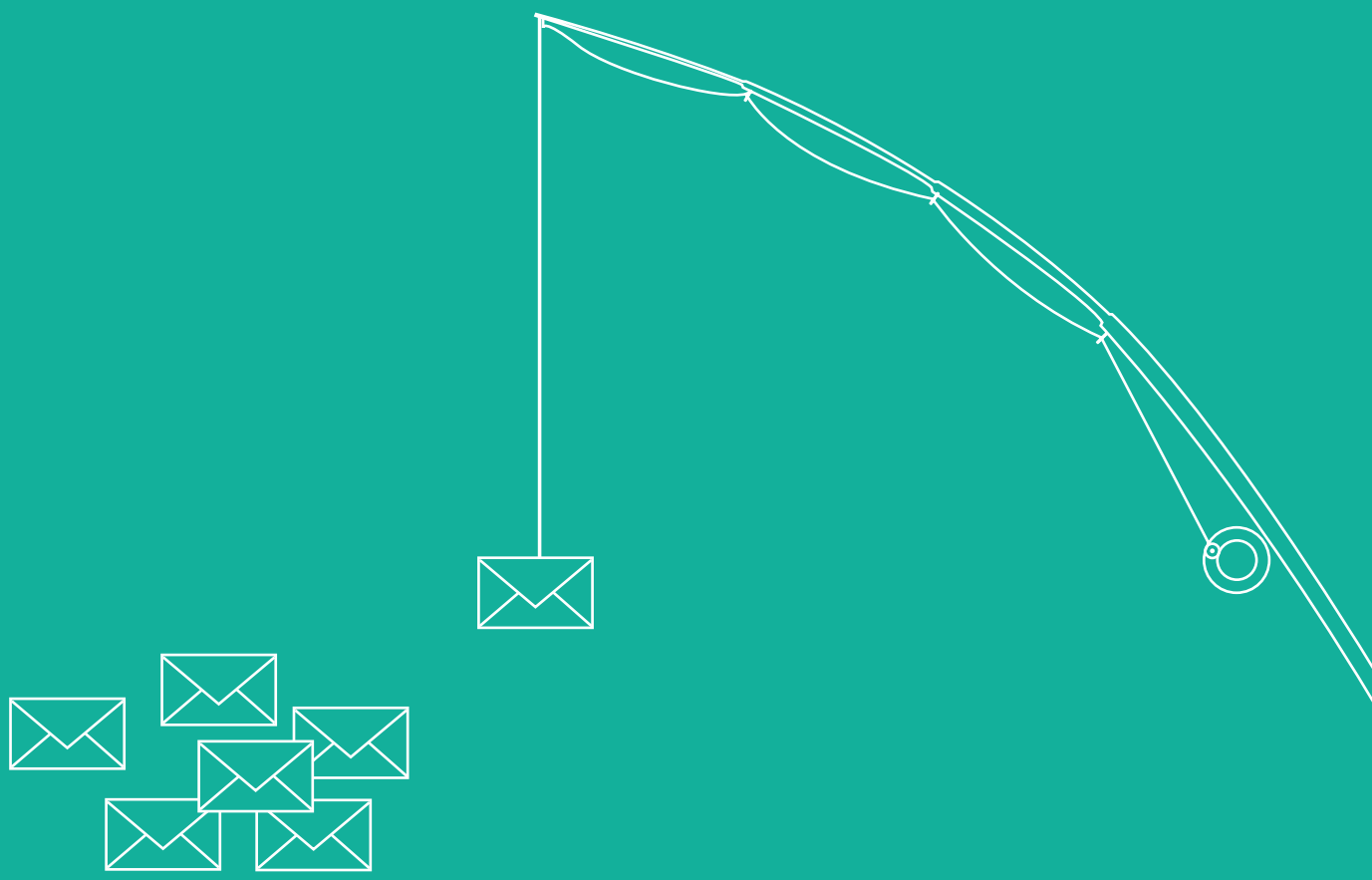


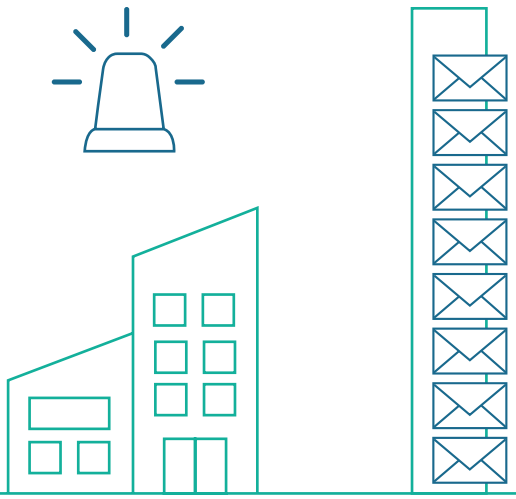
Best Practices: Phishing Simulations

Dos and don’ts for sustainable awareness building in organizations

SoSafe
Cyber Security Awareness

Table of Contents

Why organizations should sensitize their employees to phishing attacks



Over 90% of attacks on organizations begin with a phishing email.

