KnowBe4
Human error. Conquered.

WHITEPAPER

Example Security Awareness Training Policy Guide

WHITEPAPER: Example Security Awareness Training Policy Guide

Table of Contents

INTRODUCTION

Social engineering and phishing continue to be the top root cause for malicious data breaches by a wide margin as compared to any other cyber attack methods. The percentages vary according to the survey and timing, but in all cases, social engineering and phishing are the number one ranked cybersecurity threat by any objective measure. Most sources place social engineering and phishing as involved in at least 40% of all successful attacks and others place the percentage at over 90%. It is clear that fighting phishing and social engineering should be the top focus for all organizations.

> *Note: You can read a KnowBe4 meta review of a 100 other security reviews that look at root causes for exploitation here: https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense.*

Fighting any cybersecurity threat means crafting a detailed, layered, defense-in-depth set of mitigations, including policies, technical defenses and training. So far, despite over three decades of the best technical defenses, social engineering and phishing attacks continue to get to end users. End users must be taught how to recognize social engineering and phishing threats and how to treat them. Accordingly, security awareness training (SAT) is among the most high-value mitigations any organization can perform to significantly reduce cybersecurity risk.

All security mitigations should have policies directing their application and use. All SAT programs should begin with or be driven by an SAT policy document. Part I of this paper covers the various components which should be covered by any SAT policy and part II gives a generic SAT policy example, which can be used as the basis of your organization's SAT policy, if desired. You can use this paper to craft your organization's first SAT policy document or use it to update or modify your existing document.

Fighting any cybersecurity threat means crafting a detailed, layered, defense-in-depth set of mitigations, including policies, technical defenses and training.

PART I: NECESSARY SAT POLICY COMPONENTS

Creating an effective SAT program requires asking and answering many questions along with making sure that your policy covers all of the needed components. This part of the paper will cover the decisions that need to be made ahead of creating your SAT policy along with the necessary components of an SAT policy.

Important: Any adds/deletes/changes to any policies or documents need to be reviewed by management and legal before implementing.

SAT Program Decisions and Components

Policy Header Information

Every policy begins with a header section which includes information such as the following:

- Policy title
- Scope
- Current document owner/sponsor/role owner
- Document history by date and version
- Current policy version number
- Location of current policy version

Your policy documents may contain more, less or different information. Follow your organization's policy standards and guidelines.

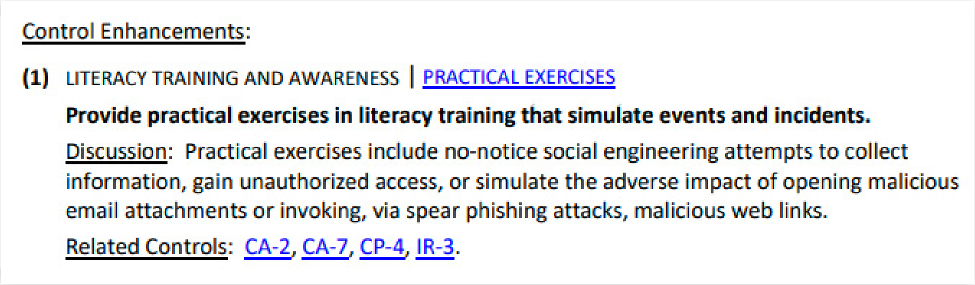
Goal

Your SAT program policy should contain the intended goals, your organization's reason for implementing. A goal might be something like, "To significantly reduce the organization's cybersecurity risk due to participant actions and decisions when faced with social engineering threats, by using security awareness training and education. Participants should be able to better recognize cybersecurity risks, understand how to report risks and threats, and where to go for help."

Control Mapping

Many security controls originate from computer security laws, requirements, recommendations or best practice guides. Tying your SAT program back to one or more compliance document(s) will likely assist you in getting approval and for justifying the ongoing expense of the program.

For example, the United States' National Institute of Standards and Technology (NIST) requires an SAT program as part of its Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf). In particular, section 3.2, Awareness and Training, subsections (1) and (3) on page 60 states the following:



Control Enhancements:

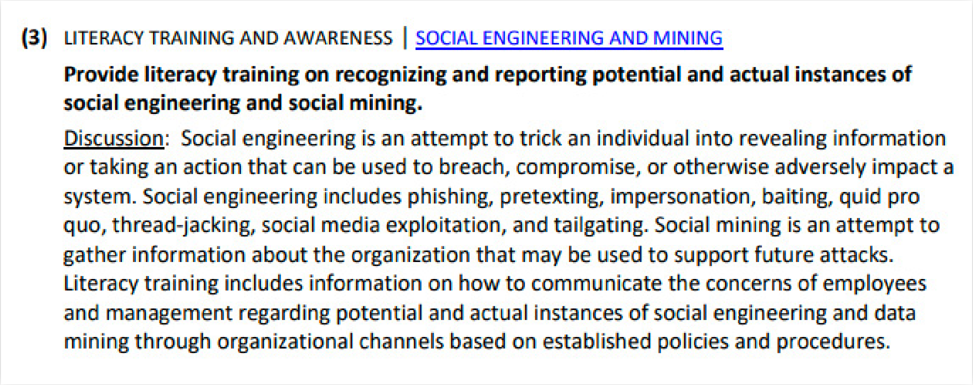
(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related Controls: CA-2, CA-7, CP-4, IR-3.

