

# Human Risk Review 2021

An Analysis of the European Cyberthreat Landscape



## Editorial

### Why is now a good time to take a closer look at the human factor in cyber security?

Last year was – not least because of the COVID-19 pandemic – a year of challenges for all of us. Cybercriminals have shamelessly exploited this situation and attacked us when we were most vulnerable. Shortly after the outbreak of the infection, we were able to observe phishing campaigns that took advantage of the tense situation. Attacks were designed that played with people's emotions and ultimately crippled entire infrastructures. It quickly became clear that the attackers are unscrupulously taking advantage of this crisis to launch social hacking attacks.

**ENISA talks of an increase of over 600% in phishing mails. Phishing websites are at a record high, according to Google.**

Various studies now clearly substantiate these observations – with some frightening numbers. The European Union Agency for Cybersecurity (ENISA) reports an increase of over 600% in phishing mails. Phishing websites are at a record high, according to Google. And an Interpol report issues an urgent warning about the cyber-threats we shall also face in a changed world of work once the crisis has passed. Consequential damage is also on the rise. According to the security company McAfee, the annual amount has more than doubled since 2018.

But what is it about the current threat situation that is so precarious and why are human-based attacks so successful? Our analyses suggest two main factors:

## Emotional uncertainty

The pandemic has had a lasting impact on people's minds and brought entire nations to a breaking point. This tense situation plays into the hands of cybercriminals – they can use social engineering and new psychological tactics such as the need for protection to trick us in a highly targeted way.

## New work and remote working models

To protect our fellow human beings, we are now working more from home – but even after the crisis has subsided, remote work will tend to be the rule rather than the exception. However, many employees are unfamiliar with the new working methods and tools, and this provides cybercriminals with new angles of attack. A large number of users have yet to learn how to handle sensitive information in the home office. In addition, the office grapevine, which is especially valuable when it comes to spotting attacks, is no longer present.

Hackers are now focusing on people and their emotions and social engineering hacks are becoming increasingly relevant. The attack level is increasing, and tactics are being refined. Methods such as “double extortion” are being used with greater frequency and they lessen the effect of measures to protect or repair damage, such as backups.

In this report, therefore, we assess the growing human risk, look back at 2020 and look ahead to the new year: Which psychological tricks are we particularly vulnerable to? What are the main threats to cyber security? And how can organizations minimize their risk of falling victim to a future cyberattack?

Our evaluation is based on four data sources: over 1.4 million data points from our SoSafe Awareness Platform; a targeted phishing awareness survey involving over 5,000 participants; analyses from the AV-TEST Threat Intelligence Platform; and a survey of over 100 cyber security experts.

If the results show one thing, it is that cyber security concerns us all. It has never been more important to protect yourself and others from online dangers. What applies to our health also applies to cyber security: prevention is better than damage repair.



Dr. Niklas Hellemann  
Managing Director, SoSafe Cyber Security Awareness

# Contents

<b>Executive Summary</b>	<b>4</b>
<b>The threat situation 2020: Cyberattacks are the greatest operational risk</b>	<b>5</b>
<b>Phishing, ransomware, trojans: How the attack potential is intensifying</b>	<b>6</b>
Infobox: Cybercrime in healthcare – a closer look	9
<b>Analysis of the European Cyberthreat Landscape 2020:</b>	
Database and methodology	11
Infobox: Privacy Shield data agreement revised – only EU service providers offer legal security	13
How security experts assess attack potential	14
Infobox: Prevention is the priority in cyber security	17
Interview: Why airbags alone do not avoid accidents – the importance of the human factor in cyber security	18
Malware: The dramatic increase at a glance	21
Infobox: Protection via the office grapevine – organizational setting as an influencing factor?	24
Psychological and technical vectors – an overview of the risk factors	25
Top 10 subject lines 2020	29
Interview: Preventive and reactive cyber security awareness – Cyber security as a joint project	35
The click behavior in detail: What is the influence of demographics, sector, and time?	37
Interview: The remote work challenge – Cyber security in times of increasing digitization	41
<b>Social engineering trends 2021: Cybercriminals continue to upgrade</b>	<b>43</b>
<b>Conclusion &amp; recommendations: How do organizations minimize their human risk?</b>	<b>46</b>
<b>About SoSafe</b>	<b>47</b>

## Executive Summary



### Working from home makes people more susceptible to cyberattacks

75% of the cyber security experts surveyed believe that the new remote work setting makes successful cyberattacks more likely. This can also be seen in the click data: our analyses show that the click rate on phishing mails in decentralized organizations (including remote working) is significantly higher than in centralized organizations (with in-office working). Accordingly, most of the decision-makers surveyed also plan to increase or at least maintain their employee awareness measures with the switch to remote work.



### The corona crisis – a feast for cybercriminals

Cybercriminals exploit crises – such as the current corona virus – and social instability for their own purposes and in times like these they ramp up the volume of their attacks. Analyses show a rapid increase in ransomware types this year, especially during the first lockdown in March 2020. The same applies to their success probability: in the first lockdown phase, the click rate for phishing mails rose considerably.



### Successful social engineering scams via virus references

From the very first weeks of the pandemic, cybercriminals were feeding corona-related content into phishing campaigns. Our analyses clearly show that this also results in a greater probability of success. Corona phishing mails or emails that address the introduction of remote tools top our ranking of the most successful phishing mails. While the average click rate is 29%, emails with the word „Corona“ in the subject show click rates of up to 79%.



### Trojans still on the rise

Trojans continue to be the most dangerous type of malware – they account for 55% of known malware. In 2020 the total volume of new malware also reached the unprecedented level of 750 million.



### Unscrupulous attacks - critical infrastructure targeted

Attacks on critical infrastructure organizations have increased significantly in the past year. The success rate of simulated phishing attacks – and thus also the risk of falling victim to a cyberattack – in hospitals, for example, is 30% higher than the average. Scruples are rare – attacks often focus on the manufacturing and supply chain for corona vaccines.



### Digital natives most frequent clickers of phishing mails

In a separate study involving 5,000 participants we analyzed the public's click behavior, taking demographic variables into account. The myth of the digital native suggests that younger users use information technology more safely. However, the results show that 18 to 29 year olds, with a click rate of 38%, click on phishing mails more often than any other age group, where the average is just 25%.

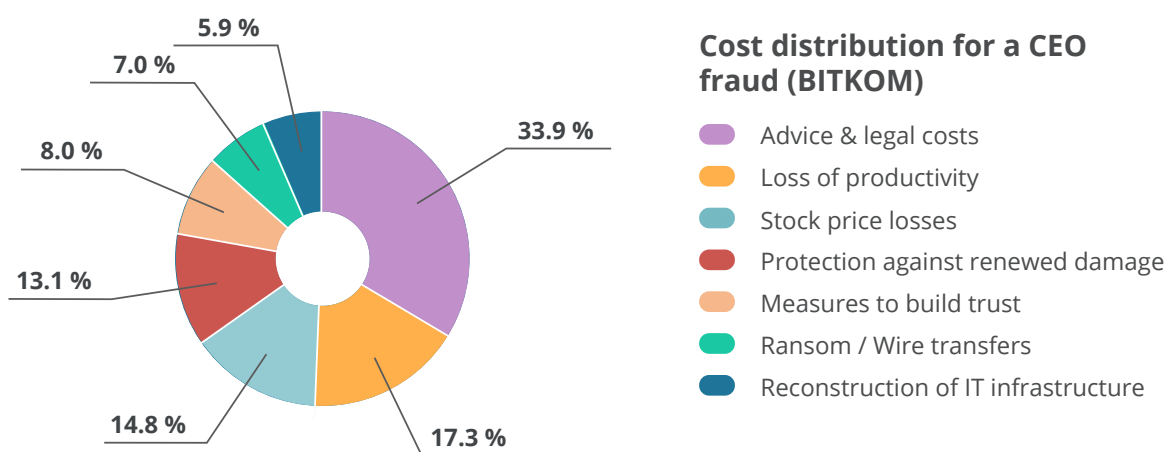
## The threat situation in 2020: Cyberattacks are the greatest operational risk

2020 brought many unexpected twists and turns – including, and particularly, in the cyber security area. But in all of this one thing has not changed: Cybercrime remains a serious threat to organizations of all sizes and in every sector. The World Economic Forum’s annual ranking judges cybercrime to be the third greatest threat to the global economy. Half of all companies fear cyberattacks and data fraud, for example due to changed work patterns such as remote working models.<sup>1</sup>

Other official cyberthreat analyses also confirm its significance. Security company McAfee estimates global losses to be over 1 trillion US dollars for the first time – an increase of over 50% since 2018, when annual losses were estimated at just under 600 billion.<sup>2</sup>

### The cost of a cyber incident can often run into the millions

For organizations, this means that successful attacks are becoming more and more likely – and they could be expensive. In a case study compiled by the German Association for Information Technology and Communications (BITKOM), it was estimated that the cost of a CEO fraud incident in a medium-sized German manufacturing company might be in excess of 6.6 million Euro. While any sum transferred in response to social engineering is minimal, at only 7.5%, according to BITKOM, the costs of repairing the damage and rebuilding trust and image after an attack are particularly high. It should be noted, however, that the sums demanded as ransom for other cyber incidents have also increased (see also p. 8). As recently as the summer of 2020, the American travel company CWT “boasted” that it had traded the blackmailers down from the original 10 million US dollars.<sup>3</sup>



<sup>1</sup> World Economic Forum (2020). [COVID-19 has disrupted cybersecurity, too - here's how businesses can decrease their risk.](#)

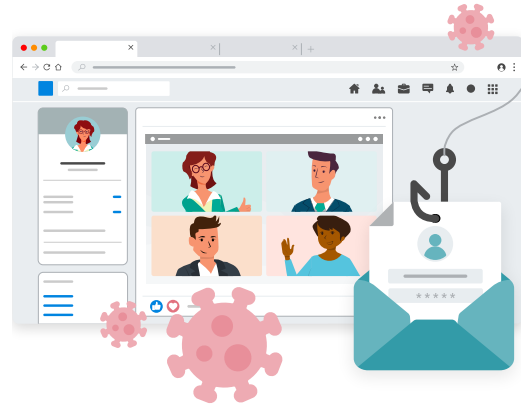
<sup>2</sup> McAfee (2020). [New McAfee Report Estimates Global Cybercrime Losses to Exceed \\$1 Trillion.](#)

<sup>3</sup> Reuters (2020). [‘Payment sent’ - travel giant CWT pays \\$4.5 million ransom to cyber criminals.](#)

## Phishing, ransomware, Trojans: How the attack potential is intensifying

For the first time, organizations themselves seem to have recognized this enormous risk potential. In the “Risk Barometer” of global insurer Allianz, companies worldwide rate cyberattacks as the greatest risk to their business.<sup>4</sup> One of the reasons for this is undoubtedly the fact that attack tactics are constantly evolving, making it difficult for organizations to both take effective protective measures and to react in an emergency. But which new tactics were most prominent in 2020? Which attacks were particularly successful? Which trends can be observed?

Based on the assessments of our experts, customers and partners, we provide an overview of cybercriminals’ complex methods and developments that have kept organizations around the world in suspense over the past year.



### The crisis is fueling social engineering

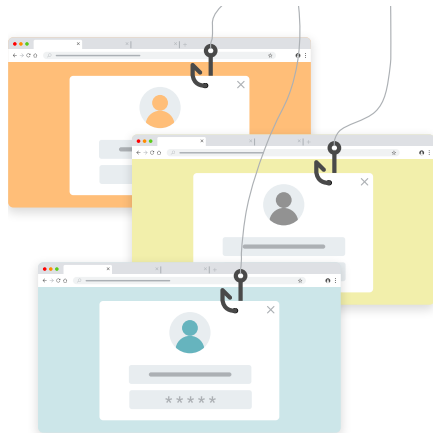
Unlike any other year, 2020 was the best time for cybercriminals to launch new spam and phishing campaigns. Social and media-effective debates were unhesitatingly misused for criminal purposes and emotionally sensitive topics were exploited. In its COVID-19 Cybercrime Analysis Report, Interpol noted a huge rise in attacks taking advantage of the crisis.<sup>5</sup>

According to ENISA, there were six times as many phishing attacks as before.<sup>6</sup> In addition, the #blacklivesmatter movement and the US elections caused a flood of perfidious (spear) phishing attacks that manipulated their victims emotionally.

<sup>4</sup> Allianz (2021). Allianz Risiko Barometer 2021: Covid-19 trio tops global business risks.

<sup>5</sup> Interpol (2020). Interpol report shows alarming rate of cyberattacks during COVID-19.

<sup>6</sup> European Union Agency for Cyber Security (ENISA) (2020). Understanding and dealing with phishing during the covid-19 pandemic.



### Phishing websites still multiplying

A new negative record: In 2020 Google detected over 2 million phishing websites – an increase of around 20% compared to the previous year.<sup>7</sup> These sites are also increasingly using SSL certificates. A simple look at the URL or the protocol is no longer enough to identify a page as dangerous. The high numbers are probably largely due to the COVID-19 pandemic – in the first six months of the year, Google registered almost 50,000 new phishing pages per week, which is far more than immediately beforehand.

But this is no short-lived trend. The numbers have increased by almost 13% per year since 2015. The corona crisis has only accelerated the general trend.

### Focus on critical infrastructures

Even during the crisis, opportunistic cyber-criminals did not shy away from attacks on critical infrastructure. With a complete absence of morality, facilities such as hospitals were attacked, infrastructures paralyzed, and sensitive data stolen in order to extort ransom money.

