proofpoint

Europe and the Middle East

REPORT

2024 State of the Phish

Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity

proofpoint.com

INTRODUCTION

Cybersecurity headlines often focus on the clever social engineering and zero-day vulnerabilities used by attackers. But cybercriminals don't always have to try that hard. According to this year's State of the Phish survey, 71% of working adults admitted to taking a risky action, such as reusing or sharing a password, clicking on links from unknown senders, or giving credentials to an untrustworthy source. And 96% of them did so knowing that they were taking a risk. People are a key part of any good defence, but they can also be the most vulnerable. They may make mistakes, fall for scams or simply ignore security best practices.

This year's global report is based on a survey of 7,500 end users and 1,050 security professionals, conducted across 15 countries—including eight in Europe and the Middle East. It also includes Proofpoint data derived from our products and threat research, as well as findings from 183 million simulated phishing messages sent by our customers over a 12-month period and more than 24 million emails reported by our customers' end users over the same period. And for the second year running, we've also compiled three regional summaries pointing out local nuances and variations.

Most users in Europe and the Middle East say they aren't sure if security is their responsibility or someone else's. And this lack of clarity can have significant consequences. Our data shows stark correlations between attitudes and outcomes across the region.

Every day, users in the region make choices between security and convenience. And this regional summary shows that most of the time they favor the latter. In the following pages we'll take a closer look at the attitudes of both security professionals and end users, as well as some key threat trends. And we'll end with suggestions that should help people change their behaviour and start putting security first.

TABLE OF CONTENTS

Key Findings: Global

Over 1 million

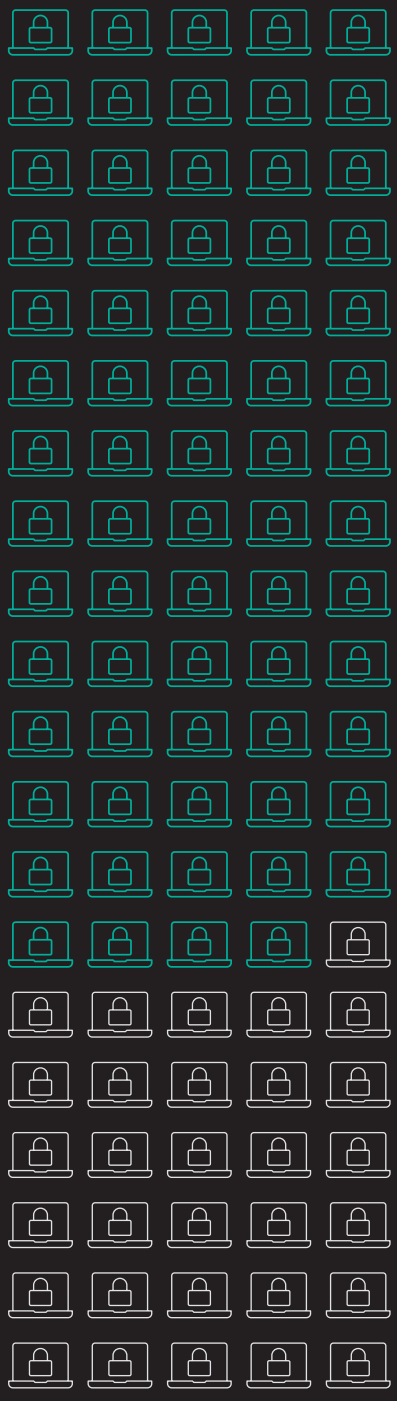
attacks are launched with MFA-bypass framework EvilProxy every month, but 89% of security professionals still believe MFA provides complete protection against account takeover.

of users took a risky action

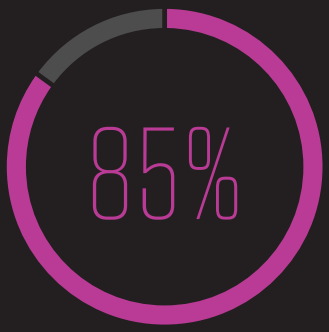
of them knew they were doing something risky

66 million

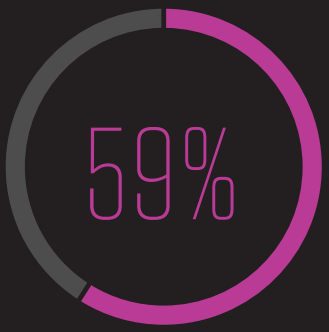
BEC attacks were detected and blocked on average per month by Proofpoint.



