

Living Secure

A global survey of the digital moments we need to protect against scams in 2024



CEO Welcome

As our lives become increasingly digital, the potential impact of scams has increased in severity, incorporating not only financial loss, but also the theft of our most personal data.

In 2023, a third of people (34%) experienced a cyber scam, while 85% reported receiving a digital scam attempt. It's no wonder, then, that 80% of people report worrying about their online safety, and 7 in 10 don't know who to trust online. Amidst the AI revolution, the threats experienced by people in their important digital moments continue to increase.

The latest 'Living Secure' survey collects insight from 7,000 people, from seven regions around the world, highlighting the digital moments we need to protect against scams in 2024.



Contents

CEO Welcome	2
Who we surveyed	4
Digital moments	6
Generation scam	8
Trust in 2024	10
Vulnerable and confused	12
Shopping and banking	13
The evolving scamscape	15
Methodology	17

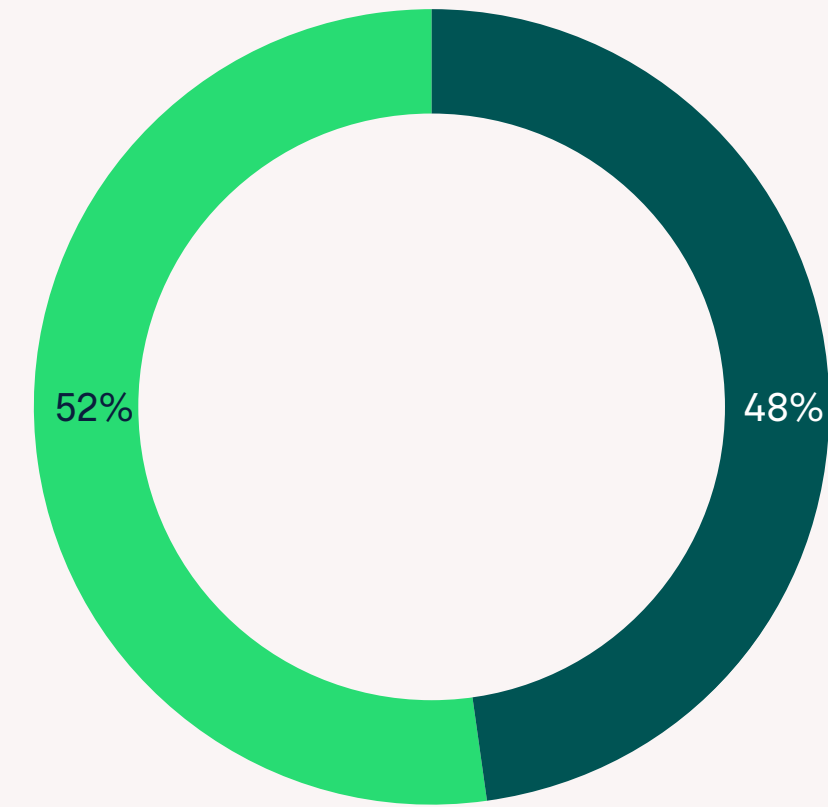


Who we surveyed

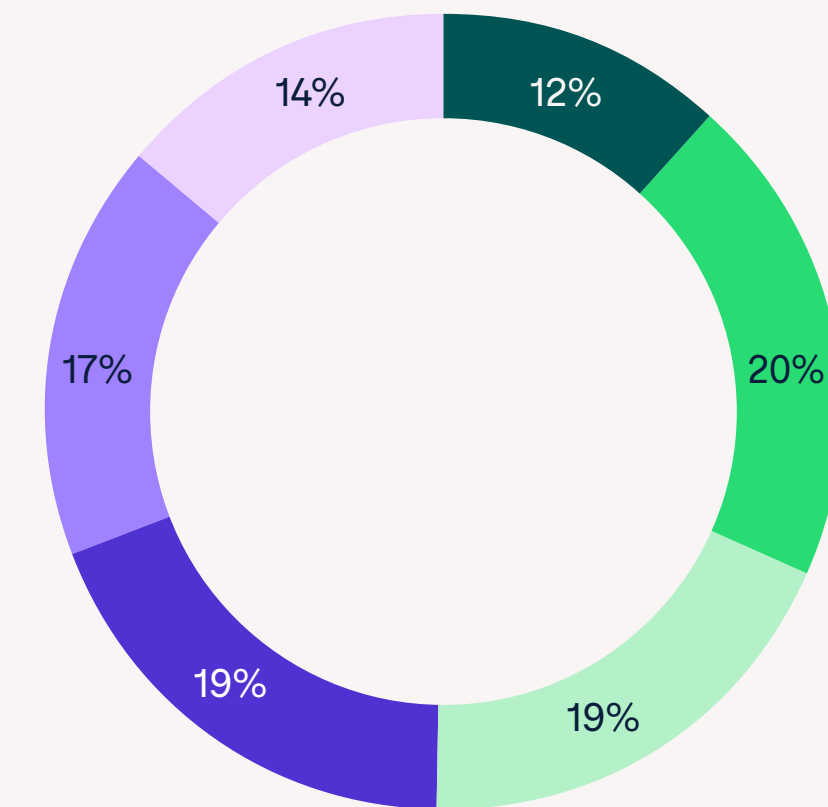
In 2022 F-Secure revealed how our lives are now punctuated by digital moments, whether that's sending emails, consuming social media, dating, working, or buying goods online. And whilst two years is a long time in technology, the findings of this year's survey reveal that—despite already being identified by participants in 2022—the main areas of online worry have still not been addressed.

The things that made us feel vulnerable two years ago are the same today, with 80% of us worrying about our online safety. And the companies working in these areas—gambling, dating, banking, smart devices, shopping, gaming, social media—haven't done enough to make us feel any safer. In fact, in some cases, such as dating, gambling, shopping, and social media usage, the feeling of vulnerability has increased.

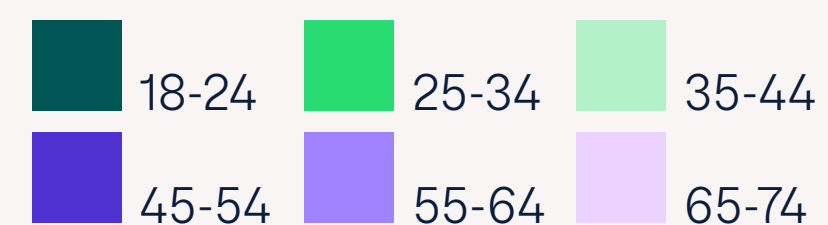
What's more, we're today seeing how our digital moments—if not properly protected - provide the perfect vehicle for scams to happen. We're now more exposed to scammers' tactics than ever—with three quarters of us using social media on a weekly basis (76%), and generative AI making it harder than ever to spot scams, misinformation, and fake news. Ultimately our findings show that effective consumer cyber security starts with education around scams as well as the right protection.



