisticated, personalized, and difficult to detect than ever before.

**Traditional Training is Failing:** Outdated security awareness training methods and technologies leave your employees unprepared for new threats.

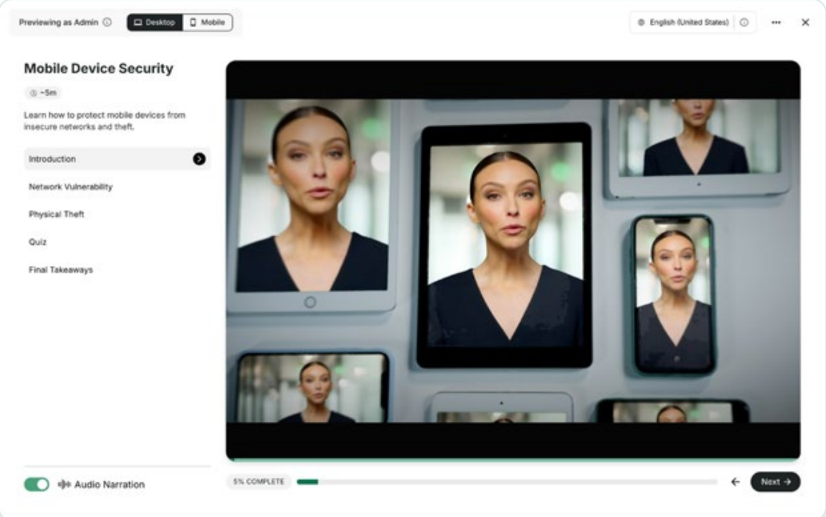
**Next-Generation Training is Essential:** A modern, comprehensive program is your best defense against AI-powered attacks.

**Empower Your Employees:** As your first line of defense, give employees the knowledge and skills they need to protect themselves and your organization.

**Continuous Improvement is Pivotal:** Security awareness training is not a one-time event; it's an ongoing process. Monitor, measure, and iterate to ensure your program remains effective after its launch or overhauling.

**Attackers constantly refine their techniques, leveraging the latest AI advancements to exploit vulnerabilities.** Don't wait until your organization becomes another statistic. Proactive, preventative action is the only effective strategy, and every day you delay implementing a next-generation training program is another day your organization remains at increased risk.

**Cybercriminals scale attacks across every channel — and device. It's critical to train employees on securing their mobile devices.**



Mobile Device Security

~5m

Learn how to protect mobile devices from insecure networks and theft.

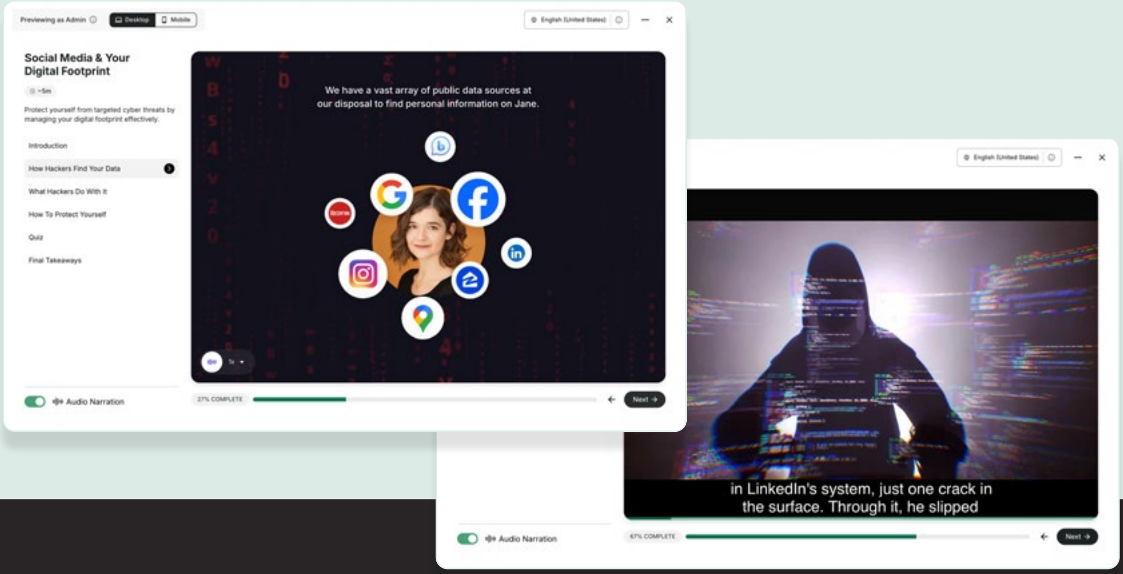
Adaptive

# Take the Next Step with Adaptive Security

Adaptive Security provides comprehensive, next-generation security awareness training and multi-channel phishing simulations trusted by leading global brands.

minted. Figma DALLAS MAVERICKS nectar bmc STONE POINT CAPITAL FIRST STATE BANK

Sunlight Financial SIERRA SPACE LUCCHESE BOOTMAKER TURING Mohonk Mountain House covertree Cass Information Systems, Inc.



Previewing as Admin

Desktop Mobile

English (United States)

Social Media & Your Digital Footprint

~5m

Protect yourself from targeted cyber threats by managing your digital footprint effectively.

- Introduction
- How Hackers Find Your Data
- What Hackers Do With It
- How To Protect Yourself
- Quiz
- Final Takeaways

We have a vast array of public data sources at our disposal to find personal information on Jane.

Audio Narration

27% COMPLETE

Next

English (United States)

in LinkedIn's system, just one crack in the surface. Through it, he slipped

Audio Narration

67% COMPLETE

Next

Ready to see how Adaptive Security helps you build a more resilient workforce and protects your organization from AI-powered threats?

Get a Personalized Demo

Connect

adaptivesecurity.com