ESI® BENCHMARK REPORT

EDITION 2023

AN EVALUATION OF OVER
1.7 MILLION SIMULATED
**SPEAR PHISHING ATTACKS
ON EMPLOYEES**

EMPLOYEE SECURITY INDEX

HORNETSECURITY

HORNETSECURITY

ESI® BENCHMARK REPORT
EDITION 2023

Chapter 1: Executive Summary

Phishing that never ceases. The prevalence of attempted fraud through bogus e-mails looks set to reach a record high. Hackers who use phishing techniques are increasingly targeting companies, as this is where the greatest financial rewards are to be held. They send apparently trustworthy e-mails to employees, to steal sensitive information, encrypt data or, in the worst-case scenario, paralyze the entire business.

The aim of this ESI® Benchmark Report is to highlight the growing risks that phishing poses to your company, as well as to outline effective defense strategies— focusing on security awareness training from Hornetsecurity. This enables you to improve your employees' security behavior and establish an IT security culture that lasts. The patented Employee Security Index (ESI®) is at the heart of our training portfolio—a scientifically grounded indicator for measuring and monitoring security awareness.

Our current ESI® benchmark illustrates exactly how this works. The study, for which we analyzed around 1.8 million simulated spear phishing attacks targeting employees in companies of all sectors and sizes, creates transparency and shines a light on ways to optimize security awareness among your employees.

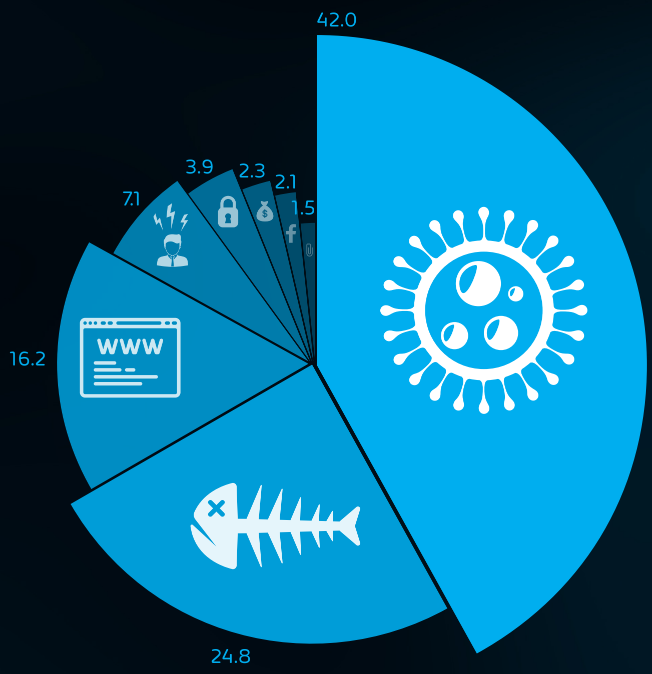
One of the main findings is that companies across all sectors achieve an acceptable level of security—equivalent to an ESI of 70—after just three months of security awareness training on average. However, as training progresses, it is difficult for companies to maintain this level. This is partly because phishing simulations become increasingly difficult to spot over time, and at the same time, new employees joining the company are just starting their training. Hence, companies are well advised to opt for an ongoing training cycle.

A finding which is ust as enlightening is that the most successful phishing scenarios exploit employees' blind faith in authority as a psychological trigger. Managers in particular need to act as role models when it comes to IT security. They must motivate their team members to take part in security awareness training and to share their experiences.

Chapter 2: Phishing– Number one among cyber attacks

Phishing has become an ever-present threat. The federal snapshot of cyber crime published by Germany's 2021 Federal Criminal Police Office (BKA) reports a significant rise in the number of phishing attacks and categorizes fraud though bogus e-mails as one of the most common types of cyber attacks.[1]

Over 90 percent of all cyber attacks start with a phishing e-mail. As the Hornetsecurity Cyber Threat Report 2021/2022 revealed, 40 percent of all e-mail traffic poses a potential threat[2], ranging from indiscriminate mass mail-outs to personalized spear phishing e-mails—where hackers may have spent weeks or even months gathering information to target their victim.



ATTACK STATISTIC	%
Other	42.0
Phishing	24.8
URL	16.2
Ransom	7.1
Executable in archive/disk-image	3.9
Advance-fee scam	2.3
Brand Impersonation	2.1
Maldoc (malicious attachment)	1.5

Fig. 1: The most popular email attack tactics in the 1st half of 2021

Dire consequences for companies

Companies affected by successful spear phishing attacks can pay a heavy financial price, and the loss of trust on the part of customers and partners can be substantial. In e-mails that appear deceptively genuine, fraudsters pass themselves off as line managers, colleagues or business partners to trick employees into disclosing highly sensitive data or clicking on malicious links and attachments. Employees can be prompted by hackers purporting to be line managers to transfer significant sums of money to bogus accounts. In other cases, a successful attack can provide the way into the entire company's network.

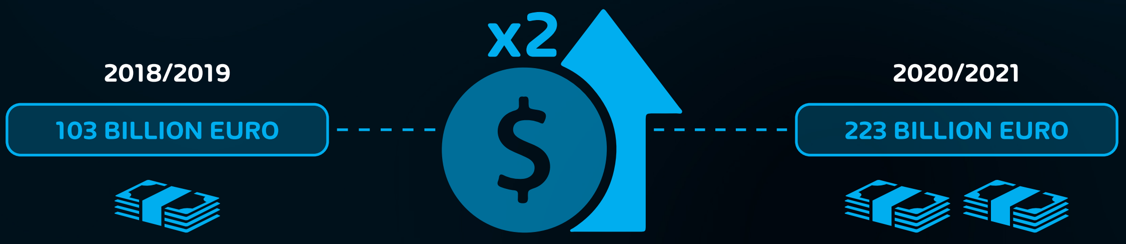


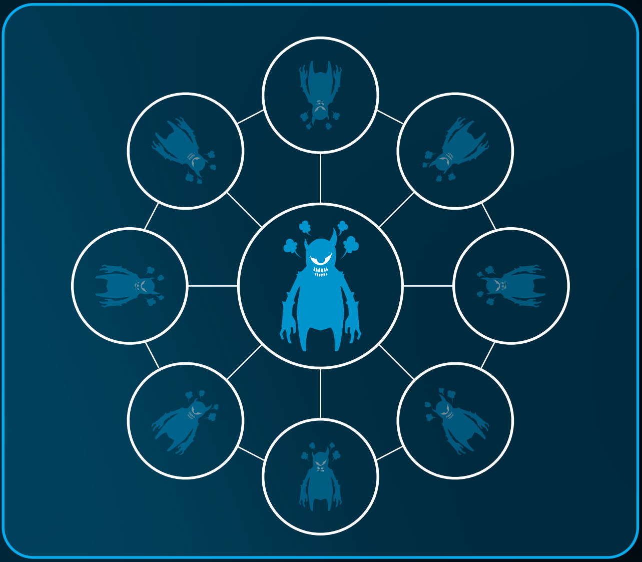
Fig. 2: Damage caused by cybercrime to companies in Germany according to Bitkom.

No respite in sight

Given the attractiveness of phishing, the current levels of phishing attacks are not likely to ease—quite the opposite. The COVID-19 pandemic, for example, has already proven to be an ominous catalyst in this respect, as highlighted in the Microsoft Digital Defense Report 2021[3], with many cyber criminals seeing their opportunity to exploit vulnerabilities arising from increased working from home and companies employing inadequate IT security measures.