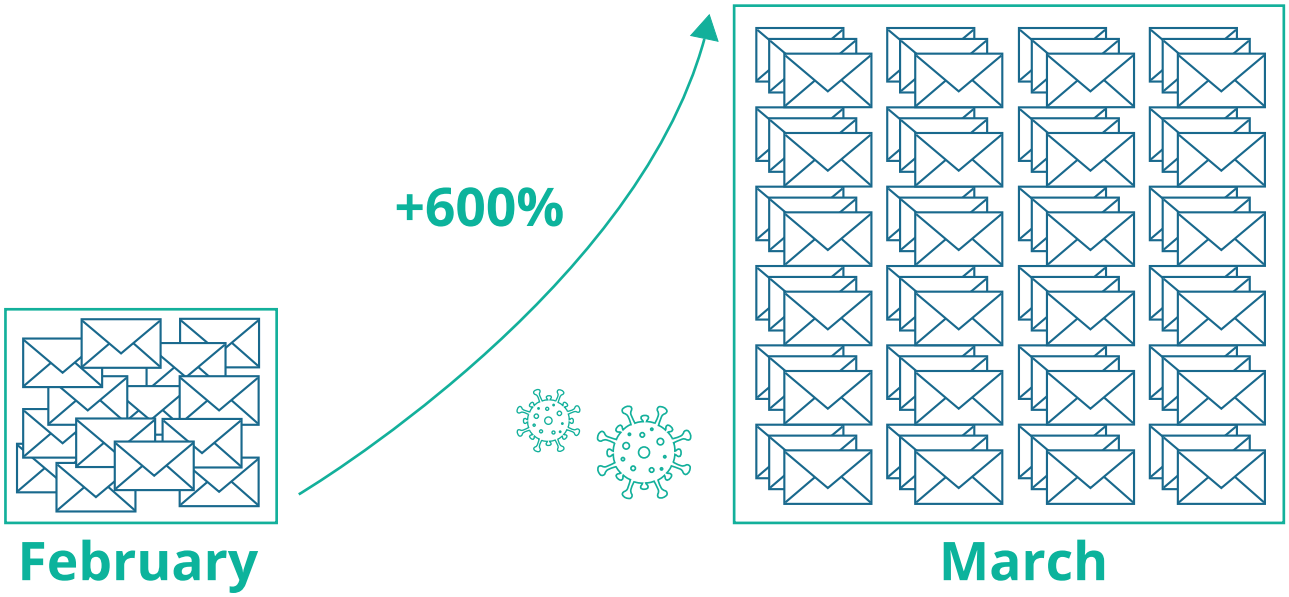
The number of cyberattacks on both individuals and organizations has increased steadily in recent years, with Interpol projecting a further upwards trend in a current report.[1] We will have to expect record-breaking losses caused by cyber incidents. According to a 2018 Accenture study on the cost of cybercrime, the cumulative value at risk from 2019 to 2023 amounts to about 5.2 trillion US dollars globally.[2] One of the reasons for this large sum: Many organizations are not yet sufficiently prepared to ward off the diverse dangers.

Phishing continues to be one of the most pervasive and most popular attack tactics used by cybercriminals. Over 90% of attacks on organizations begin with a phishing email.[3] As a reaction to the coronavirus crisis, the number of phishing emails additionally rose by almost 600% between February and March 2020 alone.[4] Similarly, Interpol was able to detect more than 1 million spam messages, 737 incidents related to malware and over 48,000 malicious URLs in just four months (January to April 2020) – all related to the COVID-19 pandemic. The hackers take advantage of the uncertainty in the economy for their own purposes – without taboos or limits.

Organizations are particularly vulnerable: they are to expect serious economic damage if they fall victim to cybercriminals. They might have to temporarily interrupt their business or pay high ransoms in the case of a phishing attack. In the Allianz Risk Barometer 2020, for the first time ever, organizations around the world rate cyber incidents as the greatest risk to their business.[5] Taking into consideration that cybercrime and phishing, in particular, has been and will be further propelled by the current developments around the coronavirus, it is likely to remain a major factor impacting business in the future that needs our attention now more than ever.

[1] Interpol (2020). INTERPOL report shows alarming rate of cyberattacks during covid-19
[2] Accenture (2019) The cost of cybercrime
[3] Verizon (2020). Data Breach Investigation Report 2020.
[4] The European Union Agency for Cybersecurity (ENISA) (2020). Understanding and dealing with phishing during the covid-19 pandemic.
[5] Allianz (2020). Allianz Risk Barometer 2020: Cyber steigt zum weltweiten Top-Risiko für Unternehmen auf.

