IT-SEAL
Social Engineering Analysis Labs

IT SECURITY
MADE IN GERMANY

Awareness Academy

Together for a sustainable security culture

Portfolio & Insights

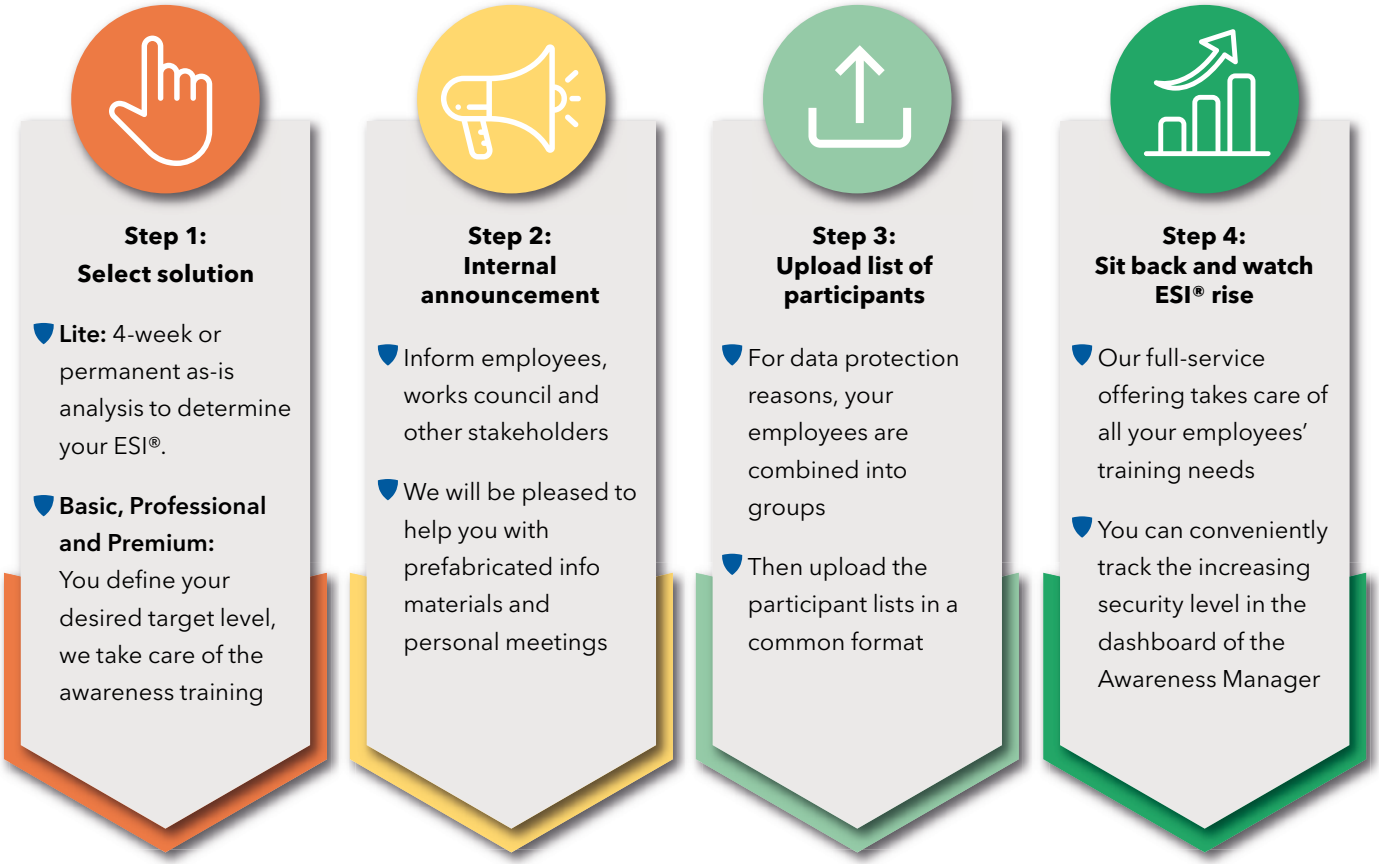
Made with ♡
in Security Valley Darmstadt

Awareness Academy

A simple and effective workflow for raising awareness among your employees.

9 out of 10 cyber attacks start with a phishing email and therefore also with a tricked employee. As the person responsible for security, you are faced with the challenge of minimizing the „human" security risk. With the IT-Seal Awareness Academy, you can easily and, above all, permanently put a checkmark on the topic of security awareness. You define the desired target security level via the Employee Security Index (ESI®) and we take care of the rest. The continuous training program includes a wide range of methods to effectively reach un-sensitized employees: From phishing simulations, e-learnings, short videos and online seminars to awareness materials and on-the-job notices. The result of the Awareness Academy is educated employees who know and take their responsibility for the security of the company seriously.

4 steps to a secure employee



- **Transparency:** Your current security level can be viewed at any time in the dashboard.
- **Sustainability:** You maintain a permanently high security level through an actively practiced security culture.
- **Up-to-Date:** Our training methods are based on current scientific findings.
- **Employee-friendly:** We involve employees and works councils at an early stage through transparent communication.
- **Plannable:** The investment in your employees' security awareness can be planned in advance and is always under control.