Another surge in phishing attacks was reported around the outset of Russia's invasion of Ukraine. Cyber criminals, purporting to be from banks and financial institutions, were claiming to be carrying out checks on customers to ensure they were complying with EU sanctions against Russia and in the process getting their hands on login details via faked bank websites.

No programming expertise is required to fake an input screen. Instead, hackers use phishing kits that are available on the dark web for just a few dollars or even free of charge. With such tools at their disposal, fraudsters can now even bypass the usual two-factor authentication (2FA), which has been considered one of the most effective ways of protecting online accounts.



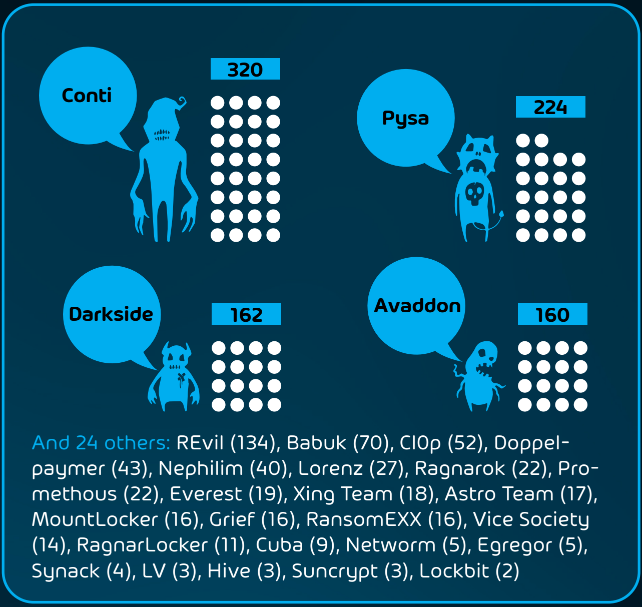
International fraud rings

As these examples show, phishing attackers are becoming increasingly unscrupulous with their methods becoming increasingly sophisticated. Internationally organized fraud rings, which bring together hundreds of members with specialist expertise, are often behind these offenses, professionally concealing the attack chain from start to finish. According to the Federal Criminal Police Office, underground elements are even increasingly offering targeted phishing attacks under a "Crime-as-a-Service" model.

Inside the cyber gangs, certain "experts" are responsible for gathering information on potential targets that can be found through social media and other online sources such as employer review sites or company websites.

Avid social media users in particular are easy prey for spear phishing fraudsters, as a joint study by the Technical University of Darmstadt and IT-Seal has shown.[4] Fraudsters are more than happy to use publicly available profile data relating to a person's current position, education, certificates, hobbies or colleagues to customize spear phishing e-mails on this basis.

Fraud ring members responsible for designing the bogus e-mails have a special role to play. As well as feigning insider knowledge, they have to master the key psychological tricks for taking in their victims. Whether recipients are driven by blind faith in authority, idle curiosity, willingness to help, time pressure or fear, anyone who targets one of these psychological triggers can be fairly certain that the e-mail recipient will follow their requests with no questions asked.



And 24 others: REvil (134), Babuk (70), Cl0p (52), Doppelpaymer (43), Nephilim (40), Lorenz (27), Ragnarok (22), Promethous (22), Everest (19), Xing Team (18), Astro Team (17), MountLocker (16), Grief (16), RansomEXX (16), Vice Society (14), RagnarLocker (11), Cuba (9), Networm (5), Egregor (5), Synack (4), LV (3), Hive (3), Suncrypt (3), Lockbit (2)

Fig. 3: The fraud gangs with the most published leaks of stolen or extorted personal data

Chapter 3: Employee Security Index (ESI®) Benchmark for learning progress

As a provider of security awareness training, Hornetsecurity combines training content, methods and tools into an innovative service portfolio.

The core USP is the patented Employee Security Index (ESI®) from IT-Seal—part of the Hornetsecurity Group since May 2022— which provides a scientifically grounded benchmark for objectively measuring and monitoring security behavior among employees.

Other measurement techniques to date have not been capable of doing this— they do not allow any standardization, and therefore there is no ability to make comparisons over longer timeframes or between departments, roles and company locations. This also brings the risk that individual security issues, errors or clicks on spear phishing e-mails may be overrated or underrated, ultimately providing companies with no transparency on the security behavior of their employees. So, they often invest too much or too little in order to achieve an adequate level of security.

Underpinned by preparation time

This is where the ESI® is different, as it is a realistic and reproducible method for measuring security awareness. In order to determine the ESI®, spear phishing attacks are categorized into different levels, depending on the amount of time that cyber criminals would have to invest in preparation and execution, for example, in obtaining information from publicly available sources, technical preparation, copying website designs, and maintaining the IT infrastructure required for the phishing attack.

This results in seven categories, each reflecting a preparation time of one hour to several days and weeks. A company's ESI® depends on how employees respond to phishing simulations of differing degrees of difficulty.

To be able to rate a company's security level in a standardized way, Hornetsecurity has defined test groups for exemplary security behavior. These values are based on "success rates" from the point of view of the attackers. Because "success rates" of 0 are unrealistic (everyone makes mistakes), the tolerance values are set at the boundary between security and feasibility. An exemplary test group with the lowest "success rates" achieves an ESI® of at least 90 on a scale from 0 to 100. If critical behavior is exhibited twice as often, the group achieves an ESI® of only 80; if critical behavior is exhibited three times as often, the group achieves an even lower ESI® of 70.

Values below 70 are regarded as problematic. The tolerance values defined by Hornetsecurity are based on the latest research and empirical data from phishing simulations in companies from a wide range of sectors.

The ESI® therefore provides companies with a tangible and reliable indicator, enabling standardized comparisons between different groups of employees. Is Sales or HR more secure? How secure is Management compared to Accounts? This is valuable information when it comes to determining the specific need for further training measures.

Chapter 4:

ESI® BENCHMARK REPORT
KEY FINDINGS AND BEST PRACTICES

How effective the ESI® is at measuring and optimizing security awareness among employees can be seen in the current Benchmark Report. For this, around 1.8 million simulated spear phishing attacks were analyzed, which were carried out between May 2019 and June 2022 on approx. 140,000 users from 350 companies of all industries and sizes.

User behavior was observed as training progressed over a twelve-month period. In this respect, it became clear, for example, what influence the type of sector has on click rates, as well as the role and position of an employee in the company. Similarly, the impact of external factors such as time elapsed, pauses in training and use of psychological tricks was examined.

