Cybercrime Trends 2024

The latest threats and security best practices

sosafe

Contents

In 2023, everything changed. It’s time to prepare for what’s to come.

The year 2023 was a turning point in our global narrative. Since OpenAI announced the launch of ChatGPT-3 in November 2022, there has been a surge of AI-driven innovation and a **profound shift in how we interact with technology**. This evolution is particularly evident in information security, where AI has emerged as a pivotal force, not only strengthening cyber security defenses but also elevating the sophistication of cyberattacks.

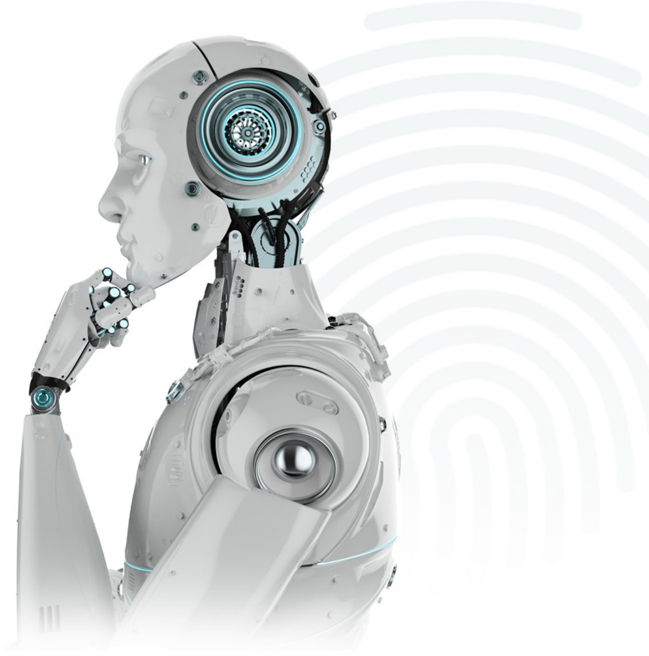
As we head into 2024, fueled by this **unprecedented speed of technological innovation**, we face a confluence of challenges: AI’s ever-growing involvement in cyberattacks, the double-edged sword of emerging technologies like 5G and quantum computing, and the maturing of cybercrime into a highly professionalized industry. This context is further complicated by the rise of hacktivism and cyberattacks amid global political crises and the rise of disinformation campaigns, making threats more complex and far-reaching. All this while cyber security professionals are battling burnout in the face of these escalating threats.

With the likelihood of an **attack resulting from human error expected to increase** in this threat landscape, a strong security culture is the only hope we have. That’s why this report focuses on the eight cybercrime trends for 2024 and provides security best practices to better prepare against this diverse array of cyber threats.

1 AI's growing role in cyberattacks: A storm on the horizon

The widespread use of AI, which is expected to reach over 300 million users in 2024 and an estimated 700 million by 2030, not only highlights the revolution underway but also raises concerns about its broader implications and security risks.[1] And, inevitably, **deepfakes** and **voice cloning** come into full focus when addressing AI's security challenges.

While bad actors have used both technologies for some time, the recent proliferation of tools capable of producing high-quality deepfake videos has made this technology more accessible, leading to an increase in its use, particularly in **disinformation campaigns and social manipulation** (more about this in the disinformation-as-a-service trend).[2]



Voice cloning is not lagging behind. A recent study confirmed that one in four people have experienced a voice cloning attack or know someone who has.[3] Police in Everett, Washington, have also warned of an increase in financial scams using voice cloning to defraud individuals.[4] But while cybercriminals mostly use these for financial scams, some of them having even faked a young woman's kidnapping, it's now also **undermining MFA systems based on voice recognition.**[5] For example, earlier this year, a journalist successfully accessed her bank account using a recording of her own cloned voice.[6] Although the journalist's experiment posed no personal risk, the broader threat is very real.

1 in **4** 🧍🧍🧍🧍

people have experienced a **voice cloning attack** or know someone who has

Source: McAfee[3]

[1] **Statista (2023).** Artificial Intelligence Worldwide.

[2] **News abp Live (2023).** Deepfakes To Disinformation: Year 2023 Brought A New Era Of Digital Deception, Driven By AI.

[3] **McAfee (2023).** Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam.

[4] **Fox 13 Seattle (2023).** Everett Police warn of AI voice-cloning phone scam after case reported in Snohomish County.

[5] **CNN (2023).** 'Mom, these bad men have me': She believes scammers cloned her daughter's voice in a fake kidnapping.

[6] **The Wall Street Journal (2023).** I Cloned Myself With AI. She Fooled My Bank and My Family.