sosafe

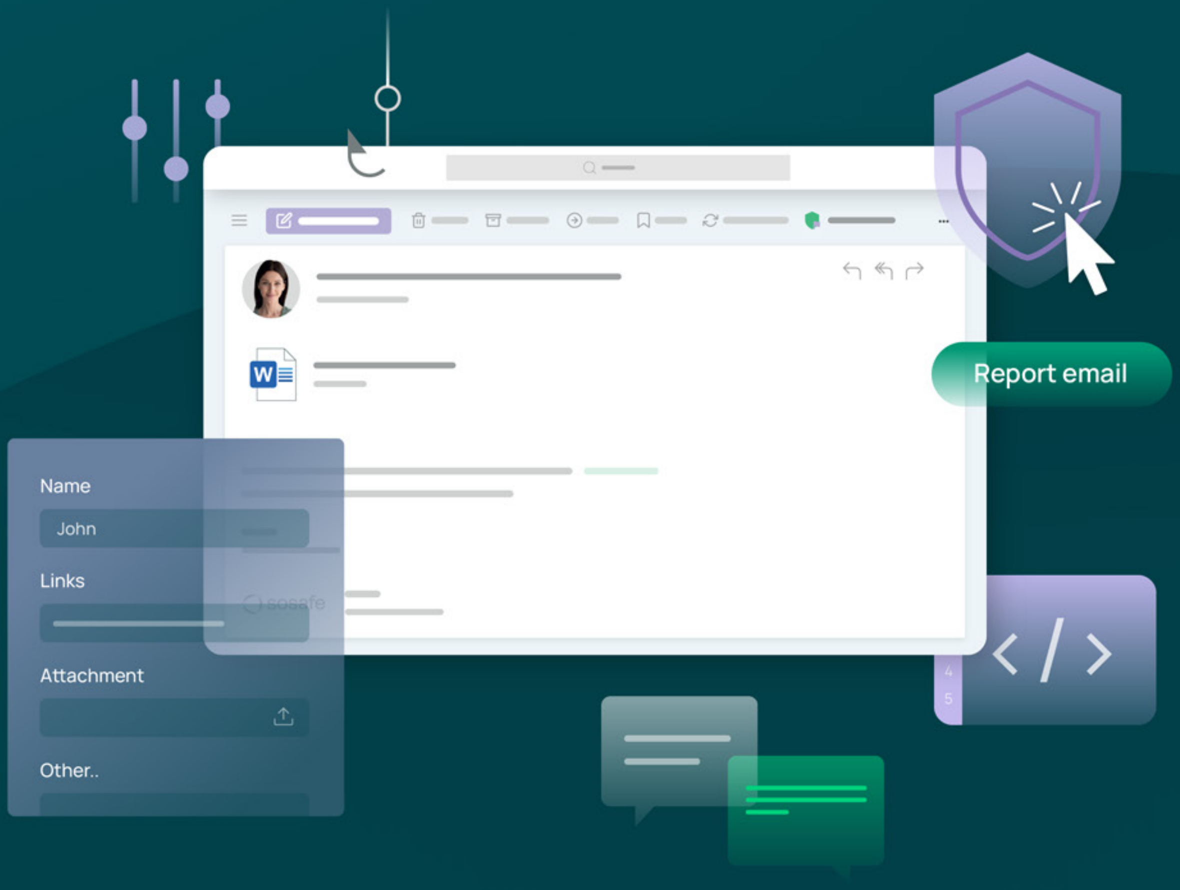
www.sosafe-awareness.com

GUIDE

Best Practices for Phishing Simulations

10 Dos and Don’ts for Sustainable Security Awareness in Your Organization

Including practical checklist!



Contents

Cyberattacks: The ever-growing danger from the web

The number, scope, and complexity of cyberattacks on individuals and organizations has continued to grow in recent years.

The Risk Barometer of Allianz insurance has for years ranked cybercrime as one of the greatest risks to businesses worldwide. According to estimates, the damages amount to billions of US dollars every year. After all, cyberattacks don't just harm organizations' reputation, but result in costly disruptions to business or demands for ransom following attacks with extortion software known as ransomware.