69% of organizations were infected by ransomware.



of security professionals said that most employees know they are responsible for security, but



of users either weren't sure or claimed that they're not responsible at all.

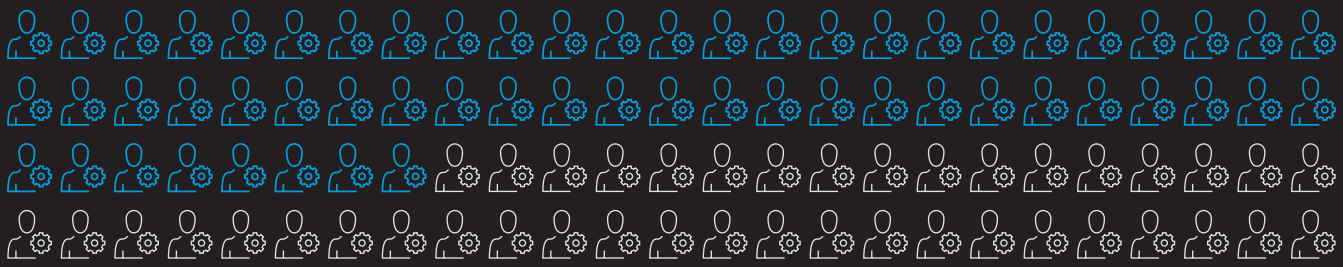
10 million

TOAD messages are sent every month.

Microsoft continues to be the most abused brand, with

68 million

malicious messages associated with the brand or its products.



58% of users who took risky actions engaged in behavior that would have made them vulnerable to common social engineering tactics.

Spotlight on Europe and the Middle East

This year's State of the Phish surveyed 7500 users and 1050 security professionals in 15 countries. This summary focuses on:

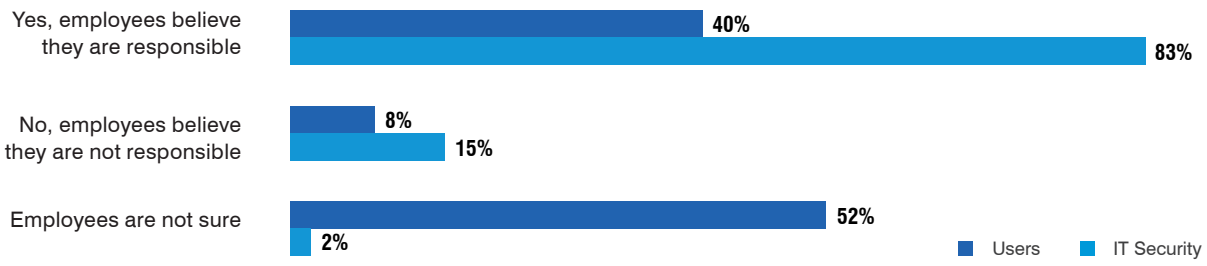
- France
- Germany
- Italy
- Netherlands
- Spain
- Sweden
- United Kingdom
- United Arab Emirates

With so many languages, cultures and levels of digital maturity, there were significant variations between regions, and between the eight countries covered by this summary. The region is diverse, geographically, culturally and economically. But in at least one respect the region shows some uniformity. Users in the region were more likely to admit to taking a risky action than the global average (76% vs 71%). Yet the number of people who said they knew the action they were taking carried risk was within 1 percentage point of the global figure (95%).

At country level, 86% of respondents from UAE said they took a risky action. This was higher than any other country in our survey. UAE organisations also reported the highest incidence of successful spear phishing attacks, showing a strong link between user awareness and security performance. But interestingly, UAE still had the highest number of users who said that they consider security to be their responsibility (62% vs 41% global average).

Users from Sweden were the least likely to say that security is their responsibility. This aligns with the higher-than-average level of users taking risky actions (82%) in Sweden.

Security Responsibility (Europe and the Middle East)

