Bitdefender

CONSUMER CYBERSECURITY SURVEY

The Year of AI Scams

November 2025
Global Insights from 7,000 Consumers

Table of Contents

Bitdefender

Summary

The internet is now inseparable from everyday life. From banking and shopping to sharing life milestones, consumers live almost entirely online. Yet while convenience drives behavior, it also opens the door to risk.

This year's survey of more than 7,000 consumers across the US, UK, France, Germany, Spain, Italy, and Australia highlights a troubling paradox: people know what they fear most (financial loss, scams, identity theft), but their daily habits around cybersecurity make those exact threats more likely.

The rise of AI-powered scams — deepfake audio, video, and super-realistic phishing — has made fraud harder to spot and easier to scale. Social media, once a place for sharing memories, has become the number one scam delivery system. And the very devices consumers trust the most – their phones – are not always protected.

Key Findings

1in7

Consumers fell victim to a scam in the past year

53%

Primarily conduct transactions on their phones, yet almost as many don't run an independent security solution on their phones.

48%

Accept cookies without review, with 75% only skimming or completely ignoring the terms – all to access their content faster

37%

Of consumers worry about AI-powered scams, like deepfakes

OTHER FINDINGS

7 in 10 consumers encountered scams overall; top categories include delivery/shipping fraud (21%) and credential phishing (19%)

Younger consumers are twice as likely to be scammed than older groups (20% vs 9.7%)

Besides fearing AI scams (37%), consumers are concerned about AI taking away human jobs (30%) and misinformation (29%)

Password best practices remain weak — 37% write passwords down; 17% reuse them across 3+ accounts; only 27% use a manager

Most consumers accept cookies blindly: 48% accept all cookies without review, with 75% only skimming or completely ignoring the terms

SECTION 1

The AI Scam Economy

Scammers sift through social media feeds looking for videos containing voice clips that they can use to sample a person's voice. Using just a few seconds of audio they mimic a person's voice with uncanny accuracy.

Story: 'Mom, I Crashed the Car!': Scammers Clone Son's Voice to Ask Parents for $15,000 Bailout

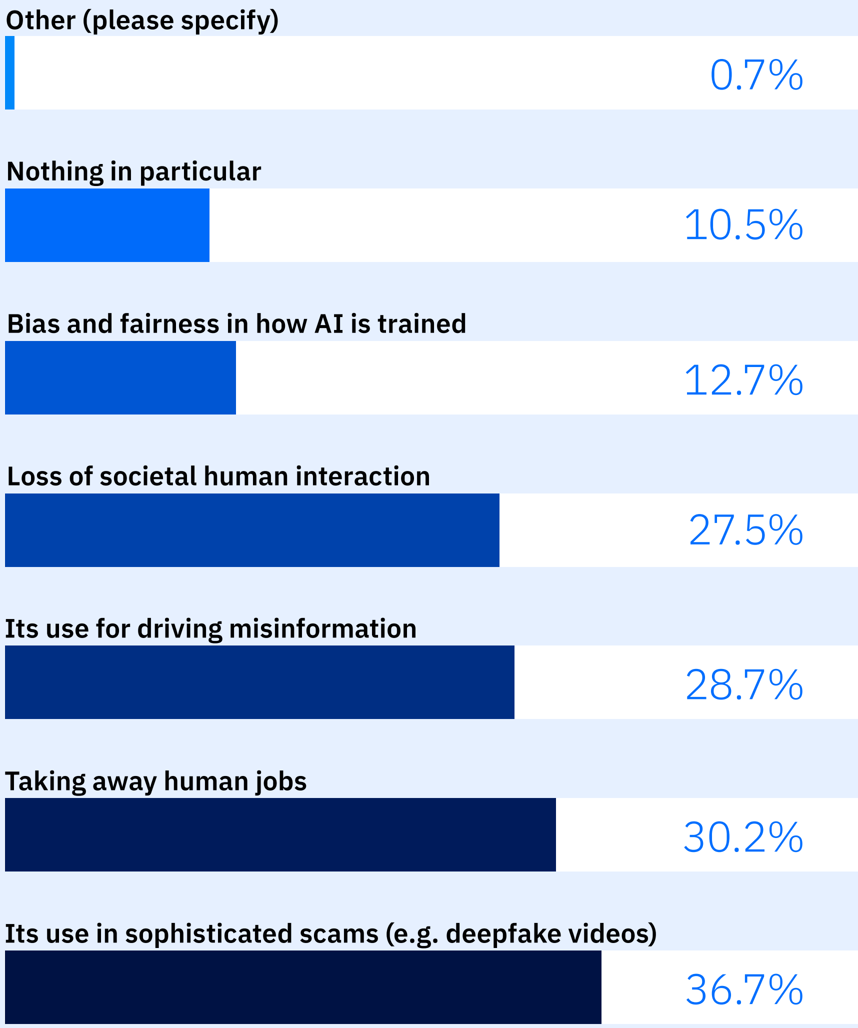
Scams are no longer a fringe problem — they are now a routine part of online life. More than seven in 10 consumers reported encountering scams in the past year, and one in seven confirmed they had fallen victim. In the context of AI, 37% named the creation of sophisticated scams (37%) like deepfake video their biggest concern. But while consumers are aware of the dangers posed by AI in the context of scams, their daily habits put them at risk (more on this below).