9 out of 10 cyberattacks start with the human factor, and phishing is still one of the most popular attack tactics by far. Complex social engineering methods like spear phishing and dynamite phishing are becoming more common in particular (see infobox on p. 7). Cybercriminals use psychological tactics and manipulate recipients' emotions in order to achieve their aims.

This is how the Trojan and "King of Malware" Emotet collected email histories via infected systems in order to automatically generate and disseminate further phishing emails, despite being temporarily suppressed in 2021. Most conventional spam filters cannot accurately identify the falsified, harmful email conversations. The phishing emails end up in employee inboxes, and this is where they begin to wreak havoc.

INFOBOX

Social engineering over time

Social engineering – the emotional manipulation of individuals in order to induce certain behaviors – is not new by any means. As early as the 17th century, criminals were using the "advance fee" scam of the "Spanish prisoner" to obtain considerable sums of money. The fraudsters send letters to wealthy persons, pretending to be stuck in a Spanish prison but aware of the location of a hidden treasure that will be disclosed upon the prisoner's release. The recipients issue a loan to the supposed prisoner to allow them to escape, so that they can ultimately acquire the treasure. Instead of treasure, however, they are met with the bitter realization that they have fallen victim to a clever scam.

The concept of social engineering has barely changed in all this time. The only difference is the vehicle: Letters have been replaced by emails, text messages, private messages on social networks, and phone calls. As the Internet became more popular, cybercriminals grew more aware of these methods in the 1990s. They have since used psychological manipulation in their phishing attacks to target human emotions for their own ends. The tactics are becoming ever more sophisticated, and with the increasing amount of data publicly available online, cybercriminals can make their attacks even more specific and deceive their victims more efficiently.

Humans as the deciding factor in the fight against phishing

Organizations should thus be particularly vigilant and teach their employees about the dangers lurking on the Internet. Trained and alert employees can react to cyber risks early, thereby preventing serious incidents in their company.

Various international compliance frameworks, such as ISO/IEC 27001 or the European General Data Protection Regulation (EU-GDPR), stipulate continuous training of employees on information security – as well as a form of simulated social engineering attacks in the case of ISO/IEC 27001. An increasing number of industry-specific regulations contain similar recommendations.

In order to achieve optimal learning success, organizations should thus not only consider training in the form of e-learning and interactive learning platforms. They can raise security awareness by combining these with behavioral training measures like phishing simulations, thereby effectively and sustainably reducing human risks in information security.

INFOBOX

Social engineering – The most popular tactics among cybercriminals

Phishing: Phishing is a scam in which the victim's personal information is "fished" from an email and misused for criminal purposes. The victim receives a message in which their trust is taken advantage of, whereupon they unknowingly provide access credentials to a third party. This scam is always malicious: The victims are supposed to suffer personal or financial consequences, while the cybercriminals are focusing on personal enrichment.

Vishing: Vishing (short for voice phishing) is a type of phishing via telephone in which the victim is tricked into disclosing personal information. This scam has become more prevalent at a time when hybrid work models are commonplace, because victims who are suspicious will have a harder time speaking with colleagues to verify the call.

Smishing: Smishing (short for SMS phishing) is a text message-based phishing tactic. The victims are usually asked to click on a link, but doing so results in infection with malware or spyware, and personal information is stolen.

Spear phishing: Spear phishing attacks, unlike "normal" phishing, target a very specific group of users that the criminals have acquired detailed information about in advance. This makes these attacks particularly dangerous, because this personal information makes the attacks seem highly legitimate. One of the most common types of spear phishing is CEO fraud, in which the cybercriminals pose as company executives, thereby allowing them to influence business processes.

Dynamite phishing: Dynamite phishing is a particularly dangerous type of spear phishing. The term was created as a result of the Emotet malware program, which secretly collects information about the victim's email history. The contents of the emails are accessed over a span of months. After a certain amount of time, other phishing emails can be created that are adapted to the victim's normal manner of communication and which are difficult for the recipients to recognize as forged. Unlike normal spear phishing, dynamite phishing emails are created automatically and sent out in bulk.