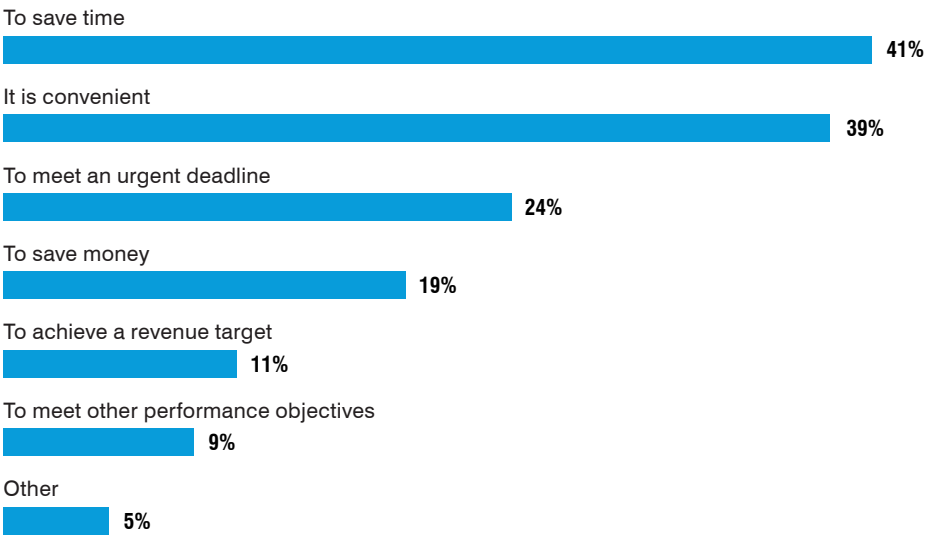


Security professionals in the region rated password re-use as the riskiest behaviour. Unfortunately, password re-use was the second most common behaviour among end users. But there's some good news for security teams: accessing inappropriate websites was the only other action from their top five to also appear among the most common user behaviours.

Rank	Risky Behaviour (Ranked by Sec Pros)	Risky Behaviour (Conducted by Users)
1	Reuse or share password	Use work device for personal activities
2	Click on links or download attachments from someone I don't know	Reuse or share password
3	Upload sensitive data to unproven 3rd party cloud	Connect without using VPN at a public place
4	Give credentials to untrustworthy source hook enabled)	Respond to a message (email or SMS text) from someone I don't know
5	Access inappropriate website	Access inappropriate website

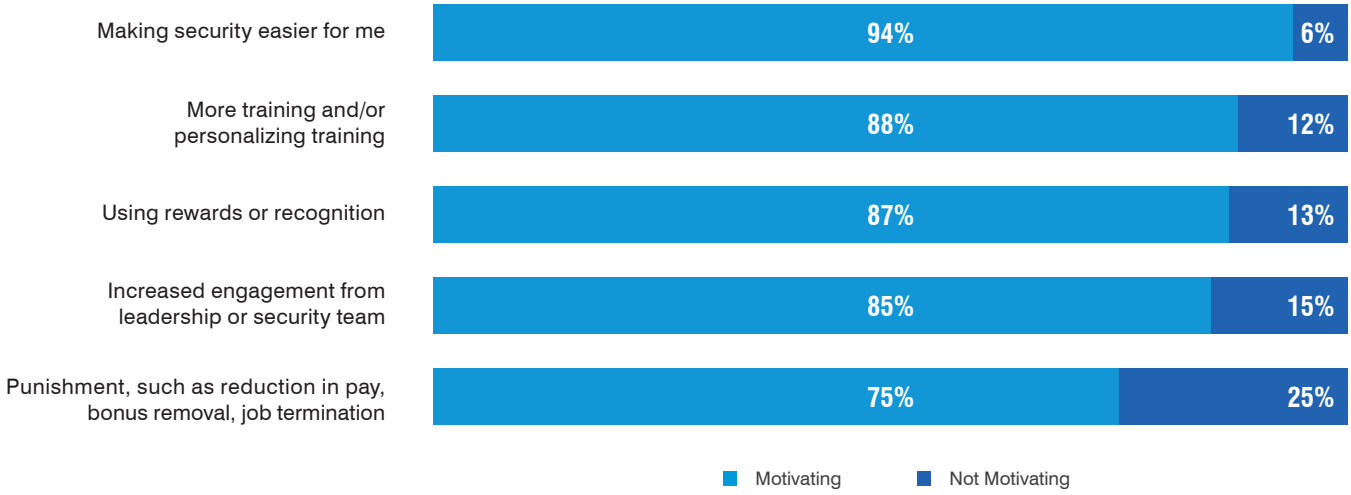
But why do users take risky actions? The most common answer was "to save time," closely followed by "convenience." In the United Kingdom, the top two responses swapped places, with more U.K. respondents citing convenience than anyone else.

Why Users Take Risky Actions



Users in Europe and the Middle East are clear about why they take risky actions. But what would motivate them to prioritise security? As with our global results, the majority cited making security easier as the most effective motivator, and punishment as the least motivating.

