



Report

Digital Uncertainty: Scams, Privacy and Artificial Intelligence

New consumer survey data reveals the platforms where scammers are targeting users most often and captures consumer attitudes on privacy-related tech trends

kaspersky bring on
the future

Internet scams have become such commonplace that users often don't bat an eyelash when they encounter one. They take various forms, appear on just about every app, site and digital platform, and are evolving as quickly as the internet itself.

Sometimes the scams involve gift cards or, most commonly, the scammers are seeking to gather users' personal information – usernames, passwords, dates of birth, banking info – just about anything they can use to either profit directly or to sell on the dark web to others who will use the data for additional targeting.

Kaspersky's most recent data shows that one of the most common scams – phishing attacks – grew by **40%** in 2023. Traditional phishing typically takes the form of an email or other message, often directing the recipient to a fraudulent website. The site is created to appear legitimate or to imitate a known brand, in an effort to trick the user into entering their information. But these sorts of scams have expanded well beyond emails and websites, and often now occur on various other platforms, from social media to messaging apps to cryptocurrency exchanges. Scammers are disguising themselves as customer service representatives, online daters, friends, celebrities, and fellow online gamers. AI tools are making it easier than ever to create these fake identities with fake images and videos, and to generate messages and have conversations.

Online scammers have **flooded** Facebook Marketplace, spreading malicious links, posting bogus listings, abusing fraud protections and employing other scams involving Zelle and Google Voice.

The modern consumer might understandably feel disoriented. In addition to scams, the emergence of artificial intelligence has many people wondering what information they can and can't trust. Furthermore, they may be wondering who they can trust with their information, given the key role that user data plays in enabling many of these new technologies.

This report captures a snapshot of consumer experiences and attitudes as they relate to a number of threats to their digital wellbeing. The results identify where consumers are encountering scams and where those scams are having the most success. They also reveal how these threats are altering consumer habits. Is the omnipresence of scams driving away users, and what specific worries do those users have when it comes to their privacy, particularly in the midst of the rise of AI and other new technologies?

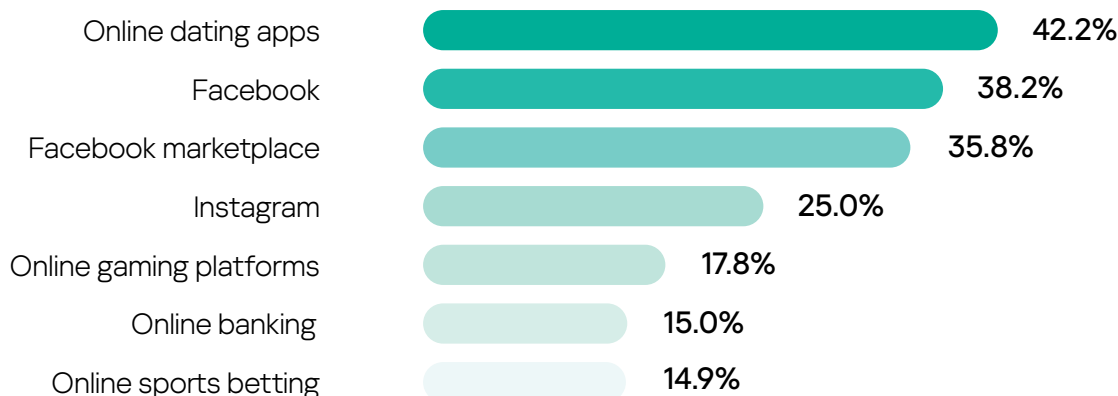


Methodology

In February 2024, Kaspersky surveyed 2,000 North American adults (in the U.S. and Canada) about their experiences with scams related to various online platforms, and also asked them about some of their digital habits, as well as their attitudes toward prominent issues affecting their security and privacy in 2024.

Primary Findings: Scams

Percentage of users of each service who have encountered a scam on the platform



42%

of users have encountered a scam on a dating app

The results show that users encounter scams at significant rates. Online dating apps turned out to be the place where it happens most often, with **42%** of users having encountered some type of scam on a dating app. Dating apps also appeared to be where fraudsters have had the highest rate of success; **24%** of dating app users said they'd actually fallen victim to such a scam.