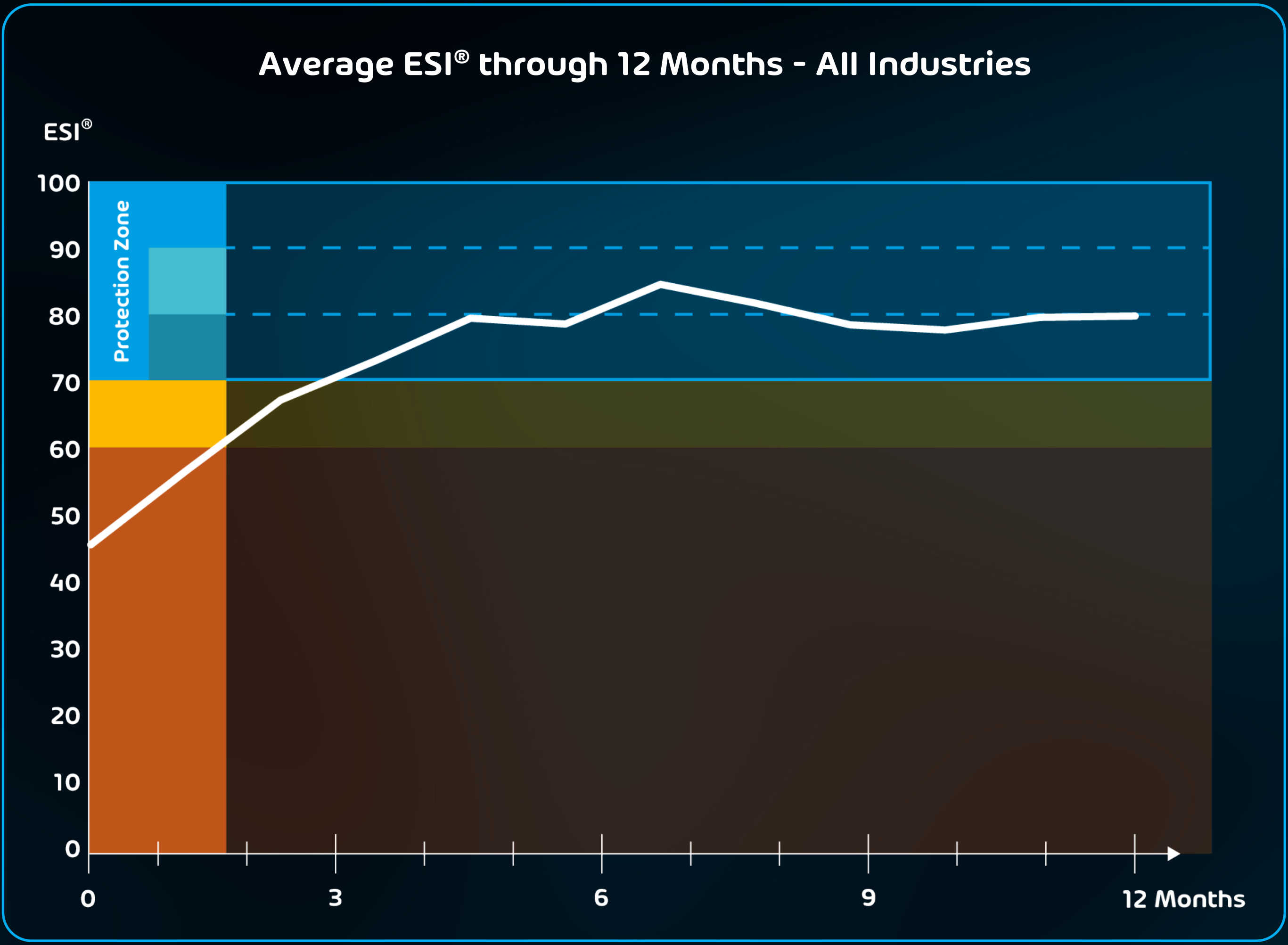
The findings of the ESI® Benchmark provide an insight into which awareness training measures can be used to optimize security awareness of different user groups.

Here's just a small selection.

HORNETSECURITY

IT-SEAL
Part of **HORNETSECURITY** group

Analysis 1: Average ESI® curve



Continuous awareness training required

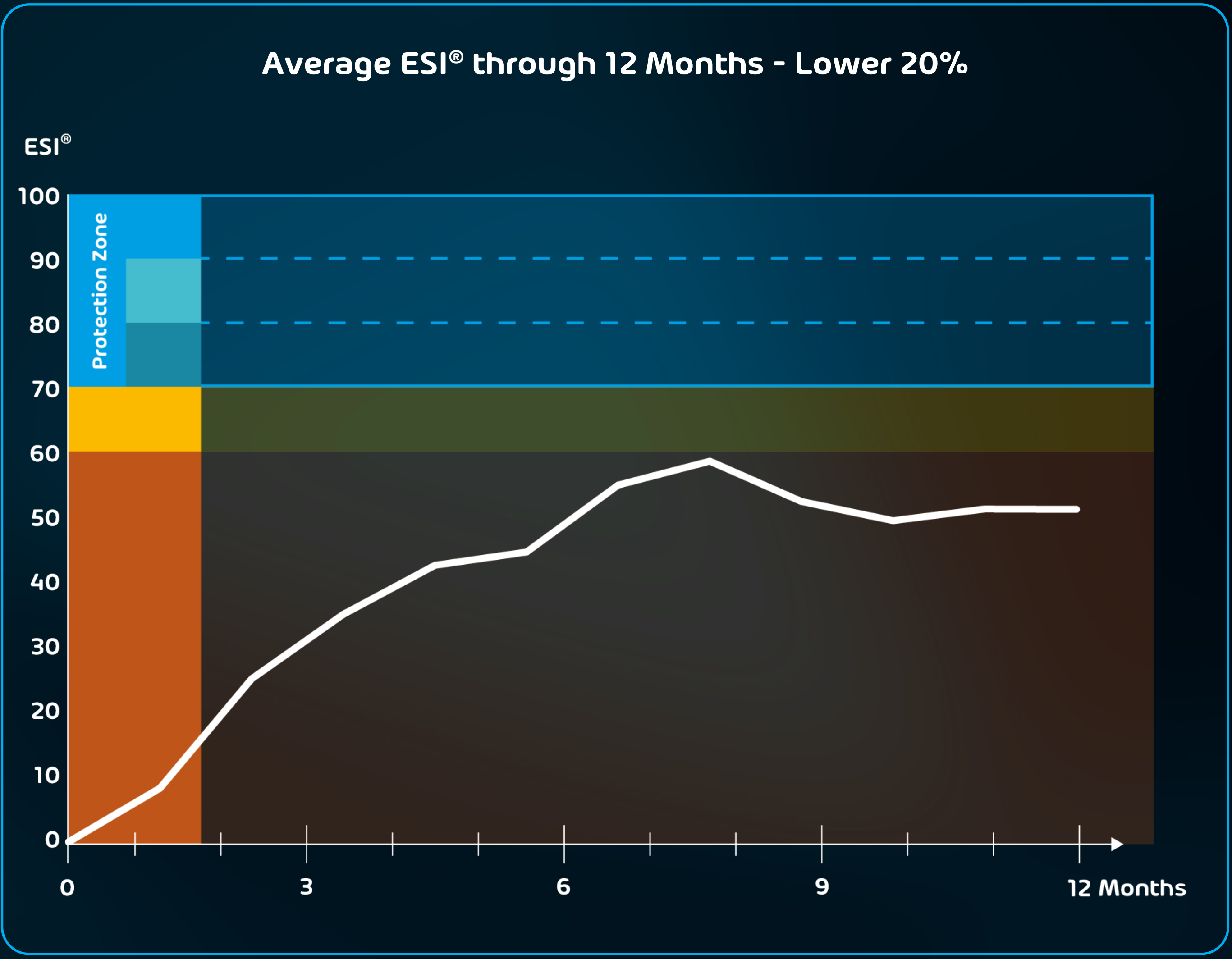
The importance of continuous security awareness training for employees is clear from the average ESI® curve over 12 months. A high level of security over a longer period of time can only be maintained if spear phishing simulations are repeated regularly and adjusted to reflect the latest techniques used by attackers.

As the graphic shows, the ESI® curve rises sharply after awareness training has started and reaches an acceptable security level after an average of three months. However, it is difficult for companies and organizations to maintain this level in the longer term. One reason for this is that, over time, employees start to forget what they have learned in the spear phishing simulations.

To keep their staff "in shape", companies and organizations should therefore adopt ongoing training cycles. Employees will only appreciate the importance of the information they have been given and retain it in their long-term memories by regularly repeating the simulated spear phishing attacks.

Another reason is that as new employees join the company, their awareness of phishing risks has to be raised and they have to be trained in recognizing fake e-mails. Continuous awareness campaigns make it possible to seamlessly integrate even newcomers into the training and to reinforce the importance of the role they play in IT security.