After one cyberattack on the Finnish psychotherapy clinic Vastaamo, the patients themselves were blackmailed using the content of their confidential medical files. In early December, Interpol also reported an increase in direct and indirect attacks on vaccine chains that were targeting not only governments but also worried individuals.<sup>8</sup> Its key social function makes doing business in the critical infrastructure area particularly lucrative for criminals (see info box p. 9).

<sup>7</sup> Forbes (2020). [Google Registers Record Two Million Phishing Websites in 2020.](#)

<sup>8</sup> Interpol (2020). [Interpol warns of organized crime threat to COVID-19 vaccines.](#)





### Cybercriminals hunting big game

Over recent years one could not fail to be amazed at the huge ransom demands that cybercriminals were making after ransomware attacks. In 2020 they went all out, attacking even the largest corporations and increasing ransoms even further. Overall, there has been an increase of over 40% in successful ransomware attacks worldwide.<sup>9</sup> In July navigation specialist Garmin allegedly paid attackers around 10 million US dollars. These cybercriminal tactics quickly came to be referred to as „big game hunting“.

The numbers speak for themselves. According to Accenture the average ransom payment rose by another 60% from Q1 to Q2 2020.<sup>10</sup> But ransomware attacks are still targeting small and medium-sized companies. Four out of five medium-sized and one in five small businesses were targeted.<sup>11</sup>



### Trojans as a proven all-purpose weapon

In January 2021, international law enforcement agencies, in collaboration with Europol and Eurojust, succeeded in disrupting the malware considered to be the most dangerous in the world, Emotet. Last year, after a brief pause in the summer, the Trojan caused turmoil among IT specialists. What is so dangerous is that, with their often polymorphic design, Trojans like Emotet or Egregor escape technical filters.

In more recent versions, for example, Emotet was opting for thread hijacking – i.e., it was stealing actual email conversations in order to resume them with harmful content. The AV-TEST data (see p. 21) show that Trojans were the most frequently used malware in 2020 so security measures should focus on them. Cybercriminals are keeping IT managers busy with new types of malware – the smashing of the Emotet infrastructure is probably just a temporary reason to take a sigh of relief.

<sup>9</sup> Heimdal (2020). This Year in Ransomware Payouts.

<sup>10</sup> Accenture (2020). Cyber Threatscape Report.

<sup>11</sup> Heimdal (2020). This Year in Ransomware Payouts.

## Infobox

## Cybercrime in healthcare - a closer look

Critical infrastructures (CRITIS), including water and energy suppliers, the food industry and the health sector, are increasingly being targeted by cybercriminals. An increase in networking and digitization mean that they are also increasingly vulnerable. If critical infrastructure fails, it could seriously impact everyday life. This makes them the perfect target for attacks on IT and demands for huge ransoms.

Due to their social relevance and specific work processes, hospitals, in particular, are currently targets of interest for cybercriminals. According to security company Check Point Security, the number of cyberattacks on such facilities doubled again between November 2020 and January 2021.<sup>12</sup> Tech company IBM's „2020 Cost of Data Breach“ report also states that a data breach in the healthcare sector costs more than in any other industry, averaging 7.13 million US dollars, and the trend is rising.<sup>13</sup> The reasons for the high attack potential include outdated systems, complex work processes (such as shift work) and, last but not least, the enormous burden caused by the COVID-19 pandemic. Ultimately, the success rate for simulated phishing attacks is 30% higher than the average.<sup>14</sup>

---

<sup>12</sup> Threat Post (2021). [Cyberattacks on Healthcare Spike 45% Since November.](#)

<sup>13</sup> IBM (2020). [IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year.](#)

<sup>14</sup> SoSafe Awareness-Plattform.

### **Case studies: Cyberattacks on European healthcare sector – German and French clinics suffer ransomware attacks**

In September 2020 there was a ransomware attack on the University Hospital in Düsseldorf, Germany. The ransomware planted in the university hospital encrypted 30 servers and paralyzed both IT systems and emergency operations for 13 days. Despite rapid decryption, it took almost two weeks for all the systems to get up and running again. Particularly dramatic was the fact that no emergency care could be provided. The journey to another hospital cost one patient her life. The German Federal Office for Information Security (BSI) has now analyzed the case and believes that it could have been avoided with appropriate preventive measures.

Two hospitals in France suffered a similar fate in February 2021. Within one week, the IT-infrastructures of clinics in the cities of Dax and Villefranche-sur-Saône were crippled by ransomware attacks, forcing staff to resort back to pen and paper, and urgent operations having to be postponed. The attacks known as “Ryuk” and Egregor” resulted in many patients, particularly those with serious medical conditions, being transferred to other hospitals to be provided with necessary care. After yet another attack on several laboratories in northern France, cybercriminals published the medical data (medical condition, blood type, health insurance, to name a few) as well as the private contact information of more than half a million patients in hacker forums on the dark net, leading experts to suspect financial gain as being the primary motivation behind the attacks.<sup>15</sup> As a result of those, and an alarming increase in the frequency of similar attacks, President Macron pledged to invest 1 billion euros to strengthen cyber security in France.<sup>16</sup> In line with observations that the healthcare sector is increasingly under attack, both in Europe and across the globe, more than a third of the funds is to be allocated to hospitals.

---

<sup>15</sup> Infosecurity Magazine (2021). [Medical Data of 500,000 French residents leaked online.](#)

<sup>16</sup> Healthcare IT News (2021). [Emmanuel Macron pledges €1bn for cybersecurity after hospital ransomware attacks.](#)

## Analysis of the European Cyberthreat Landscape 2020: Database and methodology

Based on a wide range of data sources, this report summarizes the risk situation in 2020 and discusses the question: “How great is and was the human risk for organizations?” The results are based on both quantitative and qualitative analyses and they enable a comprehensive overview of the status quo and current developments in the European cyberthreat landscape, with a particular focus on the human factor. Specifically, the report contains four datasets / analyses:

### Dataset 1: Malware analysis from the AV-TEST Threat Intelligence Platform

Analyses by the AV-TEST Institute, a leading independent IT security research institute, shed light on the threat situation from a technical perspective. The AV-TEST threat intelligence software (AV-ATLAS<sup>17</sup>) automatically analyzes and classifies malware.

**3 million**

files scanned per day

**25**

virus scanners for fully automated threat intelligence

**> 700 million**

malicious programs entered in the database

The AV-TEST analyses enable a statistically informed review to be carried out on the technical side of the cyberthreat landscape in 2020. Which malware categories were most common and what conclusions can be drawn from their evolution over time?

### Dataset 2: Response data from the SoSafe Awareness Platform

In contrast, exclusive response data from the SoSafe Awareness Platform provide insight into the psychological side of the attacks and also answer questions about the likelihood of success by various human-based attacks, such as phishing.

**1.4 million**

simulated phishing attacks from 2020 evaluated

**200**

customer organizations captured in response analyses

For the SoSafe Phishing Simulation, millions of data points are gathered on the current threat situation and employee responses to a supposed attack – the latter are completely anonymous (given the importance of processing data within the framework of the GDPR and by EU providers, see infobox p. 13).

<sup>17</sup> AV-TEST - The Independent IT-Security Institute (2021). AV-ATLAS.

In addition to technical and psychological factors that quantify the success of phishing mails, the analyses also include sector-specific comparisons and insights into users' click behavior, for example with regard to times. So the analyses both enable conclusions to be drawn about cyber security weak points in organizations and enable approaches to be developed to strengthen cyber security based on the data.

### **Dataset 3: Phishing simulation „Phish Test“ to record general awareness**

Another data source is an annual study carried out by SoSafe and the non-profit security initiative "Botfree.eu" on general phishing awareness among the public. Over 5,000 users took part in the last phishing simulation in October 2020. Once registered, all the participants received, within a week, three simulated but realistic phishing mails which they needed to detect. Analyzing the results, taking into account the participants' demographic data, enables more in-depth conclusions to be drawn about their click behavior.

### **Dataset 4: Survey of cyber security experts**

Finally, the data-driven analyses in this report are supplemented by a representative survey of over 100 experts from the cyber security sector. The replies provide information about how cyber security managers perceived the danger situation shaped by the COVID-19 pandemic in the past year. They also give an impression of the current status of awareness efforts in organizations. The role of the human factor and awareness measures will be analyzed and evaluated even more intensively via interviews with selected experts.

Infobox

**Privacy Shield data agreement revised - only EU service providers offer legal security**

In the so-called Schrems II ruling of July 16, 2020, the European Court of Justice declared the "Privacy Shield" agreement between Europe and the USA to be null and void. In doing so, Europe's highest judicial authority makes one thing clear: the level of security required by the General Data Protection Regulation for processing data from EU citizens cannot currently be guaranteed outside of Europe.

What the decision makes clear is that the GDPR requires employee data to be treated particularly carefully, not least in the context of phishing simulations and employee trainings during which behavioral data of staff is being processed. To make sure they fully comply with GDPR standards, organizations should therefore choose software providers that are based in the EU, on the one hand, and ensure that all data are processed on servers within the EU, on the other. If opting for non-EU providers or providers with the parent company outside the EU, organizations risk being fined up to 4% of their global annual turnover as well as disputes with employees since there remains legal uncertainty after the Schrems II ruling. It is important to note that this obligation applies to all companies employing staff within the EU.

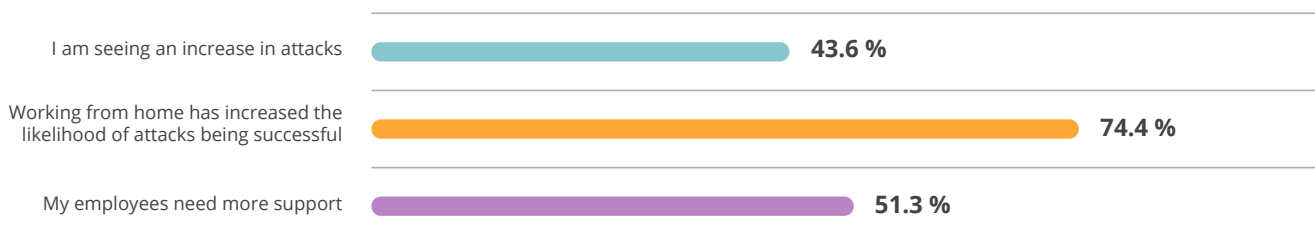
## How security experts assess attack potential

### Organizations recognize heightened attack potential

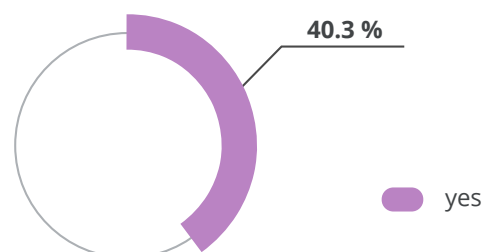
Our survey of cyber security experts (dataset 4) confirms that organizations are well aware of the increase in cyberthreats and recognize that the corona pandemic directly impacts cyber security in their organization.

Over half of those surveyed state that employees need more support during the crisis. Almost 75% believe that working from home also increases the likelihood of successful cyberattacks. Indeed, four out of ten respondents have noticed the aggravated threat situation themselves and seen COVID-19-related phishing mails.

#### In your opinion, what impact did COVID-19 have on cyber security?



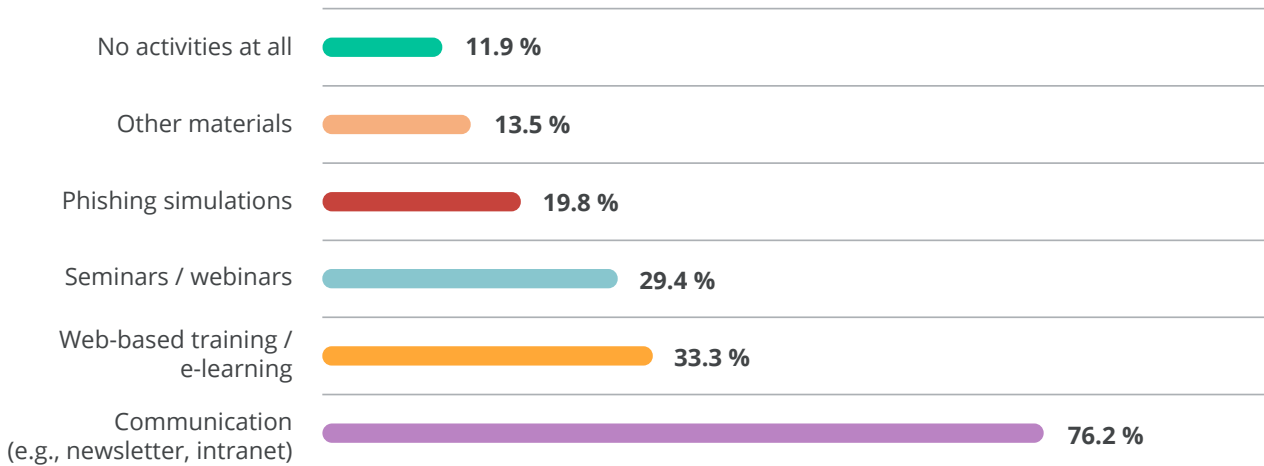
#### Have you noticed corona-related phishing mails?



### Awareness measures: Many have recognized the need

Most of the experts and organizations surveyed respond to the increased incidence of human-based attacks by involving staff. Over three quarters of those surveyed state that they communicate in some way, for example by posting on their intranet or sending messages to staff. To date, though, organizations have taken proactive, long-term awareness measures to counter such dangers less frequently and on an ad hoc basis. Only a third of those surveyed are using e-learning or web-based training and only one in five use phishing simulations. One positive finding is that only a small percentage exclude their own employees from protective efforts – around 11% do not take any measures in this area.