Next up were Facebook and Facebook Marketplace, where **38%** and **36%** of users encountered scams, respectively. Users fell victim to scams on both of those platforms at a rate of **18%**. Meanwhile, one in four Instagram users said they had encountered a scam on the platform. **15%** of Instagram users said they'd fallen victim to one.

Nearly one in five online gamers said they have encountered scams on gaming platforms, with **10%** saying a scam had worked on them.

Scams targeted users of online banking and sports betting at a rate of **15%** each. Online sports betting scams appeared to be slightly more successful; **14%** of online sports betters said they fell victim to scams targeting their accounts. Nine percent of online banking users said the same.

On the positive side, **46%** of all respondents said they have never encountered any scams on these platforms, while **68%** said they'd never fallen victim to one. However, setting aside **3%** who said they were unsure or preferred not to say, that leaves at least **29%** of users who have fallen victim to some type of scam on one of these platforms.

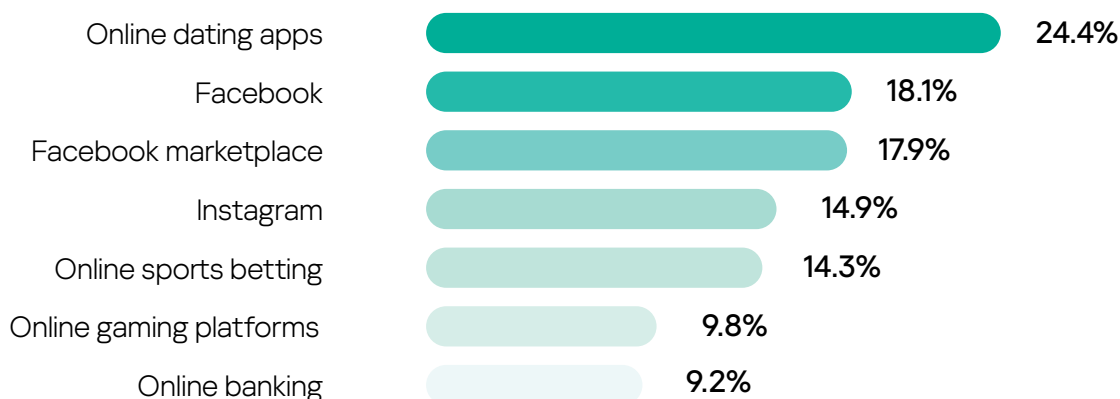
1 in 4

users have encountered a scam on Instagram

29%

of users have fallen victim to some type of scam on one of these platforms

Percentage of users of each service who have fallen victim to a scam on that service



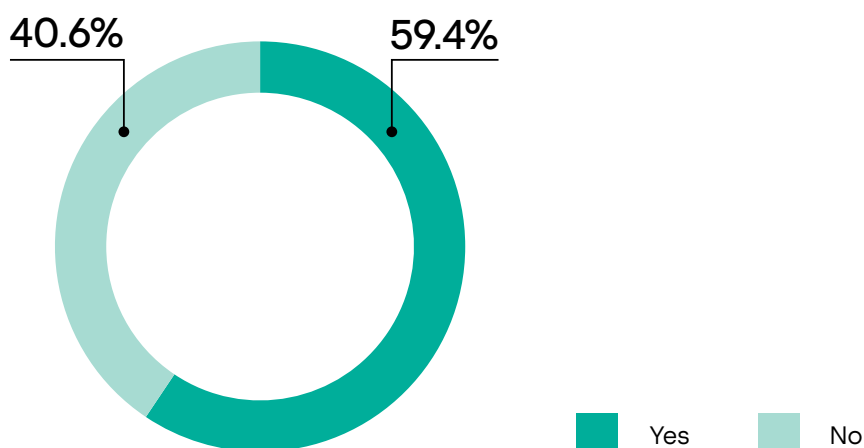
39%

of those who had encountered and/or fallen victim to a scam on Facebook marketplace said they were less likely to use the service as a result

Experiences with scams appear to be pushing a significant number of people away from using these services. Facebook Marketplace users appeared to be the most put-off by the presence of scams. **39%** of those who had encountered and/or fallen victim to a scam on the marketplace said they were less likely to use the service as a result. Online dating apps were close behind, with **37%** saying the same. Those were followed by users of online gaming platforms (**33%**), Facebook (**30%**), Instagram (**26%**), online banking (**17%**), and online sports betting (**13%**).