10 dos and don’ts for your phishing simulation

Phishing simulations are realistic imitations of cyberattacks that sensitize employees to the dangers of such attacks. In a phishing simulation, phishing emails are sent out that appear as if they are supposed to obtain sensitive information. For example, they contain fake attachments or links that lead to websites with falsified login screens. The only difference is that the simulated emails are not actually dangerous. The simulation makes employees aware of the dangers of phishing and helps them learn secure habits.

There is a pitfall to the implementation of phishing simulations, however. They have often been used purely as a testing tool in the past to identify which specific employees pose a “security risk”. Naturally, this leads to frustration among participants. Instead of categorizing employees as a risk to an organization’s information security, a phishing simulation should always operate on the opposite assumption: The individual should serve as an additional security barrier through their awareness of cyber risks and careful handling of dangers. The individual can then protect an organization against costly attacks.

With the following tips and best practices, you can effectively configure your phishing simulation, promote secure behavior among your employees, and establish a protective security culture at your company:

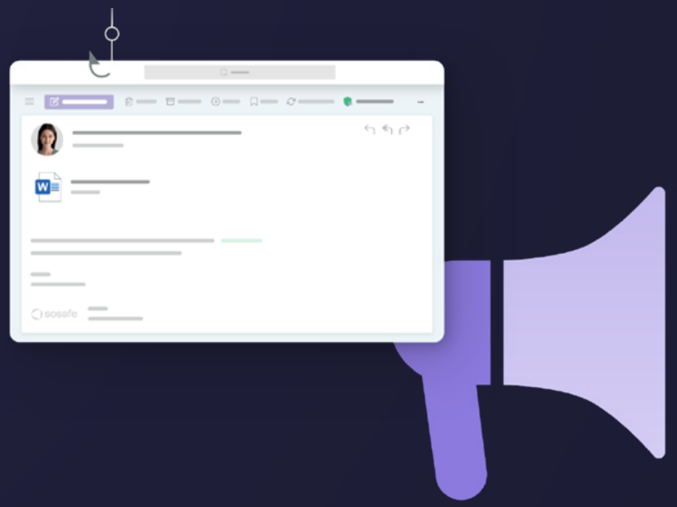
1.

Technical checks instead of live adjustments

Conventional technical filters cannot always recognize that a simulated phishing email is a harmless training measure. In order to ensure that the emails end up in employees' inboxes, your IT systems must be prepared for the phishing simulation. For example, the mail servers' IP address must be placed on the whitelist of the respective cyber security systems. Compile all the relevant information together with your simulation provider and adjust the respective systems accordingly. The service provider should prioritize data security and advise you on how to meet all the security standards for the whitelisting.

Instead of just starting the simulation, it should be continuously tested. By sending out test copies of select phishing emails that reflect the breadth of the simulation, you ensure that everything will function correctly when done live in the future. It is also worthwhile to get IT or your Helpdesk on board. Your colleagues in these departments can then take all the necessary precautions while also being ready to respond to any questions employees may have during the simulation. This is very helpful in facilitating a smooth, effective simulation.

2.



Announcing instead of surprising

Communication before, during, and after the simulation is the alpha and omega of any learning-oriented phishing simulation. The planning and execution should not only involve IT and Helpdesk, but also executive management and, if applicable, the Works Council and Human Resources department.

However, it is also crucial that the recipients are notified early on. There are a number of reasons for this, the first of which is that you prevent uncertainty. Present the simulation as a learning opportunity that imparts knowledge to your employees that they can also apply outside of work. Announcing the phishing simulation in advance also increases employees' motivation. If they are aware that the simulation leads to a stronger security culture and protects the organization against attacks, they will take a more active approach to the content.

Introduce the upcoming phishing simulation a few weeks before launch (e.g., in a circular email) and make it clear that this is a learning opportunity for the employees. Or you can set up the awareness measure as a "friendly competition" among coworkers.

The announcement could contain:

Context: Why are you conducting the simulation and what effects do you hope to achieve?

Scope: What can your employees expect? Give the participants an impression of the scope of the measure without disclosing how many emails there will be.