#### What measures do you take to increase your staff's awareness?

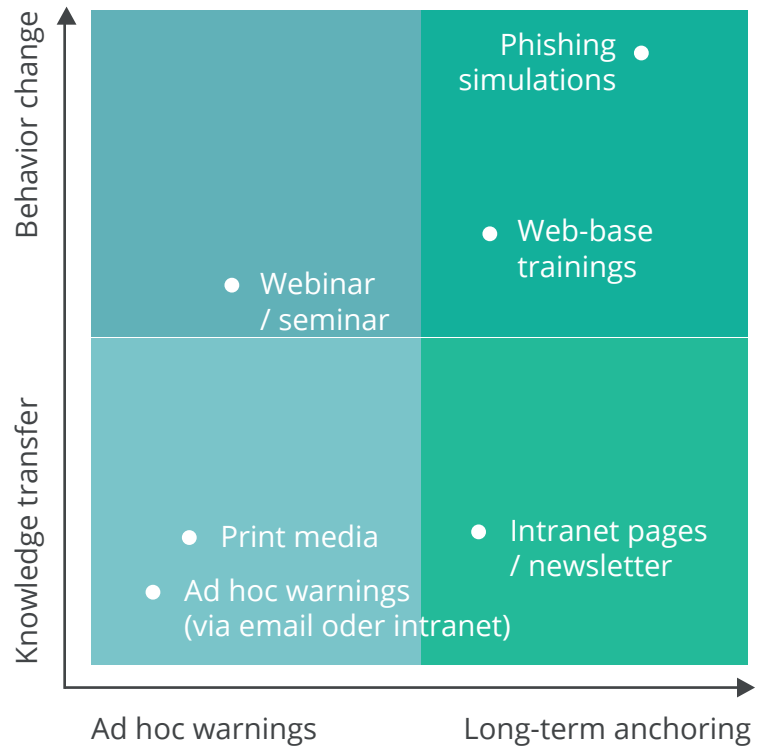


The results also match an underlying cyber security awareness maturity model (see chart on p. 16), in which one-way communication (such as ad hoc email alerts) is a simple and opportune first step. While such measures can be implemented quickly and without many resources, they are nevertheless of a more reactive nature and have to be implemented by specialist staff, who are scarce, especially in the cyber security area.



So, in extending awareness measures, the focus is increasingly on activities and tools that enable organizations to anchor security awareness and training in ongoing processes, for example via continuous measures and a reliance on data and KPIs. The focus is also shifting towards proactive risk minimization through demonstrable changes in employee behavior, such as the increased recognition and reporting of suspicious emails. Larger companies, or those with a higher degree of maturity, are therefore increasingly using interactive and digital training or active measures such as phishing simulations, which aim to change behavior instead of just conveying information.

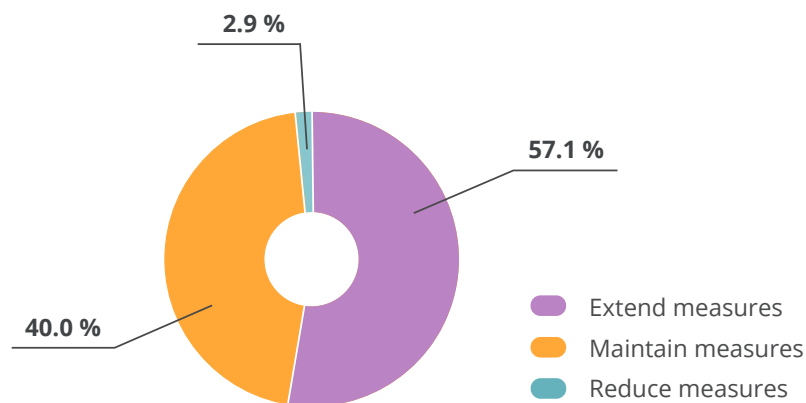
**Various awareness measures against the background of their target function**



**The signs point to change**

There is a glimpse of hope. Almost six out of ten respondents wish to extend their measures to raise employee awareness in the future, 40% will at least maintain their current measures. So most of the respondents seem to be conscious that the topic is relevant. Looking at the results, however, there is no question that there is still some catching up to do in terms of implementing security ambitions.

**What is your plan in terms of raising employee awareness?**



## Infobox

### **Prevention is the priority in cyber security**

A case that caused a stir. After a 40 million euro CEO fraud, the automotive supplier Leoni sued ex-boss Dieter Bellé for damages. This action clearly emphasizes the special responsibility that managers have for cyber security and data protection.

The fact that sufficient prevention can also have liability implications can be explained by examining the relevant framework conditions, for example those specified by the GDPR. The ISO-27001 IT security standard even encourages organizations to carry out ongoing social engineering simulations. Should an incident actually occur, as it did, with serious losses, in the case of Leoni, companies have to prove they have complied with these obligations. Where there is any doubt, management are liable for failing to take appropriate preventive measures.



## Why airbags alone do not avoid accidents – the importance of the human factor in cyber security

An interview with Bert Skaletski, CISO at Merck KGaA



Bert Skaletski is Chief Information Security Officer at the science and technology company Merck KGaA in Darmstadt. As longstanding security and risk management professional (e.g., CISM, CISSP), he is responsible for Merck's global information security management system, including overseeing security awareness training for its nearly 57,000 employees in 66 countries.

**Looking at the current threat landscape, the human factor seems to play a key role. Why can we not yet rely on technical barriers?**

A lot of people believe that technology alone is the solution to solve all the cyber security threats we face right now but I don't think it's likely to solve the issue soon. The threat actors adjust techniques, tactics and procedures and we as defenders must counteract. At the end of the day, it comes down to managing the overall risks, likelihood and impact. In this equation we still need to consider the human factor, including the fact that technology and machines we are talking about are man-made as well.

I often compare cyber security with automobile examples: We buy cars full of fancy safety features designed around the risks of a potential crash: airbags, EPS, ABS, automatic braking, you name it. A car full of technology – in cyber security terms this would be antivirus scanner, advanced email filters, for example – won't remove the need for us humans to be cautious and drive defensively. The state demands that you take hours of driving lessons and pass a driver's exam. Why wouldn't we train people on how to act in certain cyber security "traffic situations" or act defensively in order to avoid or minimize cyber security "accidents"? Neither technology nor our behavior will be able to protect us one hundred percent but if we combine both factors, we can greatly reduce risks to the point that we are able to operate and conduct our business.

### **Will that need for prevention and caution ever go away?**

The speed of change in technology is accelerating, keeping us and the end users on their toes – there is no doubt about that. It is undeniable that attackers continue to be one step ahead in finding the loopholes in technology. An employee recently complained about one of our simulated phishing emails, a different and more complex version than what we had previously simulated. But it was exactly the kind of training needed! As attackers switch gears, it reminds us to take precautions. It requires anticipating new types of attacks and weaving them into our trainings. Simulating email types, we have not yet observed helps the employees become more attentive. Again, it is about shaping technology and human behavior. I strongly believe in the “always up-to-date” motto and think this will remain one of the guiding principles in the realm of IT security.

### **During the COVID-19 pandemic, attackers specifically triggered fear and insecurity – what challenges did you see at Merck?**

Many people had never worked from home before, so we had to ensure they had the right technical setup. The attackers very quickly modified their email phishing campaigns to play on the COVID fears, but we too ramped up our cyber defense and our awareness campaigns including email phishing simulations.

### **What kind of skills do you think staff as well as executives will need in the future to adapt to the new normal?**

Attackers invest a good amount of time picking their targets. It is not always executives in focus. Finding an untrained person and getting that person to click on a mail by emotionally manipulating them is what the bad guys have in mind. That is why it is so crucial to also focus on training all employees not just executives. Everyone needs to develop a healthy dose of suspicion and skepticism towards every single email. I always emphasize: If an email message sounds too good to be true, it probably is. Pockets where lack of knowledge exist, from top to bottom in an organization, can be eliminated by continuously educating all employees.

**From a psychological point of view, we are talking about heuristics here. People need to develop a feeling for potentially harmful situations, and they need to be able to react quickly.**

Exactly. But it is hard to train people on how not to be emotional or impulsive when clicking or reacting to certain subject lines, for example. Users being urged to update their credentials and type them into a form is very powerful. When I talk to colleagues in the industry, it is exactly these types of attacks which are specifically targeted on exploiting the end users' emotions that are the most dangerous and effective – the conclusion being, that we need to try and find different ways to train the users for these scenarios.

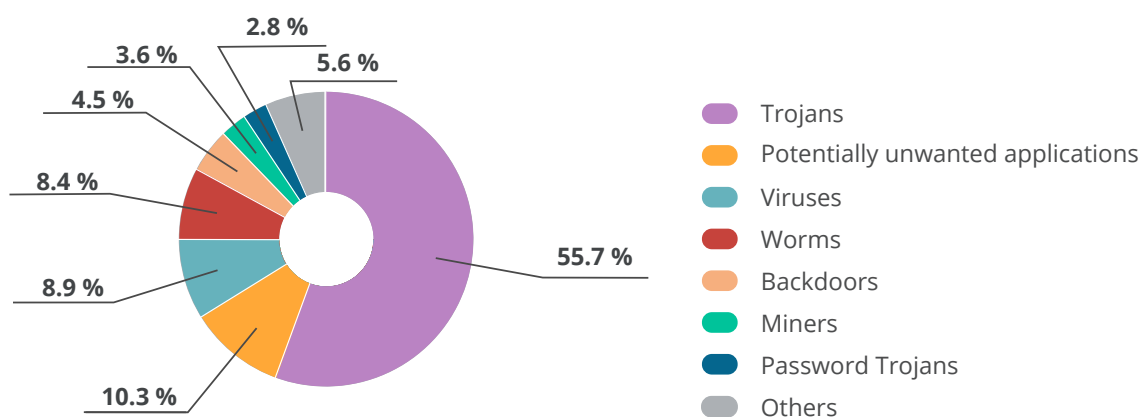
**Do we have to expect that it will get more challenging to detect attacks?**

Definitely. But like I mentioned, follow your gut feeling, have a healthy dose of mistrust and skepticism, as this will go a long way to overcome the challenges. We need to find a balance between regularly updating systems, on the one hand, and training our employees, on the other. From my point of view, the latter is the key to success. Traditional education eventually stops. But learning does not, it is a lifelong journey. Continuous training is so essential, especially in cyber security which is marked by diverse and dynamic attack techniques, tactics and procedures.

## Malware: The dramatic increase at a glance

### Over half the malware types detected are Trojans

#### Frequency distribution of different malware types



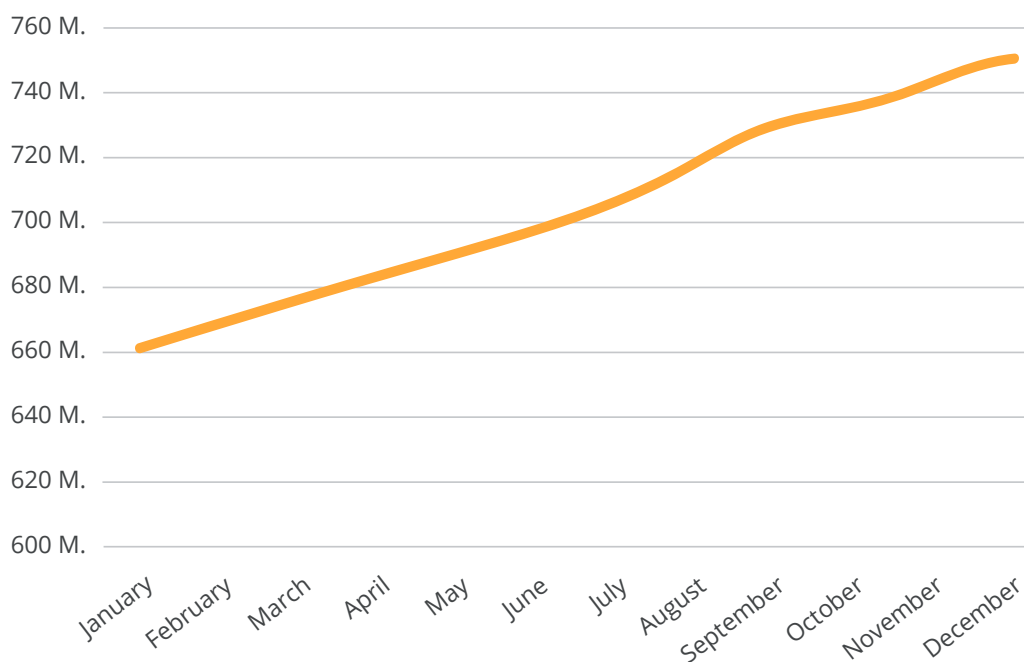
As the analyses from the AV-ATLAS database (dataset 1) show, Trojans such as Ryuk and Egrogor were again the most frequently used malware in 2020. Their complexity makes them particularly dangerous. Hidden on websites, in emails, in software or in files, they run additional malware on the device, encrypt data or install bots and crypto miners. Their malicious code, often polymorphic, makes them difficult to identify and block using secure email gateways. At the same time, the attackers employ tactics (for example, running Office macros) that are specifically designed to circumvent technical barriers. This illustrates the importance of a human firewall – that is, a workforce that knows how to deal with cyber security risks.