As a reaction to the coronavirus crisis, the number of phishing emails additionally rose by almost 600% between February and March 2020 alone.



Spam filters alone are only half the battle

Although technical barriers such as spam filters and antivirus programs already retain some of the harmful emails and malware, with 'spear phishing' ,(see infobox p.5) gaining popularity they are no longer sufficient to reliably protect against cyberattacks.

According to Avanan's Global Phish Report 2019, a quarter of all phishing emails still manages to get through Microsoft's Advanced Threat Protection Filter and ends up in users' mailboxes.[6]

In addition, hacking attacks become increasingly sophisticated and complex attacks such as 'dynamite phishing' more common. In recent years, the Trojan Emotet, for example, has used infected systems to collect existing mail histories to automatically generate and distribute further realistic phishing mails based on the data. Most spam filters are not able to process such an approach and fail in identifying the respective attacks.

[6] Avanan (2020). 2019 Global Phish Report.

Spear phishing and social media crawling

In the case of spear phishing, cybercriminals deliberately deceive their victims with the intention of causing financial or personal damage. In comparison to 'normal' phishing, spear phishing attacks are targeted at a narrowly defined user group about which the perpetrators have precisely informed themselves in advance.

One of the best-known forms of spear phishing is CEO fraud in which hackers impersonate CEOs or other employees in leading positions and use their pretended authority to influence business processes. In the case of automotive supplier Leoni, the cyber criminals were able to capture almost 40 million euros.[7] The criminals find useful information from many sources - from social media profiles and professional networks to company websites and even personal conversations at trade fairs or with suppliers and clients. One should therefore always be cautious when sharing internal company information as well as private information on the Internet.

Considering that this tactic is used increasingly frequently, phishing simulations should of course also depict spear phishing attacks. However, organizations should be careful when enriching the simulated phishing mails with social media data or other individual employee data. While the simulation may reflect phishing a little more realistically by using such data, the use and enrichment of personal data (even if it is accessible in public space) is highly problematic from a data protection perspective. If employees have not given you their consent, the use of the data is not explicitly permitted according to GDPR. This applies to all companies with employees or customers in the European Union. (see interview infobox p. 14)

[7] Handelsblatt (2017). Betrugsmasche „CEO Fraud“: Abgezockt vom falschen Chef.

The human factor in IT security

For organizations, it is therefore essential to be particularly vigilant and to continuously sensitize employees to dangers from the Internet. Cybercriminals frequently use psychological tactics targeted specifically on employees and manipulate the emotions of the recipients to achieve their goals. In the case of social engineering (see info box p. 7), for example, the hackers rely on creating pressure, arousing curiosity or triggering fear so that the recipients of phishing emails interact with them and disclose their data.

Trained employees who know how to consciously deal with such cybersecurity risks can react early on and thus ward off serious incidents in the organization. This is one of the reasons why various compliance frameworks, such as ISO 27001 or the GDPR, demand continuous training of employees in IT security topics - in the case of ISO 27001 also a form of simulated social engineering attacks.

In addition to information campaigns on cybersecurity as well as training employees, for example in the form of digital and interactive learning platforms, phishing simulations are well suited to sustainably build awareness in organizations.

Cybercriminals frequently use psychological tactics targeted specifically on employees and manipulate the emotions of the recipients to achieve their goals.

A brief history of social engineering

Social Engineering – emotionally manipulating people to induce certain behaviors - is far from being a new phenomenon. As early as the 17th century, fraudsters captured large sums of money with the 'advance fee' scam of the 'spanish prisoner'. They pretended to serve time in a Spanish prison and sent letters to wealthy people claiming that they knew the location of a buried treasure which they would only reveal upon their redemption. The receivers finally lent the alleged prisoners money to enable them to buy themselves out of prison and to get hold of the treasure with their help. Instead of a treasure, however, they soon had to realize that they had fallen victim to an elaborate fraud.

The principle of social engineering has hardly changed to this day, only the channels are different ones - emails, text messages, private messages in social networks and telephone calls replace the letters of the past. With the popularization of the Internet, cybercriminals became aware of the methodology in the 90s. Since then, they have been using phishing as a way of exploiting human emotions and manipulating them psychologically to achieve their goals.

The tactics are more sophisticated than ever: with the increasing amount of data that is publicly available on the Internet, hackers can attack and deceive their victims in a more and more purposeful manner.

Phishing simulation: Test for the case of emergency

In the course of phishing simulations, cyberattacks are imitated in order to sensitize employees to the dangers of such attacks. There are, however, some pitfalls to be aware of when implementing these simulations. In the past, they were often merely used as a testing tool to determine which employees pose a ‘security risk‘ on an individual basis.