and



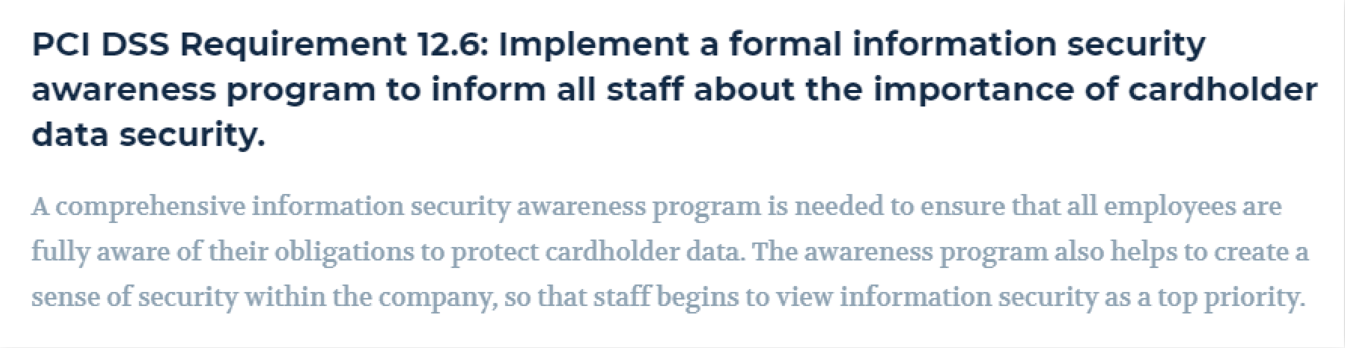
(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

See related article: https://blog.knowbe4.com/nist-updates-you-should-be-aware-about.

Here's another example requirement from Payment Card Industry Data Security Standard (PCI-DSS):

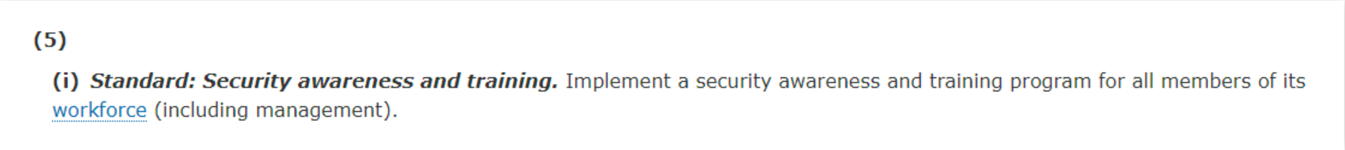


PCI DSS Requirement 12.6: Implement a formal information security awareness program to inform all staff about the importance of cardholder data security.

A comprehensive information security awareness program is needed to ensure that all employees are fully aware of their obligations to protect cardholder data. The awareness program also helps to create a sense of security within the company, so that staff begins to view information security as a top priority.

From: https://www.pcidssguide.com/pci-dss-requirements/.

Here's an example from Health Insurance Portability and Accountability Act (HIPAA), Security Rule 45 C.F.R. § 164.308(a)(5)(i):



(5)

(i) ***Standard: Security awareness and training.*** Implement a security awareness and training program for all members of its workforce (including management).

Many computer security regulatory documents and recommendations require security awareness training. Most organizations fall under one or more regulations requiring security awareness training, but regardless, all organizations should implement a security awareness training program. If you do fall under one or more regulations requiring security awareness training, it cannot hurt to "map" (i.e., link) to the specific control in the document as part of your policy. This helpful page displays some popular security awareness training requirement mappings: https://www.knowbe4.com/resources/security-awareness-compliance-requirements/.

Get Senior Management Approval and Sponsorship

As with any security mitigation, senior management should be convinced of its need and supportive of its implementation. Senior management must drive the organization's security culture. A successful security awareness program will enable other parts of the overall business to prosper; and should be communicated that way. Additionally, senior management's ability to act as an evangelist and lead advocate for the program will yield lasting benefits in adoption and engagement across the business. Every SAT program should have support of senior management and have an official senior management sponsor. Here's another page with hints and ROI tools to help with getting approval: https://www.knowbe4.com/resources/getting-approval/.

Determine Where SAT Program Originates

Different SAT programs originate (e.g., support, responsibility, budget, etc.) from different units within a business. Many SAT programs originate from within IT or IT Security departments. Others may be assigned to a centralized training department or Human Resources. It is important that wherever the program originates that the SAT program is provided strong support given its importance to the organization.

Scope

All policies should indicate the scope of what the policy applies to. This includes the types of participants and roles, locations, business units and even what languages the SAT program should/must cover if the organization has participants across geographic locations with different languages. Will the SAT program be required of contractors, partners and other types of third parties? The most common scope is described as "All Participants," but it is essential to consider requiring its use by any entity that has access to your network or data. Hackers often target trusted third parties and vendors, leveraging a compromise in them to access other targets. Accordingly, an SAT policy scope may include something like, "All participants, vendors, contractors and third parties with access to our confidential data."

Definitions

All technical terms, such as phishing, spear phishing, smishing, vishing, URL, etc., should be described to ensure all readers have a common understanding of them. Never assume that anyone or everyone understands all terms. Definitions can be placed at the beginning or the end of a policy document, depending on your organization's policy formatting.

Note: Consider using KnowBe4's online glossary for your definitions: https://www.knowbe4.com/knowbe4-glossary/

Use Mostly Internal or Mostly External Resources

Will your SAT program use only/mostly internal resources or use external resources and services? A good SAT program is difficult for any organization to develop and service using only internal resources. But even if an external vendor is used, you will have one or more internal participants who are responsible for your SAT program.