#### **Trojans remained the most frequently used malware in 2020.**

The strong position of Trojans – they make up over half of the total amount of malware – suggests that social engineering and ransomware are still on the rise. Often, the use of ransomware, also known as blackmail Trojans, targets the victims' emotions. But potentially unwanted applications (PUA), traditional viruses and worms, are also still widespread. PUAs include adware and spyware, which make up over 10% of the malware detected. Even when the damage is not immediately apparent in such cases, users' data can subsequently be misused for undesired purposes. The different types of malware are also increasingly appearing in bundles.

## The volume of new malware is reaching new heights

### Number of malware types detected in 2020



In 2020, the total amount of new malware has also reached a dangerous high. On average, new malware types are developed at a rate of 4.2 instances per second. By the end of 2020, a total of over 750 million new malware programs had been detected. The increase in malware and mass malware can be observed on an ongoing basis.<sup>18</sup>

**On average, new malware is developed at a rate of 4.2 instances per second.**

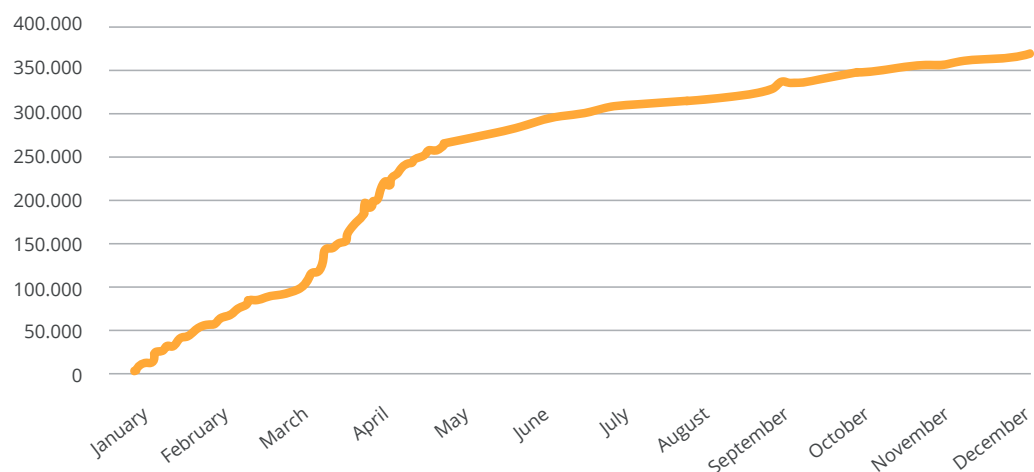
A look at the AV-TEST data on development from previous years illustrates the magnitude of the trend. In 2016, 127.5 million new developments were recorded, while there were 121.7 million new malware programs in 2017.<sup>19</sup> In 2020, there was an unprecedented amount of new malware instances, and the number of unreported cases is likely to be much higher.

<sup>18</sup> AV-TEST - The Independent IT-Security Institute (2020). Security Report 2019/2020.

<sup>19</sup> AV-TEST - The Independent IT-Security Institute (2018). Security Report 2017/2018.

## The COVID-19 pandemic is fueling the development of ransomware

### Number of newly detected ransomware instances in 2020



The dynamic development of new ransomware in 2020 highlights one thing in particular – cybercriminals always have their finger on the pulse. Between March and May 2020 in particular, there was extremely strong growth in new ransomware. The hackers obviously took advantage of the general uncertainty caused by the COVID-19 pandemic and substantially increased their activities. The speed is impressive. The dramatic increase in new ransomware coincides almost simultaneously with the beginning of the first lockdown in large parts of Europe.

**The hackers take advantage of the general upheaval and changes caused by COVID-19, and develop ransomware with pandemic-related content.**

Cybercriminals seem to be able to react to new circumstances such as social upheaval, new technologies or even a global pandemic without any real delay. This observation demonstrates yet again that general and timely prevention, including raising the awareness among staff, is of utmost importance.

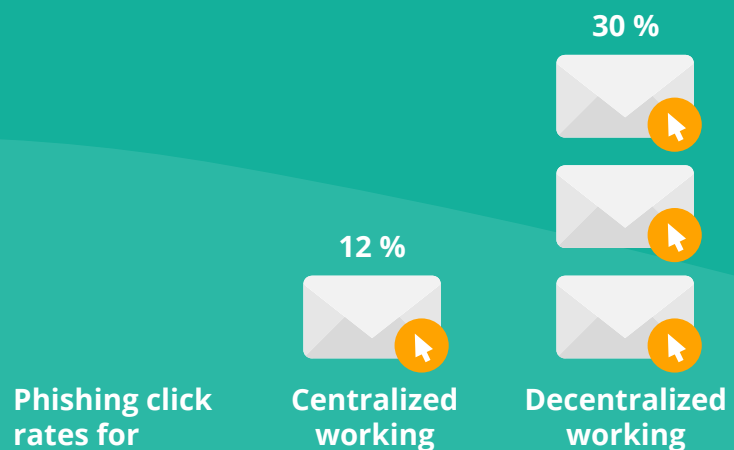


## Infobox

**Protection via the office grapevine - organizational setting as an influencing factor?**

In 2020 many of the content and psychological tactics in the social engineering sector revolved around remote working models and the coronavirus. In addition, however, the question arises as to whether remote work itself and the organizational structure of the company already represents an increased risk for social engineering attacks. To get to the bottom of this question, we carried out an analysis to compare different types of organization: centralized organizations in which all the staff work in one place and often sit together in open-plan offices, and decentralized organizations that have made working from home their usual work mode. In both cases, comparable phishing mails with a relatively low level of difficulty were sent to all employees.

The results show that the click rate in the decentralized organizations is three times higher, at an average of 30%. In comparison, employees in centralized organizations click far less often at 12%. The analysis suggests that centralized organizations are rather better protected against social engineering attacks. One reason for this could be that employees in offices more often share suspicious emails. One could also say that the office grapevine offers protection. So, in the current situation, where almost every organization is opting for remote work, it is particularly important to sensitize employees to phishing mails and thus to address the higher risk through prevention.



## Psychological and technical vectors - an overview of the risk factors

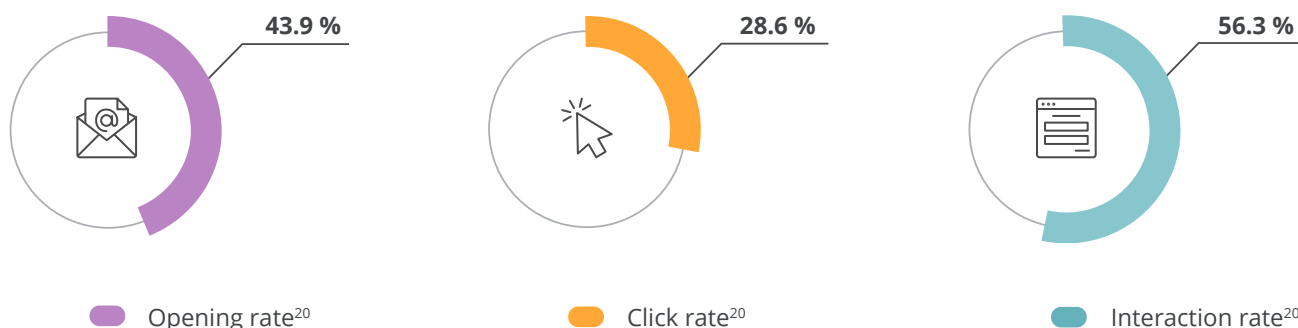
### Click, open, interact: numbers suggest high human risk

The 2020 results from the SoSafe Awareness Platform (dataset 2) show that the attack potential or the probability of success for phishing attacks is enormous.

**Most organizations' staff are initially unable to recognize harmful emails.**

If no systematic awareness measure (e.g. in the form of phishing simulations or web-based training) has been taken and anchored, almost every second user opens phishing mails. Of these users, almost 30% click on links or attachments in the email. 57% of users also interact with simulated emails that contain or link to elements such as fake forms – for example, they enter login information or personal data in fake login screens.

This clearly shows that most organizations' staff are initially unable to detect harmful emails. By handling phishing mails carelessly, they can put their organization in a dangerous position which needs to be taken seriously.



### These technical vectors provoke most clicks on phishing mails

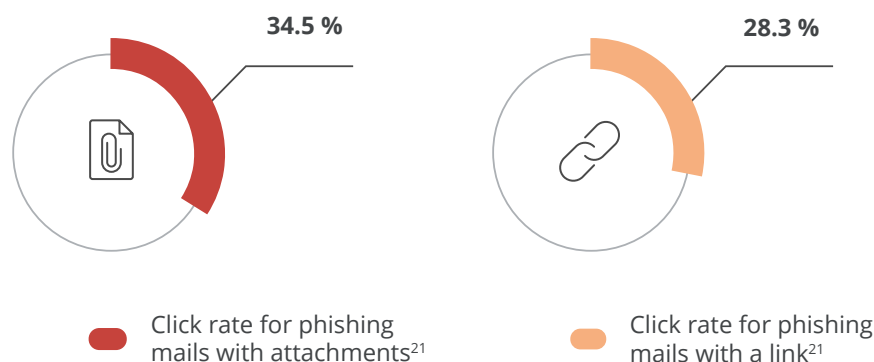
The vectors, with an average of almost 35%, show that the click rate is highest when the simulated phishing mails include an attachment.

**Phishing mails with malicious attachments are the most successful – over a third of recipients click.**

But using links also prompts almost a third of recipients to click. So it seems that emails that promise an interesting interaction hit the mark.

<sup>20</sup>Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.

## Click rates on selected technical vectors

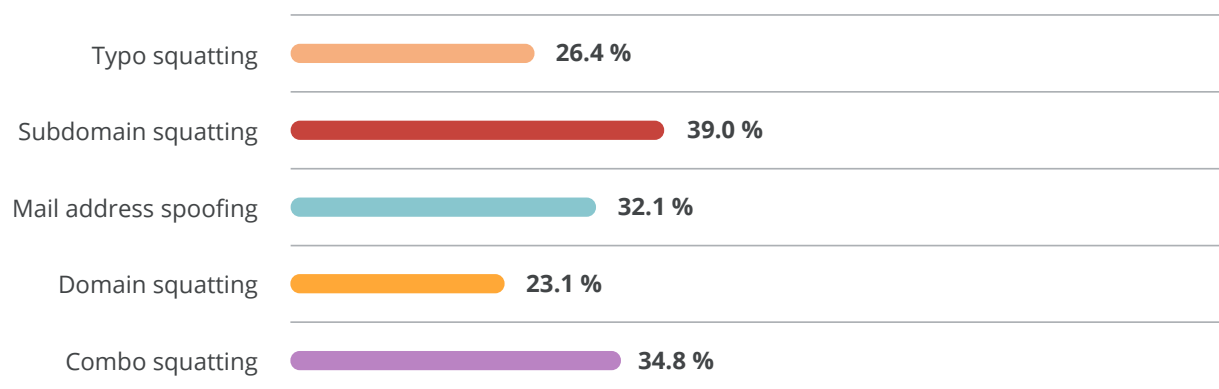


## New techniques for address manipulation are particularly successful

Cybercriminals often manipulate sender addresses to optimize the likelihood of their attacks being successful. For example, in so-called “domain squatting”, domains are registered that are similar to the target domain, for example amazon.com in an attack aiming to imitate a sender from the amazon.com domain. Traditional „spoofing“, in which the sender is overlaid in the email header, is still in use too. If you look at the various manipulation techniques that the SoSafe Platform uses in simulated attacks, it is particularly the more complex techniques that are highly successful. For example, emails that use “subdomain squatting” are clicked on by almost 40% of recipients.

So-called “combo squatting” also results in a click rate of almost 35%. With „subdomain squatting” a term from the target domain is placed in front of an inconspicuous top-level domain, whereas in „combo squatting”, in the context of a brand new domain, it is used alongside other terms. The SoSafe Cyber Security Glossary ( [www.sosafe-awareness.com/cyber-security-glossary/](http://www.sosafe-awareness.com/cyber-security-glossary/) ) also provides a more detailed explanation of various manipulation methods.

## Click rates for address manipulation techniques<sup>19</sup>



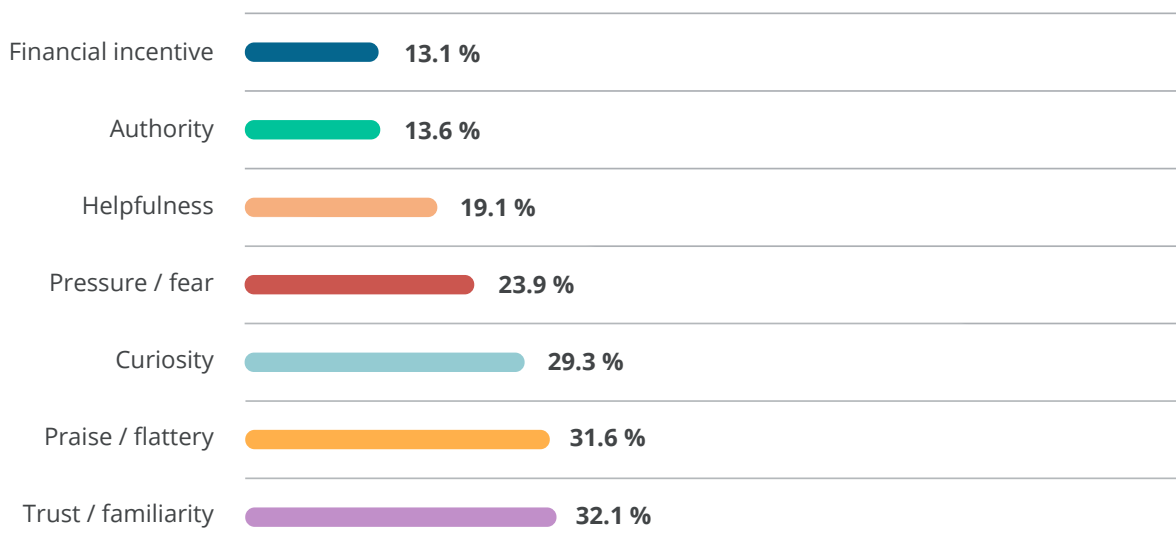
<sup>21</sup> Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.

