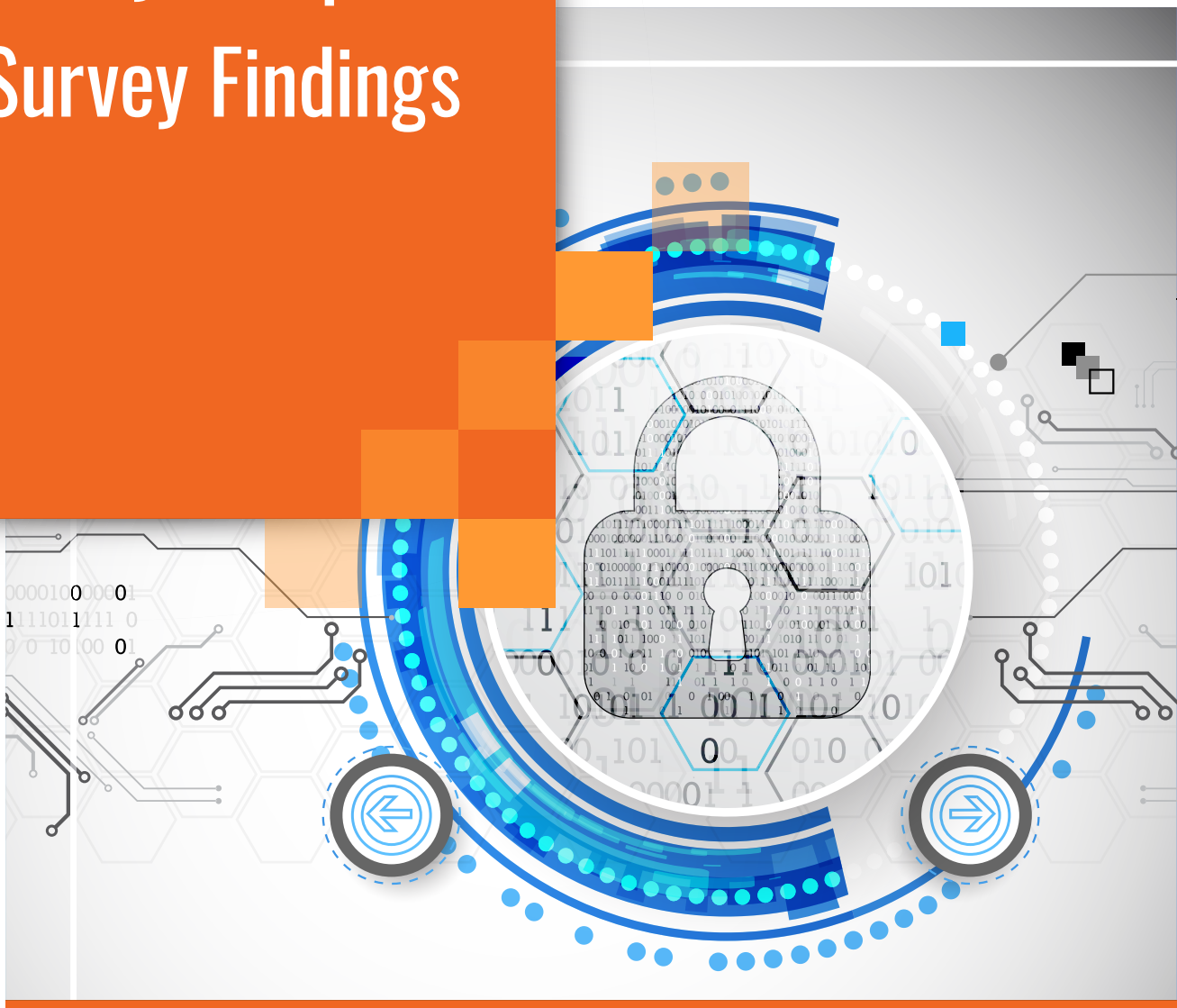
KnowBe4

Infosecurity Europe 2024 Survey Findings



Part 2

KNOWBE4 INFOSECURITY EUROPE 2024 SURVEY FINDINGS PART 2

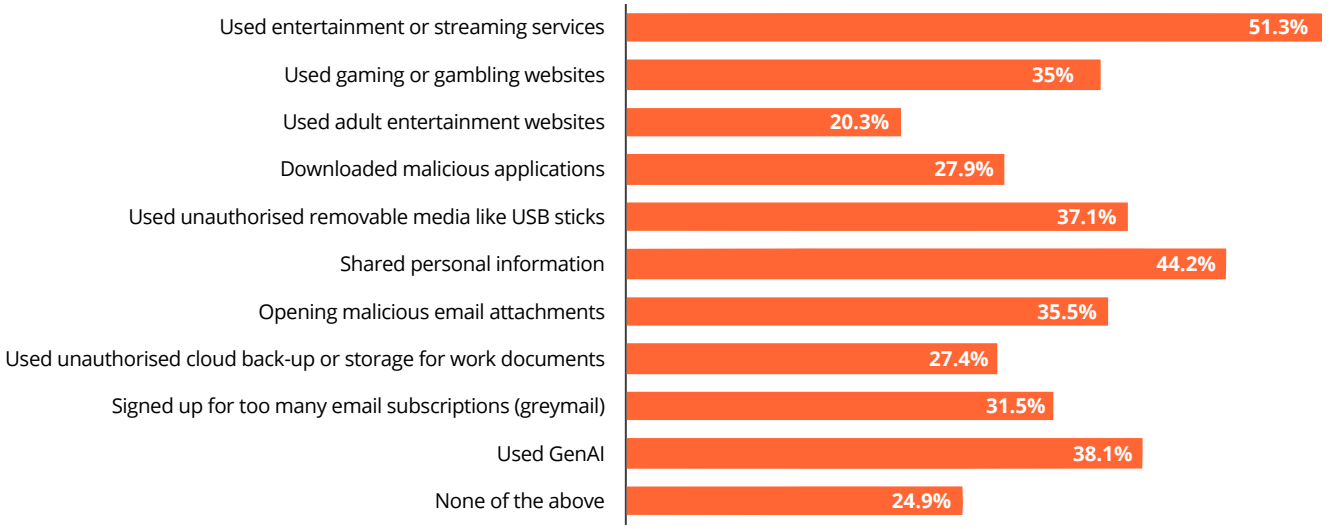
Welcome to the second part of KnowBe4's Infosecurity Europe 2024 Survey Findings, which has helped us capture insights on the cybersecurity issues that are foremost in the minds of over 200 security professionals that attend the three-day conference this year.