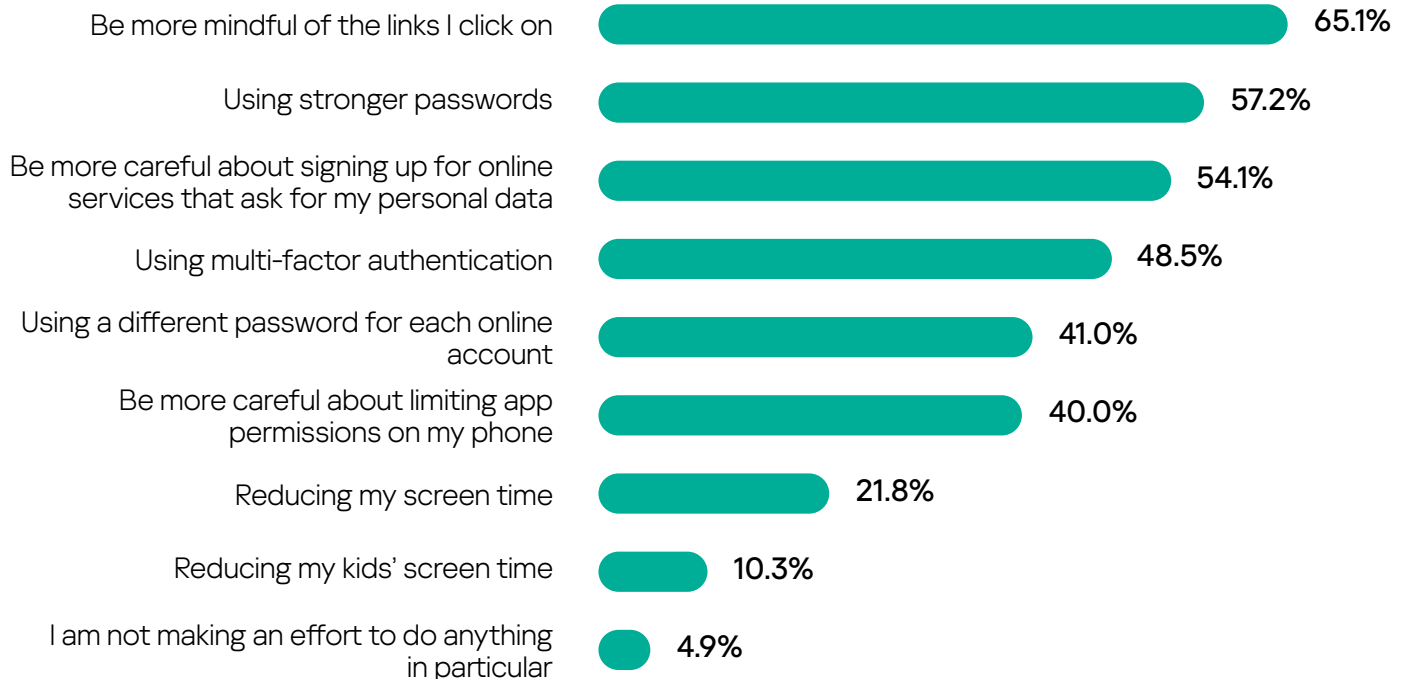
Overall, nearly **six in ten users said they have had to change a password for security reasons in the past six months.**

Have you had to change any of your passwords for security reasons in the past months



Primary findings: Digital Habits

Percentage of users who want to improve each of the following habits



The survey also asked consumers about digital habits they wish to change this year. Some of them indicated that people are interested in better protecting themselves from scams and other online threats. **65%** of respondents said they want to be more careful about the links they click on, while **57%** said they are making an effort to use stronger passwords, and **54%** are trying to be more careful about signing up for apps and other services that ask for their personal data. **49%** of respondents said they are planning to take better advantage of multi-factor authentication, **41%** are trying to start using different passwords for each online account they use, and **40%** are trying to be more careful about limiting app permissions on their phone.