Question

What, if anything, worries you most about AI?

Respondents selected up to two of their top choices.

Survey Results



The financial impact is tangible. With global estimates of over $1 trillion in scam-related losses annually, and an average scam loss of $545 per victim*, that equates to over $534,000 lost among our survey participants alone. Overall, consumers are mostly concerned about AI's power to aid the creation of sophisticated scams (37%) like deepfake video. But many are also concerned about AI taking away human jobs (30%), its use in driving misinformation (29%), and its toll on human interaction (27%).

**Source: Exploding Topics, "How many people have been scammed (2025 statistics)," June 5, 2025.*

SECTION 2

The Phone Problem

Consumers increasingly treat their phones as wallets, ID cards, and lifelines to the digital world. Yet protection has not kept pace.

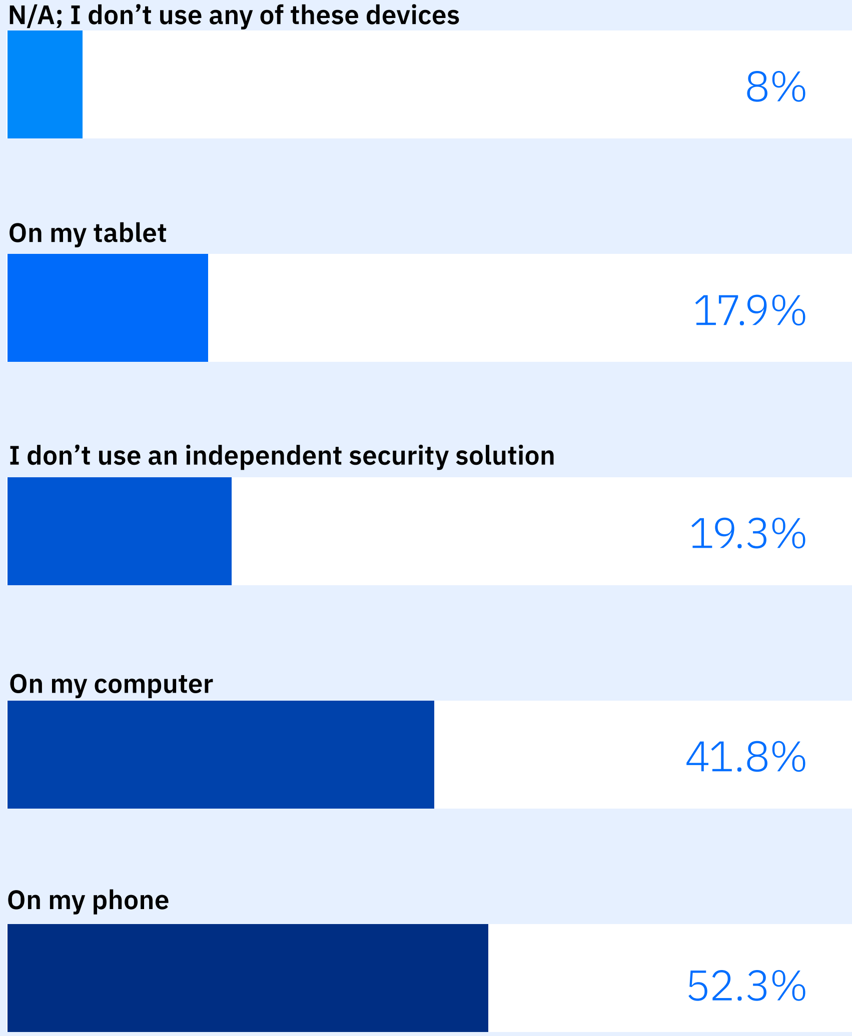
While over half (53%) say they bank, shop, and share from mobile devices, nearly half admit they run no mobile security at all.