 # Patented spear phishing engine: *OSINT phishing based on publicly available information*

 # Awareness-Engine: *Individual learning on autopilot using the Target ESI®.*

 # ESI®: *Tangible performance indicator based on scientific approach*

 # Demand-driven training: *Increasing levels of difficulty without frustration*

Continuous training in four versions

Security Awareness is a continuous process - just like our awareness solutions (all solutions can be cancelled on a monthly basis).

Measure once or permanently	Permanently measure & training		
Lite	**Basic**	**Professional**	**Premium**
ESI®-Messung	**Target ESI®:** 70	**Target ESI®:** 80	**Target ESI®:** 90
Get to know us and your level of security to create awareness.	**Inexpensive, standardized security awareness training developed by professionals.**	**High-quality security awareness training tailored to the individual user.**	**The high-end solution for the best possible security in the area of security awareness.**
4-week as-is analysis or continuous phishing simulation	Target ESI® of 70 as goal agreement	Target ESI® of 80 as goal agreement	Target ESI® of 90 as goal agreement
Patented Spear Phishing Engine	All Lite features included	All Basic features included	All Professional features included
Full-Service Setup	**Awareness Engine: Training on Autopilot**	Online Seminars	Employee-OSINT: Best Phishing Simulation
	All E-Trainings included	Awareness Materials	Social Engineering: Site visit included

All packages contain the features of the subordinate packages. The overview shows only a part of all features.

The principle of the Target ESI®

Security awareness is a time-consuming challenge. Not only do you as the person responsible for security have to invest time in planning awareness measures, your employees also need time to participate in them. Our full-service Awareness Academy packages (Basic to Premium) relieve you of this effort: You define the desired security level in the form of the Target ESI® and we take care of the rest. We use a wide variety of training methods, from phishing simulation to e-learning and more. Your employees save time by only scheduling training when their security level is below the desired target level. Once the employee has reached the Target ESI®, they are given a break, at least until the next measurement. In the meantime, you can sit back and relax and take care of your other tasks. Put a permanent checkmark on the topic of security awareness!

Academy features in detail

Sustainable Security Culture

	Measure once or permanently	Permanently measure & training		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Sustainable security culture: Our common goal Our common goal is a sustainable security culture. To this end, we get all employees involved step by step and show them how relevant this is in both their professional and private lives. They will learn the basics of cybersecurity in order to be able to act in unison - thereby recognizing their responsibilities in the workplace and assuming them effectively. We support your employees in line with their specific needs, based on key figures and group appropriately: as much as necessary, as little as possible.	✓	✓	✓	✓

ESI® and the Target ESI® (Employee Security Index)

Features	Lite	Basic	Professional	Premium
ESI® and Target-ESI® (Employee Security Index): Your Benchmark The ESI® is a scientific benchmark to measure security culture across industries. With the Target ESI®, you choose your own security level, which serves as a joint target agreement. Each group will be trained based on key performance indicators and specific needs. When a group reaches the Target ESI®, training is put on hold, after which the ESI® is measured again after 3 months. Groups that need more support receive more assistance through additional training. As a KPI, the ESI® benchmarks you against companies of the same industry and size.	ESI®	70 Target ESI®	80 Target ESI®	90 Target ESI®

Awareness Engine

Features	Lite	Basic	Professional	Premium
Awareness Engine: Our technological heart The Awareness Engine is our technological heart and provides the live analysis of the security behavior of your participants. It Is always active, with individual groups active or paused. Based on the Target ESI®, it decides which groups receive which training at which time. Each participant therefore obtains just as much training as necessary, but at the same time as little as possible.		✓	✓	✓
Full service by awareness experts Structured communication with stakeholders is the key to a sustainable security culture. Your personal Awareness Consultant will support you with best practices from hundreds of successful customers in setting up and maintaining your security awareness program. This includes internal communication with stakeholders (employees, management, works or staff council, data protection officers, IT support), configuration of the project, support with whitelisting and test mails as well as material for internal announcements.	✓	✓	✓	✓
Security Hub: One-Stop-Shop for Training & Communication To ensure an optimal learning effect, we need a convenient and consistent learning experience. The Security Hub combines your employees' personal e training in one central location. We focus on individual learning paths because we know how each individual learns. Employees can access their e training sessions from any location and review their own phishing scenarios. Your employees are automatically logged in via Magic Link and do not have to remember any access data.	✓	✓	✓	✓