Dedicated SAT Staff

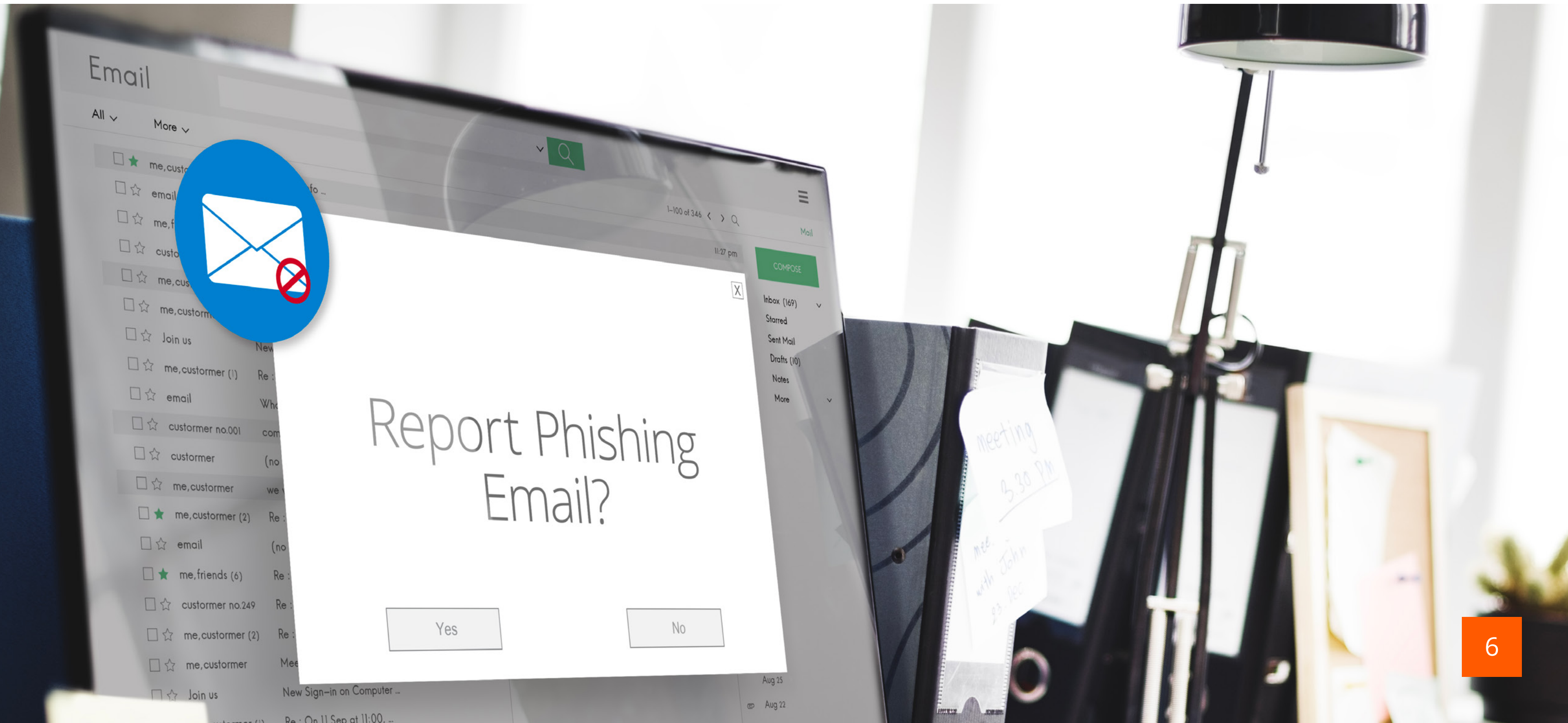
You need to decide whether your SAT program is the responsibility of a single, completely dedicated, participant or participants, the part-time responsibility of one or more participants or outsourced to a vendor who administrates the SAT program on your organization's behalf. Certainly, a dedicated participant(s) or an outsourced vendor who is able to concentrate on your SAT program is better than a part-time resource, although the size and resources of the organization can be a restraint to having dedicated resources. Many smaller companies outsource their SAT programs to other vendors and many SAT companies, like KnowBe4, offer to manage your program for you, as another option. Whether you chose internal or external resources, dedicated or shared part-time resources, the resources administrating your SAT program should understand your organization's particular culture, needs and goals.

Training Specifics

Your SAT program policy should cover the types of training, types of training content, when performed, frequency and how it is performed. For example, an SAT policy should state if training is conducted in-person, remotely, using in-person instruction, using pre-recorded videos, printed and/or electronic posters and newsletters, formal presentations, informal "lunch-n-learns," games, quizzes, etc. It should also document if simulated phishing is used as part of training or if that is out-of-scope. The frequency and timing of standard SAT trainings should also be documented. For example, is a longer computer security training done when each participant is hired and then a shorter one conducted monthly thereafter, with longer annual renewals. The position or person responsible for overseeing the security awareness training program should be documented here. If some of the trainings will require scored quizzes and/or pass/fail competency checks, it should be noted here.

Simulated Phishing Campaigns

KnowBe4 recommends all organizations do simulated phishing campaigns as a critical part of their SAT training process. Simulated phishing allows an organization to measure the success of their training program, measure security culture and be able to identify people who need more training. Simulated phishing can also "gamify" the process of reporting suspected phishing attempts, where participants are actively looking out for the simulated phishes to report them. Simulated phishing helps participants report real phishing attempts with more accuracy.



Your organization needs to decide if it will use simulated phishing or not. An SAT program without simulated phishing campaigns will rarely be as successful at truly reducing human risk as one that includes simulated phishing exercises.

Why?

If simulated phishing is used, what will it be used for? In general, simulated phishing is used as part of the training and education in an SAT program. It is also used to collect stats on who specifically appears to need or not need more training.

> *Note: If you collect information on individuals regarding simulated phishing tests, you may need to update your employee monitoring policy to include that type of data collection. In some states and countries, collecting the results of simulated phishing tests may count as personal data collection. Consult with your privacy advisor, lawyer, or local works council.*

Who

Who will get simulated phishing exercises? KnowBe4 and all known security guides recommend that all staff, including senior management, IT and IT Security, get “no notice” phishing exercises. Any excluded group increases the risk of a real-world phishing attack being successful. Do not let real world phishes be the only tests that specific groups of employees receive. However, it is critical that everyone understand the importance of “no notice” simulated phishing exercises. They should understand why they are necessary and empathize with their need. They absolutely should not be thrust among management or end-users as a “surprise.” That rarely goes well for anyone involved.

Two good articles to read about this are: https://blog.knowbe4.com/the-dilemma-should-you-phish-test-during-the-covid-19-pandemic and https://blog.knowbe4.com/testing-1-2-3-.

Frequency

If simulated phishing is used, the program should only indicate the frequency (e.g., once-a-month, one-a-week, etc.), but not the specific dates. A policy statement should say something like, “Simulated phishing campaigns are used as part of our SAT program and participants can expect a simulated phishing attempt at least once a month.”