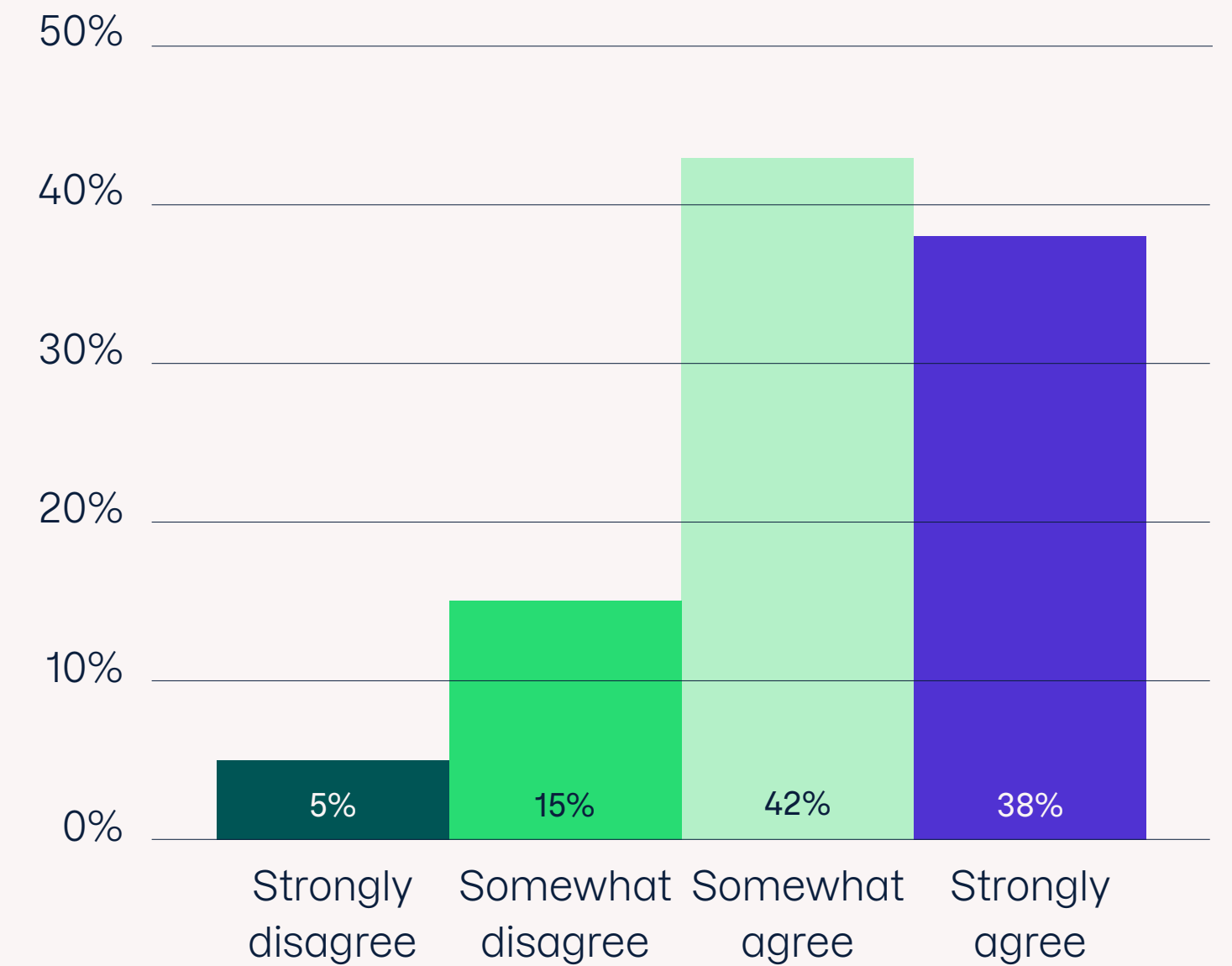
Gender



Age



I worry about my safety online

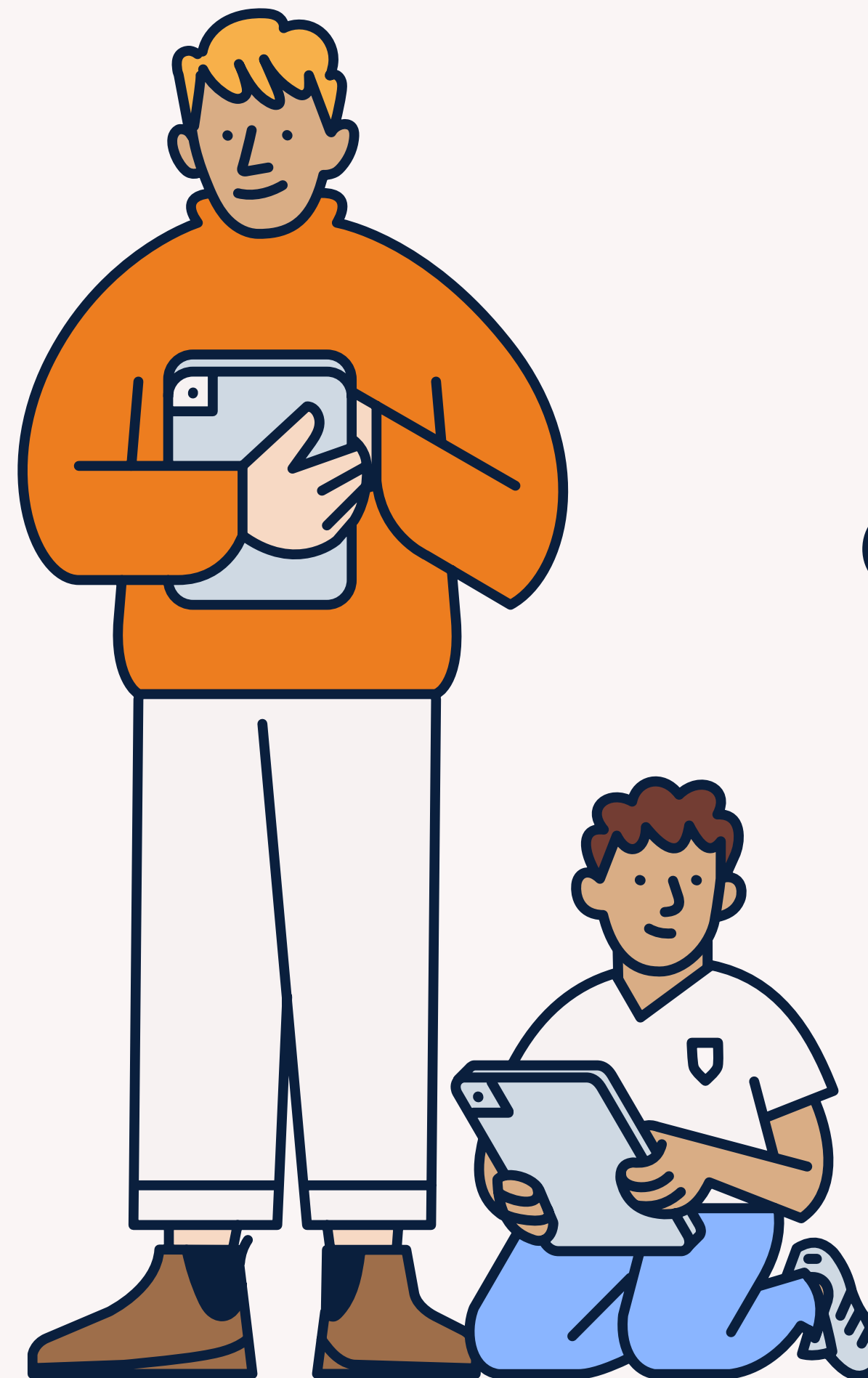
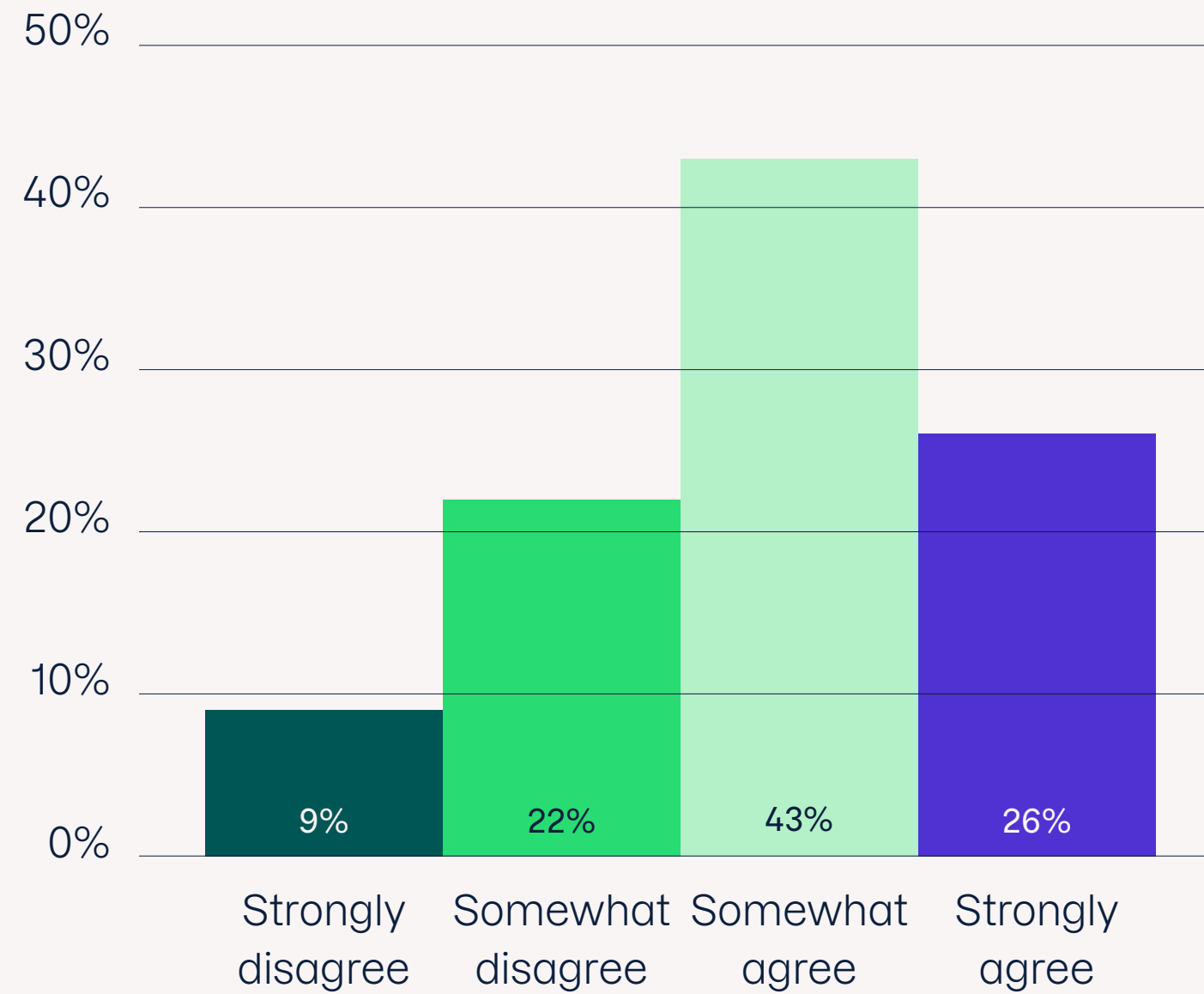