Awareness Engine

	Measure once or permanently	Permanently measure & training		
Features	**Lite**	**Basic**	**Professional**	**Premium**
"Most Teachable Moment": Awareness at the right moment The „Most Teachable Moment" is a valuable pedagogical and didactical moment for effective learning and for informing employees about potentially harmful misconduct. For example, an interactive explanation page uses the actual phishing e-mail clicked to show what to look out for and what psychological trick was used in the process.	✓	✓	✓	✓
Interactive e-training that is fun to use IT-Seal e-training provides participants with entertaining, easy-to-understand content on security culture, information security and data protection in the form of e-learning sessions, short videos and most teachable moments.	optional	✓	✓	✓
Company certificate as proof for ISO 27001, etc. You will receive a company certificate as proof for security audits (IS027001, TISAX, BSI IT-Grundschutz,...) and for customers. Further employees receive certificates of participation.	✓	✓	✓	✓
Individual branding: customized for your company Adapting the e-training, the Security Hub, the notification e-mails and the awareness materials to your corporate branding strengthens your image among employees. In addition, the explanation page with your company logo prevents any feelings of mistrust.	✓	✓	✓	✓
Customized configuration: Adapted to your employees Configure the awareness training according to your individual requirements or add your own content: From the number of simulated emails (phishing intensity)to individual text elements in your e trainings.	✓	✓	✓	✓
Online seminars & „Stay alert!" awareness material In interactive online seminars, participants are taught the basics of secure behavior in the workplace by an awareness coach. Our awareness materials include posters, flyers, webcam covers, mouse pads, writing pads, grape sugar and energy drinks.	optional	optional	✓	✓
Classroom training & social engineering site visits In classroom training sessions, participants are taught the basics of secure workplace behavior in person at your site. For the social engineering penetration test, we assume the role of an attacker and check how vulnerable your site is.	optional	optional	optional	✓
Phone attacks (vishing) & manipulated USB sticks With fake telephone attacks, we try to obtain sensitive information or instruct payments. We inform the affected employees directly and sensitively. Manipulated USB sticks are used as another attack vector.	optional	optional	optional	✓

Academy features in detail

Patented Spear Phishing Engine

	Measure once or permanently	Permanently measure & training		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Patented Spear Phishing Engine: The Best Phishing Simulation Based on freely available information, our patented Spear Phishing Engine generates individually tailored phishing attacks (spear phishing/dynamite phishing).This is fully automated: Each employee narrates individual scenarios at individual points in time.	✓	✓	✓	✓
Company OSINT: Open Source Intelligence Our company OSINT searches your website, job portals, employer rating portals or professional social networks for individual company characteristics. The information obtained serves as the basis for company-specific spear phishing e-mails.	✓	✓	✓	✓
Employee-OSINT:Open-Source-Intelligence Our employee-OSINT sea rches professional social networks for usable information. We collect information from your employees who have not set their privacy settings correctly. The obtained information is used as a basis for employee-specific spear phishing emails.	optional	optional	optional	✓
Spear phishing mails: Level 1-3 The level of our spear phishing mails is based on standardized classifications (the higher the level, the greater the time required by an attacker). The automated selection of spear phishing mails is based on individual person, department, company and industry scenarios. Just like real attackers, they use potentially dangerous links, fake logins, pages, macros and encrypted file attachments.	✓	✓	✓	✓
Outlook Add-In: Reporter Button The Reporter Button serves as a reporting tool and simplifies the reporting process for real attacks. It also provides positive feedback for detected phishing simulations.	✓	✓	✓	✓
Custom spear phishing emails We create phishing emails that are individually designed according to your specific needs.	optional	optional	optional	✓

Employee friendliness & data protection

Features	**Lite**	**Basic**	**Professional**	**Premium**
Security and Privacy by Design Collaboration and data protect ion are paramount, which is why the results of the phishing simulation are always analyzed on a group basis. From the very beginning, our process and data base structures have been created according to the principle of “Security and Privacy by Design“.	✓	✓	✓	✓
Respectful and sensitive communication From the outset, we have understood that we need to involve all employees step by step, communicating in a respectful and sensitive manner. Together with your employees, we want to work together to achieve the goal of a sustainable security culture.	✓	✓	✓	✓
Individual opt-out solutions To make processes as privacy-friendly as possible, your employees have various options for objecting to certain measures. This gives you the opportunity to address each participant individually and in line with their wishes.	✓	✓	✓	✓

Awareness Engine

Train employees - fully automatically with the Awareness Engine

Security awareness training for employees is essential to effectively protect a company from cyber attackers, because 90% of cyber attacks start with a phishing email. Nevertheless, this is a challenging task for many IT security officers, as sustainable employee training can be time-consuming and take up many resources.

Not with us: IT-Seal has developed the innovative Awareness Engine for you. This awareness technology trains your employees on demand and fully automated for a sustainable and efficient sensibilization. The result is an active security culture and educated employees who know and realize their responsibility for their company. The Awareness Engine forms the technological core of our Awareness Academy and provides training on autopilot: Each participant receives as much training as necessary and as little as possible.

Save working time and costs

With the Awareness Engine, your employees receive as much training as necessary and as little as possible

Training on autopilot

The Awareness Engine offers training on autopilot and automatically pauses or starts the training of your employees

Key indicator-based, group-specific, needs-based

Awareness training is targeted and metrics-based thanks to Target ESI®

With the awareness engine to the Target ESI®

At the beginning of the joint awareness campaign, you define your target ESI®, which you want to achieve and maintain in the long term. The ESI® is a control instrument that can be used to regularly check the security awareness in the company. Thus, there is transparency about the progress of your employees. Our Awareness Engine uses your Target ESI® to train your employees in a targeted manner based on key performance indicators. It checks the effectiveness of individual training measures and derives concrete training needs.

Patented Spear Phishing Engine

OSINT-based Attack Potential Analysis

Today's phishing emails are becoming increasingly sophisticated. To prepare spear phishing attacks, attackers gather information from publicly available sources to get a comprehensive picture of the target. In espionage lingo, this is described as Open Source Intelligence (OSINT).