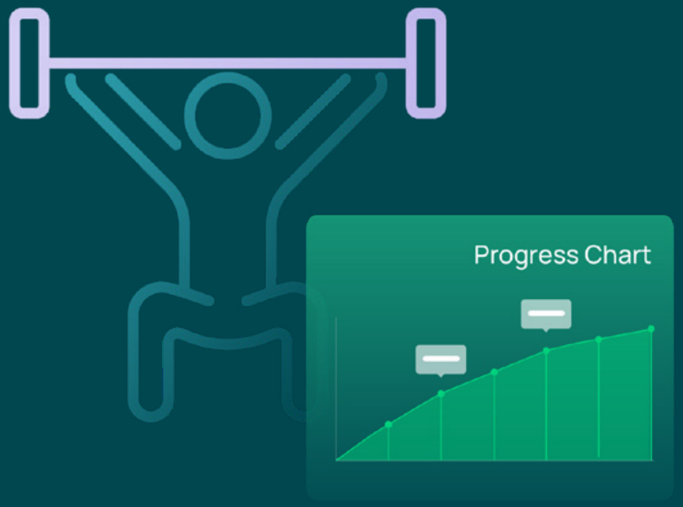
Start time: When will the simulation begin? Provide a time frame instead of a specific date.

Process: What will be the process of the simulation, and what is expected of employees?

Communication: Whom can employees contact with questions about the simulation?

Goal: Why should employees not view the simulation as a test, but rather as a learning opportunity?

3.



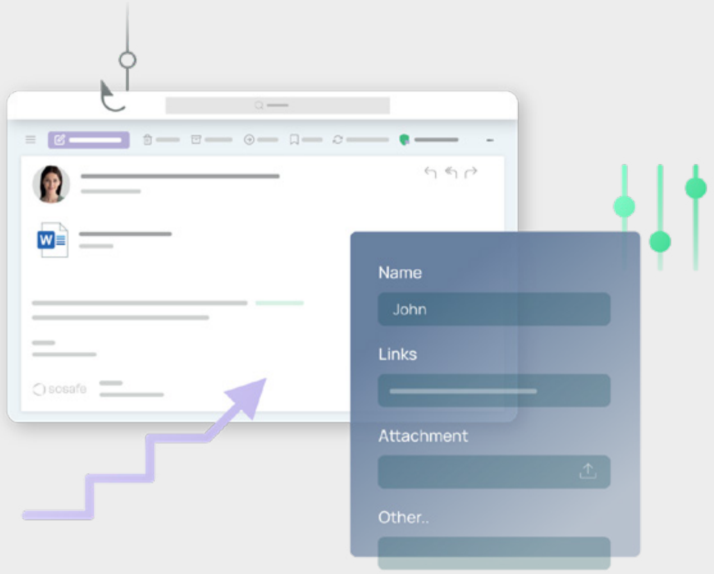
Training instead of testing

As a conventional penetration testing tool, phishing simulations frequently used to focus on identifying security gaps. Some of the simulations were thus person-specific, and employees were even sometimes confronted about their conduct or even faced individual consequences. However, placing blame has a negative impact on employees' willingness to learn and motivation.

It is more effective and sustainable if you conduct the simulations anonymously, i.e., without recording and processing data on individuals' behavior. It should be made clear to the users in the announcement of the simulation that the measure is not a test. The users should not feel like they are being monitored, but instead have the opportunity to undergo the phishing simulation at their respective learning pace and to the best of their ability. By making employees aware of their role as a "human firewall", you improve the effectiveness of the training measure.

In specific instances, organizations still opt for personal simulations, for example if they want or have to ensure that groups of individuals who work with particularly sensitive information are sufficiently trained. The behavioral data obtained from the simulation provide an overview of individuals' knowledge. In this case, however, you should ensure that this type of monitoring solely aims to improve employees' learning and is not intended to punish unsafe behavior. Use the data that you obtain to give your employees positive reinforcement as they learn and provide them with more or less learning content so that they can effectively prevent potential cyberattacks. Supplement the measure with frequent and transparent communication, thereby ensuring participants do not feel like they are being monitored.

4.