KEY TAKEAWAYS

- 34%** of people experienced a cyber scam in 2023
- 85%** of people reported receiving a digital scam attempt
- 80%** of participants worry about their online safety
- 54%** of cyber scams are conducted via email
- 7 in 10** people do not know who to trust online

A need for simpler scam protection

We asked people whether they agreed with the statement: "I find cyber security too complex."



72% say smart device makers aren't ensuring online safety and privacy.



36% of our respondents said they had children under the age of 15 currently living with them.

Digital moments

Our 2024 results reveal that our most important digital moments are largely unchanged in the last two years, with the top seven positions remaining the same (see p7).

The only moment to drop out of the top 10 list was 'Making voice calls', which was ranked as 8th most important in 2022 ('Look for information & study' having replaced it). However, whilst the moments we deem to be important were essentially the same, there were some significant changes in frequency (see p7).

Sending and receiving emails remained the top digital moment that we do at least weekly (at 88%). But other topics increased significantly. Sending messages on apps such as WhatsApp was at 83% (up from 72%); checking the weather forecast was up to 80% (a 13% increase); consuming social media jumped from 64% to 76%; and reading the news increased from 67% to 75%.

These results show a marked increase in digital interaction since 2022. Voice calls are down, but every other social activity has gone up (such as social media usage, emailing, and instant messaging). This has increased our general exposure to digital scams and fake news, in an era when generative AI is making them increasingly difficult to spot.

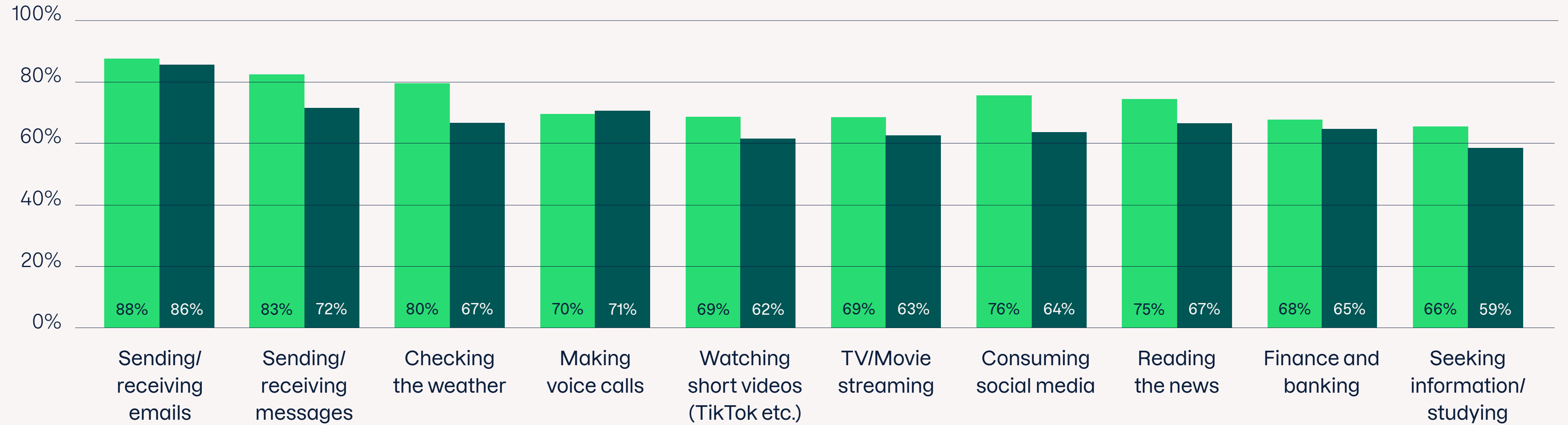


76% of people consume social media (at least weekly) in 2024. Which is a 12% increase in just two years.

Top 10 most frequent digital moments (2024 vs 2022)

The frequency of our most important digital moments has increased (at least weekly).

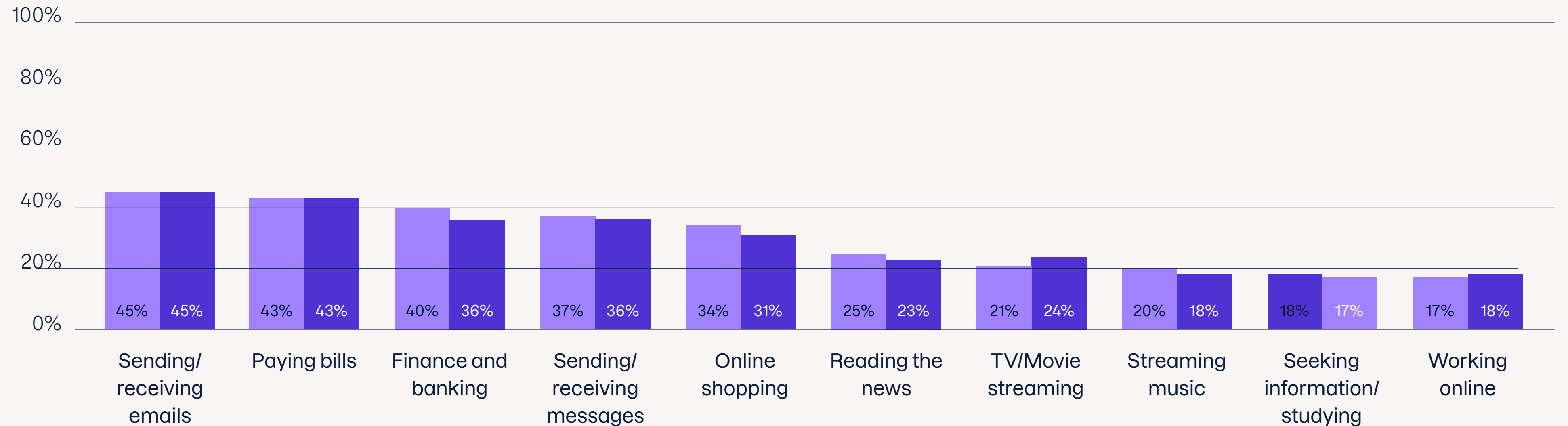
2024 2022



Top 10 most important digital moments (2024 vs 2022)

We asked our survey respondents which online activities were of most importance to them. The list is largely unchanged over the last two years.