Question

On which of the following devices, if any, do you use an independent security solution?

Respondents selected all that applied.

Survey Results



In the U.S. and Australia (45%) fewer than half of users protect their phones, while Europe is more cautious, with an average 55% of Europeans deploying a purpose-built security solution on their phones.

Bitdefender

Question

On which of the following devices, if any, do you use an independent security solution? (by region)

Survey Results

UK

On my phone	50.1%
On my computer	34.9%
I don't use one	25%
On my tablet	18.1%
I don't use any of these devices	8.1%

USA

On my phone	44.9%
On my computer	42.3%
I don't use one	23.7%
On my tablet	18%
I don't use any of these devices	10.4%

France

On my phone	56%
On my computer	45%
I don't use one	15.9%
On my tablet	16.2%
I don't use any of these devices	6.1%

Germany

On my phone	54.4%
On my computer	43.6%
I don't use one	16.2%
On my tablet	20.8%
I don't use any of these devices	8.1%

Spain

On my phone	57.6%
On my computer	40.7%
I don't use one	16.8%
On my tablet	19.7%
I don't use any of these devices	5%

Italy

On my phone	57.5%
On my computer	43.1%
I don't use one	15.8%
On my tablet	17.7%
I don't use any of these devices	6.6%

Australia

On my phone	45.3%
On my computer	42.8%
I don't use one	22%
On my tablet	14.7%
I don't use any of these devices	11.6%

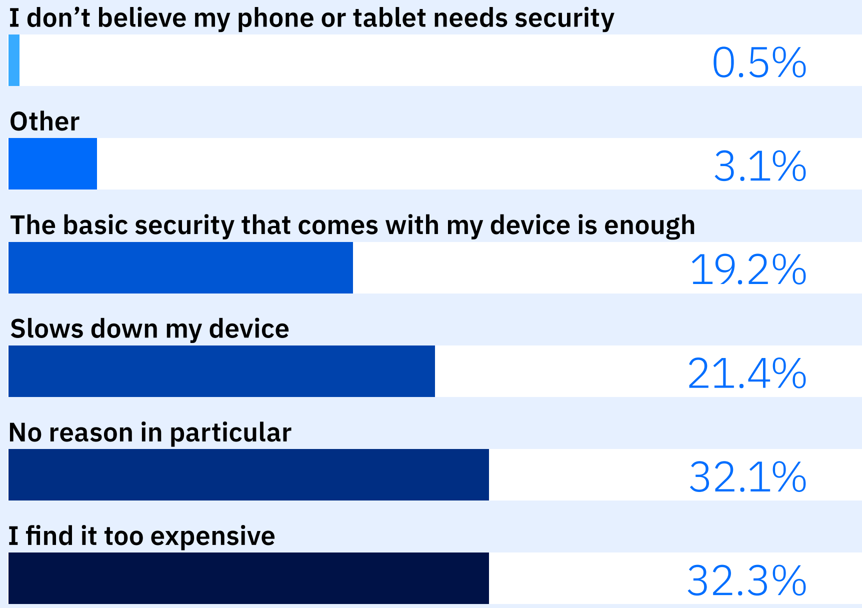
Almost a third (32%) of respondents find independent security apps too expensive, and around a fifth believe it will slow down their device. Around 19% believe their device's built-in security is good enough, while 32% stated they have no reason to eschew security apps.

Question

Why don't you use an independent security solution on your devices?