Individualization instead of generalization

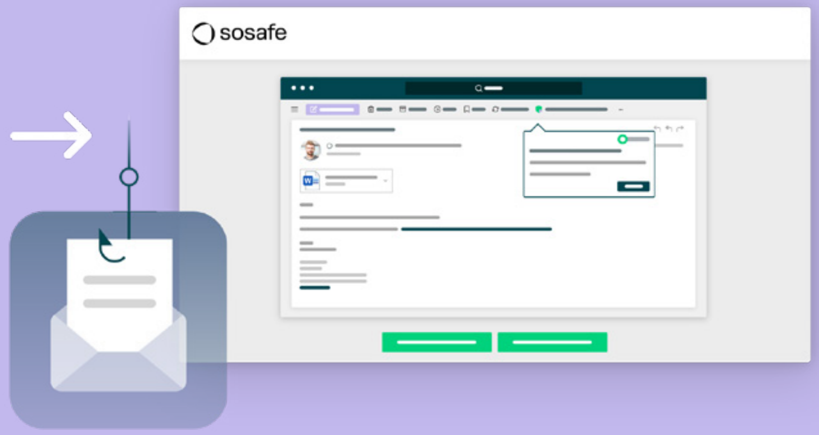
You should adapt the phishing simulation to employees' respective knowledge and needs so that they don't feel shamed. If all of the simulated phishing emails are too easily recognizable as such, user motivation is impaired. They feel ready for such attacks, even though they often utilize sophisticated psychological tactics. But simulation emails that are also difficult to detect also have a negative impact on user motivation. At worst, they feel deceived and entrapped – and this must be avoided.

Balance is key: Combine easy and challenging emails in the simulation so that users can regularly experience success. This also reflects the actual spectrum of phishing emails. You avoid user frustration, the statistics that you gain from the simulation reflect the actual risks of phishing, and the learning aspect is always in focus.

Tailor the contents of the phishing simulation to the specific recipients – similar to spear phishing. For example:

- → **Addressing by name**
- → **Company-specific email signatures**
- → **Topics relevant to the target group**
- → **Basing the message on known processes**
- → **Using particularly successful psychological schemes**
- → **Realistic design**
- → **Role and department affiliation**
- → **Linguistic aspects**

5.



Educational instead of daunting

Supplement the phishing simulation with matching learning content, such as in the form of e-learning. These should provide the users with information about everyday secure conduct. Ideally, the phishing emails themselves should be followed by learning content. If clicking on the simulated phishing email does not lead anywhere, the recipients might not know whether this is part of the simulation or an actual attack. IT Support must expect a greater influx of tickets, and the desired learning effect is hampered.

This also applies if a click merely leads to an info page that states that the respective email was a simulated phishing attempt. Instead, the phishing emails should be accompanied by explanatory learning content. For example, after clicking or interacting with the simulated email, users could be presented with short videos or walkthroughs that explain the deceptive aspects of the email. Instead of frightening employees, the learning content encourages them to be more careful next time, and they are taught to be more diligent.

6.

Chain of reporting instead of chaos

What is the best way to react if you receive a phishing email? Every minute counts in the event of a cyberattack, which is why your employees should be able to answer this question at any time. Before starting your simulation, establish a chain of reporting so that the recipients of the simulated phishing emails know what to do in the worst-case scenario. This chain of reporting should be as direct as possible, and also function outside of the simulation itself. This is because, according to ISO/IEC 27001, there should be a clearly defined and structured procedure if an emergency occurs.

It is recommended that users be instructed to immediately contact their company's IT department if they suspect anything. The following should also be made clear: better safe than sorry, and prevention is better than damage repair. With transparent communication, you can establish a security culture in your company before, during, and after the simulation, while assisting your employees in taking a diligent approach to cyber security risks. Reporting buttons integrated into the email program – e.g., as used on the SoSafe Platform – are an optimized form of such a chain of reporting.