Make Security a Priority for Users



78%

of German organisations experienced TOAD attacks, but only

21%

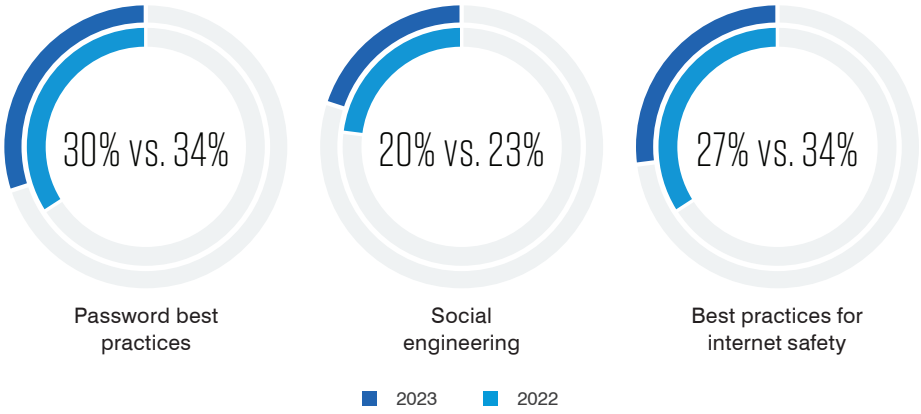
train on the technique

Opportunities for Improvement

95% of organisations in the region already use threat intelligence to inform their security awareness training programs. But there are significant gaps. While most organisations reported being targeted by telephone-oriented attack delivery (TOAD), less than a third train on this tactic. In Germany, 78% of organisations experienced TOAD attacks, but only 21% train on the technique—one of the largest gulfs between daily attacks and training topics.

Overall, more time is being devoted to security awareness training across the region. Spain saw the largest increase, with a 120% rise in organisations spending three or more hours per year.

However, the number of organisations training on essential topics seems to be declining:



These are all critical security basics. And if fewer users know how to set secure passwords, avoid common lures and surf the web safely, cybercriminals will surely take advantage.

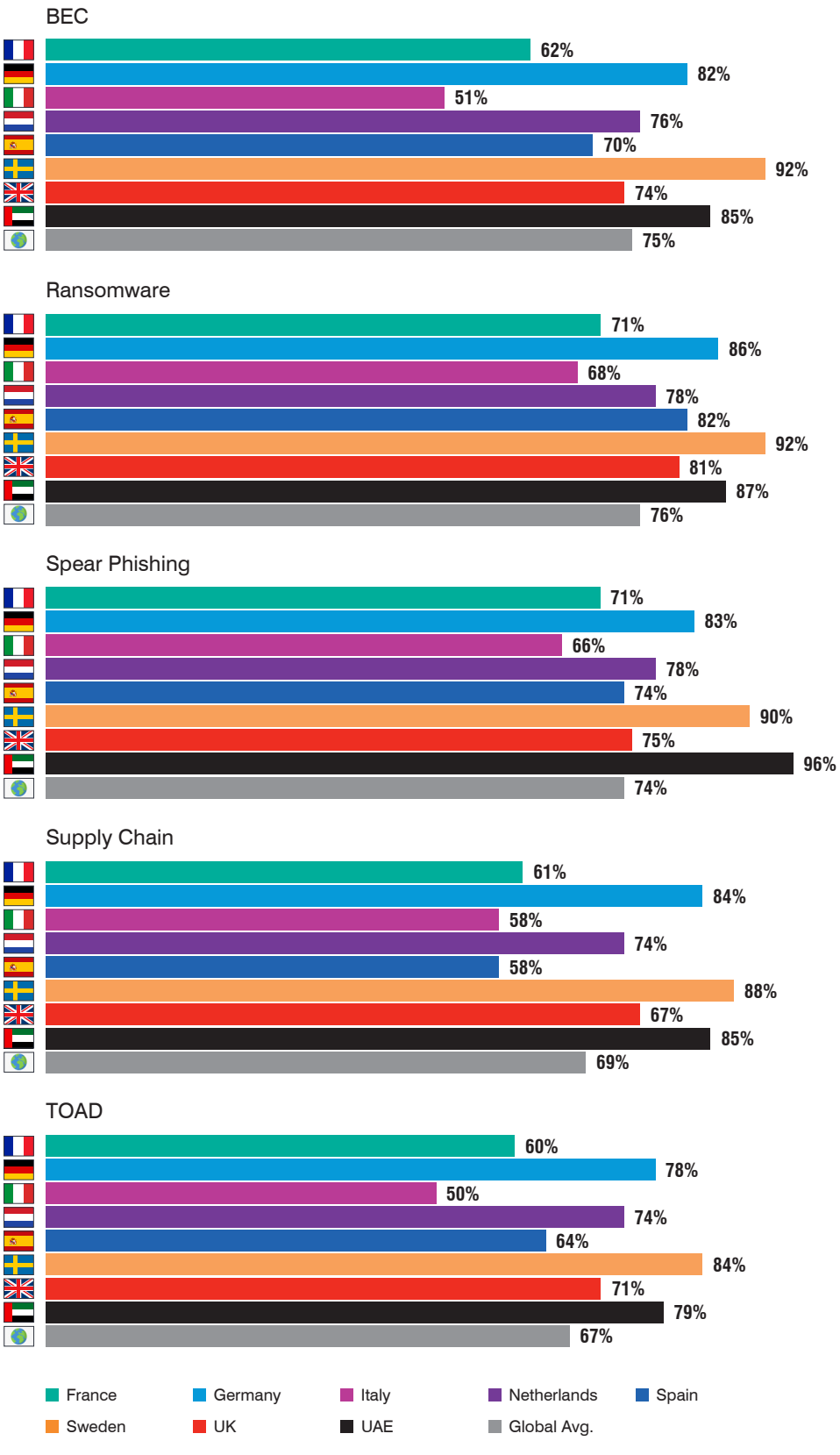
Europe and the Middle East Threat Landscape