2024 2022



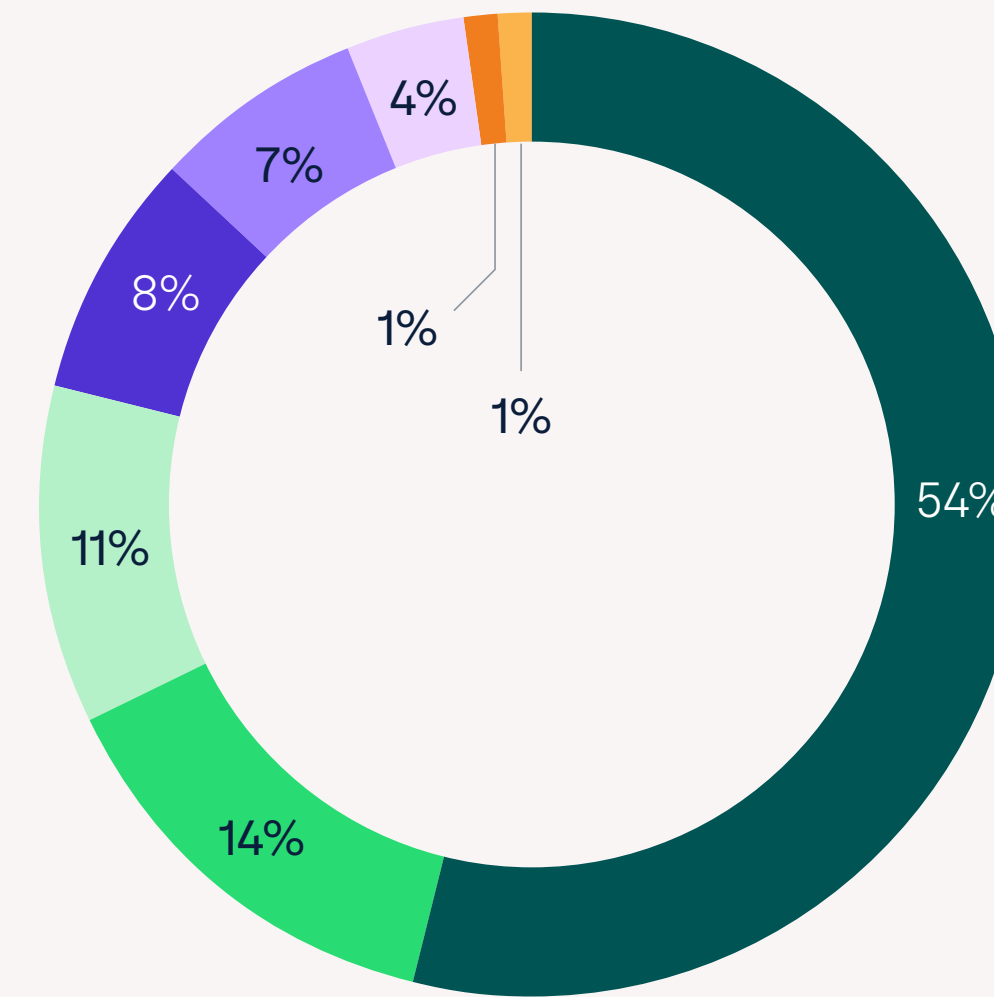
Generation scam

The Living Secure survey reveals that cyber crime has never been more prevalent; **85% of our survey respondents said they had received a digital scam attempt**, with 4 in 10 people getting them on a weekly basis. And of the 7,000 people we questioned, 36% said that they get more scam attempts now than they did 12 months ago.

It isn't just attempts that are on the increase, either. Our 2024 survey found that a third of people (34%) experienced a cyber scam over the past 12 months, which was a 7% increase since 2022. For the 34% of people that experienced cyber crime, a quarter suffered financial loss of some type. And over a third (36%) said that it had led to a loss of time. (See the effects of a cyber scam opposite.)

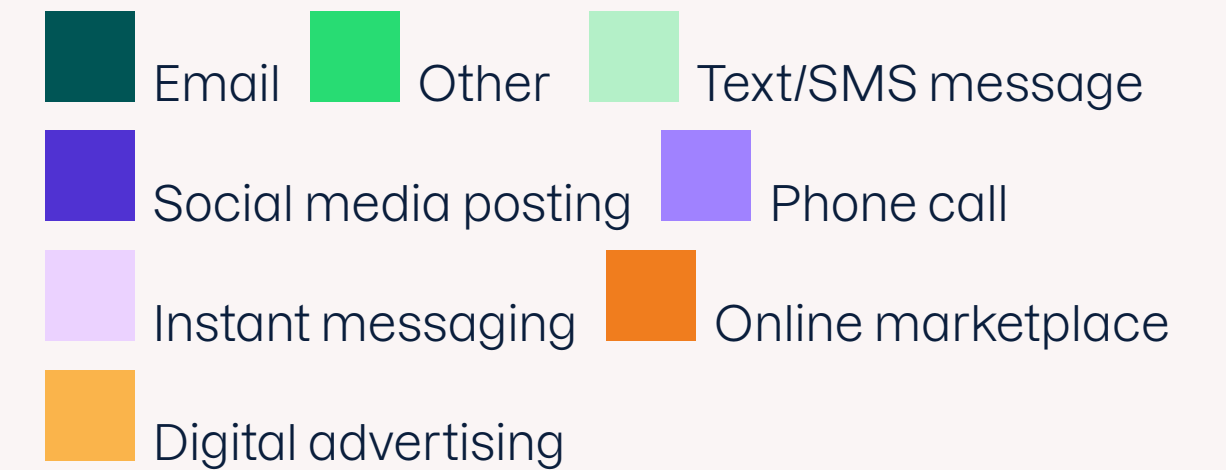
Despite the growing prevalence of scams—and the continued sophistication of generative AI in creating convincing content of all kinds, including images, video, text, and audio—77% of people believe they know how to recognize an online threat. However, of those people that were victims of cyber scams, almost half (45%) said they were unable to identify the scam that affected them.

34% of people have experienced a cyber scam during the past 12 months.