In part two, we will dive into what risky security behaviours have been observed in the workplace as well as the types of risky security behaviours security professionals have admitted to committing.

75% of security professionals have witnessed employees displaying risky security behaviours at work.

The findings of the survey showed three-quarters (75%) of security professionals have witnessed employees displaying risky security behaviours at work. The type of risky behaviours witnessed included using entertainment or streaming services (33%), sharing personal information (14%) and using gaming or gambling websites at work (10%).

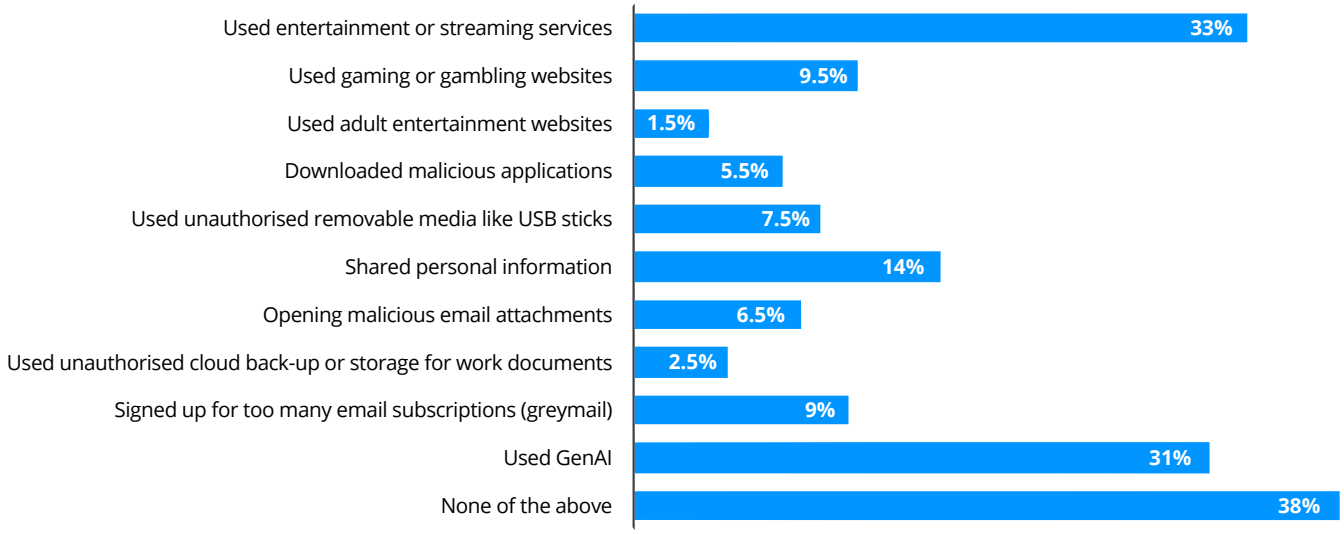
How many of these activities have you observed others doing at work?



These were risky security behaviours conducted by non-security employees.

Alarmingly, almost two-thirds (62%) of security professionals admitted to performing the same type of risky behaviours themselves. For instance, one in ten security pros confessed to using gaming or gambling sites at work and 14% have shared personal information.

How many of these activities have you done at work?



When you consider that the majority of breaches worldwide (68%), stem from non-malicious human actions, which include errors or susceptibility to social engineering attacks, poor security behaviour can evidently expose organisations to cyber threats, underlining the critical role of effective security awareness training.

The multifaceted nature of cybersecurity challenges faced by organisations is clear when looking at the survey results. While technological advancements like AI and deepfakes present new risks, the human factor remains a critical piece of the cybersecurity puzzle.

However, these results show risky behaviours in the workplace continue to be a serious issue, which is evidence of a weak security culture. Cultivating a strong security culture means going beyond educating staff on cyber threats. Teaching them how to respond and identify threats as well as which behaviours can be risky and why will help with prevention of these behaviours and increase protection of the organisation. Security culture requires a shift in attitude, behaviour, approach, and perception of responsibility. It must be an organisation-wide priority if visible change is to be made.

To navigate this complex landscape, organisations must prioritise the development of a strong security culture, where cybersecurity is embedded into the fabric of the organisation, and everyone plays a role in maintaining a secure environment. This involves empowering security professionals, providing effective training, and fostering open communication and collaboration across all levels of the organisation. With adequate training and coaching, the human risk that exists in all organisations is reduced and secures not only organisations, but also employees from falling victim to cybercrime.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E07K01