## These psychological tricks get most clicks

More and more cybercriminals manipulate their victims in a targeted way using psychological tricks – a method that is subsumed under social hacking or social engineering. So the SoSafe experts deal with issues relating to the psychology of hacking: What are the most successful phishing scams? What psychological mechanisms do cybercriminals use? How do phishing scams change, based on current events?

In this context, attackers deploy a broad set of psychological tactics that address a wide variety of human emotions, including stress, fear, belief in authority and curiosity. The SoSafe Awareness Platform is able to evaluate the success rate of these various tactics by categorizing attacks and tagging them. Overall, this gives an interesting perspective on the most successful psychological tactics.

### Click rates by psychological tactics<sup>22</sup>



**Almost every third person clicks when the email simulates a trusting relationship or flatters the addressee.**

At first glance, it becomes clear that phishing mails that aim to arouse positive emotions such as trust are more likely to lure recipients into the trap than those that evoke negative feelings such as pressure and fear. Almost every third person clicks when the email simulates a trusting relationship or flatters the addressee.

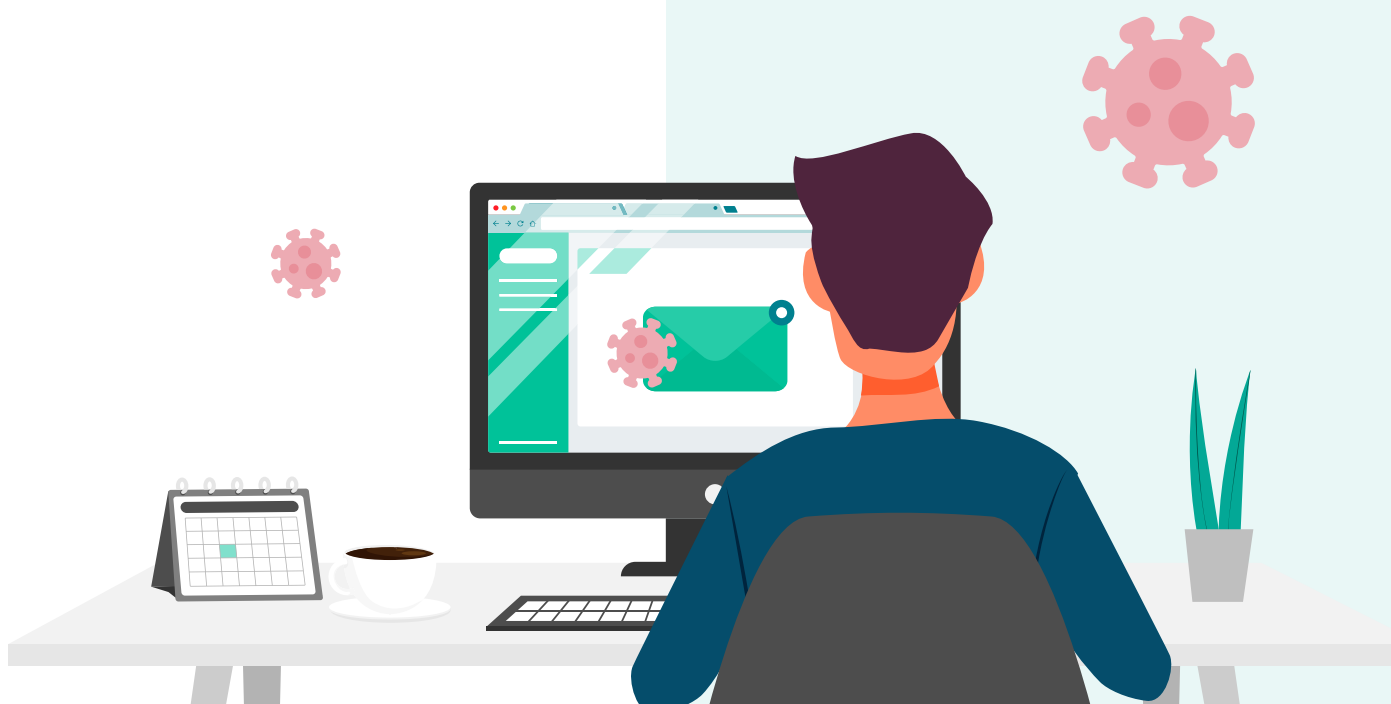
<sup>22</sup>Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.

The click rates are also particularly high if the content aims to arouse the curiosity of the phishing attack victims.

**The combination of curiosity and addressing the COVID-19 pandemic is most likely to encourage people to click on potentially harmful emails in 2020.**

In 2020, numerous simulated phishing mails were specifically designed to exploit the “Corona” curiosity factor, thereby reflecting what was happening in reality. The two most frequently clicked subject lines in the SoSafe Phishing Simulation clearly highlight the scam: The combination of curiosity and addressing the COVID-19 pandemic is most likely to encourage people to click on potentially harmful emails in 2020. The virus emails described have a far higher click rate, of up to 79% (see subject line analysis p. 29).

Emails aiming to build stress and time pressure, on the other hand, only fool a quarter of the recipients. With an average click rate of 13%, employees are least likely to be fooled by financial promises or scams. Traditional phishing subject lines such as „You have won the jackpot“ seem unable to maintain their previous strong effect.



## Top 10 subject lines 2020

The analysis of the most frequently clicked subject lines in 2020 again shows, in more detail, which emotional manipulation attempts were most effective.<sup>23</sup> Unsurprisingly, many virus-related topics are among the most successful attack attempts. What is interesting, though, is that the COVID-19 issue can be exploited in different ways by the attackers.

### 1. Agenda for our meeting next week



Agenda for our corona meeting next week



### 2. Corona crisis delivery procedures - package 5380499815 not delivered



### 3. Account service: Please authenticate your account.



### 4. Server migration - please validate data



### 5. Important: Migration to Office 365



### 6. Safety note: New evacuation plan



### 7. Interesting candidate for you?



### 8. We are looking for candidates like you!



### 9. Urgent: Email quota used up



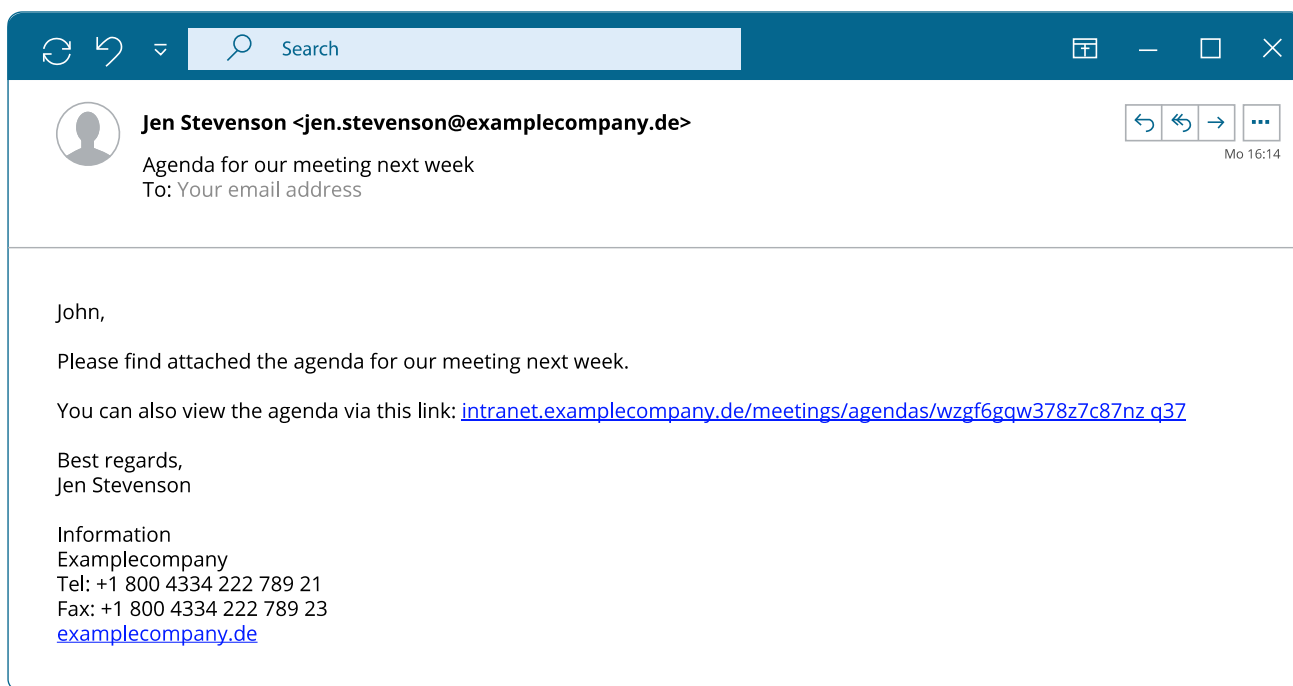
### 10. Important: Office 365 renewal



<sup>23</sup>Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.

## 1st place - 58.8% click rate

### Psychological tactics: routine concern / authority / curiosity



With a clickrate of 58.8 %, this subject line is simple, yet very effective. This social engineering scam is based on several psychological factors. Firstly, the issue is just routine. Many employees get emails like these in their inbox each week. This is particularly dangerous because it makes them less vigilant for potential phishing indicators.

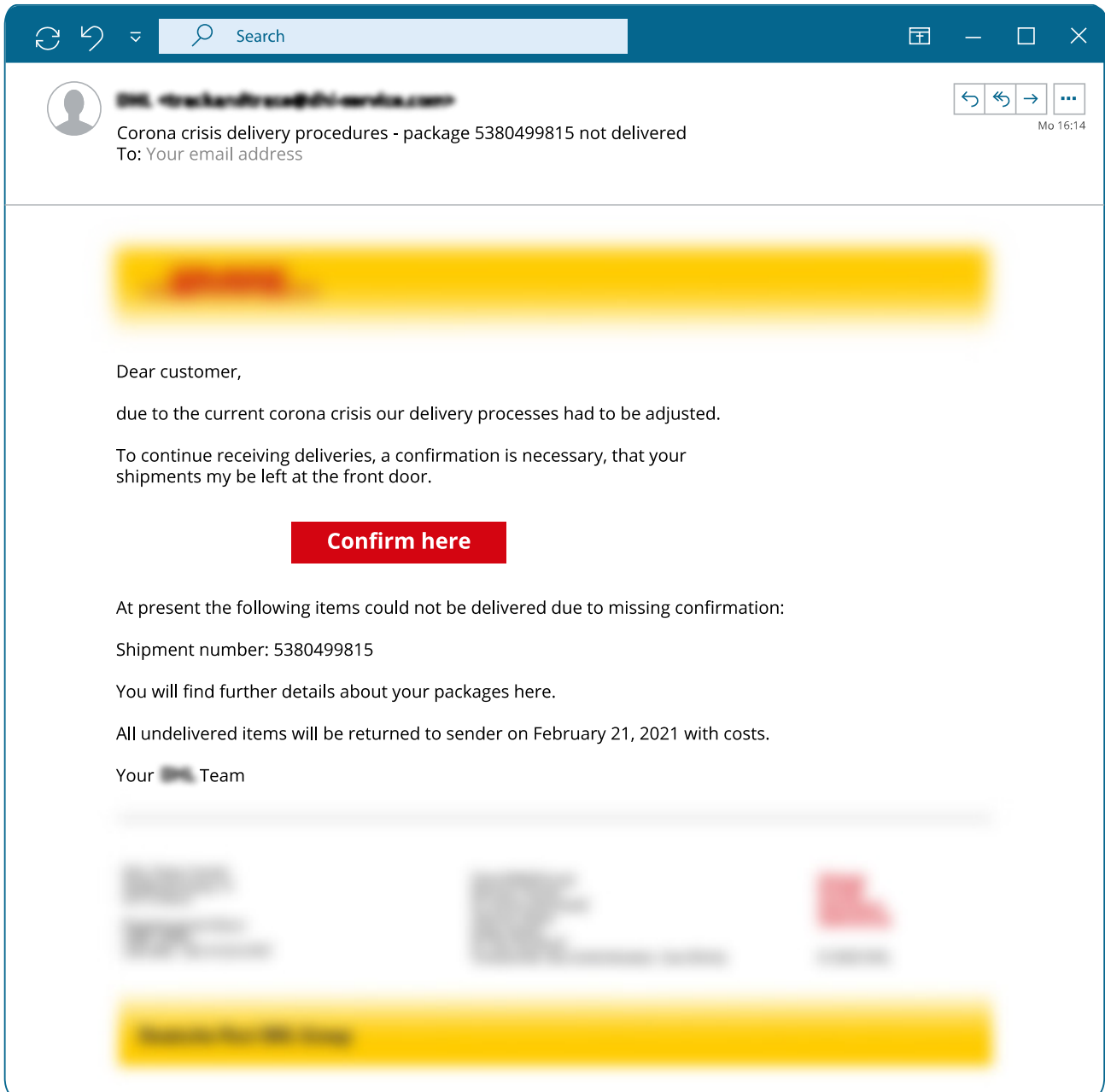
**Using the word „corona“ in the subject line increases the click rate by up to 50%.**

Moreover, cybercriminals are exploiting the company's natural dynamics. Because preparing for upcoming meetings is part of everyday staff obligations, there is a certain pressure to comply. Last but not least, curiosity also plays a role. The drastic change in work processes caused by COVID-19 has brought about an increased need for information. Overall, it is a dangerous combination that makes this subject line the most-clicked subject line of 2020.