> *Note: Participants should not be told specific dates, times or periods when simulated phishing will occur. This defeats the purpose of the training. NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf). In particular, section 3.2, Awareness and Training, subsection (1), specifies “no notice” phishing exercises. Some organizations may be required to notify IT staff or managers of specific pending phishing campaigns, but even this procedure is not recommended. Giving “heads up” notice to specific staff makes them less likely to get the full value of a simulated phishing test, as they will be more able to pick up on the phishing test, be less likely to fail those tests and their true ability to handle real-world phishing campaigns predicted less accurately. You want simulated phishing campaigns to be able to determine who does and does not need more training.*

Platform Types

You should indicate what type of simulated phishing is done. Is it only simulated phishing emails or is simulated phishing done across other platforms: SMS messages, voice calls, social media sites, etc.?

Content Type

Is the public information of the organization allowed to be used? Is non-public information, such as projects or information on organizational newsletters allowed to be used (i.e., simulated spear phishing attacks)? Is an employee’s personal or public information allowed to be used? Can other company’s branding be allowed? Many real-world phishes act as if they are coming from well-known brands. Will simulated phishing cover generic topics, be specialized for the organization’s industry or the organization itself (i.e., spear phishing), be a blend of generic and spear phishing topics, change based on participant's role, change based on season, change based on newsworthy events, change based on social engineering and phishing trends in a timely manner? All of the allowed and denied decisions regarded simulated phishing campaigns should be covered.

> *Note: It is best if some subjects, like surprise bonus programs or raises, should not be used as simulated phishing subjects, as severe negative participant reactions have resulted from this type of test in the past. Participants do not like being tricked about getting increased compensation. Many other organizations expressly forbid the use of subjects involving politics, sex, race, religion or other issues with heightened sensitivity and emotions involved. This can be tricky if real phishing attempts use those "triggering" subjects to induce more potential victims. A simulated phishing test should not result in decreased morale, even if a person passes it. Always have involved subjects approved by the appropriate people when they could be considered sensitive. Do not risk your personal reputation or the program's reputation simply to create a "great" simulated phish.*

Will You Have a Champions Program?

Many SAT programs benefit from having internal participants who want to actively and personally assist with reducing cybersecurity risk. Usually, these individuals have a low rate of clicking on simulated and real phishing campaigns, are happy to be involved with the program and have the ability to effectively communicate the program's education and objectives to others. There are many different names for these types of more personal, "one-on-one" SAT initiatives, but many organizations refer to them as their "Champions." Champion programs can be a very effective way to reduce cybersecurity risk, and if one exists or is used, it should be covered in the SAT policy information.

> *Note: Champion programs go by many names depending on the organization using them, including: Rock stars, liaisons, ambassadors, officers, culture carriers, etc.*

A good related article to read on this subject is: https://enterprise-services.siliconindia.com/viewpoint/cxoinsights/build-a-network-of-champions-to-increase-security-awareness-nwid-21979.html.

Expected Participant Behavior

The SAT policy should cover expected end user behavior as it applies to the SAT program. For example, it should say that participants are expected to complete all required training in a timely manner and to report both real and simulated phishing campaigns to IT Security. It should set the expectation of both training and responsiveness to simulated phishing tests.

Although not necessarily a part of describing an SAT program, the policy might also include other expected end user behaviors, such as employees being required to "hover" over URL links and inspect them, to never give out passwords to requests from email, SMS or voice calls and to report all suspected phishing attempts using the organization's recommended method (e.g., using the KnowBe4 Phish Alert Button tool). This sort of information should be covered in other computer security policies but can be included here for repetitiveness and completeness.

Employees may be told that they should actively report their interaction with any simulated or real phishing campaign to the Help Desk or IT Security and that late reporting (before discovery by others) will not result in penalties. You want to create a culture where reporting suspected phishing events is always encouraged, even if it is late. You may want to communicate that if any employee types in their login credentials to even a simulated phishing test, that the employee will be asked to immediately change their passwords, based on a conservative conclusion that if the employee typed in their credentials to a simulated phishing campaign, they may have done the same to a real phishing campaign. So, to be safe, an employee should always be required to change their login credentials(s) if they have typed in their login credentials to a simulated or real phishing campaign.

Rewards and Consequences

It is important that the consequences of participants taking or avoiding education and simulated phishing campaigns be documented within the policy. KnowBe4 recommends approaching this objective using more positive reinforcement than using only negative consequences, whenever possible. However, all organizations likely need to document what a participant can expect if they fail to take required training in a timely manner, fail educational quizzes or fail one or more simulated phishing simulations.

Start by defining the positive reinforcement that will be given for an employee completing all required testing in a timely manner and successfully reporting real and simulated phishing campaigns. For example, state that every successful report of a real or simulated phishing event will result in a positive notification to the participant. Another example, if all the employees of a business unit complete all required testing in a timely manner as a group, they will get a "pizza party." Some organizations even offer individual and departmental bonuses for beneficial SAT program outcomes to individuals and business units or include the results as part of each employee's annual review.

Each SAT program should clearly communicate the actions that will be taken for an employee not taking required education in a timely manner, for failing educational quizzes (if involved), and for failing one or more simulated (or real) phishing campaign(s). An example might be that an employee can expect a meeting with their supervisor for falling behind on required testing under less than two weeks late and a meeting with HR and possible separation of employment if they have not taken required education within two months.

Setting the expectation of what happens from one or more successive simulated (or real) phishing failures should also be clearly communicated. For example, in any moving 12-month period:

- Zero failures, $100-$1000 additional bonus added to their annual compensation
- For one failure, additional SAT, short to medium (3-5 minutes) in duration
- For two failures, additional SAT, longer (5-10 minutes) in duration
- For three failures, additional SAT, longer in duration (10-15 minutes), plus a meeting with their supervisor
- For four or more failures, additional SAT, longer in duration (30 minutes), meeting with SAT expert and/or HR
- For five or more failures, additional SAT, longer (30-60 minutes) in duration, possible suspension of services, serious disciplinary actions, including separation of employment

The key to the success of any SAT program is to make the employee understand that the actions are not meant to be individually punitive, but are meant to help the employee understand the risk to the organization involved and to help them improve their own cybersecurity risk posture. If your SAT policy only covers negative consequences, it probably needs to be re-thought and re-communicated to be more reflective of positive reinforcement.