The regional threat landscape largely followed global trends last year. Business email compromise fell overall, but non-English-speaking countries saw an increase. This could be linked to the rise of generative AI tools such as ChatGPT, which can be used to write convincing email lures in multiple languages. Similar trends were visible in other non-English-speaking countries worldwide. Overall, 75% of organisations saw at least one successful phishing attack, down from 88% in 2022.

The region saw slightly more TOAD attacks—70% vs the global average of 67%. 84% of Swedish organisations experienced a TOAD attack—the highest level in the region.

As with our global findings, organisations in Europe and the Middle East reported an increase in negative consequences from successful attacks. Financial penalties increased by 122%. This was slightly lower than the global figure, which may point to GDPR fines already being levied in previous years.

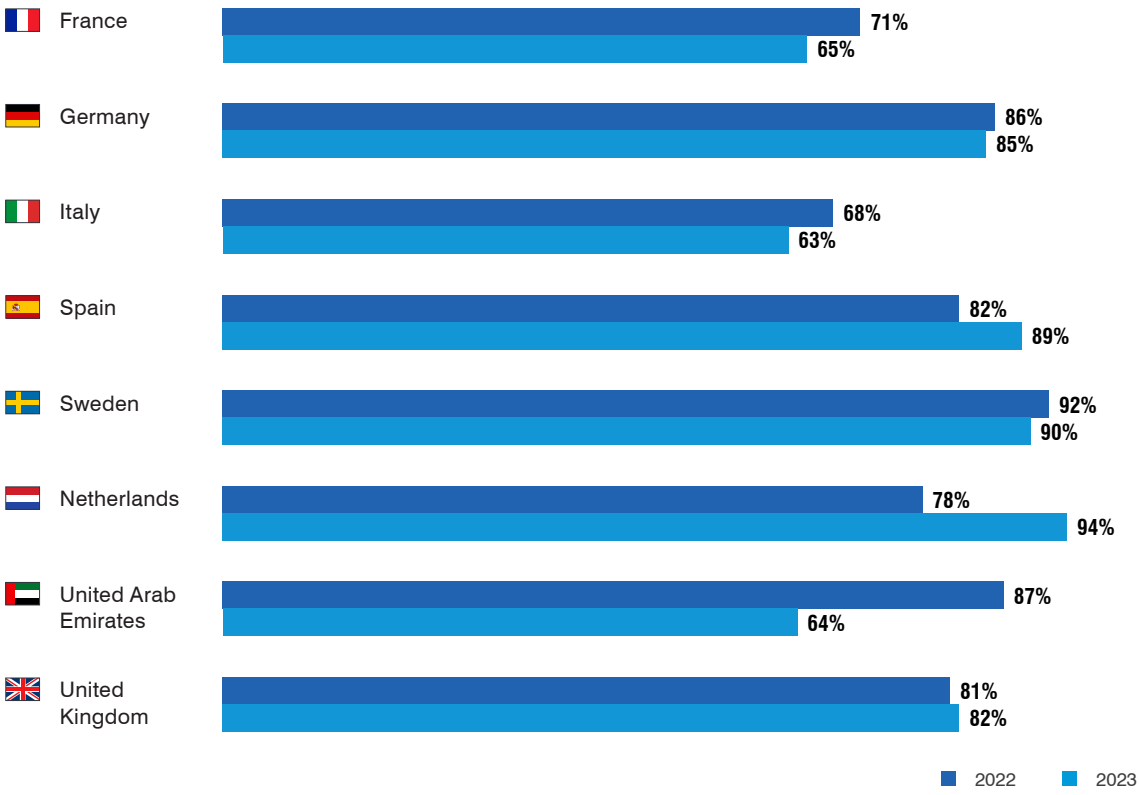
Percentage Affected by Targeted Attacks



Ransomware

Ransomware remains a serious threat to organisations in the region; both attacks and infections have risen in the past year. However, the details vary between countries.