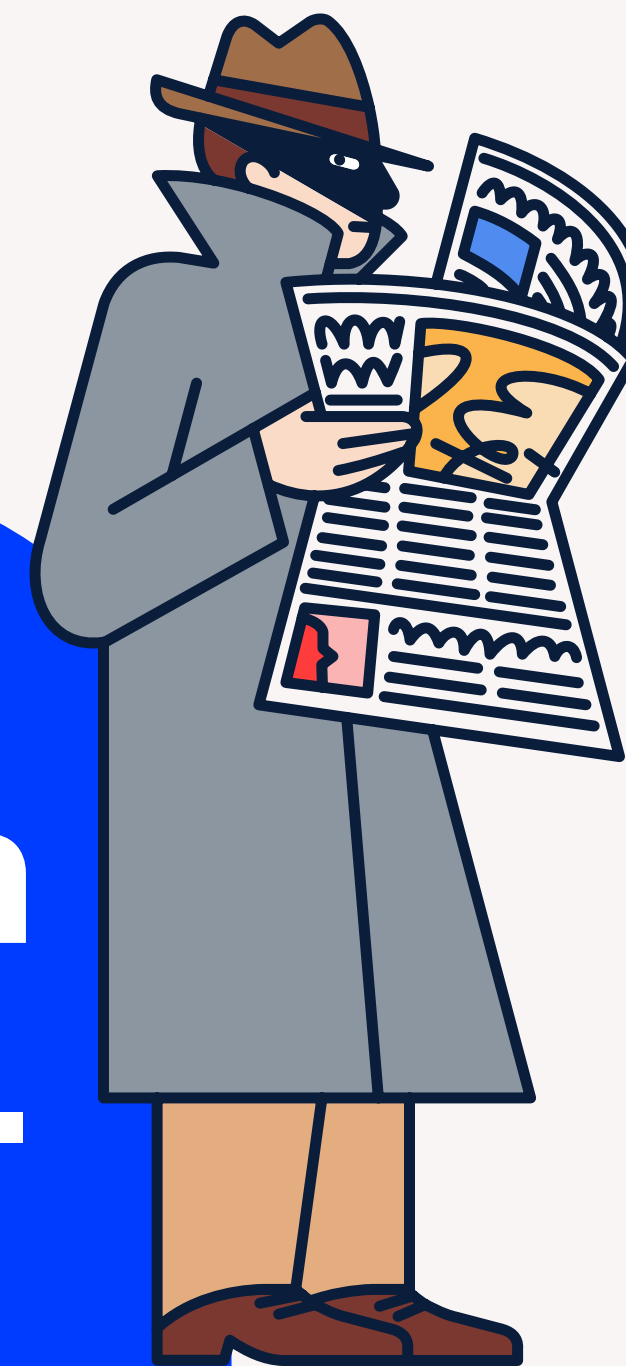
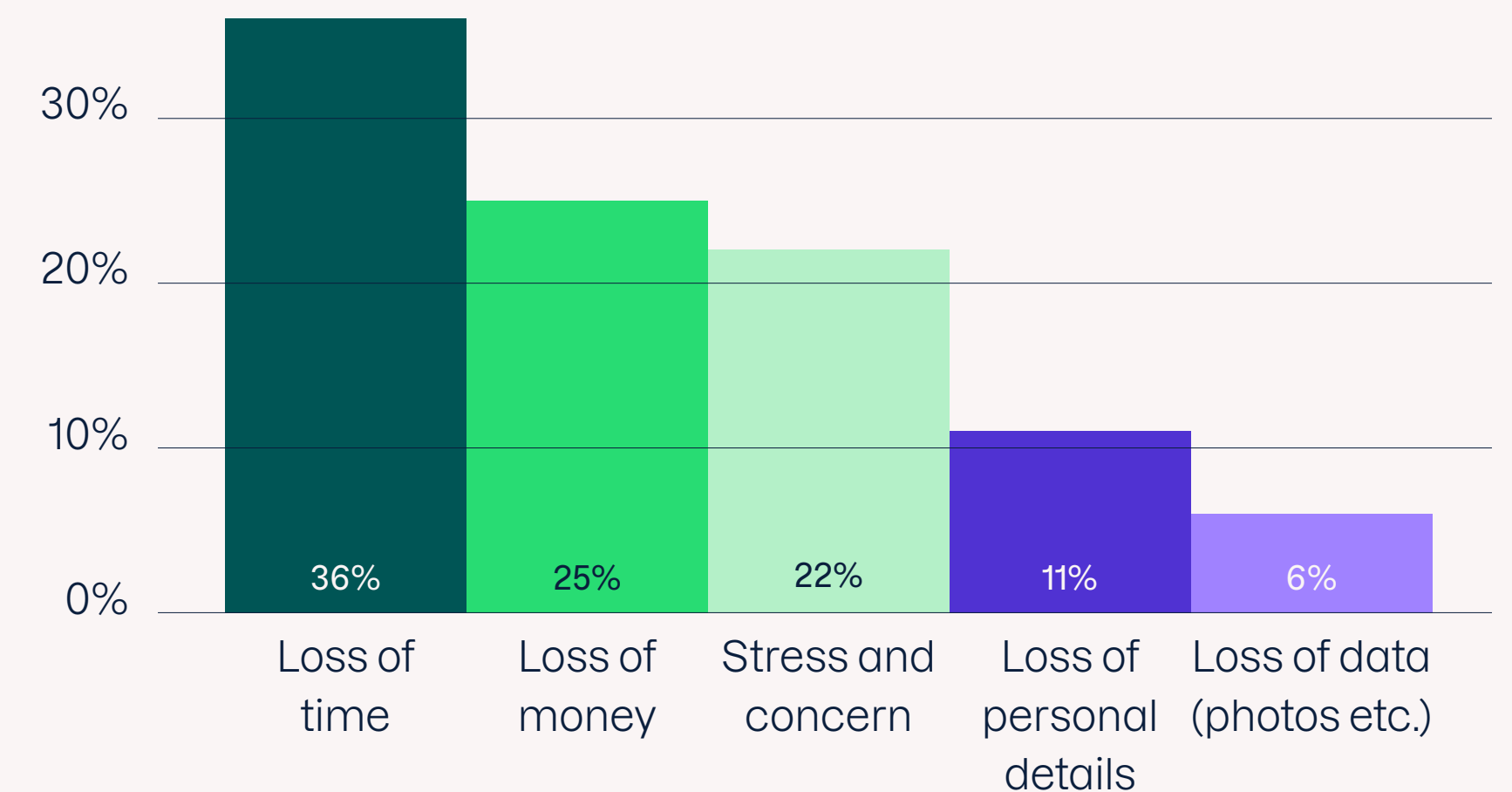
Scam attempts by channel

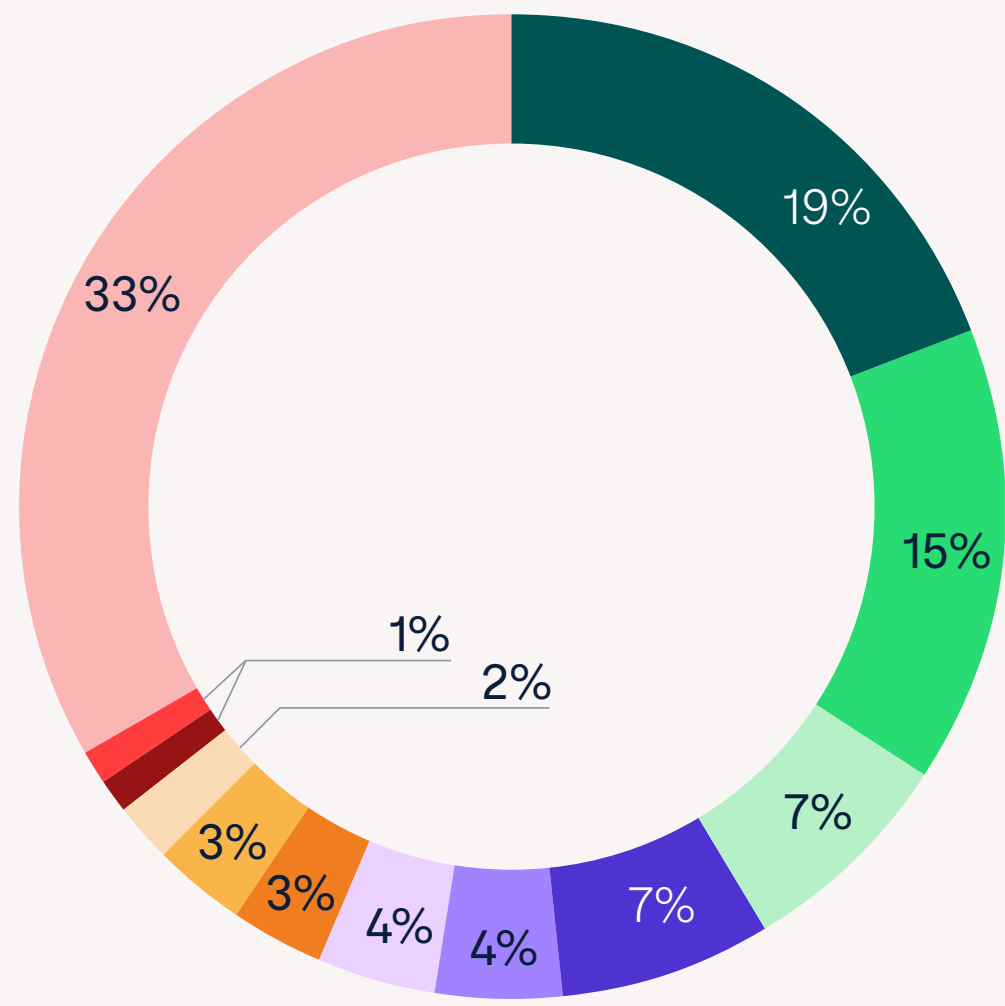
Discover the main channels being used by cyber scammers in 2024