Respondents selected all that applied.

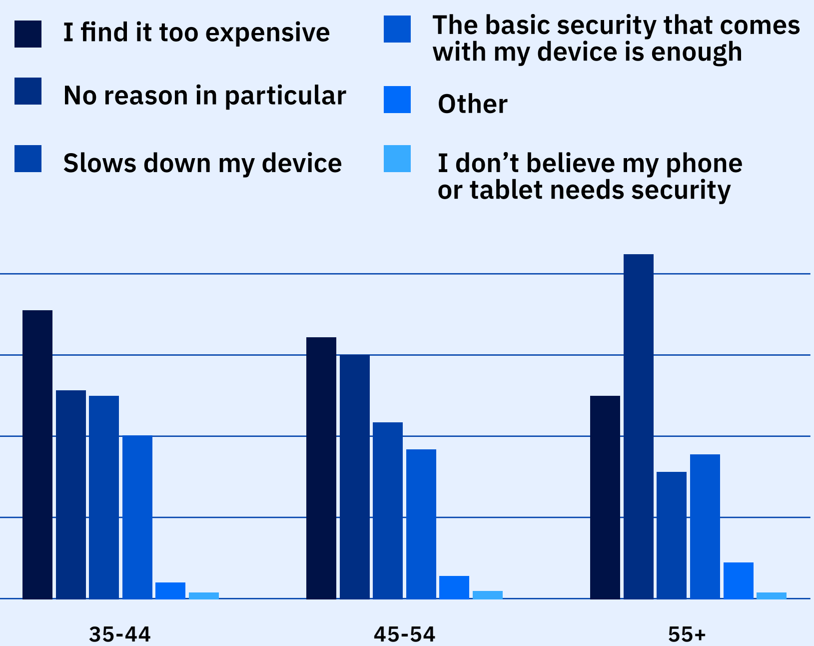
Survey Results



Older consumers are particularly complacent — almost half (44%) of those 55 and older say they have "no reason" to add protection , even as AI-voice scams disproportionately target retirees*.

Question

Why don't you use a third party security solution? (by age)



* Source: Bitdefender Consumer Insights ([Florida Woman Loses $15K to AI Voice Scam Mimicking Daughter in Distress])

Misconceptions fuel the problem: some believe a monthly factory reset is “good enough,” or that Apple devices are immune. Additionally, 8% of respondents are even using work or school devices for personal transactions, exposing both themselves and their organizations.

53% of consumers primarily use their personal phone for transactions.

48% admit they don’t use an independent mobile security solution.