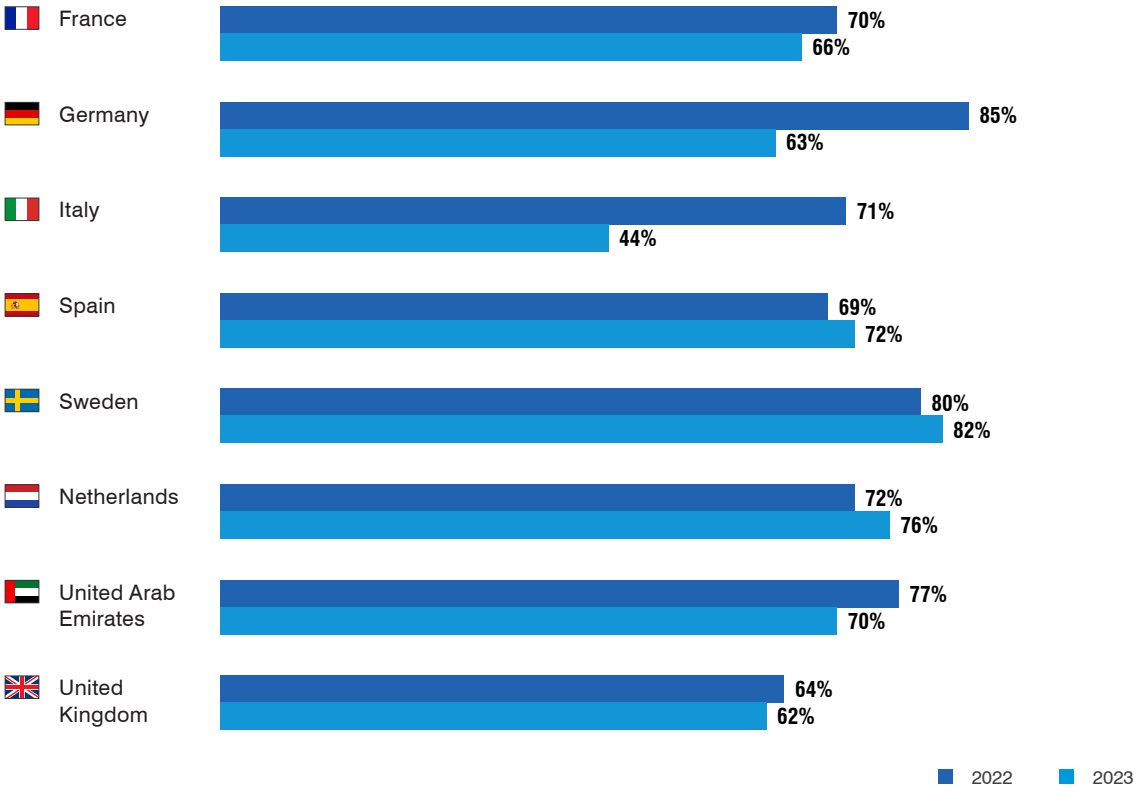
Email-Based Ransomware Attack Trend



Italy, for instance, reported the largest increase in successful ransomware infections, from 44% in 2022 to 71% in 2023—despite facing the same level of attacks as everyone else. This prompted the Italian authorities to issue a warning in June about the growing number of ransomware attacks exploiting a VMware bug.