Effects of a cyber scam

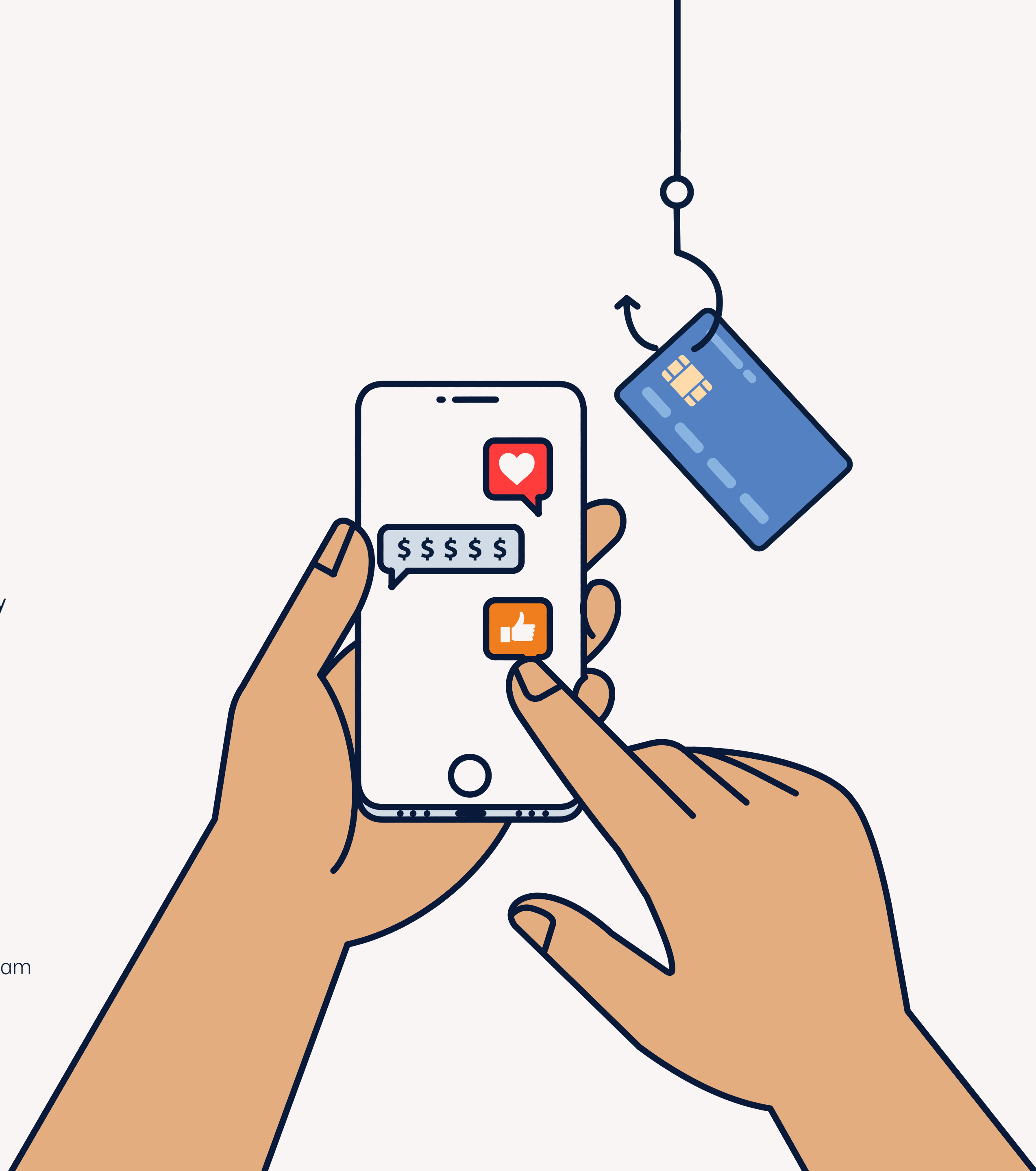
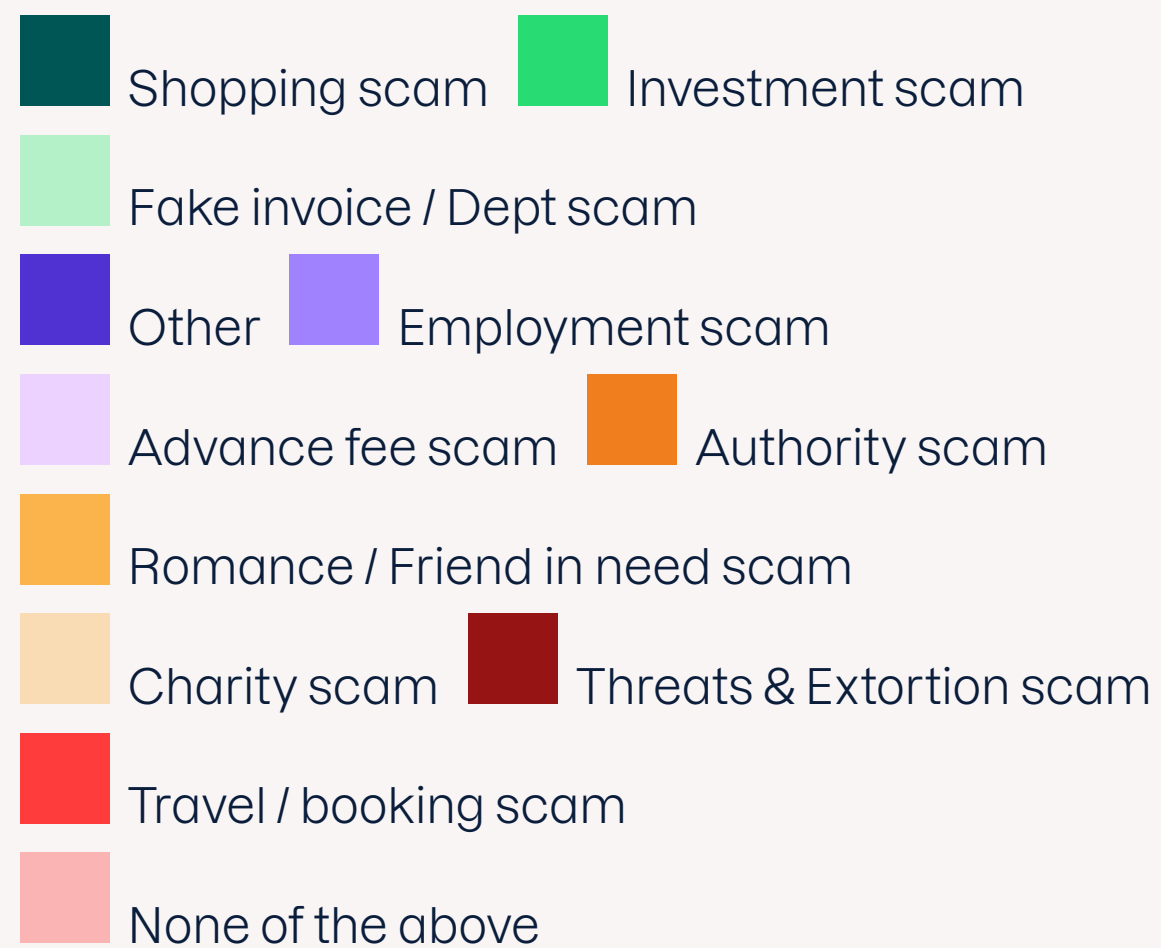
Discover how people were affected by cyber scams in 2024





2024 scam breakdown

An overview of the scam attempts received by our respondents in the last year.



“

EXPERT INSIGHT

Scams pose a unique threat to our online lives. Modern day scamming employs both the manipulation tactics that appeal to our emotional sides with the readily available technology to deliver them. This makes them a real problem for everyone.

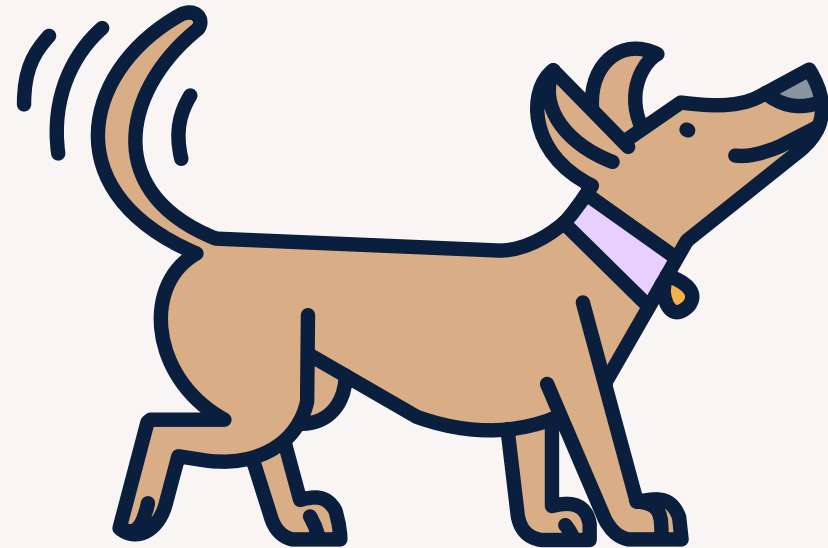
Laura Kankaala,
Threat Intelligence Lead
at F-Secure.