People were also interested in improving their digital habits in general. **22%** said they want to reduce their screen time, while **10%** said they want to reduce their kids' screen time.

Meanwhile, **5%** of users said they aren't making an effort to do anything differently.



Kurt Baumgartner,
principal security
researcher,
Kaspersky

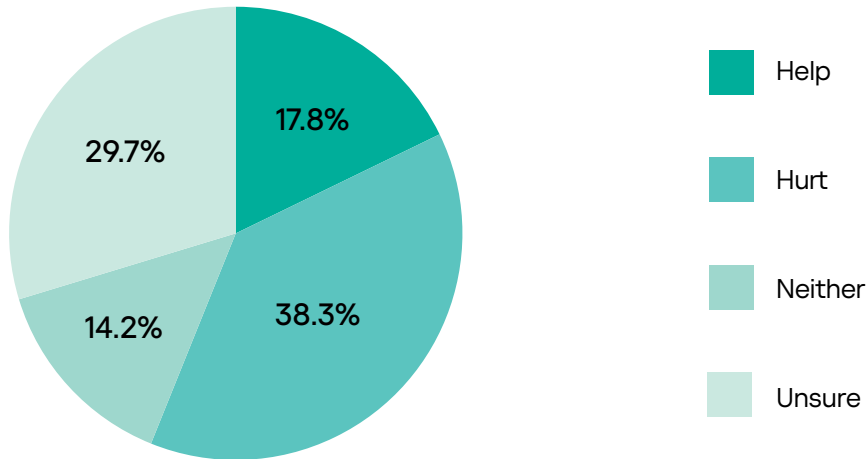
“There’s no corner of the internet that isn’t, to some extent, being infiltrated by bad actors looking to take advantage of people,” said Kurt Baumgartner, principal security researcher at Kaspersky.

Consumers should always keep their guard up, apply a baseline level of skepticism and take basic steps to protect their online security, such as using multi-factor authentication, avoiding password reuse and limiting app permissions.”

Primary Findings: Attitudes on technology and privacy

There are many other potential threats to user security and privacy besides scammers. The survey asked about a number of other tech-related issues about which respondents might have concerns.

Do you believe AI will mainly help or hurt your digital privacy and security in the future?



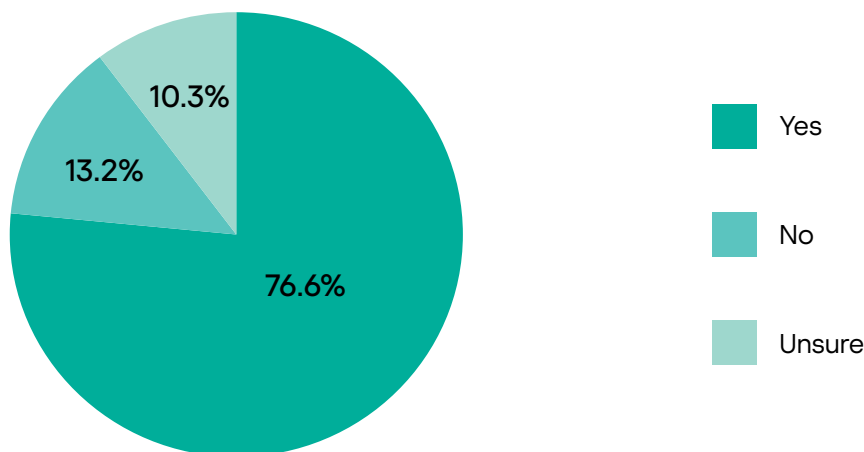
More than 3/4
said they are concerned
about the use of AI-
generated deepfake
videos and voice
recordings to spread
misinformation

After the release of Chat GPT in late 2022, Artificial Intelligence was almost undoubtedly the story of the year in 2023, setting off a wide range of opinions about the future potential of the technology, for better or for worse. Respondents to this survey tended to lean toward "worse," with more than twice as many people saying they believe AI will hurt, rather than help, their digital privacy and security in the future. AI platforms rely on large quantities of data and can present the risk of gathering or inferring personal user information, as well as the risk of unauthorized use or dissemination of that data.