Such a procedure understandably frustrates the recipients - not only, but especially when those emails end up in their inboxes without prior notice. This misses the actual purpose of the simulation as a teaching and learning tool. The recipients feel embarrassed and lose interest in genuine phishing prevention.

Therefore, phishing simulations should rather focus on the aspect of learning. To ensure this, the simulation has to be communicated transparently in advance and be accompanied by learning units. Immediately after clicking on a simulated phishing email, employees should receive an explanation on how they could have recognized the attack, for example by being guided through the corresponding email. Like this, they get to know diverse phishing tactics, all without taking a real security risk.

This increases the recipients‘ awareness of such cybersecurity risks and they are enabled to act responsibly in the event of an actual attack. So instead of classifying employees as a risk to an organization’s IT security, a phishing simulation should be driven by the opposite assumption: By being aware of security risks and by dealing with them adequately, humans can represent an additional, security-relevant barrier.

Instead of classifying employees as a risk to an organization’s IT security, a phishing simulation should be driven by the opposite assumption: By being aware of security risks and by dealing with them adequately, humans can represent an additional, security-relevant barrier.

Advisable for EU and non-EU organizations: GDPR compliant phishing simulations

You do not get around discussing data protection issues when designing a phishing simulation that focuses upon employees and their security awareness. That is because employee data will inevitably be processed in the course of the measure. Generally speaking, participants are of course happier the less invasive data collection and processing procedures are. Oftentimes, they will feel controlled or even deceived if personal data is used in the simulation without their consent. That is why you should opt for providers that make data protection a priority.

Regardless of the dramatic effects data privacy might have on the employees' acceptance and motivation, processing too much data might also have legal consequences. The GDPR calls for fully protecting personal data of data subjects in the European Union. What should not go unnoticed: These regulations are also relevant to non-EU organizations if the 'targeting'-criterion applies, i.e. when they offer services to people in the EU or monitor their behavior for this purpose – both of which might be the case with phishing simulations.

Organizations active in the EU face another problem: The GDPR only allows for the processing of data in countries that have regulations with a similar degree of protection to that of the GDPR. Since the Privacy Shield has been annulled, collaborating with companies whose servers are based in the US is a gray area, for example. Consulting EU-based providers is the safer choice for all organizations that want to bypass legal conflicts since they can guarantee full compliance with GDPR and do not need to worry about objections by employees or even about being fined. Data privacy helps making all stakeholders happy. (see interview on p. 14 for more information)

Best Practices Phishing Simulations

Despite their controversial use in the past, phishing simulations are popular tools to increase the cyber security awareness of employees in a modern way. When planned systematically and focused on the employees' learning success, they can sustainably reduce click and interaction rates with phishing emails and thus protect organizations from serious (financial) damage.

However, it is important to remove the mentioned obstacles so that a simulation can achieve the desired effect. The following tips will help you design your phishing simulation effectively and establish a protective security culture in your organization.

1 Setting the technical course for the phishing simulation

In a phishing simulation, your organization distributes phishing mails that mirror real hacker attacks aiming at intercepting user data. The emails might contain fake attachments or links that lead to websites with fake login masks.

The only difference is that the simulated mails do not pose a security risk, of course. Conventional technical filters may, however, not be able to recognize that a simulated phishing email is a harmless training measure.

To ensure that the messages end up in the recipients' mailboxes, it is therefore inevitable to prepare IT systems for the phishing simulation. For example, the IP address of the mail servers used must be included in the whitelist of the corresponding IT security systems. Consult with your simulation provider to gather all relevant information for the phishing simulation and identify the systems that need adapting. The service provider itself should also make data security (according to the GDPR) a priority and advise you individually on how to comply with all security standards during the whitelisting.

By sending test mails which reflect the whole spectrum of those mails included in the simulation, you can then ensure that they actually arrive and that they are displayed correctly. Especially when technically preparing a phishing simulation it is worthwhile - if the campaign is not controlled by the department anyway - to get IT and the helpdesk on board. As the first point of contact for cybersecurity issues, the colleagues can not only take the appropriate precautions, but are also prepared for any queries from employees during the simulation. This significantly contributes to a stable and effective process.

2 Announcing the phishing simulation

The most important thing in any learning-oriented phishing simulation is communication - before, during and after the measure.

Not only IT and the works council should be involved in the planning and implementation, but the recipients of the simulated phishing mails must also be informed early on. This makes sense in several respects: On the one hand, it helps to avoid insecurity or upset. The simulation is introduced as a learning measure that provides employees with knowledge that they can also use in a private context.

