Press release
SoSafe GmbH • Ehrenfeldguertel 76 • 50823 Cologne
Cologne, March 24, 2021

Human Risk Review 2021: COVID-19 and remote work lead to higher success in cyberattacks

SoSafe report reveals the most successful gateways for cybercriminals in organizations in the pandemic year 2020

SoSafe Cyber Security Awareness, provider of an interactive training platform for cyber security and one of the market leaders in awareness building in the DACH countries (Germany, Austria, Switzerland), has published its "Human Risk Review 2021". The results of the annual report show: During the COVID-19 pandemic, employees have been in the focus of cyberattacks and therefore play a significant role in protecting organizations from these threats. In addition to a general look at the cyberthreat landscape, the report particularly highlights the human factor and the technical and psychological tactics cybercriminals use to provoke clicks on phishing mails. For the first time, the report powerfully shows that the likelihood of cyberattacks succeeding has increased during the pandemic and in times of remote working. The data is based on more than 1.4 million data points from the SoSafe Awareness Platform, malware analyses by AV-TEST, an awareness study with more than 5,000 participants, and a survey of more than 100 cyber security experts.

On the basis of exclusive response data, the SoSafe Human Risk Review illustrates what various reports have already indicated in recent months: The threat situation has been further exacerbated by the COVID-19 pandemic. Social hacking, which is designed to provoke clicks on phishing mails by manipulating emotions, is becoming increasingly popular among cybercriminals in these uncertain times. The majority of cyber security experts surveyed believe that the probability of attacks being successful has increased during the crisis. More than 4 in 10 have perceived an increase in cyberattacks. The analysis of the SoSafe reaction data solidifies these assumptions: The temporal connection to and thematic integration of the coronavirus has made phishing attacks more successful. The SoSafe Human Risk Review also provides unprecedented insights into the technical and psychological mechanisms underlying cyberattacks, such as which vectors criminals used last year and which they were particularly successful with.

Key findings at a glance:

- **COVID-19 pandemic makes social engineering attacks more successful - up to 4 in 5 recipients click on Corona-related phishing mails:** During the first lockdown, a rapid increase in ransomware types was observed. The SoSafe analyses show that the probability of success of such attacks also increased at the same time - the click rate on phishing mails was significantly higher during the lockdown phases. Phishing mails referring to the COVID-19 pandemic are particularly promising for cybercriminals. While the average click rate is 29%, phishing mails with the word "Corona" in the subject line provoke click rates of up to 78.8%.
- **The introduction of new collaboration tools makes employees more vulnerable to phishing attacks:** The shift to remote work also offers increased potential for attack. Half of all employees click on phishing mails sent in the context of introducing remote tools such as Microsoft Teams or Slack.
- **The "office grapevine" protects - detecting phishing mails is more difficult in decentralized organizations:** As the SoSafe analyses reveal, when working remotely the click rate on phishing mails is generally higher than in the office - in decentralized organizations click rates are three times higher than in centralized organizations.
- **Digital natives click on phishing mails most often:** Contrary to the assumption that younger users would have higher digital literacy, SoSafe shows just the opposite in a separate study of over 5,000 citizens. With an average click rate of 38%, 18- to 29-year-olds are well ahead of other age groups, who clicked on only one in four phishing mails.

The human factor and cyber security are growing closer together

The review also gives an outlook on future developments. The most important hypothesis: Social engineering and cyberattacks that take advantage of new work models such as remote working will continue to have a decisive influence on cyber security in organizations and should therefore be the focus of respective security and training measures. A positive outlook: As many as 6 out of 10 cyber security experts surveyed are planning to expand their awareness measures in the future. Employees play a decisive role when it comes to cyber security. With the Human Risk Review 2021, SoSafe provides a comprehensive overview of the current threat landscape around the human factor and provides organizations with initial guidance on how to minimize their human risk.

You can find the full report here: https://sosafe-awareness.com/human-risk-review-2021/

***

About SoSafe

The SoSafe awareness platform sensitizes and trains employees in dealing with the topics of cyber security and data protection. Phishing simulations and interactive e-learnings teach employees effectively and sustainably what to pay particular attention to, for example, when using emails, passwords, or social media. The employer receives differentiated reporting and can finally make awareness building measurable - completely GDPR-compliant of course.

If you have any questions, feel free to contact Mr Florestan Peters via press@sosafe.de