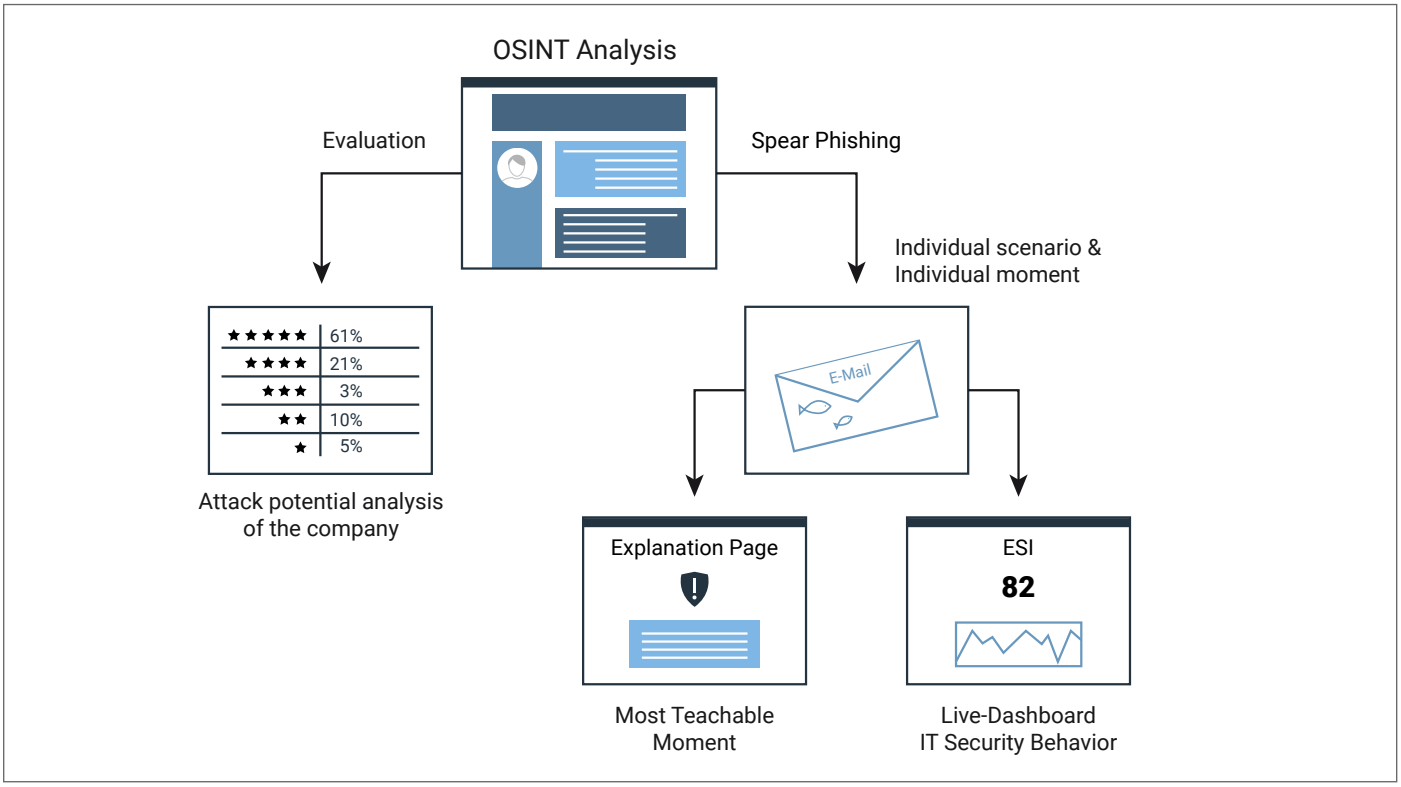
To assess your company's exposure to threats from publicly available information on social media, we have developed our Attack Potential Analysis. How much (critical) information do your employees disclose on job-related social media?

Which employee groups should you specifically point out to the associated risks? For which groups is training in the use of social media worthwhile? The topic of data and employee protection is, of course, a central component here. The analysis is always group-based, never person-based. We only analyze information that has been published by the employees themselves.

From Mass To Spear Phishing

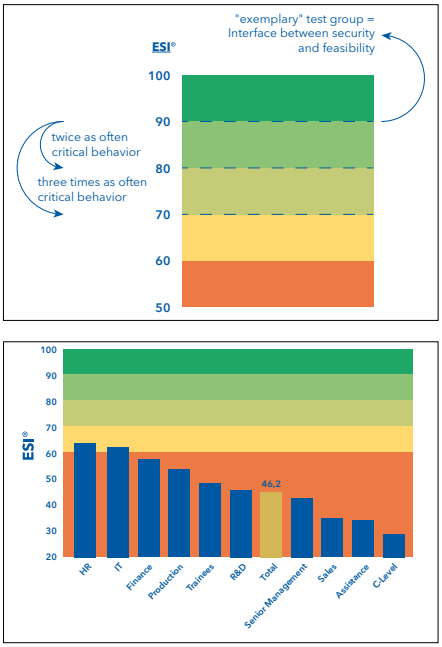
Like a real attacker, we use the collected data to make our social engineering simulation even more targeted: „Invitation to the company sports hiking group," „You used to work there - what do you say to that message?"

