The 8 cybercrime trends to watch out for

Who will harness new technologies and the psychology of human behavior more effectively – **us or the cybercriminals?**

SOSAFE TODAY

Market leader for Human Risk Management in Europe

GERRY WEBER · SOS CHILDREN'S VILLAGES · CLARK · WWF · DeepL · ALDI · DAIMLER TRUCK · TUI · ADAC

BAUERFEIND · SCHÜCO · Handelsblatt · VORWERK · DACHSER Intelligent Logistics · CANYON · WAGO

Why customers love us

Driven by behavioral science

400+
employees from diverse backgrounds

Easy to use, customize, and scale

4,500+
customers across all industries

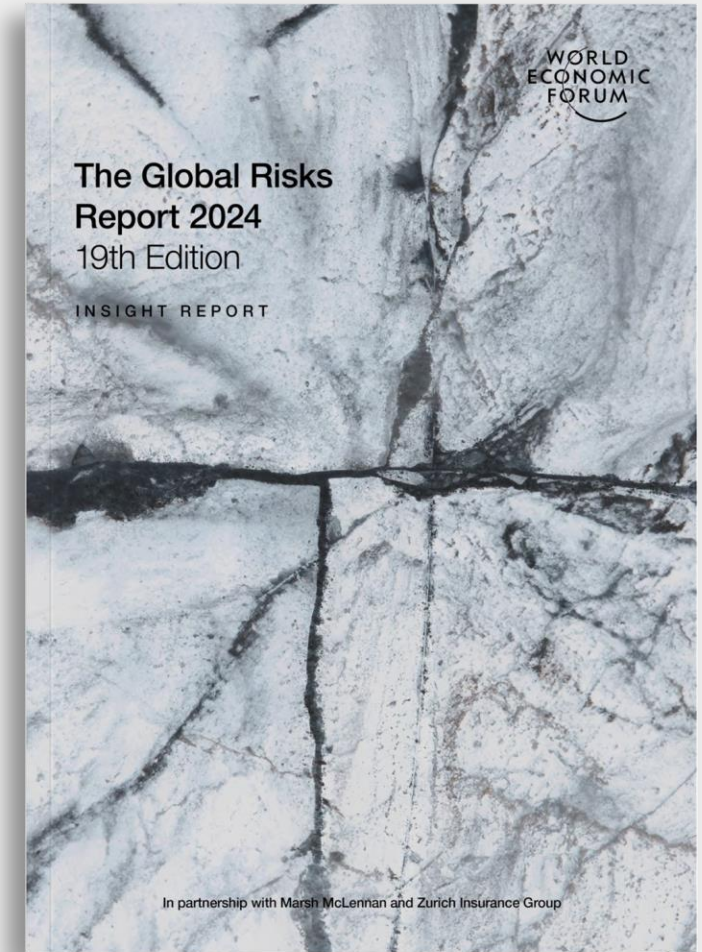
100% GDPR-compliant and ISO 27001-ready

3,000,000+
users across the globe

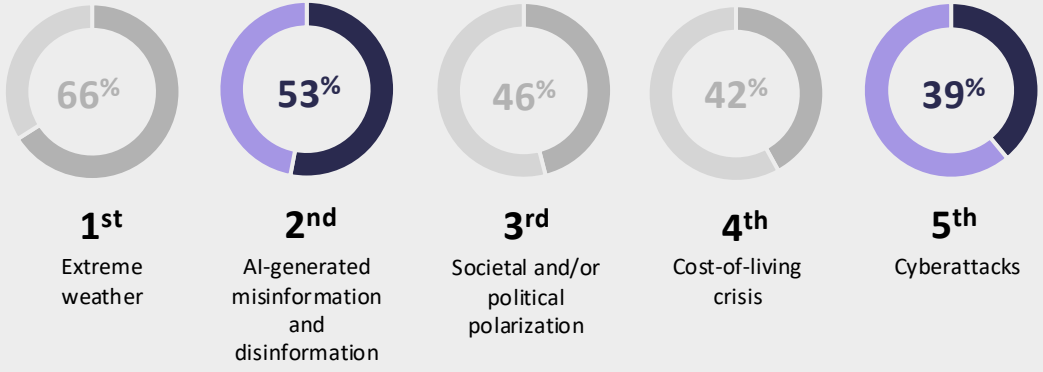
sosafe

GLOBAL EXPERTS AGREE

Two of the biggest risks to society in 2024 are AI-generated disinformation and cyberattacks



WORLD ECONOMIC FORUM



Sources: World Economic Forum, 2024.