Trust in 2024

When compared to our 2022 results, it's clear that trust continues to be a huge issue in our digital lives, with 80% of people surveyed in 2024 saying that they worry about their online safety—a 5% increase in the last two years.

Alongside general concerns about their online safety, the Living Secure survey also found that 7 in 10 people don't know who they can trust online. And it's easy to see where the lack of trust comes from, when you consider that over half of our survey respondents (54%) said they had no idea if their digital devices were secure or not.

Given their increasing ubiquity within our homes, smart devices drew particular attention. According to [Statista](#), household penetration for smart home devices will hit 18.9% in 2024, with it expected to reach 33.2% by 2028. And our survey found that—rather than addressing the security concerns of their growing user base—smart home device manufacturers have actually lost trust since 2022 (28% worry about their smart home security in 2024, compared to 25% in 2022).



How people feel about security (2024 vs 2022)

We asked people to provide us with responses to the following statements.



7 in 10 people say that they don't know who to trust online.



80% of people are now worrying about their online safety, which is up 5% since 2022.

“

EXPERT INSIGHT

Consumer trust is plummeting due to an explosion of scams and uncertainties about online security. People are increasingly unsure about who to trust, whether their devices are secure, and how they can protect themselves online. This trend is expected to intensify with the prevalence of deepfakes and AI-generated content.

Paula Al Soufi,
Director Portfolio
Strategy at F-Secure.

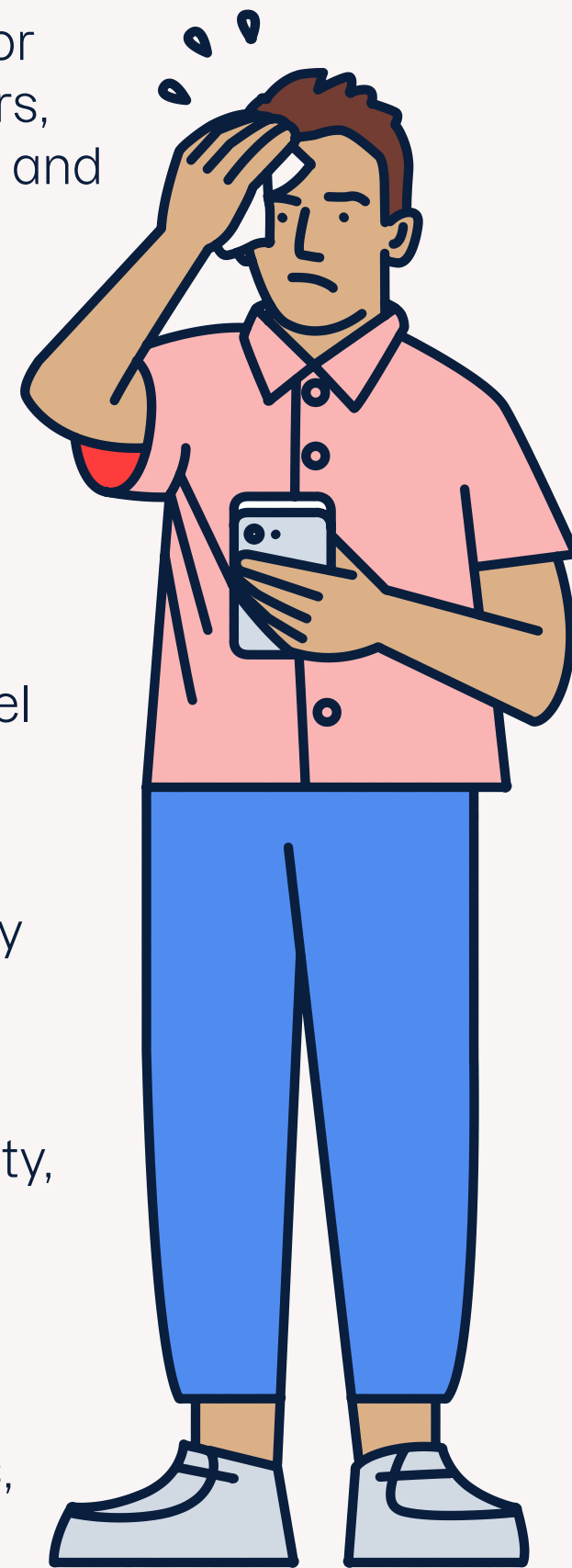
Vulnerable and confused

Our results show that a lack of trust, alongside poor transparency from service and hardware providers, has contributed to people feeling more vulnerable and confused when it comes to protecting their digital moments.

Across almost every sector, worries remain (see comparisons opposite). And huge marketing campaigns (such as Santander's award-winning 'Bank of Antandec' series) appear to have had no impact in the last 24 months. In both 2022 and 2024 the same amount of people said that they feel vulnerable when banking online (24%).

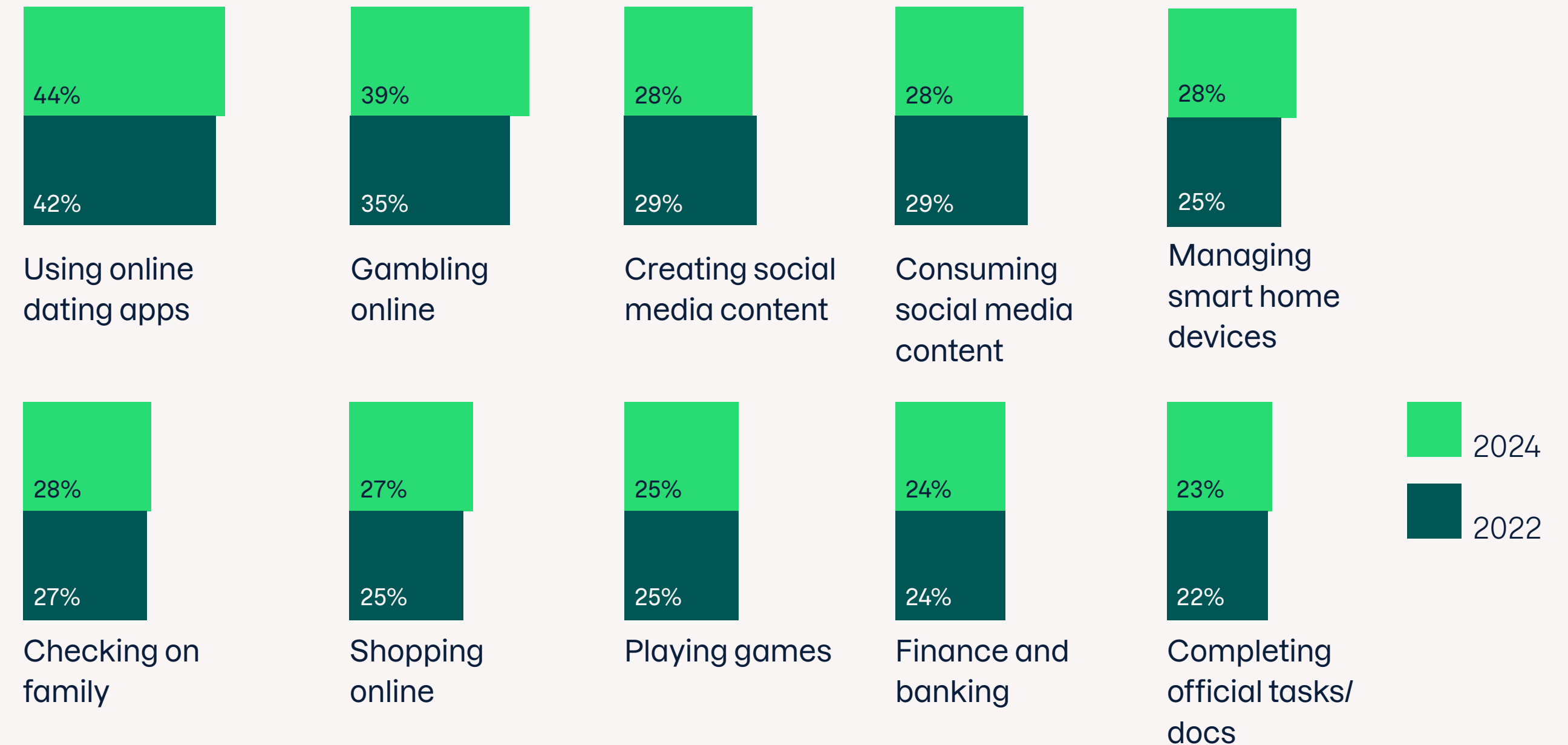
Elsewhere, people feel more vulnerable online shopping than they did two years ago; digital worry has increased for those gambling online; and the safety of dating apps continues to concern users.