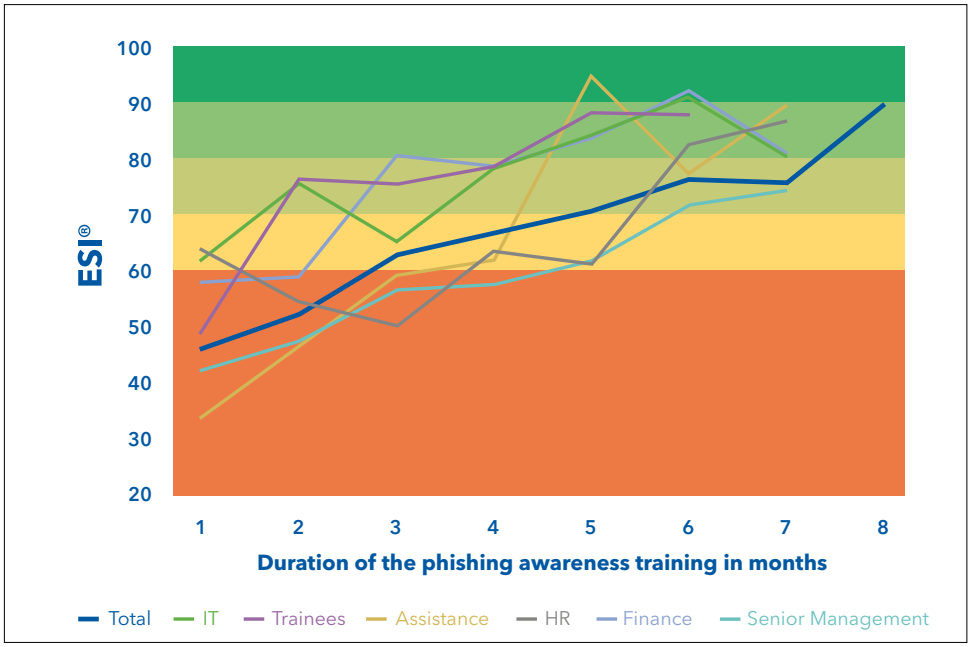
This allows us to map a wide range of attack scenarios from mass to spear phishing and comprehensively analyze your threat situation. Alternatively, we can also automatically simulate targeted attacks without OSINT by using just a few pieces of information (department, position).



ESI® benchmark as a KPI: The Employee Security Index

The ESI® offers transparency and comparability





Measurements of the Employee Security Index (ESI®) as part of the Awareness Assessment and Awareness Academy

Security is a factor difficult to measure

Against what, under what conditions and to what extent is one secure? This question brings major challenges when it comes to securing the company and making investment decisions. For Social Engineering and Phishing Awareness, IT-Seal has developed a benchmark, the „Employee Security Index" (ESI®). Based on the current state of research and our experience with phishing simulations in companies of different industries, we have derived tolerance values for the behavior of employees towards social engineering attacks. The respective tolerance value depends on the preparation time an attacker has to spend for the corresponding attack.

At the interface between absolute security and achievability, we define a „secure" company as one that achieves a score of 90 on a scale of 0-100. Which ESI® does your company achieve in comparison? Who is more secure, sales or accounting? We determine the ESI® for individual employee groups in a transparent and comparable manner in order to identify potential risks and make it possible to plan further training measures. The size of each group includes at least 30 employees to protect the privacy of individual employees.

„The ESI is the first and only IT security metric that has made it into our corporate KPIs!"
- Customer from the energy industry -

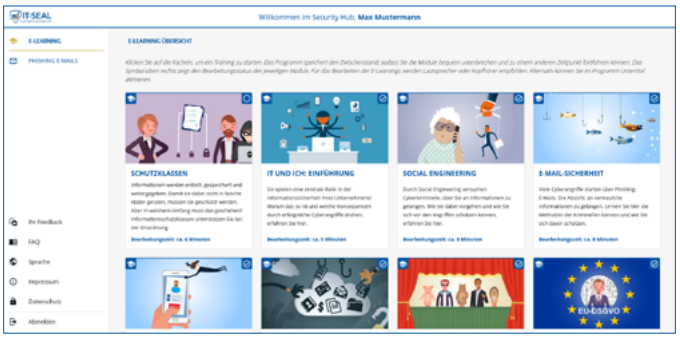
Compatible and communicable

Our concept makes social engineering attacks repeatable. With the ESI®, you can easily integrate the development of awareness in your company over time into your SOC via API. Our key performance indicator is also easy to understand for management and makes the topic of awareness tangible.

Further Awareness Technologies

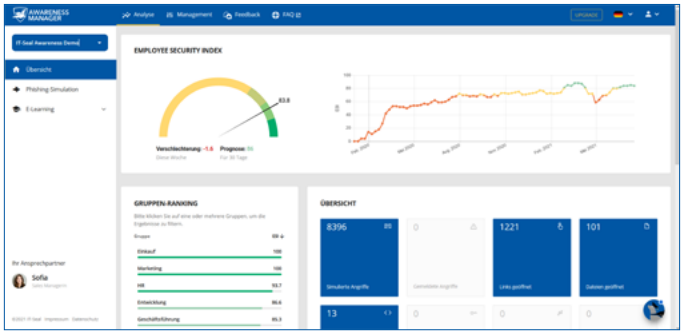
Security Hub

The Security Hub brings together your employees' personal learning content centrally and conveniently in one place. Your employees are logged in automatically and do not have to remember any access data. There, they can access their booked and assigned e-learnings and other learning content. The Security Hub stores all interim training statuses, and employees can also view learning content they have already completed at any time. Each employee can also view a personalized report on the phishing emails they have received from IT-Seal. The FAQ section also provides employees with information from our knowledge database.