There are many benefits to this:

- **An improved reporting rate.**
- **More efficient monitoring of ticket numbers, as simulated emails are not forwarded to the Helpdesk.**
- **Positive reinforcement for employees during the learning process via the Button.**

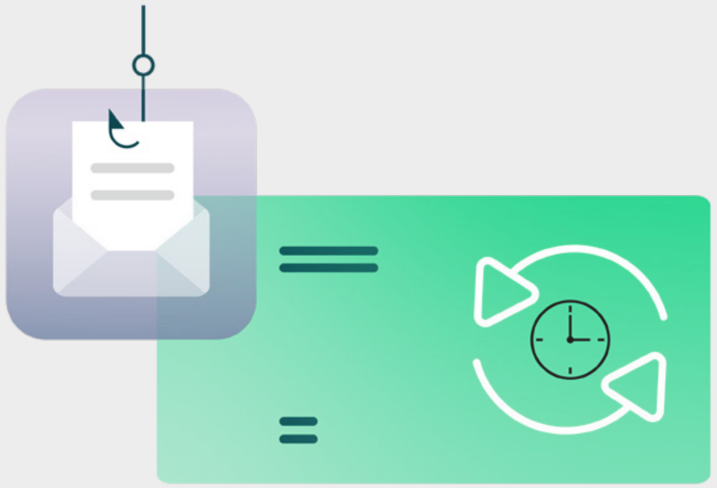
INFOBOX

Sustainably increased reporting rates with smart reporting

The first step toward a secure organization is ensuring that employees can accurately recognize phishing emails. However, in the worst-case scenario, it is more important that users react quickly so that IT can implement the appropriate measures and prevent potential attacks against other employees. The reporting rates in phishing simulations are one pertinent value for measurement in this regard.

Findings from the SoSafe Awareness Platform have shown that the Phishing Report Button considerably increases reporting rates. Direct integration into the organization's email program is supposed to make it easier for employees to easily report dangerous emails to IT. On average, each employee reports one out of every two phishing emails directly via the Button.

7.



Continuous instead of sporadic

A phishing simulation should always be operated on a continuous basis, because this is the only way that learning success can be achieved sustainably and for the long term. Findings from habit research have shown that learning measures spread out over a larger period of time are more successful than sporadic measures at promoting secure behavior. As a result, the users' cyber security awareness is continuously trained via recurring nudges through the phishing simulation throughout the day. This nudging encourages constant preoccupation with the topic of phishing.

INFOBOX

Distributed learning as a key to learning success

It has been known since the mid-20th century that continuous learning levels out the forgetting curve. Data from the SoSafe Awareness Platform also show that click rates for phishing emails increase by almost one third after a short time if employees do not regularly interact with the learning content.

In order to impart knowledge about cyber security, organizations should thus utilize approaches rooted in educational psychology. Highly modularized training and frequent nudges that encourage learning can flatten the forgetting curve, thereby minimizing human risks in the long term. Results from the SoSafe Awareness Platform show that nudging continuously increases the engagement rate by 30 percent, and even up to 90 percent in the introductory phase. This lets employees learn effectively and sustainably.

8.

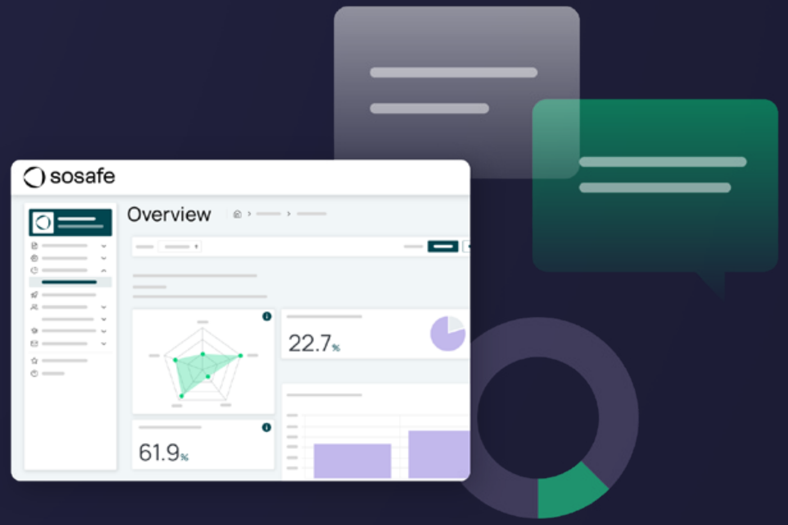
Randomized instead of synchronized

Randomization of the simulated phishing emails is also linked to the simulation's success. If all the recipients are sent an identical simulation email at the same time, news might spread quickly. If the simulated phishing emails are sent in a randomized manner, oversaturation is far less common. But the users are not the only group to benefit from this approach – you can as well:

The KPIs are always meaningful in real time. With sporadic campaigns, the click or reporting rates often correlate heavily with the difficulty of the respective email. The randomization of a large number of emails and the simultaneous sending thereof make it possible to equally present the respective email types in the KPIs at all times. As a result, figures can be continuously analyzed, and the measure's effectiveness can be demonstrated.