On the other hand, announcing the phishing simulation early on can motivate the employees. If they are aware that the simulation helps to improve the security culture and to protect themselves and the company against security-related attacks, they are more willing to deal with the learning content. Therefore, you should present the upcoming phishing simulation a few weeks before the start, for example in a newsletter, and emphasize the fact that the employees can learn from it.

Consider mentioning the following aspects:

- The simulation as a training and learning opportunity
- Scope and time frame of the simulation
- How the simulation is carried out
- Anonymity of the simulation (see section 3)
- Contact person for questions regarding simulation

Data from SoSafe simulations shows that such an announcement about two to three weeks before the start of the simulation does not significantly bias the collected data - for example click and interaction rates. Yet, you should not mention an exact start date. This could give the impression that the employees only need to be cautious from that date onwards. As current statistics on phishing make clear, however, it is more important than ever to always be aware of the risk of a potential attack.

---

3 Emphasizing the anonymity and learning aspect of the phishing simulation

As a tool of classical penetration testing, phishing simulations in the past have often focused on identifying security gaps.

As a tool of classical penetration testing, phishing simulations in the past have often focused on identifying security gaps. The simulations were therefore sometimes carried out on a person-specific level, employees were confronted with their behavior or even dismissed.

Finger-pointing, however, has a negative effect on the employees' willingness to learn as well as on their motivation. It is therefore more sustainable and effective to conduct simulations anonymously, i.e. without collecting and processing individual behavioral data. Users should not feel monitored but should have the opportunity to complete the phishing simulation at their own pace and to the best of their ability.

Underline and communicate that the simulation is not the same as a test. Rather, it is a way to protect individual employees and the organization from harmful cyber incidents. By making employees aware of their role as a 'human firewall', you can increase the effectiveness of training.

To avoid exposing individual employees, it is also important to adapt the phishing simulation to the knowledge and requirements of the user base.

If all simulated phishing mails are too easily recognized as such, the users' motivation will inevitably decline. They will feel prepared for real attacks, even though these are often based on sophisticated psychological tactics and purposefully deceive victims. However, simulations that exclusively use mails which are difficult to detect have a negative effect on the motivation of the users, as well. In the worst case, they will feel betrayed and trapped - this has to be avoided by all means.

Underline and communicate that the simulation is not the same as a test. Rather, it is a way to protect individual employees and the organization from harmful cyber incidents.

Balance is key here: mix easy and challenging emails to regularly give users a sense of achievement. This also reflects the real phishing spectrum - not all phishing mails are necessarily spear-phishing attacks, and not all phishing mails are designed generically. By offering a balanced and well-rounded simulation, you are able to avoid frustration, the statistics realistically reflect genuine phishing attacks and the learning aspect remains the focus of the measure.

Interview:
Data protection for phishing simulations

Interview with Benedikt Woltering, lawyer and legal advisor at SoSafe GmbH

Are phishing simulations harmless from a data protection perspective?

Yes and no. Basically, phishing simulations are of course a data protection issue, because you usually process personal data in the course of the measure. Many providers enrich the simulated phishing mails with employee data, for example, to realistically reflect real cyber attacks. If this data is only used to an appropriate extent and for the purpose of performing the employment contract - for example, to strengthen IT security - the simulations are harmless from a data protection perspective.

What does a GDPR compliant phishing simulation look like?

According to the GDPR, employee data must be protected in any case. Phishing simulations become more realistic the more data you integrate, but you quickly enter a legal gray area. To what extent does the use of data still serve the purpose of employment contract performance and increased IT security? It is important to only use a reasonable extent of data and to avoid invasive procedures for employees such as social media crawling.

At the same time, users should not have to fear any direct consequences. I would clearly recommend: Evaluate phishing simulations anonymously and do not carry out person-specific checks. In addition, organizations should rely on providers from the EU.

Why should companies which are not based in the European Union care about GDPR?

Even if a company is not based in the EU, as long as it offers services to EU customers, it is obliged to comply with the data protection regulations. That means it will have to stick to procedures that are permissible in terms of GDPR when starting a phishing simulation or, elsewise, it might have to expect legal consequences. Choosing providers from the EU is therefore the better choice since they will automatically adjust their processes to align with GDPR and the protection of individual user data, meaning you are on the safe side and fulfil all GDPR compliance regulations.

4 Adapting the phishing simulation to the users

For phishing simulations to be effective, they should ideally be tailored to the group of recipients.

This includes both adapting them to individual recipients (e.g. personal salutation) and to the staff as a whole (e.g. use of company-specific email signatures). You might consider the following questions:

- Which topics are currently particularly relevant to the organization?
- Which processes and current events could be picked up by real attackers?
- Are there special scams that might work particularly well for certain functions in the organization, such as the human resources or sales department? Executives are also often targeted (see info box p.5).