Cybercrime Trends 2024

- How is **AI** contributing to the **professionalization** and sophistication of **cybercrime**?
- Why are **phishing** and **social engineering** more **successful** today than ever before?
- **Featuring:**

Ralf Schneider
Allianz Senior Fellow and Head of Cyber Security and NextGenIT Think Tank

John Noble
Non-executive director and chair of the Cyber Security Committee of NHS Digital in England

Download here!

THIS YEAR, THE REAL BATTLE BEGINS

The cybercrime trends to watch out for

1 **Artificial intelligence**

2 **Quantum hacking**

3 **Professionalization of cybercrime**

4 **Global tensions & hacktivism**

5 **Disinformation-as-a-service**

6 **Public sector and critical infrastructure**

7 **Pretexting and multichannel tactics**

8 **Rising burnout rates**

AI IS EVOLVING TOO RAPIDLY

AI-generated deepfakes look too real – and are scamming people

CNN

World / Asia

Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

1 in 4

Have experienced a **voice cloning attack** or know someone who has

Source: McAfee

CEO of world's biggest ad firm targeted by deepfake scam

Exclusive: fraudsters impersonated WPP's CEO using a fake WhatsApp account, a voice clone and YouTube footage used in a virtual meet

Mark Read, CEO of WPP, the largest global advertising and public relations agency. Photograph: Toby Melville/Reuters

THIS YEAR, THE REAL BATTLE BEGINS

The cybercrime trends to watch out for

1 Artificial intelligence

2 Quantum hacking

3 Professionalization of cybercrime

4 Global tensions & hacktivism

5 Disinformation-as-a-service

6 Public sector and critical infrastructure

7 Pretexting and multichannel tactics

8 Rising burnout rates

sosafe

THANKS TO RANSOMWARE-AS-A-SERVICE

The professionalization of cybercrime will reach a new level of maturity by 2024

31%

of the companies that experienced a cyberattack in the last 3 years were attacked with **ransomware**.

4.54 mil. USD

The **average cost** of a successful ransomware attack per company - ransom not included.

x 2

In **2023**, the number of **ransomware victims doubled** compared to 2022.

Ransomware-as-a-Service: Cybercriminals are now just a visit to the dark web and a crypto payment away from having all the tools they need to launch destructive ransomware attacks:

INSIDER

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack

The Guardian

Ransomware hackers demand $70m after attack on US software firm Kaseya

Quellen: Human Risk Review 2023, IBM's Cost of a data breach 2022; Black Kite, 2023.