The number of tickets is minimized. Instead of sending out the simulated emails to all employees at specific times, thereby initiating the chain of reporting, randomization spreads the workload for IT across the entire simulation period.

9.



Giving feedback instead of moving on

As illustrated by the preceding sections, early communication of the course and goals of the phishing simulation are integral to the method. However, it is also important that users receive progress reports. This helps the employees estimate their own performance, and they are reminded of what they have learned. Even if specific scenarios cannot be addressed, as this would create anticipation, you should provide meaningful feedback. For example:

→ **Which psychological tricks do employees fall for most frequently?**

→ **Which KPIs are particularly high or low, and what does this mean for the employees and the handling of risks?**

→ **How successful have you been at reducing risks in your organization with the phishing simulation?**

The findings should be formulated in a comprehensible way. Technical and scientific KPIs do not mean very much to most employees, whereas click rates and interaction rates are easier to understand. Here, too, you can emphasize the learning aspect. Provide positive instead of negative feedback and focus on values that reflect employees' learning success. Many providers offer suggestions that help you communicate success to your employees.

10.

GDPR-compliant instead of legally questionable

Interview: Data protection in phishing simulations: GDPR, Privacy Shield, and others.
Interview with Benedikt Woltering, attorney and Legal Advisor at SoSafe

Are phishing simulations safe from a data protection perspective?

Data protection is relevant to phishing simulations, of course, as they usually involve the processing of personal information. For example, many providers supplement the simulated phishing emails with other employees' personal information in order to reflect what real hacking attacks look like. If this information is used within reasonable bounds and "solely for purposes relating to employment" (§ 26 BDSG) - e.g., to improve cyber security – the simulations are safe with regard to data protection regulations.

What does a GDPR-compliant phishing simulation look like?

The GDPR stipulates absolute protection of employee information. Phishing simulations become more realistic the more information that they contain, but this is a slippery slope into a legal gray area. For example, to what extent is the use of this information solely for purposes of employment and improved cyber security? A balance in this regard is necessary, and invasive methods like social media crawling must be avoided. At the same time, the users should not have to be concerned about direct consequences. This is why phishing simulations should be evaluated anonymously, and no personal inspections should be conducted. Furthermore, companies should utilize providers who exclusively process data within the European Union.

Why is it so important to select a provider from the EU?

The misconception persists that processing data on a dedicated EU cloud is sufficient. Yet many legal entities, for example in the USA, can compel the local authorities to disclose data at any time. This automatically results in a compliance issue, especially with sensitive behavioral data obtained for phishing simulations, for example. The solution is as simple as it is logical: Opt for a service provider that only has business entities in the European Union, and whose servers are also located in the EU.

Summary

Sustainably minimizing human risks with phishing simulations

Systematically planned and conducted phishing simulations increase awareness of cyber security in the long term and strengthen organizations against cyberattacks. The human factor and humans' need to learn should always be the primary focus. As the best practices listed previously illustrate, organizations should take precautions on a variety of levels.

Cross off these best practices and establish a strong security culture in your organization so that you can effectively protect yourself against the increasing number of cyber risks in the long run.

Checklist

Learning-oriented phishing simulations

□ I have laid the technical groundwork for the phishing simulation, updated whitelists, and sufficiently tested that the simulation emails are received and properly displayed.

□ All employees are aware that they will undergo a phishing simulation and that it aims to raise their awareness.

□ I have ensured that the phishing simulation will not be used to shame employees, but instead will motivate them to learn.

□ The simulation emails are individually adapted to the recipients and their respective context (e.g., department).

□ In addition to the phishing simulation, the employees receive learning content that expands their knowledge and teaches them about safe conduct.

□ The employees are aware of whom to report potentially dangerous emails to and how so that IT can act quickly.

□ I have planned the simulation out in the long term so that the learning success and risk minimization can be continuously ensured.