AI also poses a challenge when it comes to the issue of deepfakes and disinformation. As AI-powered generative video platforms rapidly improve in quality, the risk of deception is higher than ever before. Survey respondents expressed worry about this issue as well. **More than three quarters said they are concerned about the use of AI-generated deepfake videos** and voice recordings to spread misinformation.



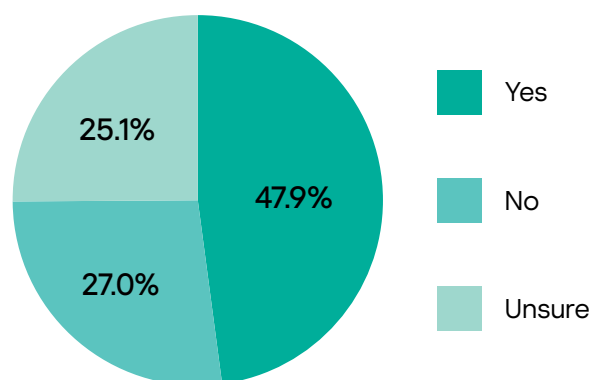
Are you concerned about the use of AI-generated deepfake videos and voice recordings to spread misinformation online?



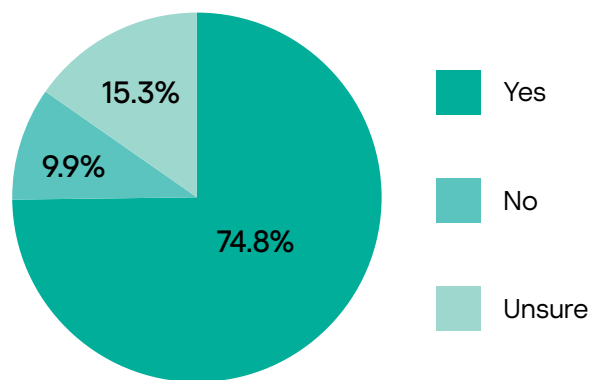
The release of the Apple Vision Pro brought the concepts of spatial computing and augmented reality to the forefront of the tech world in February, 2024. It also raised some privacy alarms, with experts noting that the device's various cameras and sensors could give it the ability to create a detailed inventory of a user's home, which could be of great value to advertisers, as well as to use facial recognition technology to gather information – even on complete strangers. Nearly half of respondents expressed privacy concerns related to these devices.

Users also expressed an interest in seeing the government take action to protect consumers, with **three quarters** of respondents saying they'd like to see new privacy regulation in 2024, with **10%** opposed and **15%** unsure.

Do you have privacy concerns related to augmented reality devices with facial recognition technology such as Apple Vision Pro?



Percentage of users who would like to see new privacy regulations designed to protect consumers in 2024



Kurt Baumgartner,
principal security researcher,
Kaspersky

As technology continues to evolve around us, we have to remember that we all have a right to privacy and be prepared to speak up when we believe things might be going too far. User data has become valuable currency, bought and sold and used as the lifeblood of so many new digital services. The reality should be that your data belongs to you. There are a number of areas where government regulation could go a long way toward protecting consumers in the new era of AI.

www.kaspersky.com

kaspersky

Cyberthreat news: securelist.com

IT security news: business.kaspersky.com

Business leaders magazine: kaspersky.com/securefutures

Enterprise cybersecurity: kaspersky.com/enterprise

2024 AO Kaspersky Lab Registered trademarks and service marks are the property of their respective owners.