Particularly fascinating is the fact that, while attackers developed very targeted attack attempts later in the pandemic, simple adjustments to existing phishing campaigns were also observed very rapidly in the very first phase of the outbreak. Given this background, it is particularly interesting that this email's click rate can be increased to 78.8% by inserting the word „Corona“ in the subject line.

## 2nd place - 50.7% click rate

### Psychological tactics: curiosity / fear





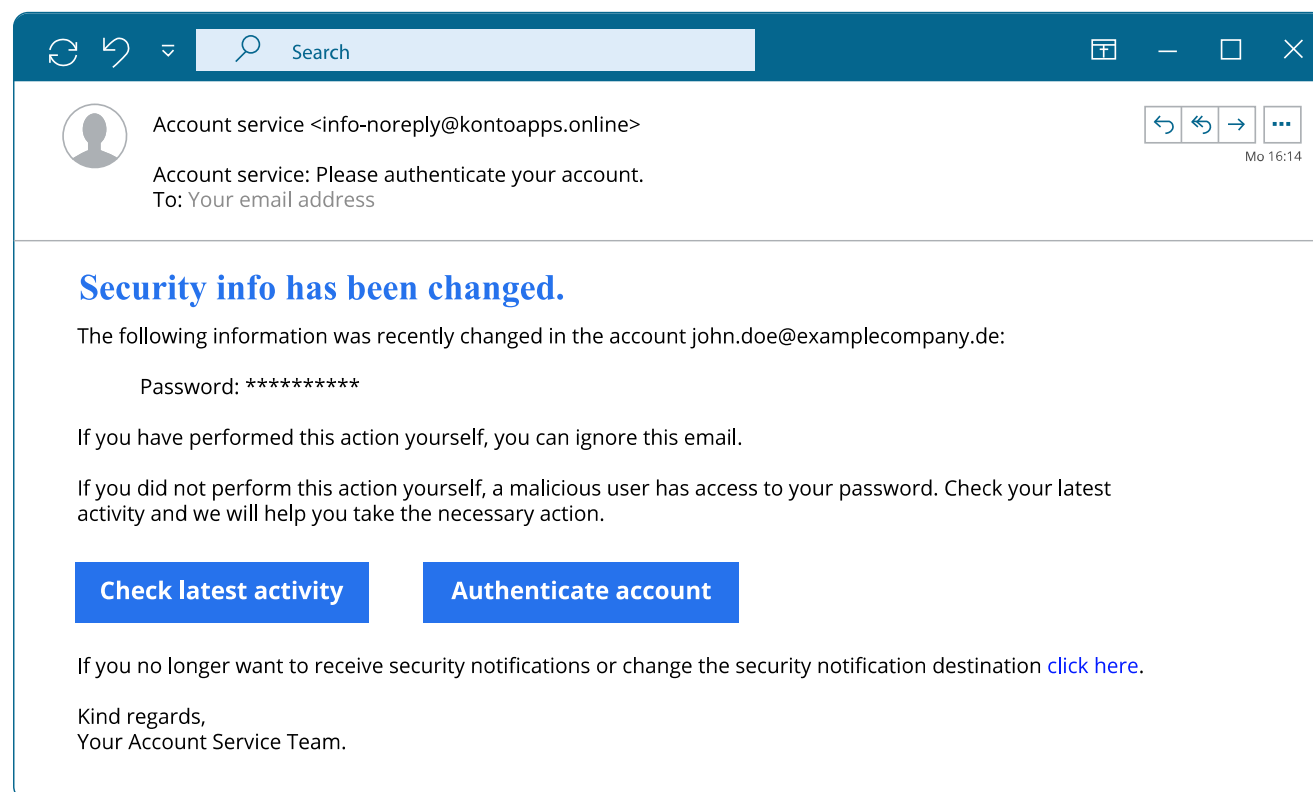
Here, the top topic of the virus is combined with human curiosity – a link that works very well with a 50.7% click rate. Due to worldwide lockdowns and closed stores, online orders rose sharply in the past year. Online payment service PayPal reported sales growth of over 20%, not least because of the pandemic.<sup>24</sup> Cybercriminals send corresponding phishing mails in order to benefit from the online shopping boom.

**This message will still apply in 2021: always be skeptical when emails related to COVID-19 arrive in your inbox.**

Another psychological factor that comes into play here is fear. In the stress of Christmas shopping, particularly, a missing gift for a family member can cause panic. So it is hardly surprising that people are exceptionally quick to carelessly click harmful links or file attachments. The hackers also know that subject lines like these still make many employees particularly curious. So this message will still apply in 2021: always be skeptical when emails related to COVID-19 arrive in your inbox.

### 3rd place - 45.4% click rate

#### Psychological tactics: urgency / uncertainty<sup>25</sup>



Account service <info-noreply@kontoapps.online>  
Account service: Please authenticate your account.  
To: Your email address

**Security info has been changed.**

The following information was recently changed in the account john.doe@examplecompany.de:

Password: \*\*\*\*\*

If you have performed this action yourself, you can ignore this email.

If you did not perform this action yourself, a malicious user has access to your password. Check your latest activity and we will help you take the necessary action.

[Check latest activity](#) [Authenticate account](#)

If you no longer want to receive security notifications or change the security notification destination [click here](#).

Kind regards,  
Your Account Service Team.

<sup>24</sup> Markets Insider (2021). PayPal shares climb as quarterly profits triple amid increasing use of digital payments.

<sup>25</sup> Email example slightly edited.

Due to the pandemic, many companies had to rapidly switch to working from home. Being more or less prepared, numerous new tools were suddenly being used, including Teams, Slack and Zoom. In particular, due to the rise in working from home, many companies migrated to providers who offer a wide range of collaboration options.

**In 2021, more attacks based on stolen credentials must be expected.**

Then phishing mails appeared that attacked and exploited the fact that many employees were still unfamiliar with the solutions and the user interface. „Account service: Please authenticate your account“ achieved the third highest click rate of 45.4%. For hackers, collaboration tools are an attractive way into companies' systems. Using so-called credential-theft attacks, which aim to obtain login data, they gain access to the tools so that they can also, often, access sensitive data. In 2021, more attacks based on stolen credentials must be expected.

Of particular interest is the fact that, for companies that had already introduced these tools, the click rate for a very similar email, one where the subject addressed the extension of software already in use, was far lower, at 25.2%. This once again shows how important it is that changes in work processes and tools should be accompanied by appropriate awareness-raising measures.

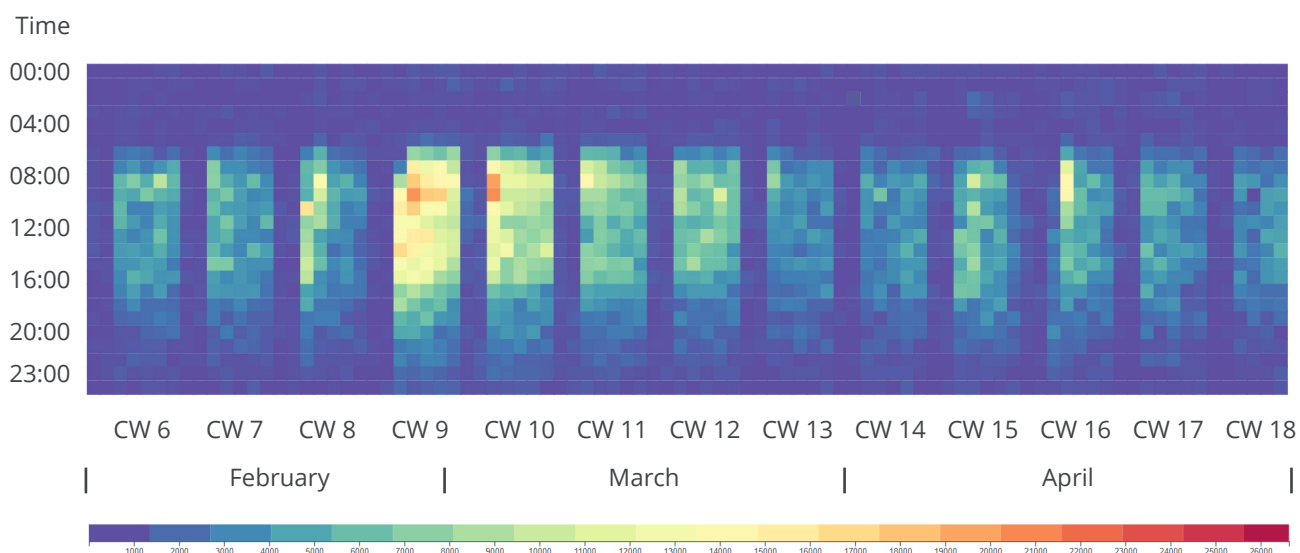


## The immediate impact of the COVID-19 pandemic: clicking was particularly common during lockdown

A look at the chronological dynamics strengthens the assumption that COVID-19 had an impact on the probability that phishing attacks would succeed. The click rate rose rapidly in March 2020 with the first lockdown in large parts of Europe, a phase in which we were particularly vulnerable.

This suggests that people's insecurity at that point influenced the way cyberthreats were dealt with, and that click behavior was particularly naive in that highly uncertain situation – especially in the new remote work setting. In addition, it was precisely in this phase that the phishing templates employed often contained direct references to Corona or changes in working conditions in the wake of the pandemic.

### Clicks on phishing mails between February and March 2020<sup>26</sup>



<sup>26</sup> Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.



## Preventive and reactive cyber security awareness – Cyber security as a joint project

**An interview with Prof. Michael Meier,  
Head of Cyber Security, Fraunhofer FKIE**



Prof. Dr. Michael Meier holds the chair for cyber security at the Institute for Computer Science at the University of Bonn and is head of the Cyber Security department at Fraunhofer FKIE. His research interests lie in the field of applied aspects of cyber security with a focus on attack, malware analysis and detection. Michael Meier is also a founding member and spokesman of the Security - Intrusion Detection and Response (SIDAR) special interest group of the Gesellschaft für Informatik eV, Co-Chair of the Detection of Intrusions & Malware and Vulnerability Assessment (DIMVA) international conference, and a board member of the Society for Data Protection and Data Security (GDD). He is co-founder of the security company Identeco.

**During the COVID-19 pandemic, there was a sharp increase in phishing campaigns. What do you think the reasons are?**

We were and are all being confronted with a lot of unusual things during the pandemic – this also brings with it great uncertainty in many areas. Some of our working methods have changed very rapidly, and there is little time to get used to new processes – they have to be reinvented on an ad hoc basis. It is precisely this uncertainty that phishers are taking advantage of. Because it makes it easier for them to lead IT users astray.

**The year 2020 yet again emphasized how important prevention and flexibility are – including in the cyber security sector. Which issues and trends, maybe even new research approaches, did you take away from last year?**

Many people have been using online services more and more since last year, some even for the first time. In addition to the general uncertainty, there are also new challenges in the area of identity data management, especially with passwords. At the same time, the general threat potential from identity theft, so-called credential-theft attacks, has increased significantly. Cybercriminals have quickly tracked down and exploited these newly emerging security loopholes.

We have worked extremely hard on this subject in recent years and, appropriately, were able to complete our EIDI (Effective Information after an Identity Theft) project in 2020. The aim was and is to restrict the impacts of such theft – for example if passwords for online services are stolen. New remote work settings have made the research results even more relevant. Because in combination with preventive measures such as employee awareness, you can reduce the enormously increased risk. Our spin-off, identeco.de, now offers appropriate security services to any interested company.

**In the “IT Security Awareness Penetration Testing” (ITS.APT) project, you have set yourself the goal of making cyber security awareness structurally measurable. Why is it so vital for organizations to keep an eye on staff awareness?**

Not only is it important that staff awareness is monitored, it should also be actively encouraged. On the one hand, this involves the preventive aspect of awareness, i.e., preventing poor behaviors so that phishing attack success rates are reduced. On the other hand, it is also important to grasp the reactive aspect – staff should help detect and report irregularities and thus limit the damage. If a link in a phishing mail is accidentally clicked, a quick response is worth its weight in gold. After all, many crew members are required to get a ship safely from A to B, not just someone to keep an eye on the radar.

**What role will the human factor continue to play in strengthening cyber security in the future?**

A big role. Because cyber security aims to protect socio-technical systems in which people interact with technology. This interaction requires freedoms – freedoms that can also be abused, as current cyberattacks clearly show. Our efforts to strengthen cyber security are constantly being confronted by new developments and technologies. With increasing digitization, we are also offering more targets. This fast-moving technical progress is not going to stop in the foreseeable future. This makes it all the more important to keep pace with developments by taking appropriate awareness measures in order to avoid incidents and to be able to respond quickly to them.

**Your research also deals indirectly with improving cyber security awareness. What advice can you give organizations?**

If I can offer organizations anything, it is this. Promote dialogue with your employees and train them on how to behave properly should a cyber incident occur. Awareness measures play a crucial role in this. Because they bring all the staff on board the ship in question. If the worst comes to the worst, everyone involved should also know how to report a potential incident, and to whom. When the experts contacted respond quickly, damage can be averted at an early stage.