It's important for SAT program administrators to be self-aware enough to consider that repeated failures could be due to the design or mis-design of the SAT program. The administrator should always consider this in their review and ask WHY someone is having repeated failures. Even it is not the SAT program's "fault," possibly trying something reasonably different to help people be more successful, if they are truly learning more and taking better actions more often, is good for the organization, even if the first approach was truly sound. Also, ask the user. A good SAT program administrator asks repeat fail users why they think they missed something or if there is anything the SAT program could do to make the user more successful. Sometimes little useful nuggets of information or new hints can be learned to improve the program and success rate. A good SAT program includes a solid feedback loop and self-inspection to help an organization reduce risk the most and fastest, without unnecessarily clinging to the "right way" if the evidence contradicts it.

> *Note: This doesn't mean that a SAT program should make the simulated phishing tests so easy that anyone can spot them with zero failures. A good program creates simulated phishes that mimic real-world attempts, and which if used properly as the educational tool that they are, reduces risk to the organization by making participants less likely to be fooled by similar real-world phishing attempts. Making simulated phishing attempts too easy or two hard could have a negative impact on an organization's cybersecurity security risk reduction.*

Incident Response

If a participant "fails" a simulated or real social engineering or phishing campaign, what types of actions require official incident response? For example, a failed simulated phishing event may require that IT reset the involved participant's passwords, so they have to be changed within 24 hours. Multiple failed simulated phishing events may result in a participant's device being "locked down" for a set period of time. Failure of a real phishing event may result in an official forensic response. Does simply opening a real phishing email result in an official incident response or does the participant have to have clicked on a URL, downloaded a file or provided login credentials? Does the official incident response require a simple "cleaning" of the involved device or does most of the device have to be "formatted" or replaced, along with resetting the user's login credentials? All of these decisions need to be made ahead of time and clearly communicated.

Which Metrics To Use

Your SAT program policy should define what metrics are used to measure the success of the program. Most organizations should do a simulated phishing exercise before their SAT program begins, and periodically thereafter, to give the program a "baseline" to measure the program's overall effectiveness. An effective SAT program will result in a significant reduction of cybersecurity risk to the organization.

The metrics that will be used should be defined here. Here are some example metrics:

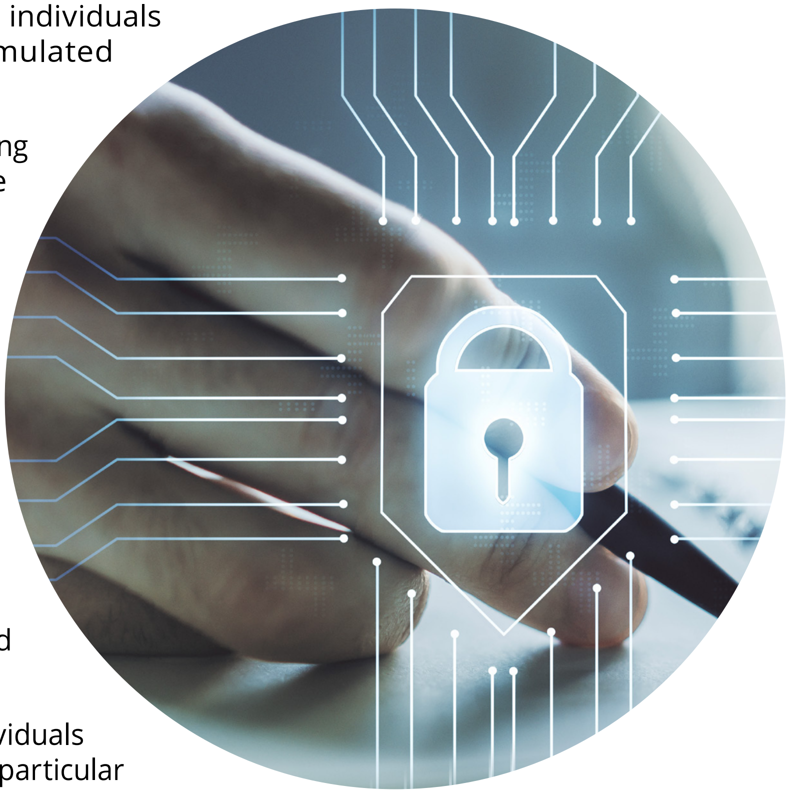
- Total number of participants covered by the SAT program
- Overall baseline of participants at the start of the SAT program and/or during subsequent baseline testing

For required training:

- Total and types of required training
- Individual training and testing results
- Total number/percentage of participants and/or individual names of participants who completed all and/or specific required training in a timely manner
- Total number/percentage of participants and/or names of individuals who did not complete all and/or specific required training in a timely manner

For individual simulated phishing campaigns:

- Total number/percentage of participants and/or names of individuals who were sent a specific phishing campaign
- Total number/percentage and/or names of individuals who "passed" or "failed" a particular simulated phishing campaign
- Total number/percentage of participants reporting simulated phishing attempt using appropriate method/tool (e.g., Phish Alert button, etc.)
- Total number/percentage and/or names of individuals who entered their login credentials within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who "clicked on a URL" within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who downloaded a simulated malicious payload within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who ran a simulated malicious payload within a particular simulated phishing campaign



- Total number/percentage and/or names of individuals who completed information requested by a particular simulated phishing campaign
- Totals or percentages of actions performed by participants across one or more, or all, simulated phishing campaigns

Even when deciding on all metrics taken and reported on, decide ahead of time which metrics define the overall success or failure of an SAT program. Decide whether routine reports will be run and distributed to those who manage the program to help increase the effectiveness of the SAT program. For example, should managers always be notified of participant failures? Should a manager be given the statistics of how their team is performing over time or corrective actions taken with a particular participant? What should managers be notified of and how frequently so they can gauge the effectiveness of the SAT program?