Analysis 2: ESI® of the "Bottom 20%"



Out with one-size-fits-all training!

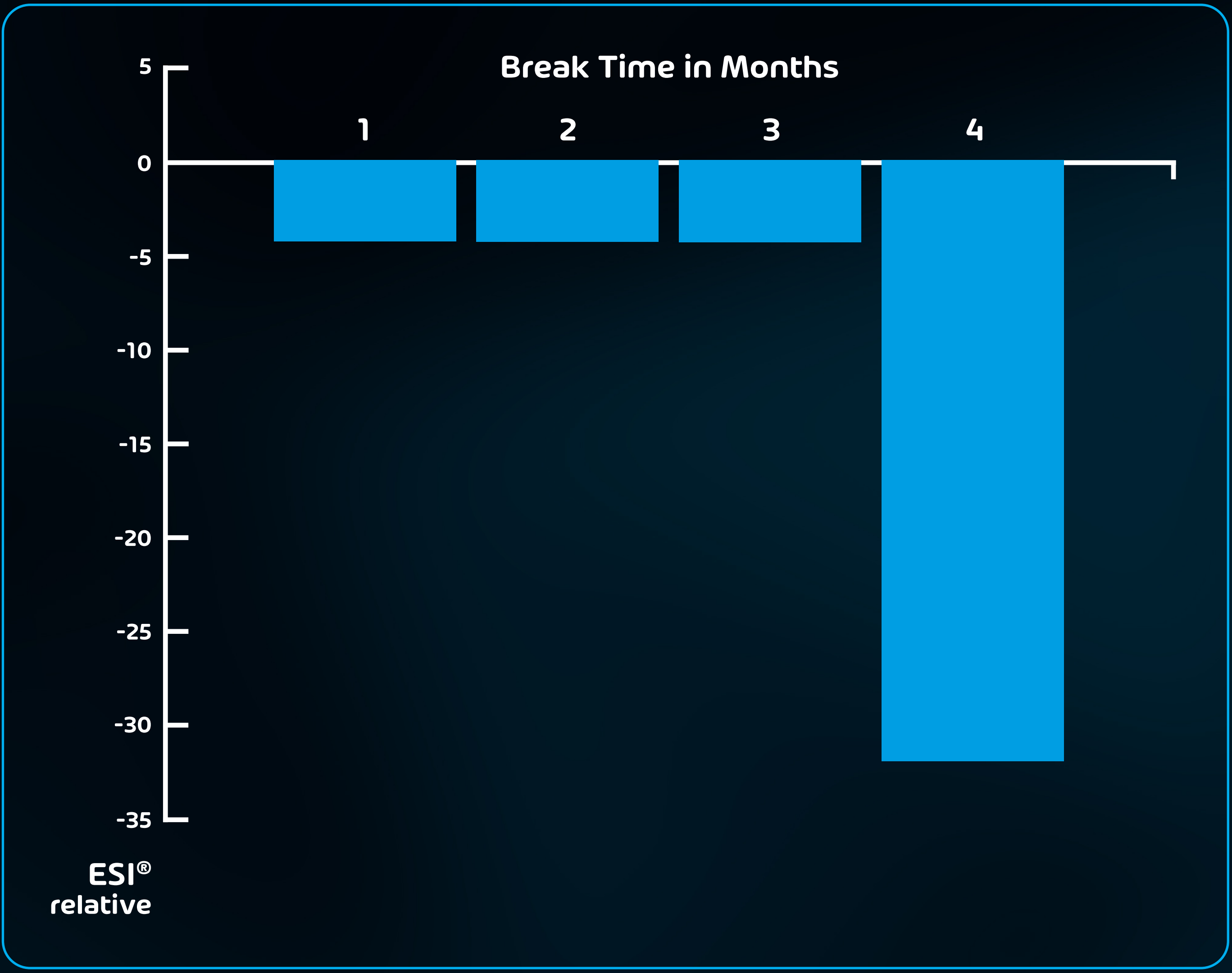
Any chain is only as strong as its weakest link. This is particularly the case for the "human firewall" used to protect against malicious spear phishing attacks, as shown by the ESI® curve for the "Bottom 20%". This refers to the user group with the highest click rates on simulated spear phishing attacks.

Although a certain learning effect is also apparent among the "Bottom 20%" within 12 months, which is apparent from the curve above, this group is unable to achieve an adequate level of security—in other words an ESI® of at least 70—at any time. And this is despite the fact that the "Bottom 20%" were given the same security awareness training as their colleagues.

The findings make it clear that security training must target individual learning needs rather than follow a one-size-fits-all approach. This is because all users do not learn in the same way at the same pace and to the same degree.

The ESI® helps companies quickly and easily address the different learning needs of their employees, as it provides a tangible and reliable indicator for documenting personal learning progress and determining the need for specific training measures. If users, like the "Bottom 20%", exhibit higher click rates, they need more intensive training.

Analysis 3: ESI® drop after a break



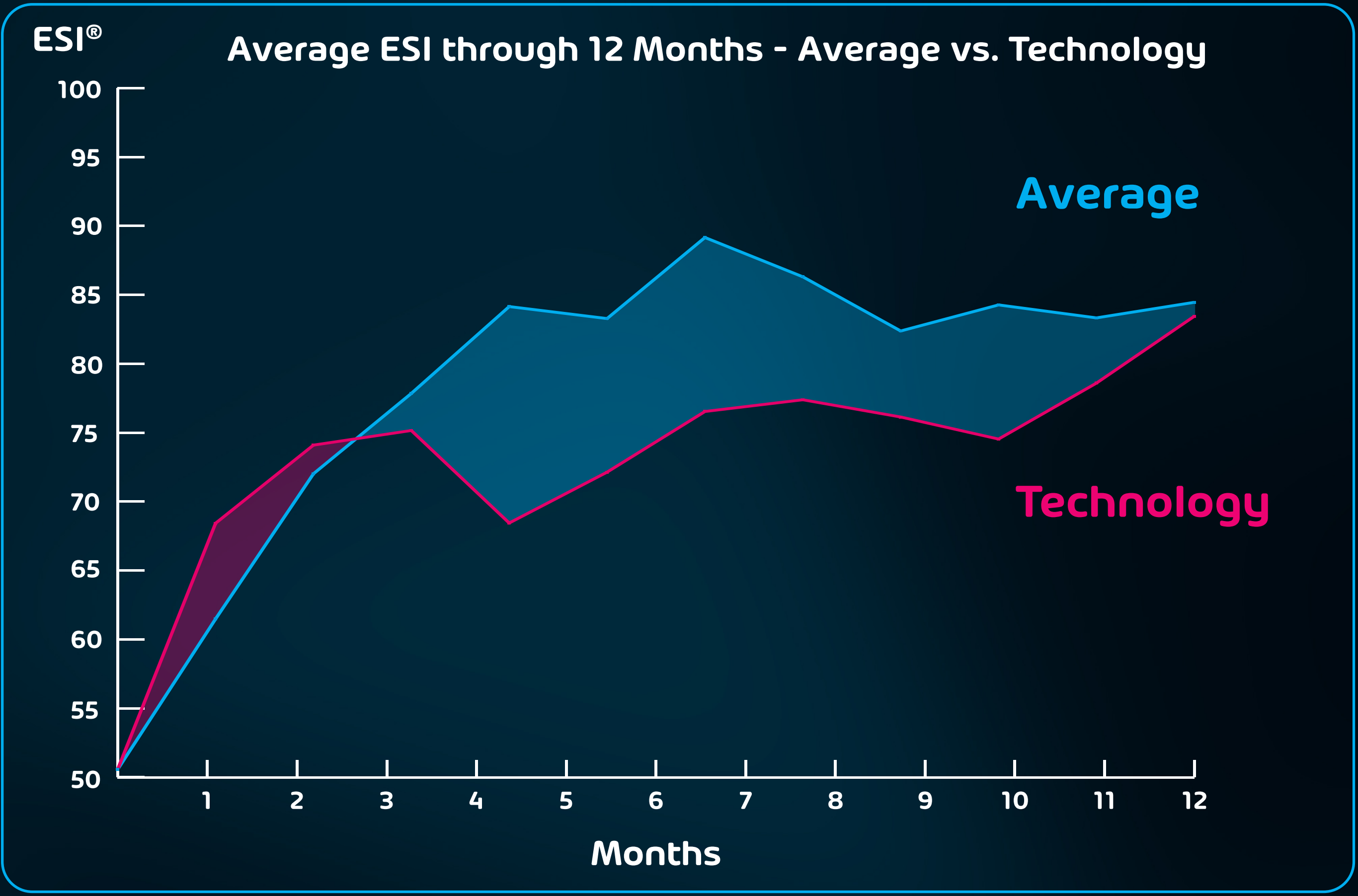
Pauses in training for long-term knowledge acquisition