## Click behavior in detail: What is the influence of demographics, sector, and time?

### **The Phish Test phishing simulation by SoSafe and Botfree records the general public's phishing awareness**

In the annual “Phish Test” public awareness campaign (dataset 3), which involved over 5,000 participants in 2020, SoSafe, together with the Botfree.eu initiative, records citizens' awareness of phishing. Whereas the SoSafe Platform is usually used by organizations and their employees, this annual initiative gives everyone the chance to put their cyber security awareness to the test. After registration, the participants receive realistic simulated phishing mails which they have to detect. If they fall for one of the mails, they are explained the respective tactics which were successful in that case. During the campaign, demographic factors are assessed as well and taken into account in the analysis.

The results provide little cause for reassurance – average awareness seems rather low. Around 31% of all participants clicked on at least one of the simulated emails that were sent for the survey. Almost every third social engineering attack would have been successful.

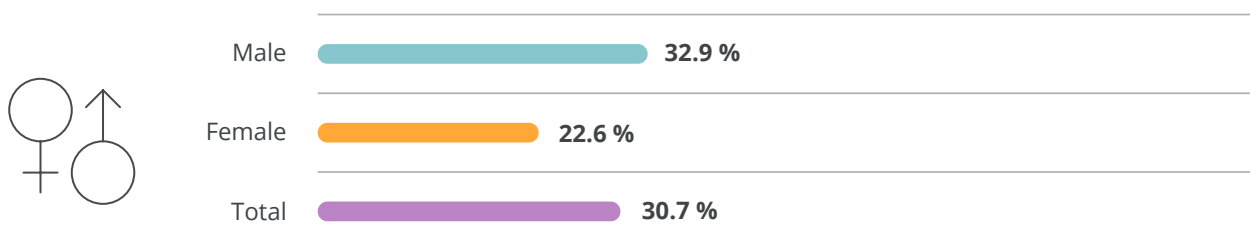
It is interesting that the analyses not only illustrate how difficult it is to identify the cybercriminals' phishing scams, but also that different demographic groups show varying levels of expertise in terms of their ability to spot those attacks.

## Phishing awareness based on demographic factors: Are digital natives more competent in terms of cyber security?

### Men click more often than women

Almost every third male participant (32.9%) clicked on at least one of the phishing mails. For women it was only 22.6%. In principle, however, men's interest in phishing was far greater than women's. 78% of the participants in the survey were men and 22% women.

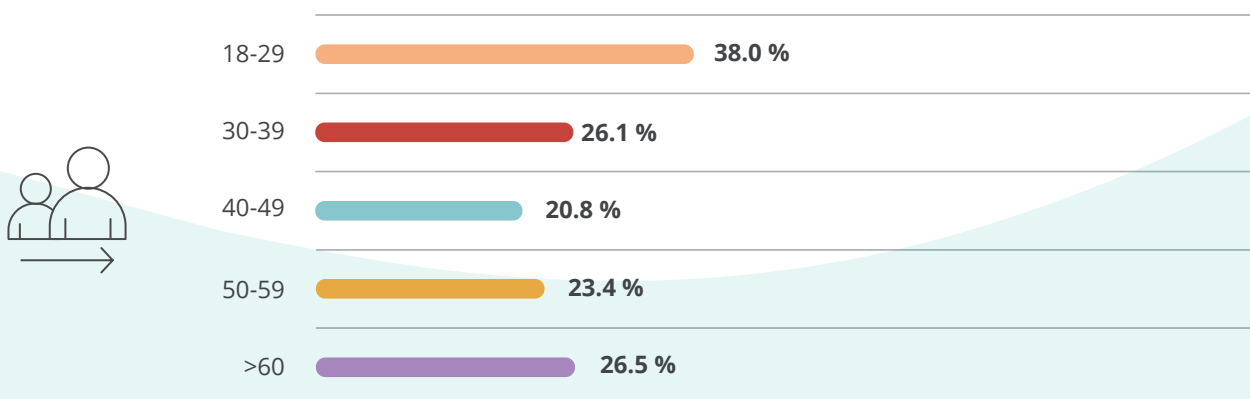
#### Click rates by gender



### Younger people click more often than older people

The assumption that younger users, or digital natives, have a significantly higher level of media skills and are therefore able to recognize phishing mails seems obvious. The simulation study showed exactly the opposite: The most vulnerable age group are 18 to 29 year olds, who had a click rate of 38%. All other age groups were significantly more skeptical about opening emails, with an average of only 25% clicking.

#### Click rates by age group

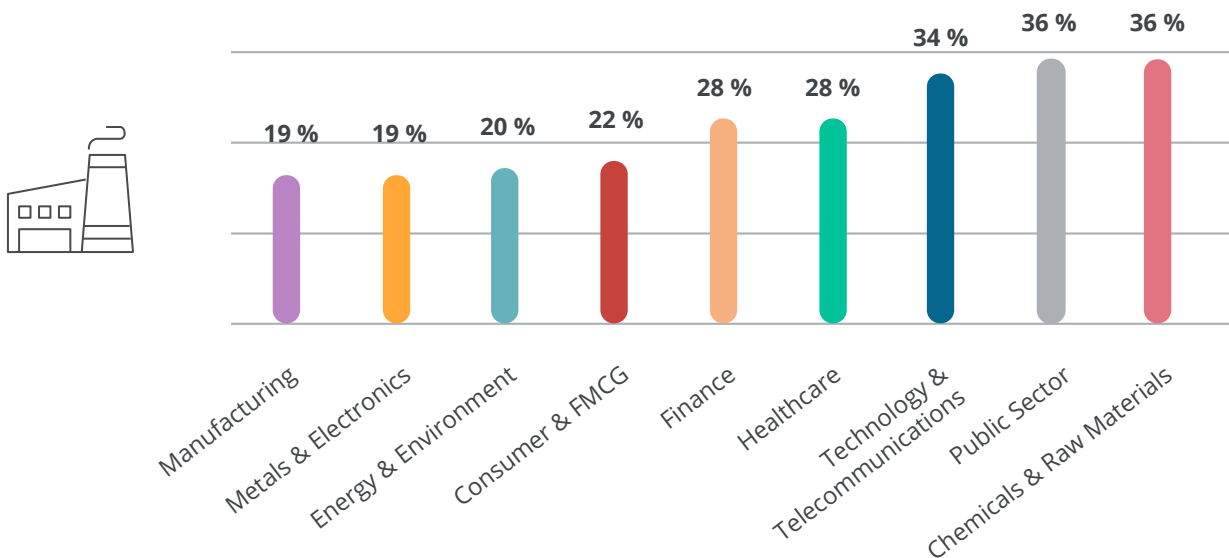


### Do specific sectors tend to have higher click rates?

In the context of the SoSafe Awareness Platform simulation data (dataset 2), we see interesting differences between different sectors. Organizations from the public sector in particular, including critical infrastructure organizations such as hospitals, seem to be the most vulnerable to phishing attacks with a click rate of 36% (the infobox on page 9 attempts to explain this). In the chemical industry, and in technology and telecommunications companies, on average, more than one in three employees click. In contrast, the average click rate in the manufacturing sector is only around 19%. One reason for this could be the lesser use of computer workstations and digital communication tools in this area. However, this would still mean that the risk of clicking on phishing mails would remain high, because it would also make employees less skilled in recognizing attacks.

Overall, a look at the level of click rates suggests that cyber security and, in particular, staff awareness in all sectors of the economy are not yet sufficiently prioritized.

### Click rates by industry<sup>27</sup>



<sup>27</sup> Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.



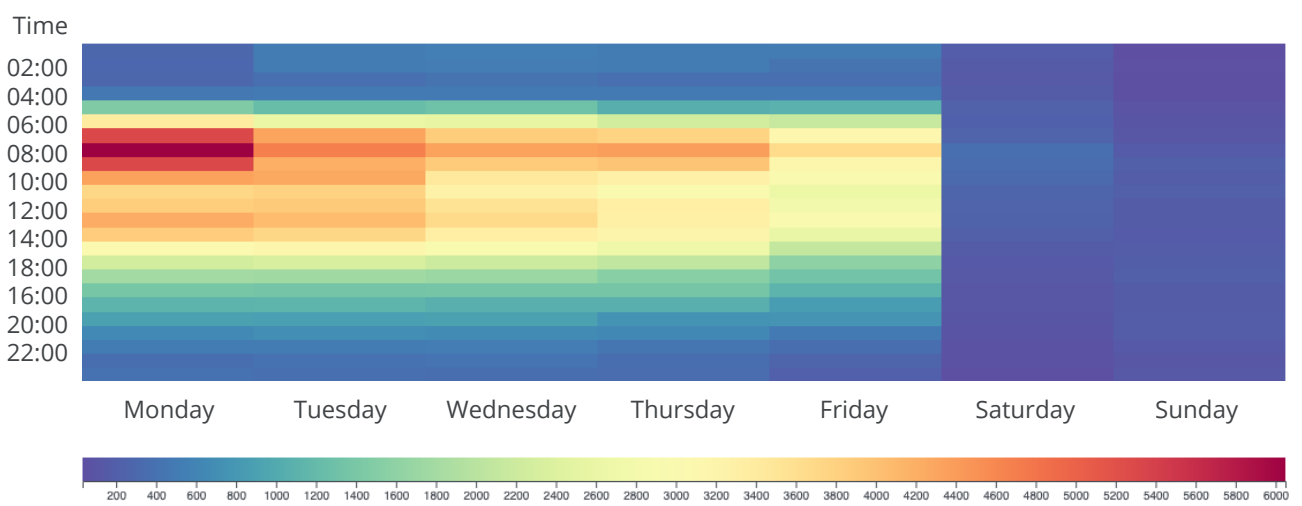
## The early bird clicks - click rates across week days and day times

The reaction data from the SoSafe Phishing Simulation (dataset 2) provide an interesting insight into the chronology of attack risk on a typical working day. The first coffee seems to have a crucial effect on click behavior. Many employees click on phishing mails before 8 a.m. on Mondays. But the risk of a successful attack seems particularly high in the morning during the rest of the week, too. There are also more clicks around lunch time than during the rest of the afternoon. Regardless, the risk seems to be higher at the beginning of the week than at the end. So it seems that at these times, employees in organizations are indeed more careless about dealing with cyberthreats.

**Employees click more often in the morning than in the afternoon, and more often at the beginning of the week.**

On the one hand, this could be due to the fact that in the morning and at noon there is often a renewed flood of emails in the mailbox waiting to be opened and employees want to get a quick overview of to-do's and news. Potential phishing mails are then quick to get lost in the crowd. On the other hand, employees could be less vigilant at these times because they have not yet immersed themselves in their current work, or they are still, or already, thinking about other things. One approach to raising awareness can, and should, therefore be to support employees in processing their emails in such a way that the risk of careless clicks is reduced.

### Clicks on phishing mails in an average week<sup>28</sup>



<sup>28</sup> Data base: 1.4 million simulated phishing attacks from the SoSafe Awareness Platform.

## DEKRA DIGITAL

*innovating safety*

# The remote work challenge – Cyber security in times of increasing digitization

An interview with Dr. Kerim Galal,  
Managing Director at DEKRA DIGITAL



Dr. Kerim Galal is Managing Director at DEKRA DIGITAL and Executive Vice President Innovation & Digitalization at DEKRA, and responsible for future issues such as strategy, innovation and digitalization. Together with partners and start-ups, DEKRA DIGITAL works on technologies such as IoT, cyber security and artificial intelligence. Before joining DEKRA, he worked for McKinsey & Company and did his doctorate at EBS in Oestrich-Winkel.

**To what extent has the last year brought change in the area of digitization, e.g., in how people work together?**

The corona pandemic has fundamentally changed the way we work together at an unprecedented speed, particularly through remote working. That was also something new for us at DEKRA DIGITAL. But as we had a good IT infrastructure and years of working with collaboration platforms such as Slack and Teams, we quickly adapted.

Working from home has also presented many other companies with major digitization challenges, especially in the area of cyber security. At home, for example, there is a great temptation to mix company systems and privately used solutions. Moving outside of the company's secure IT infrastructure is particularly dangerous for cyber security.

**What connection do you see between digitization and cyber security?**

All areas of life are increasingly being digitized. Whether we drive to the office, use a voice assistant or open our laptop, data and the associated risks are omnipresent. This networking has many advantages, but it also presents a target for hackers and clearly impacts the cyber security of companies and individuals.

Our company has worked in the security sector for almost 100 years and our mission is to protect people at work, while traveling, and at home. And we want to transfer this to the digital arena. And that is why DEKRA DIGITAL is bringing experts together in the "Cyber Security Hub". We bundle expertise from various areas in order to continue to guarantee security in an increasingly digitized world – this also includes cyber security.

**DEKRA is a leader in both the field of safety certification and staff training - in the year to come, what challenges do you see at the interface between security and the human factor?**

The new remote work setting will continue to play a key role at this interface in the coming year. For employees, compliance with certain minimum cyber security standards is essential to protect themselves and the company.

Even the home workplace can be problematic. The coffee table, where the rest of the family plays or watches TV, lacks not only basic ergonomic requirements, but also cyber security requirements.

So, particularly in this current situation, companies should not only define guidelines and introduce technical security measures, but also sensitize their staff to the increase in cyber risks – think „social engineering“ – and refresh the relevant cyber security training.

## **Social engineering trends 2021: Cybercriminals continue to upgrade**

2020 was marked by the outbreak of the pandemic and a clear worsening of the threat situation – especially with regard to the human factor. It was a difficult year for organizations and security specialists – but a successful year for attackers and ransomware groups. Unfortunately, there is no cause for relaxation. In the future, we can expect an increase both in the number of attacks and new types of attacks. Because innovation has become an integral part of a highly professionalized hacker industry.