Summary

These are the types of questions and answers which needed to be decided before a formal SAT program policy is created. Every organization is going to have different needs and requirements based on the culture and policy requirements. Use this document as your guide to assist with your custom policy. Part II below will give an example SAT program policy which can be used to help craft your policy, if desired.

Additional Resources

KnowBe4 Resources
https://www.knowbe4.com/resources

Book – Cyberheist: The Biggest Financial Threat Facing Organizations Worldwide by Stu Sjouwerman, CEO of KnowBe4, Inc.
https://info.knowbe4.com/free-e-book

Book – Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors by Perry Carpenter
https://www.amazon.com/Transformational-Security-Awareness-Neuroscientists-Storytellers/dp/1119566347

Book – A Data-Driven Computer Security Defense by Roger A. Grimes
https://www.amazon.com/Data-Driven-Computer-Defense-Way-Improve/dp/1092500847/

PART II: EXAMPLE SECURITY AWARENESS TRAINING POLICY

This is an example security awareness training policy which can be copied and adapted, if desired. Consult senior management and legal before updating or adding any policies.

Acme Security Awareness Training Policy

Version 2.1

Senior Management Sponsor	Title/Role
Kathy Smith	Chief Information Officer
Policy Owner	Title/Role
Amanda Smith	Chief Information Security Officer

Scope

All employees, contractors, partners and third parties which handle Acme confidential information across the globe.

Document Version History

Version	Date	Owner	Description
1.0	January 1, 2019	Jacqueline Smith	First version
1.5	December 20, 2020	Erich Smith	Scope broadened, sections added
2.0	April 21, 2021	James Smith	Simulate phishing section added
2.01	April 22, 2021	Jelle Smith	Foreign language versions created
2.1	June 1, 2021	Javvad Smith	Added metric section

Note: The latest version of this document can be found on \\internalnetwork\policies\satpolicy.

Policy Goal

To significantly reduce Acme's cybersecurity risk due to participant actions and decisions when faced with social engineering threats, by using security awareness training and education. Participants should be able to better recognize cybersecurity risks and understand how to treat them.

Control Mapping

United States' National Institute of Standards and Technology (NIST) requires a Security Awareness Training (SAT) program as part of NIST Special Publication 800-53, release 5, Security and Privacy Controls for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf). In particular, section 3.2, Awareness and Training, subsections (1) and (3) states the following:

> *"Provide practical exercises in literacy training that simulate events and incidents...Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links."*

and

> *"Provide literacy training on recognizing and reporting potential and actual instances of social engineering and mining."*

Definitions

This section defines various related definitions that may appear in the policy or SAT-related program documentation.

BEC

Short for business email compromise, which is also known as CEO fraud.

CEO Fraud

Spear phishing attacks focusing on people in Accounting, claiming they are the CEO and to urgently transfer large amounts of money. CEO fraud is a form of social engineering that took flight during 2015.

Cybercrime

The term cyber- or computer crime encompasses a broad range of potentially illegal activities. In our context, it means crimes that target computer networks, devices, operating systems, applications and their users.

Endpoint

Another word for the workstation that is used by an end user in an organization. Refers to a computer or device at the end of a network cable.

Exploit

An exploit (French, meaning "achievement") is (usually malicious) software that takes advantage of a bug, glitch or vulnerability in other code in order to cause unintended or unanticipated behavior to occur, and control of a computer system can be gained.

Forensics

In our context, “digital forensic science” that deals with legal evidence found in computers and digital storage media. The goal is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting evidence of a cybercrime.

Gamification

Gamification is the addition of gaming features or principles to something that typically does not have a gaming element—in our case, security awareness training and e-learning content. Gamification has been shown to improve user engagement by increasing people’s inherent ambition to compete, achieve or master. Studies have shown that when people are intrinsically motivated to complete a task, they learn better and retain more information.

HIPAA

The Health Insurance Portability and Accountability Act, was enacted by the United States Congress and signed by the President in 1996. It requires healthcare organizations to protect personal health information.

Hacker

Originally: A person who has advanced computer skills, is enthusiastic and skillful, regardless of intent. Definition has changed and can indicate someone who commits cybercrimes or is involved in unethical cyber activity.

Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Malware

Malware is a shorter version of the term “malicious software.” It is an umbrella term used to refer to a wide range of viruses, worms, Trojans and other programs that a hacker can use to damage, steal from or take control of endpoints and servers. Most malware is installed without the infected person ever realizing it.

PHI

Protected health information. PHI is all recorded information about an identifiable individual who relates to that person’s health, health care history, provision of health care to an individual, or payment to health care. The U.S. Health Insurance Portability and Accountability Act (HIPAA) governs the protection of PHI.

PII

Personally identifiable information. PII is defined as any instance of an individual’s information if it can be used to uniquely identify a specific individual. Most laws and regulations require that the possessor of other people’s PII must protect it against unauthorized access.

Patch or Update

A software update intended to add features or repair a vulnerability that was discovered after the product was released for general use.

Phishing

Phishing is the process in which cybercriminals using a false identity try to trick a potential victim into revealing sensitive information or taking a potentially dangerous action, like clicking on a link or downloading a malicious file attachment. It is commonly done using email, websites, instant messaging, SMS, voice-based calls and in-person. It’s a form of criminally fraudulent social engineering. Also see Spear Phishing.

Pretexting

The act of creating an invented scenario in order to persuade a targeted victim to release information or perform some action. Pretexting can also be used to impersonate people in certain jobs and roles, such as technical support or law enforcement, to obtain information. It usually takes some back-and-forth dialogue either through email, text or the phone. It is focused on acquiring information directly from the actions taken by the targets.

Ransomware

Ransomware is malware which cryptographically denies access to a device or files until a ransom has been paid. One of the most dangerous forms of malware today.

SAT

Security awareness training. Education to make participants aware of how to recognize particular types or signs of threats and take the appropriate action.

Security Policy

A written document that states how an organization plans to protect its physical assets and information.