Graphic aspects can also play a role:

- Do you want to imitate the corporate design of your or another organization in the phishing mails?
- Should fake signatures be used?

Cyber criminals often use data from public sources or gather internal information in order to target employees. Consult with your provider and use your knowledge of the users to mimic this behavior and create appropriate simulations.

In addition to adjusting the level of difficulty, it should also be possible to include the function of the recipient in a simulated phishing email or to adjust the language of the emails to ensure a smooth simulation. Users will then be more likely to click. It is also important to adapt the emails thematically. Topics and contexts should be mixed: Emails supposedly from internal colleagues and external partners, from the business and private environment.

After all, phishing emails appear in the most diverse situations. The criminals often take up current social topics (source: Interpol). The simulation should mirror this variance so that the recipients can learn and react accordingly in the case of harmful emails.

[8] Interpol (2020). INTERPOL report shows alarming rate of cyberattacks during covid-19

5 Supplementing the phishing simulation with learning content

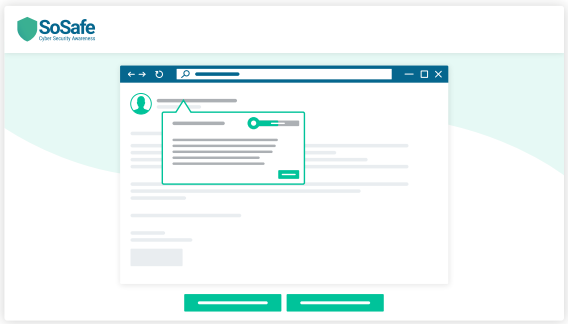
A phishing simulation familiarizes users with typical phishing scenarios, but the method is only effective as a training measure if it is accompanied by suitable learning content.

To increase the learning success, you can offer additional e-learnings, for example. Here, users are made aware of the hackers' intentions, how phishing mails work and how they can recognize them.

At the same time, learning content should ideally separately follow the simulated phishing mails. If a click on the simulated phishing email does not lead anywhere, the recipients may not know whether it is part of the simulation or a real attack. In that case, IT support must expect an increased ticket volume and the desired learning effect is lost.[8]

The same applies if the click merely leads to an information page explaining that it was a simulated phishing email. Instead, the phishing mails should be accompanied by educational content. For example, a click or interaction can be followed by short videos or a walk through the fake phishing email to explain the deceptive elements that were successful in the case. Instead of scaring off the recipients, the learning content encourages them to be more careful next time and thus trains their attention.

Learning pages on the SoSafe awareness platform encourage caution and deepen the knowledge.



6 Establishing a reporting chain

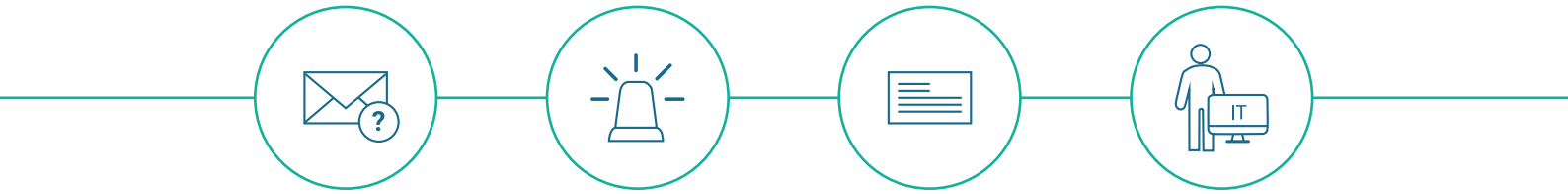
What is the best way for users to react when they identify a fake phishing email as such?

Establish a reporting chain before you start your simulation so that the recipients of the fake phishing mails know what to do in the case of an incident. This reporting chain should be as immediate as possible and, of course, it should also work beyond the simulation. After all, according to ISO guidelines, there should be a clearly defined and structured process in the case of an incident. It is, therefore, always a good idea to let users know that they should contact your organization's IT support immediately if they encounter any suspicious emails. They should not hesitate: Better safe than sorry. Establish a security culture in your organization by communicating transparently before, during and after the simulation and encourage the employees to deal consciously with IT security risks.

An optimized form of such a reporting chain are report buttons integrated into the mail program, as used on the SoSafe platform. Such a plug-in has numerous advantages:

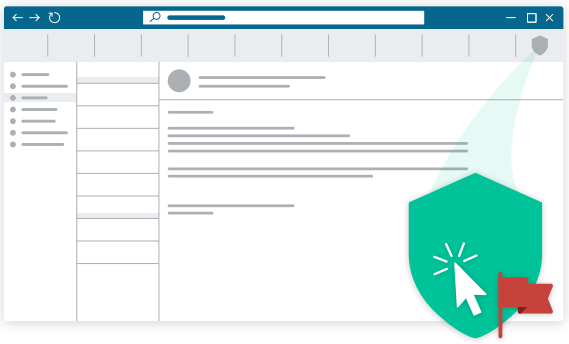
- Statistics and key figures, such as the reporting rate, are improved.
- The ticket volume can be better controlled because simulated emails are not forwarded to the helpdesk.
- The employees are positively encouraged during the learning process by the button.