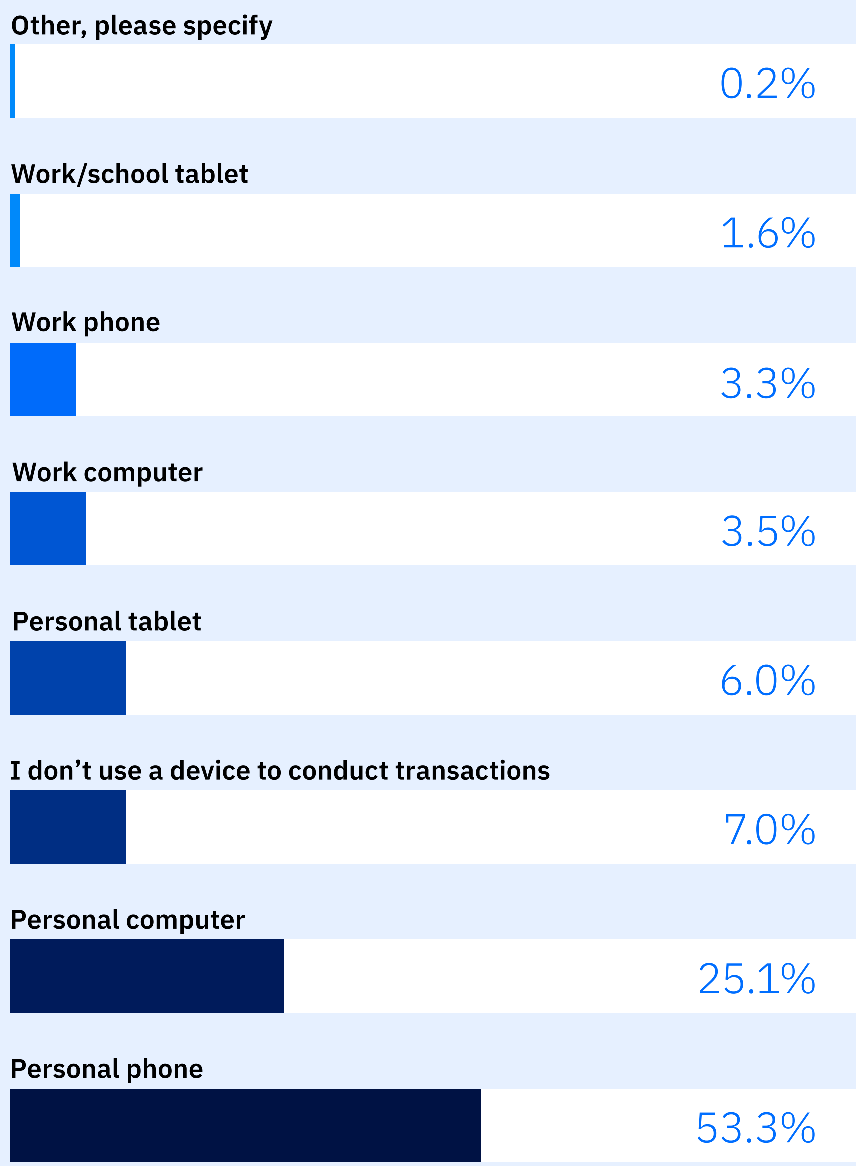
Among those who don’t protect their phone, top reasons include cost (32%), “no reason” (32%), and concerns about performance slowdown (21%).

This creates the perfect storm: the device people rely on most is often the least defended.

Question

Which device, if any, do you most commonly use to conduct transactions (pay bills, shop online, submit personal data, etc)?

Survey Results



SECTION 3

Social Media — Scam Central

Oversharing fuels fraud. Cybercriminals don't need to hack accounts when people willingly post the raw material for identity theft and scams. Younger users, who post and share the most on social media, are twice as likely to be scammed (20%) compared to older generations (9.7%).

Social media has overtaken email as the top scam delivery channel (34%), a sign of how AI-assisted deception is blending seamlessly into platforms where people already spend their time.