Awareness Manager

Awareness Manager gives you a live overview of the status of your awareness campaign and the current security level at any time. The results can be viewed project-wide and on a group basis. You can also see how many links and file attachments were opened and what ESI® was achieved. You can also view the specific phishing scenarios sent, including the success rate, and the employee progress for the e-learnings sent.

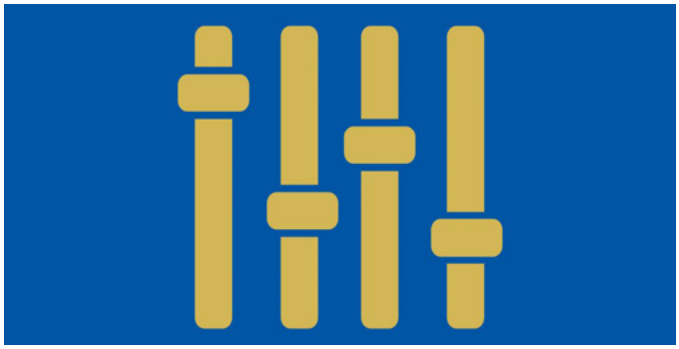


Training According To Need

Our phishing simulation starts with simple scenarios and increases individually if the employee successfully defends against them - all the way to increasingly elaborate spear phishing e-mails. In this way, we avoid both demotivated employees who experience frustration one failure after the other, and security fatigue: employees receive exactly the right level of difficulty between boredom and overwhelm.

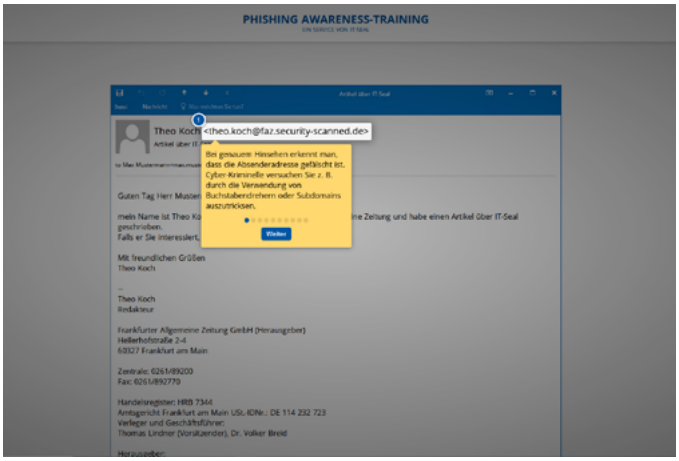
Define Phishing Intensity

Certain events or phases of extraordinary stress can be reasons to throttle the phishing simulation for your employees. In some cases, a permanently low sending rate of simulated phishing emails can also be useful. In consultation with your awareness consultant, you can easily and quickly adjust the intensity of all phishing emails sent globally to the needs of your employees.



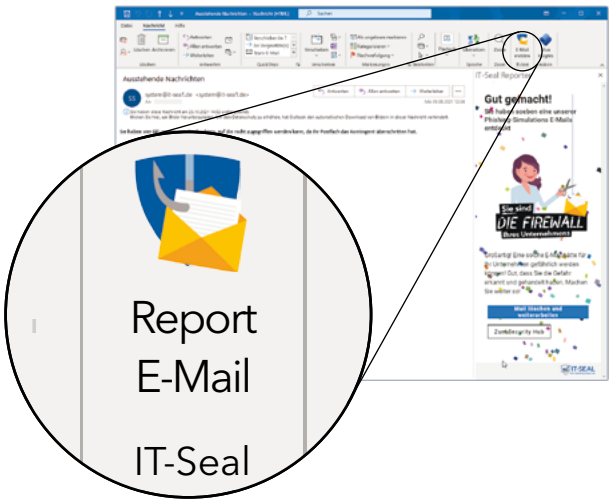
Individual Explanation Page

If an employee opens a risky link or file attachment or enters login data on fake pages, he is redirected to the IT-Seal explanation page. The exact example of the e-mail just opened is used to show specifically how he could have recognized the phishing attempt. At this moment of misconduct, the employee is particularly receptive to a lasting explanation: the so-called „most teachable moment" can fully unfold its learning effect. Also, frequently used psychological tricks (curiosity, fear, habit, ...) are pointed out.



Reporter Button for Outlook

The reporting chain is a central element of IT security in the company. To support this, IT-Seal offers the Reporter Button as an add-in for Outlook Desktop and Mobile. It enables employees to forward a suspicious email to a predefined location with one click. If the email is an IT-Seal spear phishing simulation, employees receive positive feedback directly. If the e-mail does not originate from IT-Seal, it is automatically forwarded as an attachment to the customer's internal IT support for analysis. The goal is to simplify the reporting of phishing incidents as well as to keep the internal company effort with the phishing simulation low. In the IT Seal Awareness Manager, it is possible to see how many of the simulated phishing emails have been reported by employees.



ISO27001 Compliant Reporting

All participants who successfully complete their scheduled e-learning modules and phishing simulations receive a personalized certificate of participation that can be used as proof within the framework of ISO 27001. The company itself also receives a valid certificate of the measures carried out to provide proof.