In any case, it is important that employees always know what to do as soon as they find a suspicious email in their inbox - especially if it is not just a simulated phishing email.



Establish a reporting chain before you start your simulation so that the recipients of the fake phishing mails know what to do in the case of an incident.

The SoSafe phishing button: A controlled reporting function increasing the reporting rate.



Case Study

dormakaba

With more than 16,000 employees in over 130 countries, the dormakaba group is one of the world market leaders in access and security solutions. Naturally, the Swiss organization has equally high standards when it comes to cyber security. 'We were looking for a sensitization solution against phishing attacks with which we could reach all employees - with specific content included,' says Oliver Severin, Deputy Vice President IT Governance.

SoSafe's team of experts - consisting of security specialists, psychologists and educationalists - created phishing attacks with associated learning pages adapted to the organization's needs. Not only the latest attack scenarios 'from the wild' were considered, but also possible future attacks. 'I was surprised how lean the process was. The SoSafe team took most of the steps off our hands and provided us with optimum support during the implementation,' reports Christoph Bergs, Global IT Communication & Training Manager at dormakaba.

After a short baselining phase to collect robust KPIs, the majority of the emails were played out according to a randomized pattern throughout the year. Shortly after the initial phase, substantial learning effects were already achieved and proven - the reporting dashboard of the SoSafe Enterprise package allows complex cuts. The organization-wide click rates could already be reduced by more than two thirds during the initial phase, with a further downward trend. At the same time, the reporting rate of suspicious emails increased. Employees thus become an active part of the IT security strategy.

7 Continuous and randomized simulation

A phishing simulation should always be run on a continuous basis, as this is the only way to ensure lasting and long-term learning success.

Findings from habit research suggest that learning measures distributed over a longer time span are more beneficial in terms of changing behavior than isolated learning measures. For example, the cyber security awareness of the recipients is continuously trained through repeated nudges in everyday life by the phishing simulation. This 'nudging' known from behavioral economics encourages a constant involvement with the topic 'phishing'.

Randomizing the simulated phishing mails is also relevant for the success of the simulation. If all recipients receive an identical simulated phishing email at the same time, the news may spread very quickly throughout the organization. Sending the emails in a randomized order rarely leads to a saturation effect of the phishing mails and templates used. This is because in that case colleagues are not able to talk to one another about their experiences immediately after. After only a few days or weeks, the information will most likely have disappeared from their active memory.

Not only the users benefit from this approach. There are also advantages for you by simulating continuously and in a randomized order:

- After a baselining phase, the KPIs are always indicative of the overall results, i.e. 'live'. In the case of isolated campaigns, the click rate often correlates strongly with the difficulty of the respective email. By randomizing a larger selection of emails and sending them at different times, the respective email types are always equally represented in the KPIs. This allows for continuous interpretation of key figures and ultimately demonstrates a solid effect of the measure.
- The ticket load is minimized. Instead of sending the fake emails to all employees at certain points in time and thus initiating massive waves of reporting, the workload for IT is distributed over the entire simulation period by sending them out in randomized order.

8 Providing useful feedback to users

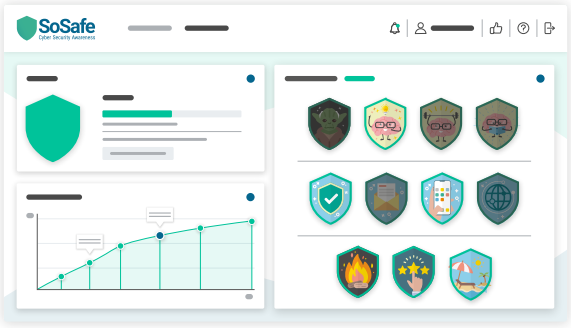
As the previous points have made clear, early communication about the process and goals of the phishing simulation is a core component of the method. However, it is equally important to communicate intermediate results to the users.

This helps employees to assess their own performance and recall what they have learned. You should give clear and comprehensible feedback, for example:

- Are employees interacting particularly often with fake websites, i.e. interaction rates are high?
- Which psychological tactics are the most successful in deceiving them?
- Are users more likely to be misled by emails that arouse curiosity or those that create pressure?