□ The dispatch of the phishing emails is randomized so that saturation does not occur.

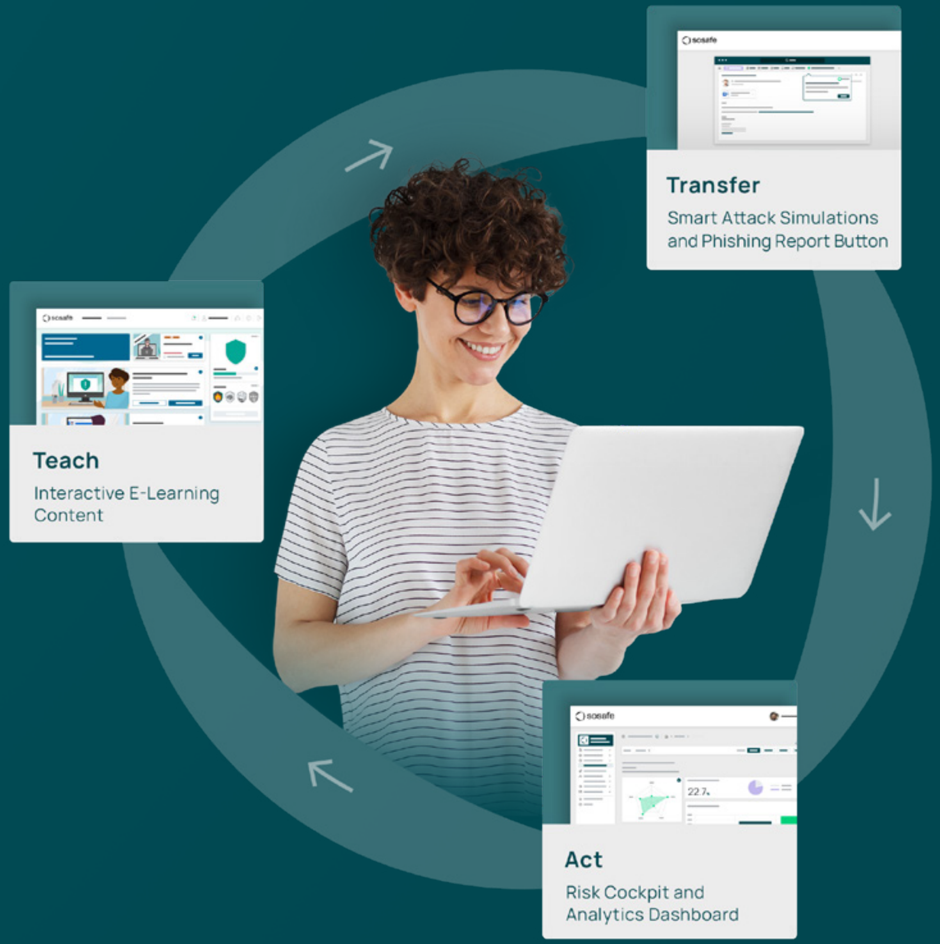
□ I regularly communicate with the employees and share results from the simulation so that they can be motivated through feedback.

Have you checked off all the boxes?
Then there's nothing stopping you from strengthening your security culture with a phishing simulation.

About SoSafe

SoSafe empowers organizations to scale agile awareness programs that build a security culture and minimize cyber risks. Employees receive smart attack simulations and personalized micro-learning experiences within their daily work environment. Our dynamic upskilling platform fuses behavioral science, smart algorithms, and a human-centered approach to empower every employee to be part of their organization's human firewall.

Beyond building secure habits among employees, you can understand exactly where vulnerabilities lie with contextual data, proactively respond, and measure the ROI of your awareness programs. The SoSafe difference is how easy it is to deploy, manage, and scale our GDPR compliant solution, saving you time and resources.


Transfer
Smart Attack Simulations and Phishing Report Button
Teach
Interactive E-Learning Content
Act
Risk Cockpit and Analytics Dashboard

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800

Disclaimer: Every effort has been made to ensure that the contents of this document are correct. However, we do not accept any liability for the content's accuracy, completeness and currency. SoSafe in particular does not assume any liability for any damages or consequences resulting from direct or indirect use.