Security Vulnerability

A programming or structural weakness which allows an attacker to gain unauthorized access or disrupt the normal operations of a network, device, operating system or application.

Sensitive Information

Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it.

Note: For our purposes, the words sensitive, confidential and private all mean essentially the same thing.

Smishing

Phishing conducted via short message service (SMS), a telephone-based text messaging service. A smishing text, for example, attempts to entice a victim into revealing personal information.

Social Engineering

Social engineering is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases, the attacker never comes face-to-face with the victim.

Spam

An unsolicited, unwanted email or message.

Spear Phishing

Spear phishing is a small, focused, targeted attack via email on a particular person or organization with the goal of penetrating their defenses. The spear phishing attack is done after research on the target and has a specific personalized component designed to make the target do something against their own interest.

Trigger

A condition that causes a virus payload to be executed, usually occurring through user interaction (e.g., opening a file, running a program, clicking on an email file attachment).

Trojan

A Trojan Horse program (shortened to Trojan), is a very common, non-self-replicating malware that pretends to perform a desirable function for the user, but instead facilitates unauthorized actions. The term is derived from the Trojan Horse story in Greek mythology.

URL, Uniform Resource Locator

A remote network location or pathway that links or points to a particular piece of content, like a website page, document or file. Often used in an Internet browser to locate content.

Vishing

A phishing attack conducted by phone.

Whaling

Phishing attacks that target high-ranking executives at major organizations or other highly visible public figures. Also known as CEO fraud.

Security Awareness Training Program Summary

This part of the policy summarizes Acme's SAT program, which involves training, testing and simulated phishing campaigns.

All newly-hired employees and others with access to Acme's networks or data will be required to take 30-45 minute SAT training education in the form of a pre-recorded video(s) or training by in-person trainers. This SAT training is required when first hired or contacted and then at least annually thereafter; although, Acme reserves the right to make any individual requiring additional training take it more frequently.

All participants will be required to demonstrate their successful understanding of the material by taking a quiz on the information. A passing rate of 70% is required. Participants failing the quiz will be required to watch the material or receive training until they receive the required passing rate. Participants who do not pass cannot have access to Acme networks, systems or data.

At least once a month, participants will be given access to required, additional, shorter (one to five minutes each) SAT content. All required training will be sent to each individual using email. Those without ready access to email should be instructed to check the company's IT Security bulletin board (https://acme.it/bb/) for information and updates. Quizzes may or may not be required with the additional content.

All training is required, unless specifically marked as optional, and must be completed within two weeks of assignment, unless on a pre-approved time-off event or emergency. In the event that a participant is out on pre-approved leave or an emergency, they must take it within two weeks of coming back to work.

All training and education are managed by Acme's security awareness team, which is part of the Information Security business unit and is sponsored by the CISO and CIO. Results of the SAT program are reported quarterly to the CEO and to the Board of Directors at least annually. Acme uses KnowBe4's platform and training content for most SAT training purposes. SAT training content includes pre-recorded videos, quizzes, posters, games and simulated phishing exercises. Acme reserves the right to have more frequent trainings and trainings of different types as desired by SAT program administrators and sponsors.

Simulated Phishing Campaigns

Acme uses simulated phishing exercises to gauge an employee's understanding of the trainings and to gauge their fitness against particular types of high-risk threats. One to two simulated phishing exercises will be sent per week without previous notice to participants. Simulated phishing exercises will have a "pass/fail" component. Any participant who clicks on a link or downloads an attached document or who follows instructions in a simulated phishing exercise will be deemed as having failed the exercise. Any participant simply opening a phishing email, message or listening to a message will not have been deemed to fail the exercise. Any participant reporting a suspected phishing exercise to IT Security or the Help Desk and not clicking on any links, downloading any files or providing any credentials will be considered as having "passed" the exercise. Any participant simply deleting and not reporting a suspected simulated phish will not reported as passing the test, but will be reported as a "soft fail." Two or more soft fails count as a full regular failure rating.

Clicking on links, downloading documents or providing login credentials to simulated phishing content may result in the end user immediately learning they failed a simulated phishing exercise. Afterwards, they are shown the "red flags of social engineering," which details why they should have detected being duped by the simulated phishing exercise. A participant correctly reporting a simulated phishing event will receive an immediate on-screen message indicating their success. A user reporting a suspected real-world phish should receive confirmation within 24 hours about whether the suspected phish was a real phish or not. If it was a real phish, the user will be sent an email congratulating them for helping to protect our environment. If it was not a real-world phish, the participant should receive an email notifying them of the outcome of the review and the submitted phishing content replaced in their inbox.

When in doubt, participants should err on the side of caution and report any content they suspect to be a potential phishing event.

A participant who clicks on a link, downloads a document or provides information during a simulated phish will have each action of potentially negative consequences assigned as an individual failure.

Hence, clicking on a link, providing login credentials and opening a document might classify as two to three failures from one exercise, depending on the phishing exercise. Individuals who believe they have unfairly failed a test can contest the finding by contacting members of the ACME SAT program or by clicking on the appeal link sent in failure notification messages.

Acme SAT program administrators reserve the right to use any information that can be learned in the public realm about Acme, its personnel, projects and news in a simulated phishing exercise. SAT program administrators can additionally use information which can be viewed, publicly, in a participant's publicly accessible social media profiles. Acme's SAT program will never use simulated phishing content involving bonuses, raises, political, sexual, racial or religious contexts. SAT simulated phishing exercises can arrive in email, SMS, using voice-based calls or by placing portable media devices/storage (i.e., USB keys) around Acme corporate locations. Testing will never be done in-person or by using an internal website unless this policy is updated in the future or the testing is covered under another policy or testing program.

Simulated phishing exercises are considered as part of the training and education and are used to gauge the overall effectiveness of the program and the security awareness of individual employees. Employees failing simulated phishing exercises (or real phishing attempts) will be tracked and assigned more training and potentially have other actions assigned. Each individual employee can follow their individual training progress and their success or failures with simulated phishing exercises. Senior management, SAT program administrators and roles in the individual's company hierarchy pathway may also be aware of the individual's success or failure rate.