Security behavior among employees is like a muscle that needs to be trained regularly to prevent it from slackening. If individual groups and employees pause their training for some time and then resume it later on, there is a clear deterioration in security behavior. These users appear to have forgotten key learning content from the spear phishing simulations and become more negligent in handling incoming e-mails.

The extent of the effect is shown as the ESI® drop in this graphic, where the bottom and top 25% have been factored out—i.e. user groups with particularly high and particularly low click rates. Even after a pause in training of just one month, the ESI® drops by five points, often falling below the target security level again. After four months without awareness training, the ESI® has already dropped by more than 30 points. In concrete terms, this puts companies almost back to square one in terms of employee security behavior.

Having said that, short pauses in training can be of pedagogical and didactic benefit to companies. Once certain groups or employees have reached the target security level, they should deliberately pause for a period of two to three months. It has been shown that acquired learning content has a more lasting impact on security behavior when it is refreshed after a certain pause. Furthermore, this helps to prevent potential "security fatigue" among employees.

Analysis 4: Technology sector vs. average



The tech-savvy overestimate their own abilities

You would expect employees from IT companies to be much more adept at dealing with cyber risks than employees in other sectors. And yet this assumption proves to be a fallacy, as shown by the above ESI® curves. The data shows the technology sector to have much higher click rates than the general average throughout the entire period under examination.

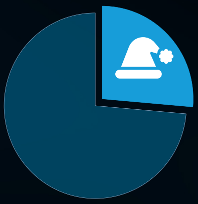
This can be attributed to the fact that people often overestimate their own capabilities, particularly in areas they work with on a daily basis. In the IT sector, this can harbor considerable IT security risks. And it concerns not only the companies themselves, but also their customers, as there is a very large number of software and data center providers in the IT sector that develop and operate applications for other companies.

In this case too, the ESI® helps address the sector-specific deficits in security behavior. IT companies are provided with a reliable indicator for determining the level of security and learning progress among employees and for determining the specific training measures needed. Awareness training can therefore be systematically adapted to the higher learning needs of IT employees.

Analysis 5: The Top 5 spear phishing scenarios and their psychological triggers

1. Authority of the sender & curiosity:

Management sends out an e-mail announcing a new organizational structure and associated responsibilities within the company. The new structure can be downloaded from the intranet.
28% success rate



2. Authority of the sender & curiosity:

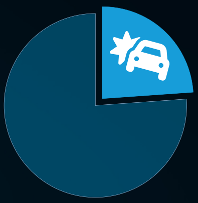
Christmas scenario: Management is gifting their favorite books of the year to all employees.
28% success rate

3. Fear of unpleasant consequences:

The recipient is informed their e-mail account is full and that the problem can be fixed by clicking a link.
24% success rate

4. Sense of duty & fear of unpleasant consequences:

The recipient is asked to sign the new policy on working from home.
24% success rate



5. Curiosity & fear:

The recipient is told that cars have been damaged in the company parking lot. They should use photos to check whether their car has been affected.
24% success rate

Everyone has different "trigger points"

Who falls for which spear phishing e-mail depends on many different factors: the stress and training level of the user, capacity for concentration, design of the e-mails, subject lines, etc.

The psychological triggers to which each and every one of us responds differently are, however, incredibly important in this respect. For example, there are users who tend to be slavishly obedient to authority and immediately click on every e-mail that purports to be from their team leader or from management. Other employees have a stronger response to scenarios that appeal to their willingness to help or sense of duty.

Curiosity, fear, faith in authority, willingness to help, vanity and many other drivers are important psychological tools for the fraudsters. They exploit these deliberately and oftentimes in individual combinations to take in their potential victims. To make employees do exactly what is asked of them, spear phishing attacks purposefully target their "fast-thinking" system as opposed to their slow and rational thinking system– a distinction made by psychologist and Nobel Prize winner Daniel Kahneman in his bestseller.[2]

Effective phishing simulations should therefore always target triggers that a user has shown themselves to be particularly susceptible to. In this way, employees learn as training progresses how to consciously arm themselves against the psychological tricks they are particularly vulnerable to.

Chapter 5: Companies beware - Quick action needed

In view of what has been said above, companies need to act quickly as phishing risks grow. They must face the fact that even the most advanced IT security technologies alone are not sufficient to protect against spear phishing. Even if IT teams are successful in filtering out millions of fake e-mails every day, a number will still manage to get through to employee inboxes.

Reinforcing the human firewall and cementing their employees' role in it should therefore be an urgent priority for companies. The need to do so has also been corroborated in a recent study by Bitkom, Germany's digital association, which found that the majority of cyber criminals exploit the "human factor" as the supposed weakest link in the security chain.[1]

An IT security strategy is most effective when it integrates the three central components of a security culture: mindset, skillset, toolset. In concrete terms, this means that employees' awareness of the threat posed by spear phishing e-mails must be heightened, they must be trained to recognize such e-mails and be supported to defend against them using suitable technical and organizational measures.

Mindset

Motivation and open communication

- Understanding the threat
- Emphasize personal responsibility
- Communication tools for all stake holders

Skillset

Acquiring skills and knowledge

- Phishing Simulation
- E-Learning
- Online seminars
- Face-to-face training
- Awareness materials

Toolset

Actively getting involved and intervening

- Live-Dashboard
- Password manager
- Security message chains
- Reporter-Button Outlook Add-In

Mindset: Developing a nose for danger

Blind faith in IT security technology is widespread among employees. Incoming e-mails are opened without hesitation and requests made in them are carried out, particularly when the message appears to be from a trustworthy source. A good piece of advice for companies is therefore to prompt a change to this way of thinking, by appealing to employees' own self-responsibility and effectiveness. They must internalize the fact that their commitment and vigilance are crucial for the functioning of the entire company.

Information campaigns initiated by management and supported by managers and IT staff are a good way to prepare for security awareness training. Experience shows that facts and figures on security incidents in the relevant sector leave a lasting impression on employees. An example here is the Austrian/Chinese engineering firm FACC, which lost around EUR 43 million when an accountant was taken in by hoax e-mails purporting to be from the CEO. He transferred this amount to online fraudsters, who fooled him into believing these were strictly confidential transactions for a company acquisition.

Information campaigns will have the maximum impact when they are communicated through various channels and encompass team meetings, videos and circulars.