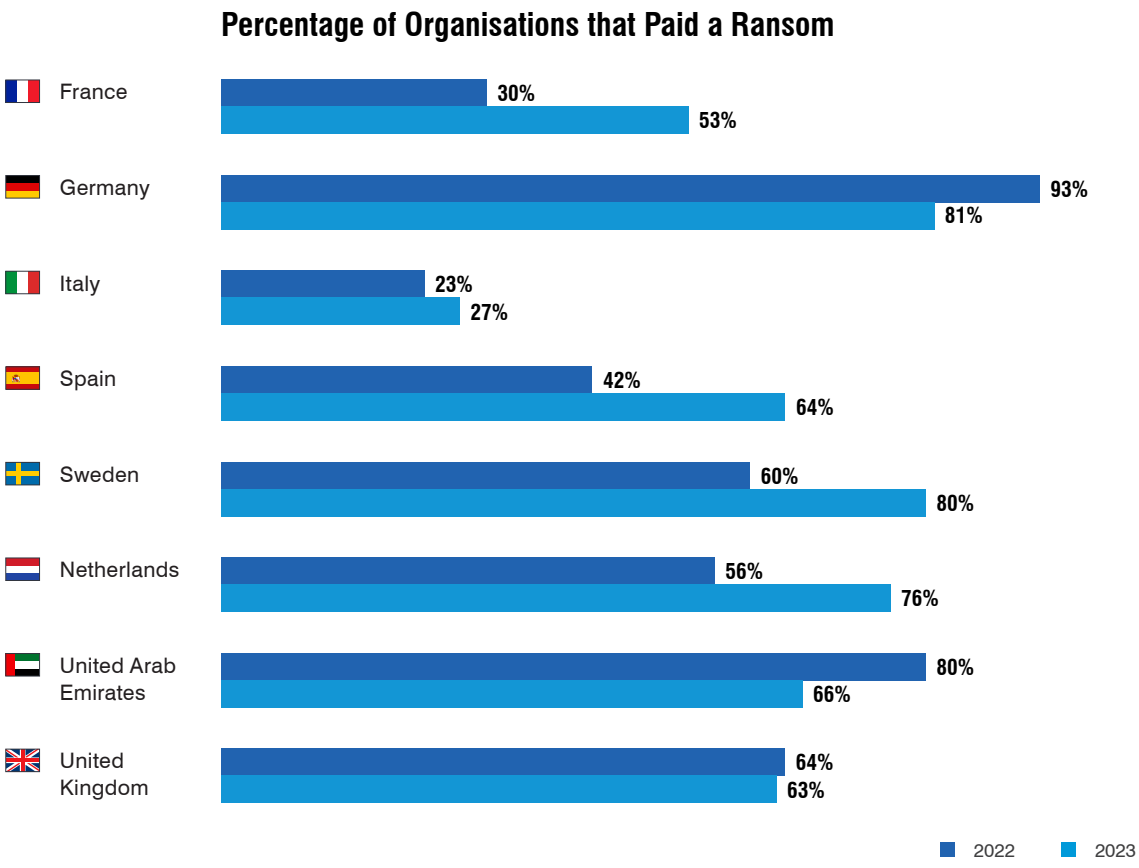
Sweden, meanwhile, experienced the highest level of attempted ransomware attacks in the world, with 92% of its organisations being targeted. This may be related to the fact that, in a previous survey, 74% of Swedish respondents cited credential theft as the biggest cause of data breaches. Prioritising defense against these attacks may reduce the likelihood of follow-on activity, such as ransomware.

Ransomware Infection Trend



On the other hand, only three countries—Germany, UAE and the U.K.—showed greater willingness to pay. Germany also had the highest proportion that paid a ransom (93% vs 54% global average).