Make sure that you formulate results clearly. Technical and scientific KPIs are not understandable for most employees - click rates and interaction rates are. Again, you can emphasize the learning aspect. You should also focus on giving positive rather than negative feedback: For example, explain to the recipients of phishing emails that it is the reporting rates during the simulation that are decisive, not the interaction rates. This is because users should be trained to identify the emails - the main focus is on making the employees an active line of defense for the organization.

Gamification can also play a decisive role in this. As psychological studies show, typical gamification elements, such as collecting points for correctly identified and reported (simulated) phishing emails, provide additional motivation for employees. In summary, giving feedback to the employees supports them in using the phishing simulation even more specifically as a learning tool and to train their awareness.



Gamification on the SoSafe Awareness platform: badges and points provide for additional motivation.

Realistic learning: The added value of phishing simulations

Systematically planned and executed phishing simulations increase cyber security awareness in the long term and can thus strengthen organizations' resistance against cyberattacks. However, the simulations are only effective if they focus on the human factor and the underlying need for learning. Like that, they can decisively contribute to cybersecurity.

As the presented best practices have shown, precautions must be taken at various levels to achieve this. A well thought-out approach to your phishing simulation will enable you to establish a stable security culture in your organization and prepare yourself for increasingly frequent cyber risks.

With full or managed service providers, you get everything from a single source - from planning and adapting the phishing emails to running the simulation and preparing the analysis. With experience gained from working with other organizations, the providers are well prepared for any queries of a technical or content-related nature and can thus support you reliably.

Checklist Phishing Simulation

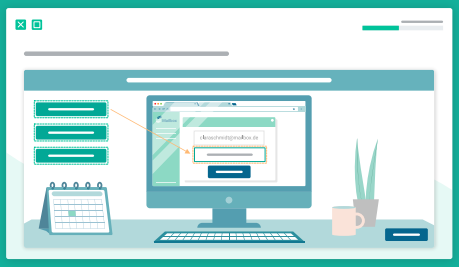
Have I...

- [ ] **technically prepared** for the phishing simulation, e.g. prepared a white listing for the provider's mail servers, and added the domains included in the phishing mails to that white list,
- [ ] **introduced** the phishing simulation to my colleagues and **announced** the start,
- [ ] emphasized the **anonymity** and the **learning** aspect of the simulation,
- [ ] **adapted** the simulation to the users,
- [ ] made sure that the phishing simulation is accompanied by **relevant learning contents**,
- [ ] established a **chain of reporting** and informed the employees about how to proceed in the case of a (simulated) phishing attack,
- [ ] made sure that the emails are sent **continuously and in a randomized** order,
- [ ] talked to the employees about the reasons for and **results of the simulation before, during and after** the measure?

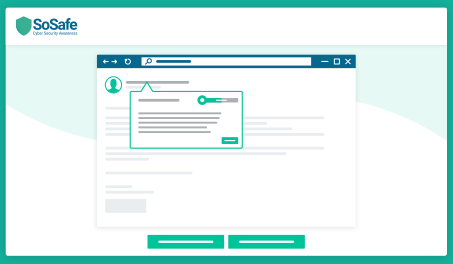
About SoSafe

SoSafe GmbH, based in Cologne, Germany, is a provider of digital training solutions specializing in IT security and awareness building. The team of around 80 people ranges from IT security experts to learning psychologists.

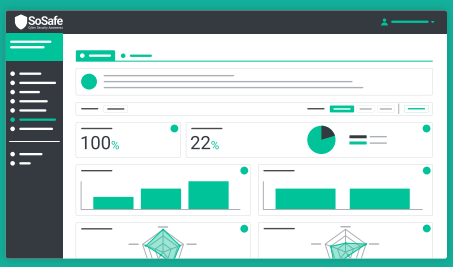
SoSafe's awareness platform sensitizes, trains and tests employees in dealing with all kinds of cyber threats. The training is interactive, motivating and 100% data protection compliant, which means that the solution is also extremely well received by staff representatives and employees. With comprehensible KPIs and differentiated reporting options, the success of cyber security training finally becomes measurable and visible.



E-Learning Platform
- Interactive modules on security and privacy
- Awareness videos
- Customizable content and layout



Phishing Simulation
- Realistic randomized attacks
- Hands-on explanations
- Continuous awareness building throughout the year



Support Tools
- Dashboard with technical and psychological KPIs
- Phishing report button
- Employee certificates

Authors

Dr. Niklas Hellemann, Certified Psychologist & Managing Director
Katharina Ketels, Corporate Account Executive
Ann-Kathrin Krane, Marketing Manager

Contact

Mail: info@sosafe.de
Telefon: +49 221 6508 3800

Further Information

www.sosafe-awareness.com
www.sosafe-awareness.com/product
www.sosafe-awareness.com/demo

SoSafe
Cyber Security Awareness