THIS YEAR, THE REAL BATTLE BEGINS

The cybercrime trends to watch out for

1 Artificial intelligence

2 Quantum hacking

3 Professionalization of cybercrime

4 Global tensions & hacktivism

5 Disinformation-as-a-service

6 Public sector and critical infrastructure

7 Pretexting and multichannel tactics

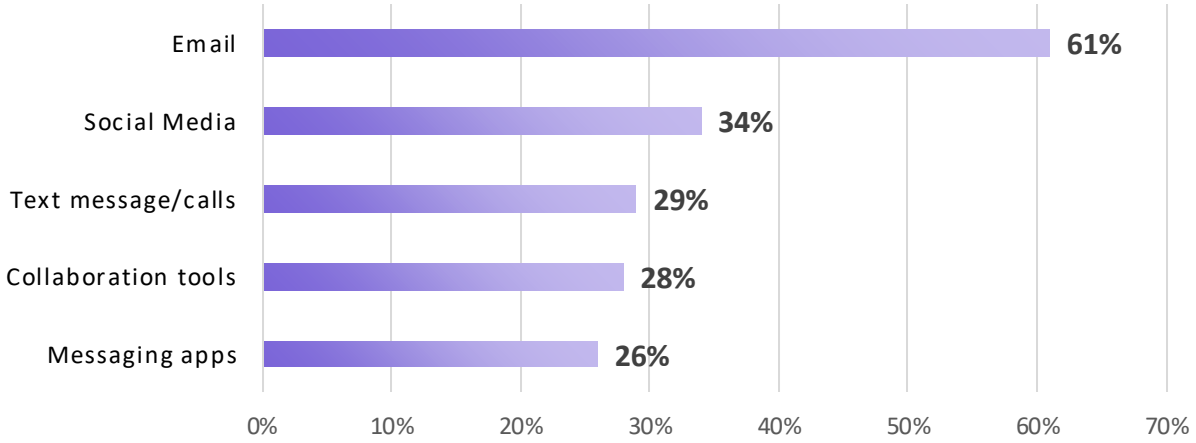
8 Rising burnout rates

sosafe

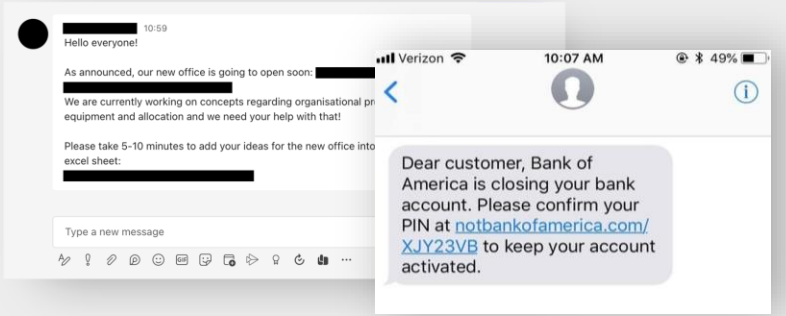
SOCIAL ENGINEERING IS BECOMING MORE COMPLEX

As we diversify our communications channels, so do cybercriminals

Top channels in which companies are targeted

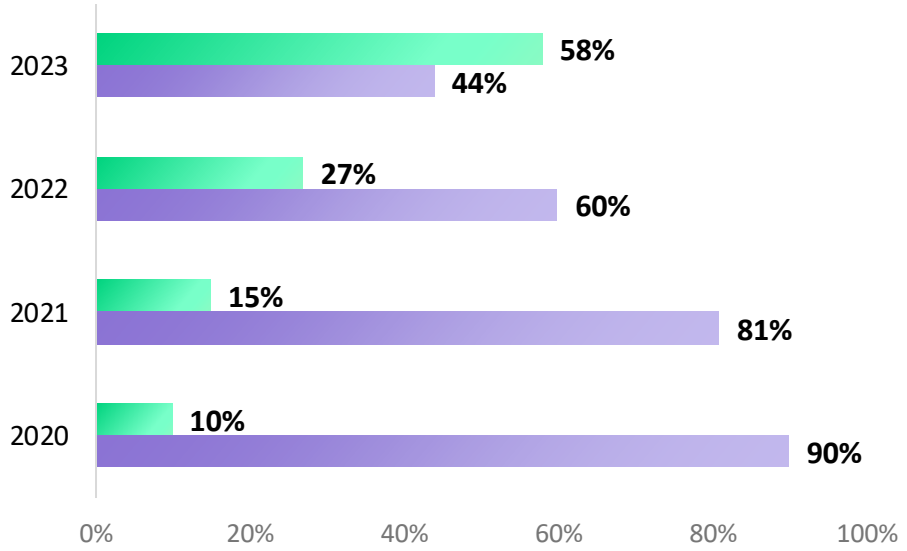


Messaging apps scams

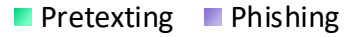


Text messages

Pretexting doubling & becoming **#1 of Social Engineering action**



Action varieties in Social Engineering incidents



Sources: Human Risk Review 2023; Verizon data breach reports 2020-2023.

TECH IS ADVANCED ENOUGH NOW

Hackers can launch automated, sophisticated social engineering attacks at scale

Channel diversity

Hyperpersonalization

Mass scalability

THIS YEAR, THE REAL BATTLE BEGINS

The cybercrime trends to watch out for

1 Artificial intelligence

2 Quantum hacking

3 Professionalization of cybercrime

4 Global tensions & hacktivism

5 Disinformation-as-a-service

6 Public sector and critical infrastructure

7 Pretexting and multichannel tactics

8 Rising burnout rates

sosafe

AS A RESULT

In 2024, expect more breaches that involve the human element

Allianz

Cyber incidents
Top business risk
by Allianz Risk Barometer 2024

FORRESTER®

90% of data breaches will include a human element

Our cyber security measures will remain incomplete until we focus on people – just as hackers do.