When a lack of trust leads to feelings of vulnerability, confusion naturally follows. And as we saw in the previous section, 54% of people said that they had no idea if their device was secure, which was accompanied by 69% saying they found cyber security too complex. Under these circumstances, digital threats and cyber scams are flourishing.



10 moments that make us feel most vulnerable (2024 vs 2022)

Discover the percentage of people that felt vulnerable in their digital moments



70% of people think that their cyber threat is going to increase next year.

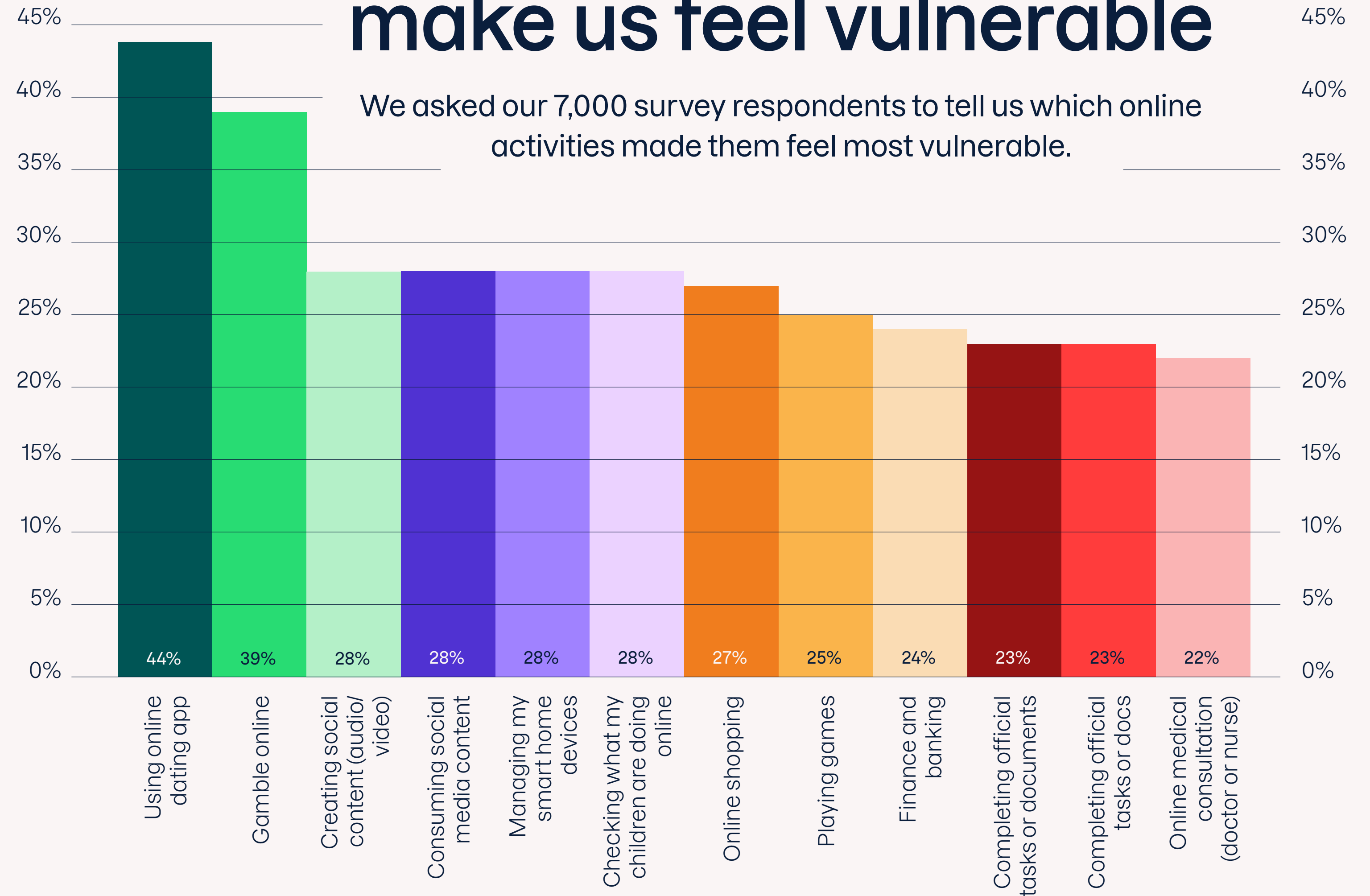
Shopping and banking

In the fall of 2023, [F-Secure](#) revealed that nearly 1 in 4 people (24%) had fallen victim to an online shopping scam in the past year. And in the same survey, F-Secure found that 6 in 10 (62%) admit they now avoid shopping with small, independent online businesses.

The findings of the Living Secure survey 2024 support these growing concerns around ecommerce, with 43% saying that they don't know how to identify a legitimate eStore, and 27% saying that online shopping made them feel vulnerable (up from 25% in 2022).

This should come as no surprise. Because when money is changing hands online, you can be sure that cyber scammers are working on ways to intercept it. Like shopping, banking and finance is also a key sector for cyber scammers. And our survey data shows that 24% of people now feel vulnerable when banking online, with 68% of people saying that they now bank or manage their finances online on a weekly basis.

Top 12 online activities that make us feel vulnerable





40% of people are now shopping online every week.

“

EXPERT INSIGHT

In 2023, we saw a rise in shopping fraud delivered through fake ads on social media. In 2024, this type of fraudulent advertisement will grow to new heights with the use of generative AI, making it hard to differentiate between fake and real ads.

Yik Han,
Researcher at F-Secure.

The evolving scamscape

Things are moving at an incredible pace in the digital world. As each year passes, digital moments are taking up more of our time. And in just 24 months, the time people spent on their top digital moments increased by up to 13% (see p7).

Sadly, despite spending more time in our digital moments, the Living Secure survey reveals that we don't feel any safer than we did two years ago; in fact, concerns have actually increased since 2022. Eight in 10 people now worry about online safety. Half of us (54%) have no idea if our devices are secure. And 69% find cyber security too complex. Given these results, 70% of people think that their cyber threat is going to increase next year.

Of our survey respondents, 85% said that they'd received a digital scam attempt, with 36% saying they get more scam attempts today than they did 12 months ago. And it's likely that these scams will not only increase in number, but also in credibility, as generative AI tools are employed to create more believable text, image, video, and audio content.



“Amidst this technological revolution, the threats experienced by people in their **important digital moments continue to increase in both quantity and credibility, making them easier to fall for.**

However, there’s a silver lining: AI helps us detect and counter threats more effectively. It also helps us develop the user experience of our security services, enabling a whole new level of **simple, effective protection.”**

Timo Laaksonen, President and CEO at F-Secure

Methodology

For the second 'Living Secure' survey, F-Secure wanted to study the importance and impact that digital moments have on our daily lives, but also expand the remit to look at digital scams. The survey captures which activities are most important to us, it covers those which make us feel most vulnerable, and it highlights how scams are increasing in a setting where generative AI makes them harder to spot.

The F-Secure consumer survey, 'Living Secure', was undertaken in January 2024. The online survey was conducted in cooperation with Dynata. And the total number of respondents was 7000, selected from seven countries: Brazil, Finland, France, Germany, Sweden, UK and USA (N = 1000/country, age 18-75 years).



f Laura Kankaala

Threat Intelligence Lead F-Secure

MEET THE EXPERT

Laura Kankaala, Threat Intelligence Lead at F-Secure

Laura Kankaala studied at Finland's Turku University of Applied Sciences before working as a security consultant for companies such as KPMG and F-Secure. Kankaala is an active speaker and podcaster, and she is a regular contributor to F-Alert, F-Secure's monthly threat report.

About F-Secure

F-Secure makes every digital moment more secure, for everyone. We deliver brilliantly simple, frictionless security experiences that make life easier for the tens of millions of people we protect and our 200 partners.

For more than 35 years, we've led the cyber security industry, inspired by a pioneering spirit born out of a shared commitment to do better by working together.

For more information visit f-secure.com today.