Modular E-Training

E-learnings and short videos for state-of-the-art learning

Interactive E-Learning

Our e-learning modules are versatile. They cover a wide range of topics in a practical way, providing employees with flexible, hands-on training in the field of IT security: From the tricks of the social engineers and vivid examples of real security incidents to know-how that can be applied professionally and privately - always with the „human factor" in focus. Interactive, entertaining and easy to understand for all target groups.

Monitoring also plays a major role for us. The training can be managed in the learning management system (LMS) and the learning progress can be tracked. All participants who successfully complete their scheduled e-learning modules receive a personalized certificate of participation that can be used as proof within the framework of ISO 27001. In addition, you can choose whether the e-learning should be conveniently made available in our internal learning management system or whether the content should be dynamically incorporated into your company's LMS. All e-learning modules are available in German, English and French. Other languages by request.

Introduction: IT and Me

Social Engineering

Passwords and Authentication

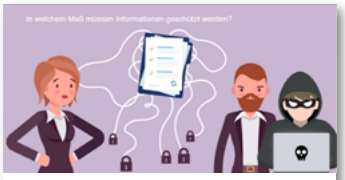
Email Security

Social Media

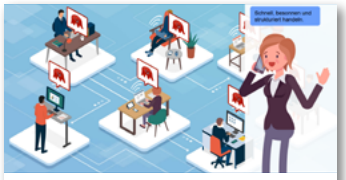
Homeoffice

Vishing

Data Privacy



Classes of Information Protection



Report Cyber Attacks

Excerpt from our comprehensive e-learning offer

Relevant and actionable

Learning content is immediately applicable in everyday life

Our experience is your advantage

Trainings created by security awareness experts, based on many years of experience.

Personalized employee certificates

All employees can receive personalized certificates attesting to their participation in the completed modules.

Employee quizzes: Put your employees to the test

Want to make sure your employees have really internalized information security topics? Put their knowledge to the test with quizzes. In various tasks, participants are challenged to test their knowledge and apply it to typical (work) situations.

- As a participant, you gain insight into your level of knowledge and can proactively close gaps.
- As the person responsible, you receive an overview of the knowledge in the company and can identify and derive the training needs of your colleagues and employees.

Short videos for in between

Integrate simple and entertaining learning content directly into the daily work of your employees. With one-minute short videos, we bring current topics from information security to the point. The videos can be accessed conveniently at any time in the Security Hub.

The short videos cover current threat scenarios and supplement the e-learnings with specific IT security knowledge such as Emotet and fake login pages. The topics are regularly expanded and are always up to date.

The concise learning modules are designed to be entertaining and easy to understand for all target groups.

Short learning videos are perfect for everyday working life

Digital learning via video adapts perfectly to the ever faster changing world of work

Consistent learning concept

Content coordinated with learning units of the IT-Seal phishing simulation.

BSI IT Basic Protection

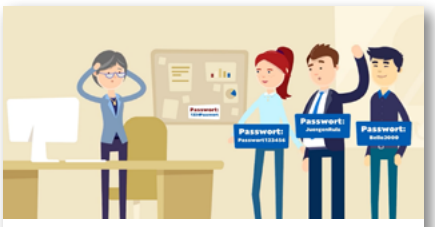
Sensitization of employees for InfoSec according to BSI IT Basic Protection (“BSI IT-Grundschutz”)

Dangerous macros: Emotet and the macro virus pandemic

- What are macro viruses and how do they reach me?
- What is the danger posed by Emotet?
- How can I protect myself from macro viruses? Who is attacking - and why me?

Don’t bite: Login pages as bait

- What is the danger of fake login pages?
- How can I protect myself?
- How can I tell if the login page is from a valid source?



Be a role model! Setting an example of information security as a leader

- Why does information security not only concern IT experts?
- What role do I play as a manager?
- How can information security become part of the corporate culture?

USPs of IT-Seal

Target ESI® and Awareness Engine

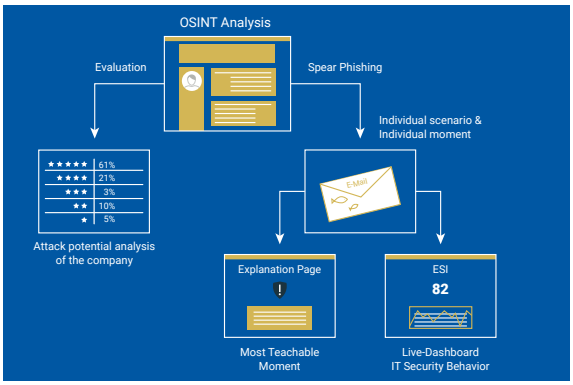
The Awareness Engine forms the technological core of your Awareness Academy on autopilot. It regularly evaluates the security behavior of your participants and decides on this basis which groups of participants should receive further training and to what extent. If a group is above the Target ESI®, it receives a training break of at least 2 months. If a group is below the Target ESI®, appropriate training measures are initiated. Each participant receives exactly as much training as necessary, but at the same time as little as possible.

Full service with stakeholder communication

We take care of your full-service awareness training, so you can sit back and watch the ESI® grow. In addition, we take care of the communication with relevant stakeholders in advance of the training. From the employees to the works council and data protection officers to the management and the executive board. We support you throughout the entire process with your personal contact person.