Skillset: Encouraging intuitive decision-making

Subsequent security awareness training should not be restricted to conventional in-person sessions, e-tutorials and webinars, as these training formats only convey the theory about phishing attacks. Realistic spear phishing simulations have proven successful at sharpening user senses. They use genuine employee and company information to simulate real attacks. If an employee is taken in by a simulated fake e-mail, they are taken to an interactive explanation page that highlights the suspicious features of the message—from transposed letter combinations in the address line and bogus subdomains to dubious links and attachments.

Spear phishing simulations are so effective because they target the impulsive decisions made by employees that are responsible for spontaneous clicks on the e-mails. In his bestseller "Thinking, Fast and Slow", psychologist and Nobel Prize winner Daniel Kahneman distinguishes this instinctive and emotional thinking from rational and logical thinking.2

In addition, simulated spear phishing attacks make use of an employee's "most teachable moment". By explaining the potentially harmful consequences of their behavior at exactly the right moment, the training to recognize attacks is particularly effective and the employee will handle incoming e-mails more cautiously in the future.

To retain this learning effect, the simulated spear phishing attacks should be repeated on an ongoing basis and adjusted to reflect the latest hacking techniques. What has been learnt is otherwise quickly forgotten, as discovered by psychologist Dr. Hermann Ebbinghaus way back in 1885.3

According to the Ebbinghaus forgetting curve, learning content needs to be repeated multiple times before it "sticks". Because of the frequency of repetition, the brain recognizes the importance of the information and stores it in the long-term memory. Security awareness training therefore needs to be an ongoing process if it is to last.

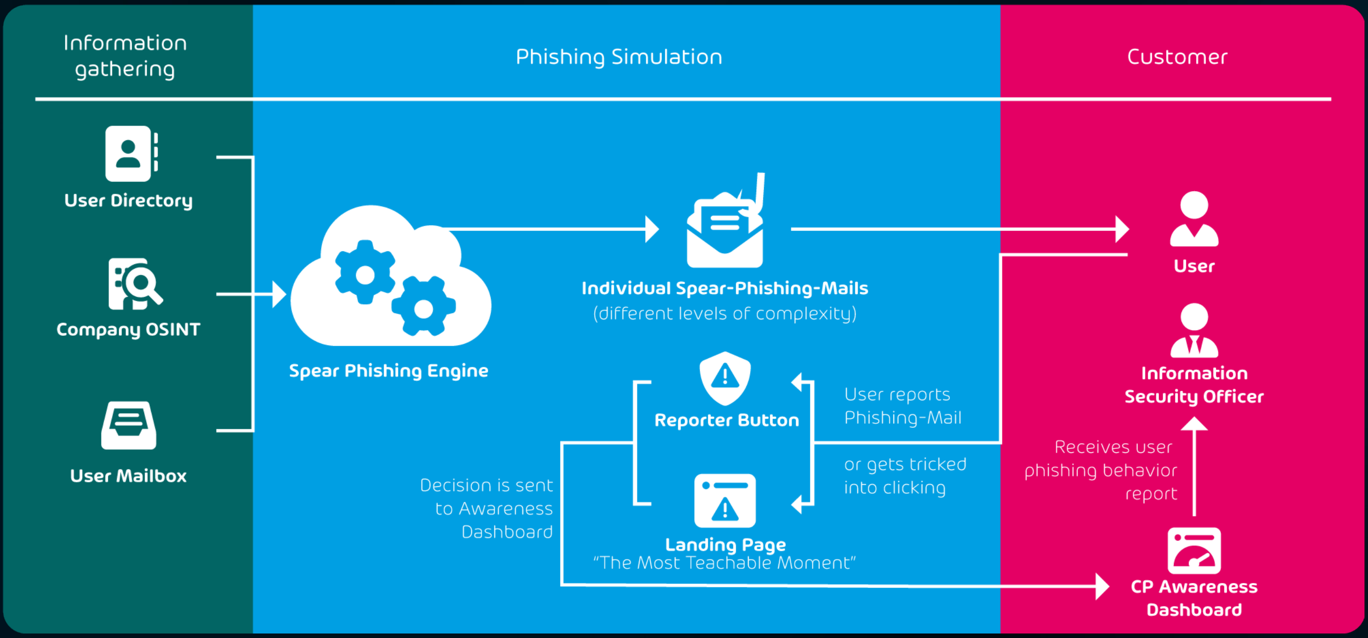

Information gathering
Phishing Simulation
Customer
User Directory
Company OSINT
User Mailbox
Spear Phishing Engine
Individual Spear-Phishing-Mails
(different levels of complexity)
Reporter Button
User reports Phishing-Mail
or gets tricked into clicking
Landing Page
"The Most Teachable Moment"
Decision is sent to Awareness Dashboard
User
Information Security Officer
Receives user phishing behavior report
CP Awareness Dashboard

Fig. 4: Spear phishing simulation process

Toolset: the icing on the cake of any defense strategy against phishing

Companies can round off their spear phishing defenses with the right toolset. Password managers that can be easily integrated into the workstation environment and enable digital identities to be stored and managed centrally are particularly advantageous.

Password managers help prevent employees from always using the same login details for convenience. If spear fishing attackers are successful in stealing an individual password, they can no longer automatically access all the other accounts belonging to this user.

To put a stop to the growing problem of 2FA circumvention, companies should switch to FIDO2 (Fast Identity Online).4 FIDO2 provides an innovative 2FA method where registration for an online service is covered by encryption that cannot be cracked even using the very latest hacking methods.

A "Reporter Button", which can be integrated directly in Microsoft Office, is another useful tool. This helps employees identify and report dubious e-mails. At the touch of a button, users are given useful tips as to whether an e-mail might be fake, and where necessary, they can forward it on to the IT security team for further examination.