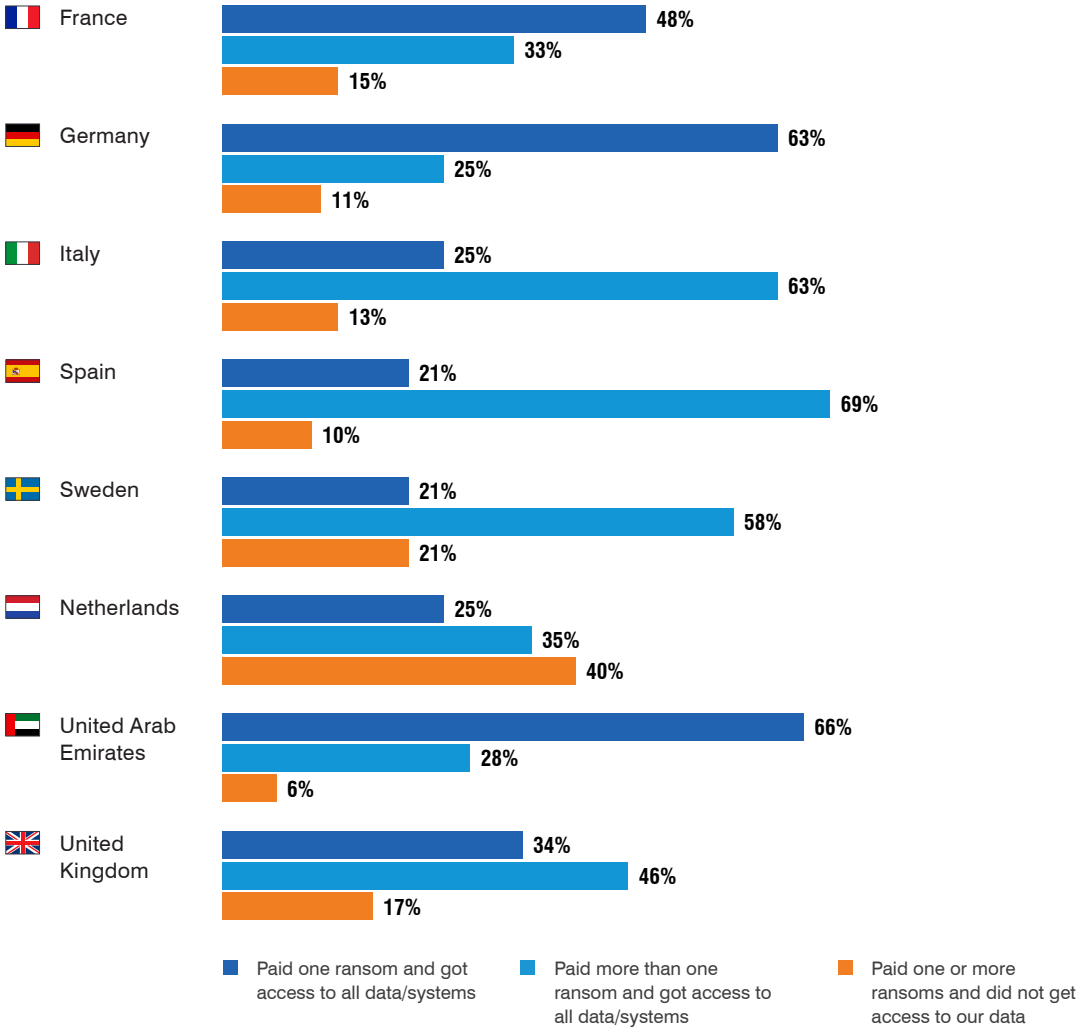
This strategy seemed to work for German and UAE organisations, which reported much higher rates of system and data recovery after a single payment. However, it also came at a cost, as 85% of German organisations reported a successful ransomware infection—the highest level in the region—suggesting a link between their readiness to pay and the intensity of targeting.



U.K. organisations, however, did not fare so well, suffering the highest rates of repeat infection. About 14% experienced 10 or more infections, compared to 5% globally. This shows that paying ransoms does not guarantee immunity from future attacks—and may even encourage them.

Globally, Dutch companies saw the least positive results from paying; 40% reported that they never got their data back, compared to 16% globally. This suggests that some ransomware groups may not honor their promises or may not always have the ability to restore data.

Results from Paying Ransom



On a positive note, cyber insurance coverage levels have improved, providing some financial relief. The only exception was France, where the percentage of fully or partially covered organisations dropped from 87% in 2022 to 76% in 2023. This is likely due to France's largest insurer announcing that it will no longer cover ransomware attacks.

Recommendations

Our survey shows that users in Europe and the Middle East understand their behaviour carries risk. But this often isn't enough to convince them to prioritise security. This might be for the sake of convenience, or to save time, or because they simply don't know if IT security is their responsibility.

For users who already understand that security is their responsibility

- Provide tools that empower people to be more proactive. Email reporting buttons make it simple to report suspicious messages. And "nudging" technologies such as email warning tags can prompt users to act. Also consider building a champions network and reward system to encourage these users to model best practice and advocate for others who are unsure of what to do.

For users who are unsure or don't believe that security is their responsibility

- Make education personal and relevant to individual roles and responsibilities. Increase communication from business and security leaders to better inform users of their responsibilities and their impact on the organisation.

It's also important to provide best-in-class security education, prevention, detection and response. Advanced solutions can help balance stricter security controls with productivity by reducing the number of threats faced by users. For example, deploying an email security solution that is 99.9% effective means that most users will never have to decide how to respond to a suspicious link.

Finally, work with business stakeholders and prioritise ease-of-use when implementing security policies. Users will be less inclined to circumvent systems if security aligns with their goals. And they are more likely to use a control if it is intuitive and does not require any training.

LEARN MORE

To learn more about how Proofpoint provides insight into your user-based risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **www.proofpoint.com/uk**

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**

proofpoint.

0402-001-01-01