Participant Requirements

Participants are expected to take required training within two weeks of their first day back to work. Participants are expected to report all suspected phishing events by using tools and procedures taught during the training events. Suspected phishing emails can be reported using the KnowBe4 Phish Alert Button, PAB, (see image below).

Any potentially suspected phishing event should be reported. When in doubt, the participant should report it using the PAB, if in email; or by calling the IT Help Desk at xxx-xxx-xxxx or emailing phishreport@acme.int. Participant must attend all required meetings related to the SAT program.

Acme Champion Program

Acme uses a "champion program" to assist with SAT education. Acme's champion program is named "Acme We Are Aware." Champions are recommended by their managers or can volunteer themselves. Duties include promoting the general cybersecurity defense initiatives of Acme, taking required and additional training proactively, scoring 85% or better on SAT quizzes and sharing what they know and learn with their business unit's participants. Acme's We Are Aware program is sponsored by IT Security and has monthly meetings. Participants will get t-shirts and other "swag" for themselves and to share. Participants will be formally recognized as having participated to better Acme and is a net positive trait to be placed on their annual evaluation for each year successfully completed and for staying a member in good standing. Champions may occasionally be given prizes (including possibly gift cards, tickets and small bonuses) to thank them for their participation; although participants are invited to be a member simply for the joy of sharing information with their co-workers. Champions can be dismissed without cause by the sole discretion of the program's leader. Dismissal from the program or quitting the program will not count negatively against the participant at any time.

Rewards and Consequences

There are rewards for successfully reporting real and simulated phishing events and consequences for failure to report or interact with real and simulated phishing events. Any employee who successfully reports all simulated phishing exercises and real phishing events to which they have been exposed without a single failure, will get an extra $500 in annual compensation, above and beyond, what was planned outside the SAT program. Members of Acme's We Are Aware program who complete at least eight months of a given year are entitled to additional $500 on top of the other $500 if they have no failures, for a total of $1,000 in extra earned bonus each year. Additional bonuses can be suspended for the program overall by senior management without notice.

Any employee who has successfully reported a simulated phishing exercise or real phishing event will be sent a "kudos" email. Any employee reporting a real phishing event will receive a record of such report in their annual review to be viewed as a positive contribution. However, any failure in the same 12-month moving timeframe can erase a positive, successful result in the participant's annual record. If all the participants of a business unit do not have a single failure event in a given quarter, that business unit will be treated to a free pizza party. Any business unit (with greater than 10 participants) without a single failure for a whole year will be treated to a "movie night" or given free tickets to the movie of their choice. A movie event can be replaced by some other approved recreational event of identical cost upon majority agreement of the group and their manager.

The consequences for each individual employee, in any moving 12-month period, are:

- Zero failures, $500-$1,000 additional bonus added to their annual compensation
- For one failure, additional SAT, short to medium (3-5 minutes) in duration
- For two failures, additional SAT, longer (5-10 minutes) in duration
- For three failures, additional SAT, longer in duration (10-15 minutes), plus a meeting with their supervisor
- For four or more failures, additional SAT, longer in duration (30 minutes), meeting with SAT expert and/or HR
- For five or more failures, additional SAT, longer (30-60 minutes) in duration, possible suspension of services, serious disciplinary actions, including separation of employment

The participant's manager, Human Resources or senior management can update this rewards and consequences policy section without prior notice, and they are not constrained by the information stated here in both reward and consequence.

Any participant failing three or more simulated or real phishing events in a 12-month period should be interviewed by the SAT program administrator, either in person or using a survey tool, to ascertain from that person why they think they failed multiple phishing tests or events. The goal is to find out if there is anything the SAT program can do to make that person more successful in recognizing real or simulated phishing events (within reasonable boundaries). Repeated failures by multiple individuals is to be expected in any SAT program, but also may indicate a need to change tactics with those individuals or by the program overall.

Incident Response

If a participant "fails" a simulated or real social engineering or phishing campaign, a failed simulated phishing event will require that IT reset the involved participant's password(s), so they have to be changed within 24 hours. If four or more failed simulated phishing events occur, the participant's device will be "locked down" for a minimum period of three months. Each additional failure within a 12-month period will result in additional lockdown periods as determined by their manager and IT Security.

Failure of a real phishing event may result in an official forensic response. If the participant clicked on a URL, downloaded a file or provided login credentials, their device should be disconnected immediately from the network and shutdown until examined by IT Security. Login credentials will need to be changed immediately. The device will be forensically reviewed and a "cleaned" device returned to the participant or a new or refurbished device used as a replacement, as determined by IT Security.

Reporting Metrics

The metrics that will be used should be defined here. Here are some example metrics:

- Total number of participants covered by the SAT program
- Overall baseline of participants at the start of the SAT program and/or during subsequent baseline testing

For required training:

- Total and types of required training
- Individual training and testing results
- Total number/percentage of participants and/or individual names of participants who completed all and/or specific required training in a timely manner
- Total number/percentage of participants and/or names of individuals who did not complete all and/or specific required training in a timely manner

For individual simulated phishing campaigns:

- Total number/percentage of participants and/or names of individuals who were sent a specific phishing campaign
- Total number/percentage of participants and/or names of individuals who were sent a specific phishing campaign and reported it using the recommend method/tool (e.g., Phish Alert button, etc.)
- Total number/percentage and/or names of individuals who "passed" or "failed" a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who entered their login credentials within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who "clicked on a URL" within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who downloaded a simulated malicious payload within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who ran a simulated malicious payload within a particular simulated phishing campaign
- Total number/percentage and/or names of individuals who completed information requested by a particular simulated phishing campaign
- Totals or percentages of actions performed by participants across one or more, or all, simulated phishing campaigns

Summary

The objective of the SAT program and the rewards and consequences is to significantly reduce cybersecurity risk, and to that end, all parts of the program can be adjusted on the fly, as-needed, by updating the policy.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

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

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

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

About KnowBe4

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

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

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

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