Patented Spear Phishing Engine

In preparation for spear phishing attacks, attackers gather information from publicly available sources to get a comprehensive picture of the target. In espionage jargon, this is described as Open Source Intelligence (OSINT). Like a real attacker, we use publicly available data from your employees and your company to make our phishing simulation even more targeted. This allows us to map a wide range of attack scenarios, from mass to spear phishing, and to comprehensively analyze your risk situation.



Opt-outs for your employees

Let your employees decide for themselves which data protection-relevant and personal awareness training measures they would like to participate in or not. For this purpose, employees can easily and conveniently object to corresponding processes via opt-out. In this way, you put the decision in the hands of the individual employees themselves, instead of letting the works council make blanket decisions over everyone's heads.

Quotes

89% of the participants state that the measures have increased their security awareness.

» I actually thought that I would recognize phishing emails directly. The campaign taught me otherwise. Now I am even more mindful. «

98% rate the awareness measure as useful.

» Much better than „just" taking online training courses! «

100% have discussed security awareness training with colleagues.

» Well constructed emails with rising sophistication. «

» In my project work, I see that our contacts greatly appreciate our full-service approach. The regular exchange with our customers enables us to respond directly to current needs. «

Antje
Customer Success Manager

» The attack methods used for cyber attacks are constantly evolving. This presents us with the daily task of creating a simulation that is as realistic as possible for the optimal training of our customers. I gladly accept this challenge! «

Christian
Technical Manager

Customers about us

From medium-sized businesses to publicly listed corporations - our customers include well-known companies from numerous industries. For data protection reasons, we have refrained from mentioning the company name.

Upon request, we will be happy to provide you with the complete reference as well as a contact person from an industry of your choice.

More at https://it-seal.de/en/references/

»Over the duration of the campaign, we were able to significantly increase our ESI® (Employee Security Index) ...“ «

- Manufacturing. 700 Participants.

After we had decided internally to carry out a further training measure on the subject of phishing awareness, we implemented this with IT-Seal. In addition to the sustainable training and sensitization of our employees, we were able to obtain an independent and concrete analysis of our security culture. The project implementation with IT-Seal was smooth and cost us very little internal effort.

The phishing simulation is based on current attacks. Over the duration of the academy, we were able to significantly increase our ESI® (Employee Security Index) and achieved a result after just 3 months that made us feel secure. We particularly appreciated the non-invasive nature of the training, which takes place without any additional time being spent on the job, and which enables us to pick up employees at their current level of knowledge.

The right awareness campaign for every industry

Machine Construction

Finance

Health Care

Energy/Utilities

Logistics

Higher Education

eCommerce

Law Firms

Manufacturing

Automotive

»After focusing on the technical part of IT security for a long time, the next step was to get our employees more involved ...«

– Finance Industry, 250 Participants

For this reason, we looked for a reliable partner and found it in IT-Seal. IT-Seal conducted a security awareness assessment for us, simulating social engineering attacks to measure the current security level of our employees. This allowed them to assess the security posture of our employees and identify any further action that needed to be taken. Prioritized measures were discussed to further increase our security. IT-Seal's phishing scenarios mapped very well what we have faced so far from real phishing attempts.

The project process was straightforward and tailored to our needs. The site assessment gave us direct insight into the behavior of the different employee groups.

The vishing simulation showed us weak points in the security behavior of our employees and is the basis for adapting our guidelines and implementing them.

»From contract signing to project end, we had great confidence in the data protection maintained by IT-Seal ...«

– Public utilities. 200 Participants

We were very satisfied with IT-Seal as a partner for measuring the IT security awareness of our employees. The topic of phishing analysis had been on our agenda for quite some time. Unfortunately, however, we were never able to find a partner with whom we could implement it in an employee-friendly way.

The project also gave us an exciting insight into the information that is publicly available about our employees and our company. This helps us to update our policies and also showed our colleagues how important it is to have the right privacy settings online.

From the time the contract was signed until the end of the project, we always had great confidence in the data protection maintained by IT-Seal. All topics relevant to data protection were competently prepared: The evaluation of the phishing simulation was consistently reported on a group basis. All employee-related data was transmitted in encrypted form, and the use of the data was transparent.

An extract of our customers

DEUTSCHE BUNDESBANK EUROSYSTEM

Schwan STABILO

DATEV

infraserv höchst

Together:
Digital and secure

Our vision

Every technology is designed to enrich human beings. If a person is able to use a technology, he can achieve great things.

People often feel that IT security in particular does the opposite: IT security systems get in the way of user productivity, and users are the biggest threat to IT security.

We believe it's time to reunite IT security with the user.

We believe that by empowering themselves, people can regain the freedom and confidence to achieve more with modern technology.

We believe that everyone can promote IT security - and vice versa.

Our values

Respect
The protection of the employee data and company internals entrusted to us is at the center.
We treat our customers' know-how with respect and value the time they spend working with us.

Professionalism
IT-Seal is known for its in-depth, cutting-edge expertise and scientific approach. We value clear communication.

Openness
We maintain open communication and clearly address ideas, suggestions and problems at an early stage. We cultivate a comprehensive feedback culture in our collaboration. We provide our customers with a transparent risk analysis.

Flexibility
We see it as a strength of our start-up character to flexibly adapt our performance to the needs of our customers and partners.

Made with ♡ in Security Valley Darmstadt

IT-SEAL
Social Engineering Analysis Labs