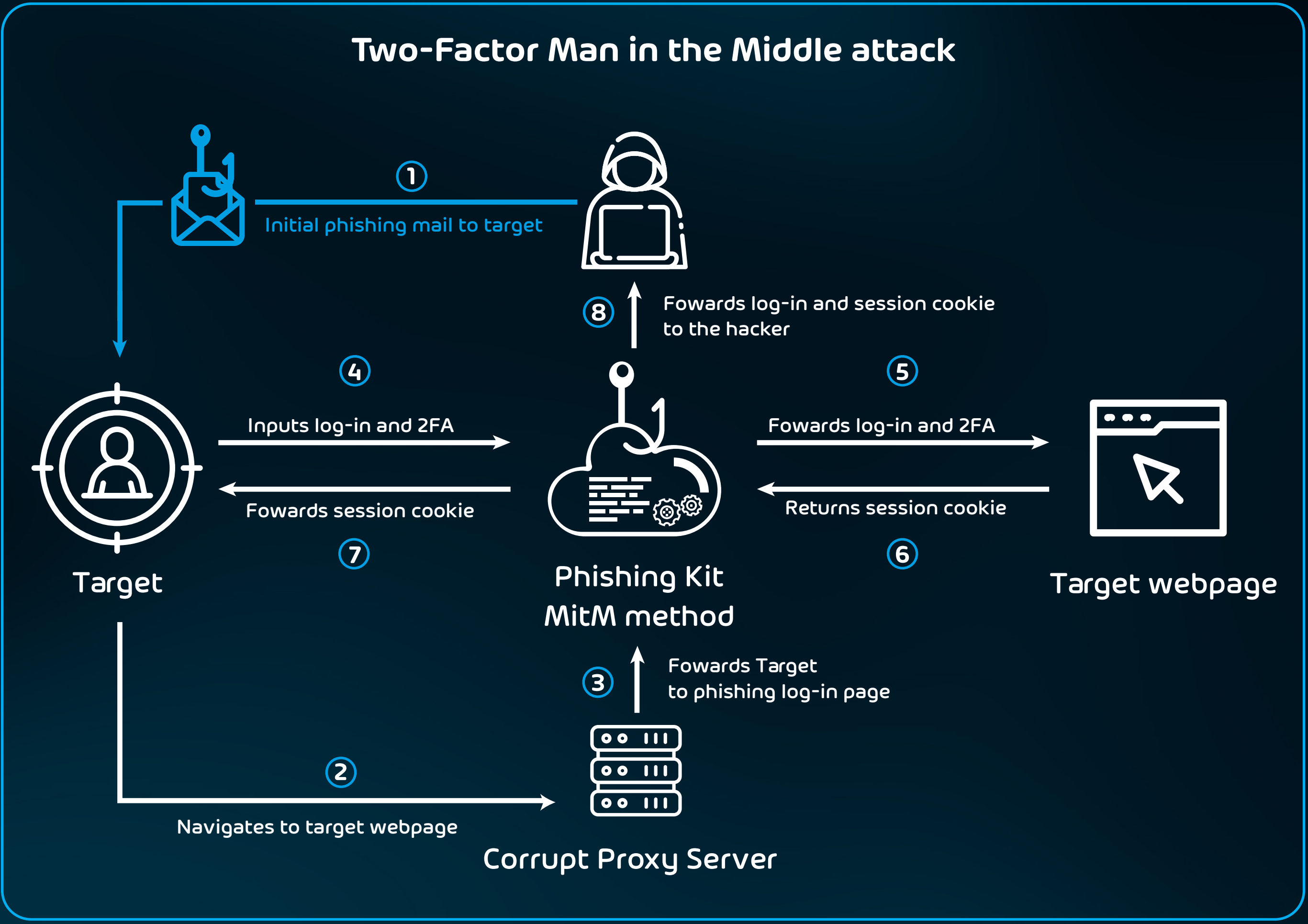

Two-Factor Man in the Middle attack
1
Initial phishing mail to target
8
Fowards log-in and session cookie to the hacker
4
Inputs log-in and 2FA
Fowards session cookie
7
5
Fowards log-in and 2FA
Returns session cookie
6
Target
Phishing Kit MitM method
Target webpage
3
Fowards Target to phishing log-in page
2
Navigates to target webpage
Corrupt Proxy Server

Fig. 5: Building a Man in the Middle Attack against 2FA Authentications

Security Awareness Service from Hornetsecurity is a complete solution

For the implementation of Security Awareness Service, Hornetsecurity has developed a complete solution that combines innovative learning formats such as e-training, "most teachable moment" and gamification with some of the most advanced spear phishing simulations. Conventional e-tutorials, video clips and quizzes provide participants with key information on growing cyber risks and the best ways to protect themselves and their company.

During the simulated phishing attacks the—also patented—spear phishing engine comes into play, which ensures the phishing attacks seem deceptively real. The spear phishing engine is based on innovative Open Source Intelligence (OSINT) technologies that automatically generate phishing scenarios that are specific to a particular company, department and employee. Publicly available data about the company (e.g. from employer review sites) and other sources are used for phishing content.

This allows realistic spear phishing e-mails to be created in which, for example, the department head enquires about an invoice that is included as an attachment. In other e-mails, fraudsters disguise themselves as colleagues or employees and refer to a discussion they supposedly had. For further information on what was discussed, the e-mail recipient receives an "interesting" link that in reality leads directly to malware. These examples show that the ploy used by spear phishing attackers is always the same. They dig deep into their box of psychological tricks and in this way cleverly target the drivers of their potential victims to make them do—without thinking—exactly what the cyber criminals want of them.

SECURITY
AWARENESS
SERVICE

Learn more!

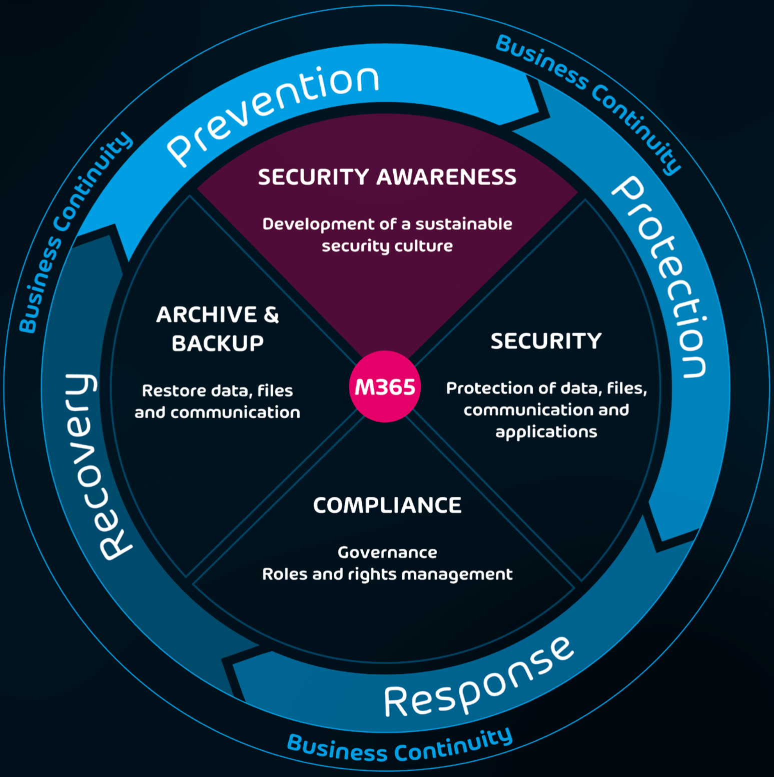

Prevention
Business Continuity
Protection
Response
Business Continuity
Recovery
Business Continuity
SECURITY AWARENESS
Development of a sustainable security culture
ARCHIVE & BACKUP
Restore data, files and communication
M365
SECURITY
Protection of data, files, communication and applications
COMPLIANCE
Governance
Roles and rights management

Fig. 6: Security Awareness as a part of the Business Continuity of Hornetsecurity

Training on autopilot

At the start of security awareness service, the target security level should be at least ESI® 70, which is then gradually increased. The Awareness Engine is deployed in order to achieve the respective ESI®. This AI-based engine means training can be switched to autopilot.

It pauses and starts the simulated spear phishing attacks automatically—on the basis of the ESI® indicator and specific need. Instead of the same one-size-fits-all training, each participant is given as much training as is necessary and no more than is required. This saves companies time, money and valuable HR resources as they no longer need to be involved in implementing and managing training.

At certain intervals, the simulated phishing attacks on individual employees are repeated and updated. A dedicated front end—the Awareness Dashboard—informs managers and IT security officers on how awareness is developing, i.e. how the ESI® indicators are progressing.

Like all other Hornetsecurity solutions, the Awareness Dashboard is integrated in the Control Panel. This is where up-to-date awareness training results can be viewed at any time. Employees themselves can track their individual progress in the User Panel. This is the learning platform for the Security Awareness Service, which all participants can individually access to obtain their individual training and test results.

Continuous training for lasting success

More than 1,000 companies of all sectors and sizes already place their trust in the tried-and-tested awareness technology from IT-Seal, which is part of the Hornetsecurity Group.

In order to achieve a long-term and lasting effect, many customers opt for an ongoing cycle of awareness training. This prevents the ESI® level that has been reached from dropping off again.

Instead, the issue of security awareness becomes firmly rooted in participants' long-term memories. An ongoing cycle also enables new employees to take part in security training as they join the company.