So what cyberattack tactics and methods do organizations need to prepare for in 2021? Our experts, customers and partners see the following trends:



### New work - new channels

By switching to working from home, collaboration tools such as Teams and Zoom were increasingly deployed in many organizations. According to a survey by auditing and consulting company Deloitte, two out of three employees in Europe believe that they will work more often, or even permanently, from home, even after the pandemic.<sup>29</sup> For attackers, the collaboration tools involved in this are an attractive way into companies' systems. In 2020, for example, numerous phishing campaigns attempted to steal access data for the relevant tools using invitation emails followed by login screens. The problem is that many employees are still unfamiliar with cloud solutions and feel relatively secure within these channels – in-house cloud chat tools are perceived as a protected space.

So it is not surprising that credential theft attacks aimed at obtaining access data for these tools have increased significantly. As these tools will become more and more important, we can expect an increase in such attacks.



### Double extortion on the rise

A new generation of ransomware was identified last year which will be a key factor in future threats too. The ransomware groups have names such as „Sodinokibi“ or „Egregor“ and work on the „double extortion“ principle. If the ransom is not paid, data may be made public – with costly results for victims.

So conventional incident response strategies and backups are no longer enough to protect against ransom payments. The Egregor Group first became active around September 2020 and now has well-known victims such as Barnes & Noble, Ubisoft, Crytek and Randstad. The attackers set off a new level of escalation, at the same time strengthening their negotiating position. So we can expect other groups to adopt the principle before long. This makes prevention all the more important.

<sup>29</sup> Deloitte (2020). May the workforce be with you - The voice of the European workforce 2020.



### AI-based social engineering is becoming more widespread

Back in 2019, at the BSI security congress, a warning was issued of a possible AI-based „voice phishing bot to pre-legitimize a malicious email“.<sup>30</sup> It described a theoretical attack that could use artificial intelligence to imitate a line manager's voice. The first actual case was announced just months later. An employee at a British energy supplier was called by the alleged CEO of the German parent company and asked to transfer money to a Hungarian bank account. The criminal stole 220,000 euros.

It can be assumed that this call was made using the aforementioned, trained AI model. While such attacks are still the exception, the proportionate use of AI in the social engineering area will continue to increase, for example to generate written text. The reason is that the models are becoming easier to train, and successful cases increase hackers' acceptance of the new technology.



### Phishing is here to stay

Classic tactics such as phishing and business email compromise will continue to be cybercriminals' core business. And the new work reality of many employees makes such tactics even more attractive. Because the intentions and the risk of potentially harmful emails are more difficult to screen in the remote setting.

The office grapevine offers protection, as was also shown by a SoSafe analysis (see p. 24): With decentralized working, the click rate on simulated attacks is three times greater than that of employees in the office. It is more difficult to validate suspicious messages if interaction is reduced to just key meetings and chat messages. This will continue to play into the hands of hackers and keep the number of attacks at a very high level.

<sup>30</sup> Hellemann, Niklas (2021). Playing with fear - Success factors of novel social engineering attacks during the COVID-19 pandemic. Journal of the 17th German Security Congress by German Federal Office for Information Security (BSI).

## Conclusion & recommendations: How do organizations minimize their human risk?

The analyses in this report show that people and cyber security are closely linked. This insight is extremely important, especially at a time that is characterized by general uncertainty and an intensified cyberthreat situation. Because if current attack tactics increasingly focus on manipulating human emotions, and technical security measures alone are no longer sufficient, it is up to organizations to stabilize their “human firewall” in the long term. Employees must be actively involved in strengthening cyber security.

But how, specifically, can organizations now counter the growing human risk, and make employees security factors rather than risk factors?



### Building cyber resilience

Give your staff resources that promote risk awareness and, thus, a company-wide cyber resilience culture. Give your staff the opportunity to acquire skills in the cyber security area through a variety of training measures. All staff, not just IT specialists, must be thought of as part of a closed line of defense against cyberattacks.



### Shape awareness holistically

You can only develop real competence in your employees by combining a variety of training measures. Based on pedagogical and psychological findings, the combination of phishing simulation, nano-learning units and storytelling creates a sustainable, effective learning context tailored to your employees' interests.



### Train flexibly and continuously

As the year 2020 once again impressively demonstrated, cybercriminals are quick to deploy new ransomware that is always based on current events. Awareness measures must also adapt flexibly and immediately address new tactics. The rapid change in cybercrime also shows that isolated learning units are only effective in the short term, so ongoing training is essential.



### Choose a GDPR-compliant provider

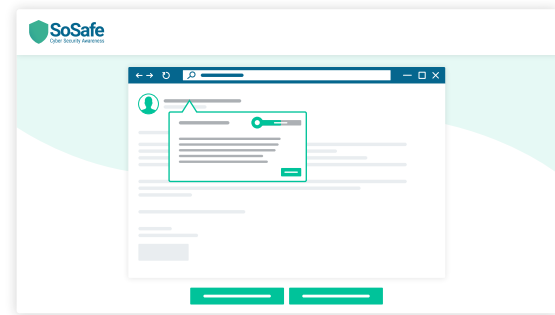
GDPR standards do not only apply if your company is located in but also if it has employees within the EU. Create absolute legal certainty within your company by choosing EU providers with data processing on EU servers. This is the only way you can ensure, and guarantee, the protection of your employees' sensitive data in a 100% GDPR compliant manner.

## About SoSafe

SoSafe Cyber Security Awareness provides an interactive training platform for cyber security and data privacy and is one of the market leaders in Europe. The 100-strong team consists of experts from diverse disciplines – from IT to psychology, and from education to communication design. The SoSafe Awareness Platform uses modern, modular e-learning and ongoing phishing simulations to raise awareness and train employees in dealing with all types of cyberthreats. The training is interactive, motivating and 100% compliant with data protection regulations like the GDPR.

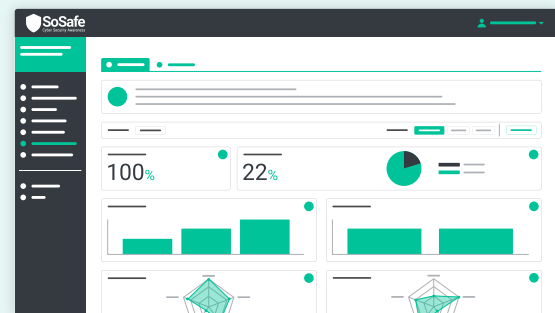


**Modular E-Learning**



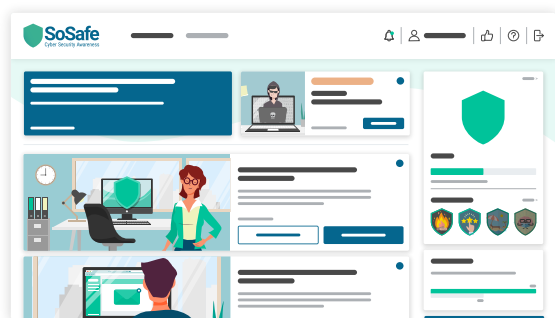
**Continuous Phishing Simulation**

With easy-to-understand KPIs and differentiated analytics, human risk as well as the effectiveness of the cyber security training measures are, at last, measurable and visible. Numerous multinational organizations from a wide range of sectors put their trust in the training effect achieved through the SoSafe Awareness Platform, including pharmaceutical corporation Merck, energy provider Vattenfall and global food discounter Aldi.



**Differentiated Analytics**



**E-Learning Platform****Branding Engine**

The SoSafe Awareness Platform is designed to minimize administration efforts for IT managers and runs employee trainings completely automatically while offering individual customization options at the same time. The platform is a cloud-based service and does not need to be integrated into an existing system. A standalone cloud LMS (learning management system) allows you to get started immediately, with no implementation. For companies with their own LMS, SoSafe is the only provider to offer constantly updated, bespoke content through what is known as SCORM streaming.



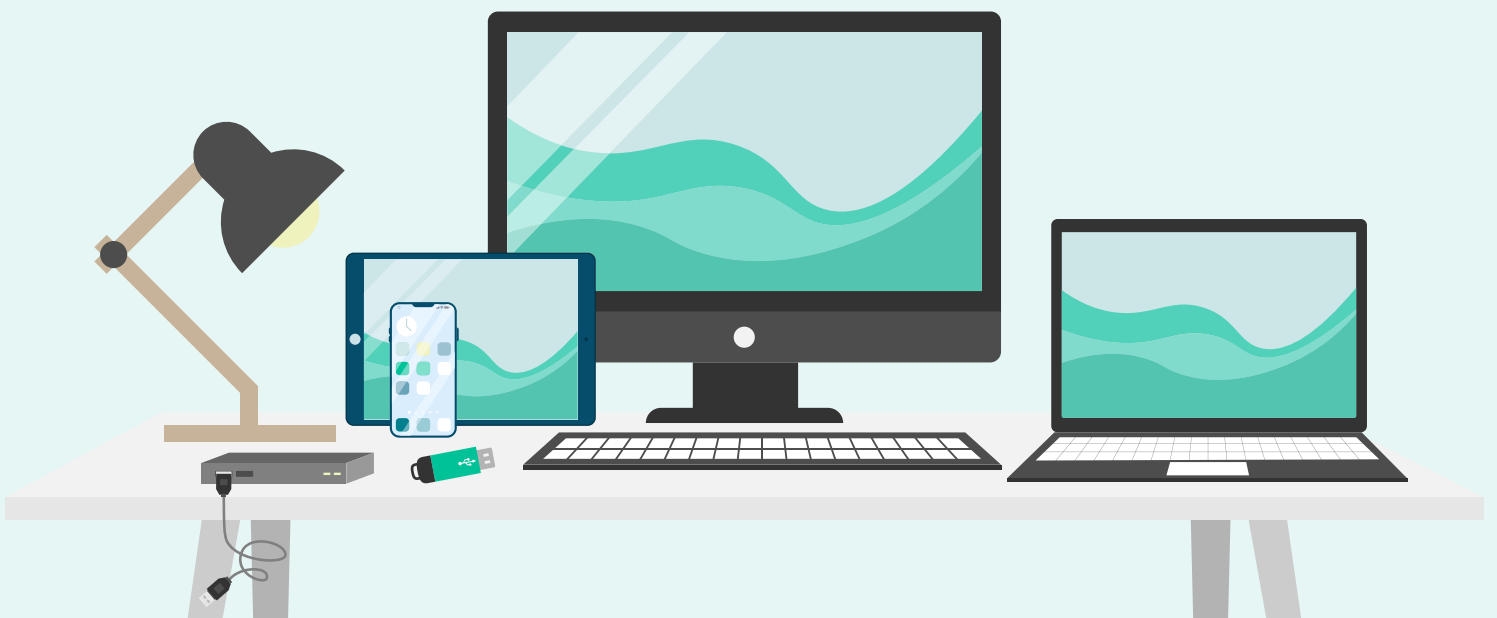
The training itself is based on the latest educational and behavioral psychology findings: Instead of monolithic and long training sessions, the content is highly modular, gamified and based on storytelling in line with current media perception preferences.



This hypermodularity enables users to take individual learning paths which are adapted to their level of expertise, making the learning experience both motivating and sustainable. The SoSafe Customization Engine additionally allows for the learning platform's content and look to be adjusted to organizations' internal policies as well as branding. The Awareness Platform is available in more than 25 languages catering to the needs of internationally operating organizations with employees in multiple countries.

Through the SoSafe Analytics Dashboard, the solution also enables decision-makers to differentiate and anonymously evaluate performance. Technical and psychological KPIs give organizations information about the level of their human risk, how effective their awareness measures are and, consequently, how employees can be sensitized with even greater precision.

SoSafe runs on certified and highly secured servers within the European Union. Data is stored and processed in full compliance with the GDPR. The special compliance dashboard also allows organizations to output the awareness status within the framework of existing compliance frameworks (e.g. ISO-27001), thus providing relevant evidence in a time-saving manner.



## Authors

Dr. Niklas Hellemann, SoSafe Cyber Security Awareness  
Ann-Kathrin Krane, SoSafe Cyber Security Awareness  
Friederike Kneip, SoSafe Cyber Security Awareness

## Interview partners

Bert Skaletski, Chief Information Security Officer, Merck KGaA  
Prof. Dr. Michael Meier, Chair for Cyber Security at the University of Bonn,  
Head of Cyber Security at Fraunhofer FKIE  
Dr. Kerim Galal, Managing Director at DEKRA DIGITAL, Executive Vice  
President Innovation & Digitalization at DEKRA

## Layout & Design

Clara Wördenweber, SoSafe Cyber Security Awareness  
Annalena Eckertz, SoSafe Cyber Security Awareness

## Contact

Email: [info@sosafe.de](mailto:info@sosafe.de)  
Telephone: +49 221 6508 3800

## Further information

[www.sosafe-awareness.com](http://www.sosafe-awareness.com)



SoSafe Cyber Security Awareness  
Ehrenfeldguertel 76, 50823 Cologne, Germany  
[www.sosafe-awareness.com](http://www.sosafe-awareness.com) | [info@sosafe.de](mailto:info@sosafe.de)

SoSafe grants everyone the free, spatially and temporally unlimited, non-exclusive right to use, reproduce and distribute the work or parts thereof, both for private and for commercial purposes. Changes or modifications to the work are not permitted unless they are technically necessary to enable the aforementioned uses. This right is subject to the condition that SoSafe GmbH authorship and, especially where extracts are used, this work is indicated as the source under its title. Where possible and practical, the URL at which SoSafe provides access to the work should also be given.