Successful spear phishing attacks can be disastrous for companies, regardless of whether they are in the finance sector, insurance or manufacturing.

How two notable companies are boosting their defenses using the Security Awareness Service:

As a leading provider of multibank-capable online and mobile banking solutions in Germany, Star Finanz operates in the highly regulated finance sector. Handling sensitive financial and transaction data from end customers and companies is part and parcel of their everyday business. To protect such data from spear phishing, in-house security training for employees had been carried out in the past.

As phishing attacks were becoming increasingly sophisticated, it became clear that a professional training provider needed to be brought in. The company opted for the Security Awareness Service from Hornetsecurity as it is a complete awareness training solution that keeps pace with the hackers. The innovative ESI® benchmark is a further benefit, which makes the security awareness of employees objectively measurable.

starfinanz

Learning progress can be perceived and measured

E-training and simulated spear phishing attacks are continuously being carried out for Star Finanz employees. Taking stock of the benefits, André Haase, Senior Security Architect at Star Finanz says: “Significant progress has been achieved and the security level among staff has markedly increased.”

For data protection reasons, the fact that Hornetsecurity processes customer information in Germany is very advantageous for Star Finanz, because it means that all training measures are compliant with the GDPR. What’s more, the company can pave the way for possible ISO 27001 certification by using the recognized security measures from the Security Awareness Suite.

For André Haase, the Security Awareness Service will definitely be staying on board in the long term to have a lasting impact on awareness training.

André Haase
Senior Security Architect - Star Finanz

Customer Success - How customers benefit from Security Awareness

If a manufacturing business is hit by phishing attacks, production can come to a complete halt. The results are lost earnings, an erosion of customer trust and deteriorating competitiveness.

Kirchhoff & Lehr, known throughout Europe as a specialist in rolled profile technology, cannot afford any such downtime. Alongside its extensive product range, the manufacturer has made a name for themselves with high quality standards, on-time delivery and value for money. As the number of bogus e-mails skyrocketed during the COVID-19 crisis, the company was looking for a solution to help raise employee awareness of phishing attacks.

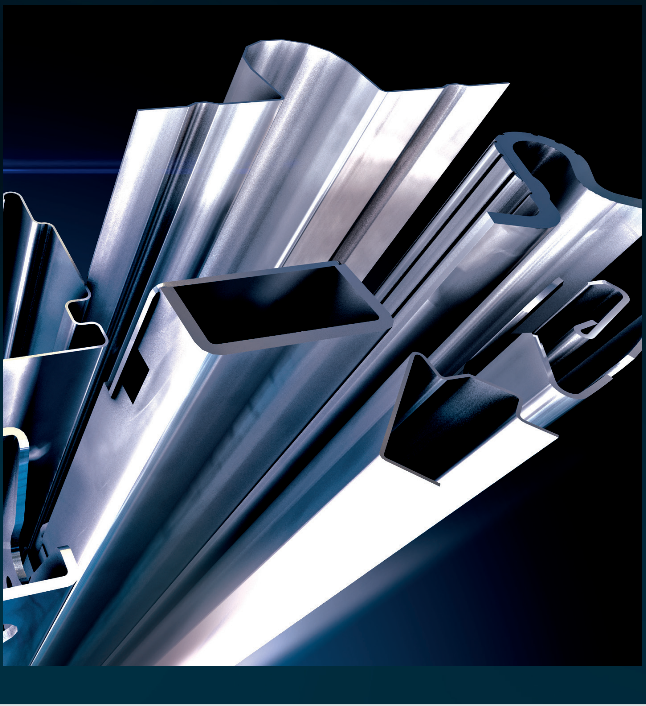
Training as a permanent fixture

After just a short time, the company opted to make security awareness training a permanent fixture for admin employees. Robert Batz, Head of IT at Kirchhoff & Lehr explains: "The main reason for this was the spear phishing simulations, which provide a considerable pedagogical and didactic benefit."

Before the awareness training started, employees were informed in keeping with data protection requirements and asked for their consent. They are now sent simulated spear phishing e-mails on a regular basis. Another aspect of their security awareness training is the use of the Reporter Button provided in the Security Awareness Service. If a user receives a dubious e-mail, they can forward it directly to the IT department for technical examination.

The increasing ESI® underlines the considerable progress that employees have made in identifying phishing attacks—in just a few short months. To keep their skills in shape and to allow newcomers to also benefit, training has been expanded far beyond the originally agreed contract term.

Head of IT Robert Batz has no doubt: "Feedback from the awareness training has been compelling, our employees have recognized the important role they play as the human firewall."



Robert Batz

Head of IT - Kirchhoff & Lehr GmbH

Chapter 7: Summary and outlook

Even the very latest IT security technologies cannot guarantee 100% security. However, effective tools are already available today to help companies limit the impact of cyber attacks.

Business operations can continue without interruption, attacks can be promptly thwarted and, in the case of a successful attack, all systems, files and data can be restored quickly. End-to-end business continuity also ensures there are no gray areas when it comes to compliance. Companies can take suitable measures so they are protected from prosecution and reputational damage in the event of a cyber attack.

Security Awareness focuses on people

Hornetsecurity already provides the most advanced solutions for e-mail security, back-up and compliance, covering all aspects of the IT security cycle from a technical point of view—from prevention to protection, response and recovery.

However, most cyber attacks still target human weaknesses, and even the most technically secure systems and tools are ultimately only as secure as the users that work with them.

The Security Awareness Service from Hornetsecurity integrates the human factor into a dedicated cyber security solution that actively fits into the IT security cycle. Continuous Security Awareness Training from Hornetsecurity systematically prepares employees for growing cyber risks. Over time, they learn how to recognize even the most sophisticated of phishing attacks and how to defend against them effectively. They master the necessary skills to prevent serious security incidents from happening in the first place, ensuring no interruptions in business operations.

Hornetsecurity also supports companies at the start of security awareness training to establish the necessary security mindset among their employees. This is the only way to ensure that the acquired skillset, in combination with accompanying processes and tools, can help to develop a proactive security culture that lasts.

Learn more!

HORNETSECURITY

References

1 Federal Criminal Police Office (BKA): Bundeslagebild Cybercrime 2021, May 2022

2 Hornetsecurity: Cyber Threat Report Edition 2021/2022, January 2022

3 Microsoft: Microsoft Digital Defense Report 2021, October 2021

4 Anjuli Franz and Evgheni Croitor, Darmstadt Technical University (TU): Who bites the Hook? Investigating Employees' Susceptibility to Phishing: A randomized Field Experiment, 2021

5 Daniel Kahneman: Thinking, Fast and Slow, 2012

6 bitkom: German business under attack: losses of more than 220 billion euros per year, 5 August 2021

7 Daniel Kahneman: Thinking, Fast and Slow, 2012

8 Wikipedia: Hermann Ebbinghaus

9 FIDO-Alliance: FIDO authentication. A passwordless vision

About Hornetsecurity Group

Hornetsecurity is a leading email cloud security and backup provider, securing businesses and organizations of of all sizes worldwide. Its award-winning product portfolio covers all major areas of email security, including spam including spam and virus filtering, phishing and ransomware protection, and legally compliant archiving and encryption. archiving and encryption. In addition, there is backup, replication and recovery of e-mails, endpoints and virtual machines. The flagship product is the market's most comprehensive cloud security solution for Microsoft 365. With over 450 employees at 12 locations, the company, which is headquartered in Hanover, Germany, has an international network of partners. Headquartered in Hanover, Germany, has an international network of more than 5,000 channel partners and MSPs, as well as 11 redundant, secure data centers. More than 50,000 customers use the premium services, including Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA and CLAAS.