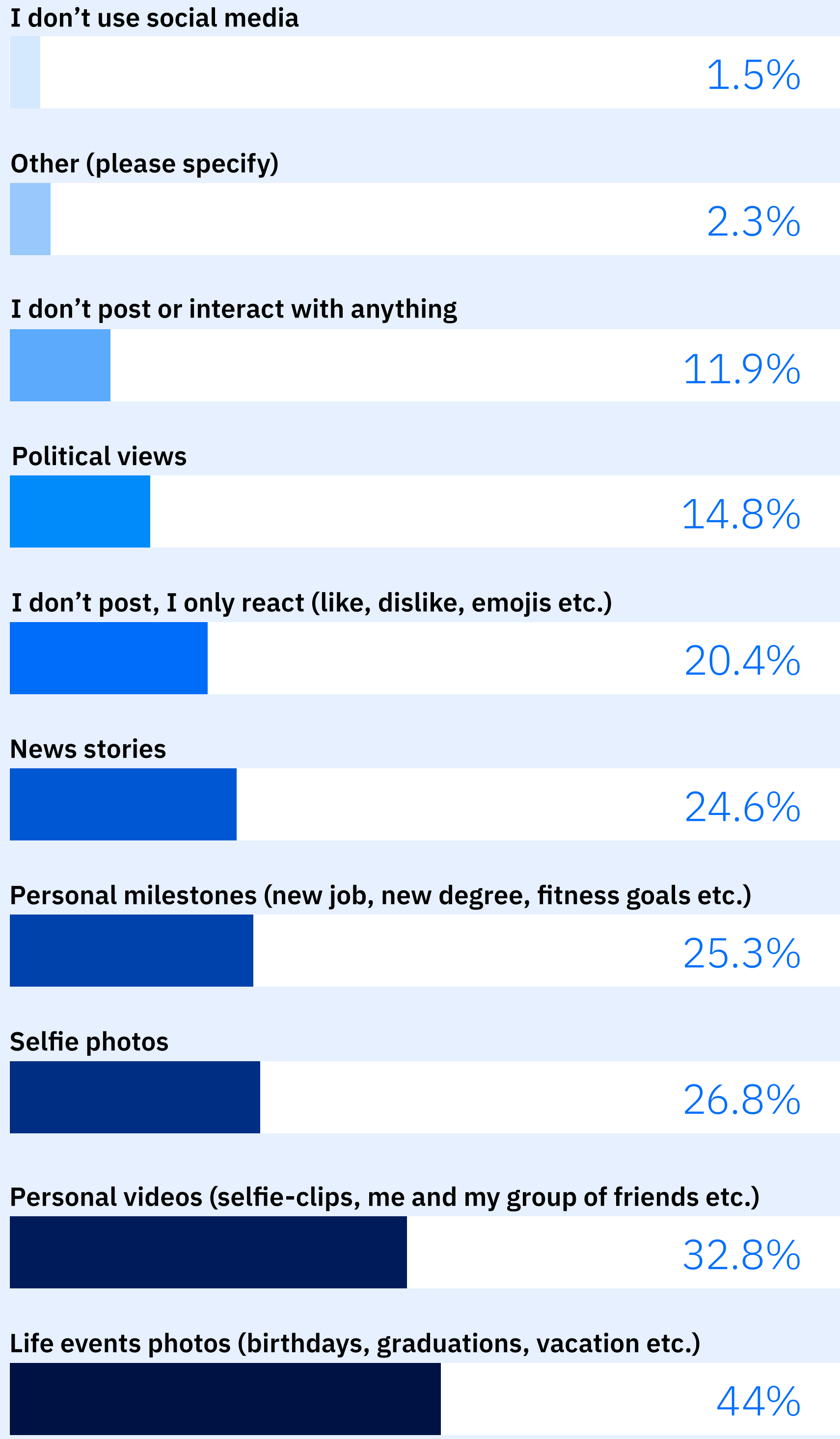
Bitdefender

Question

What type of information do you post on social media?

Respondents selected all that applied.

Survey Results

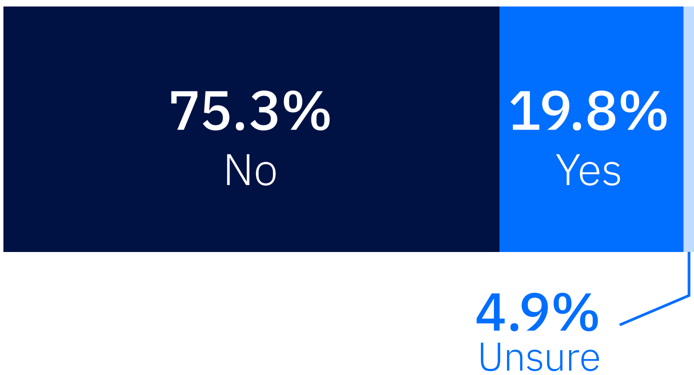


Question

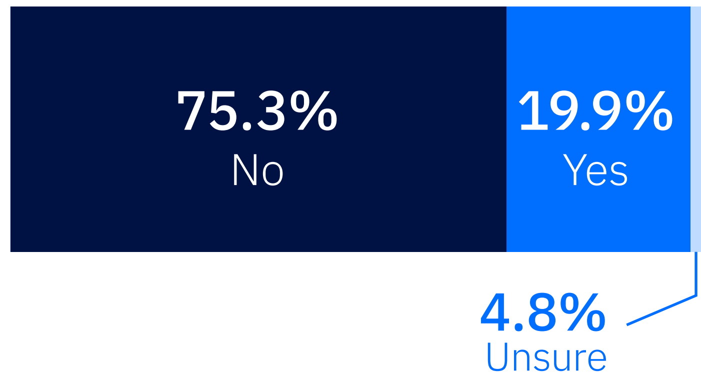
Have you fallen victim to a scam in the last 12 months (by age)?

Survey Results

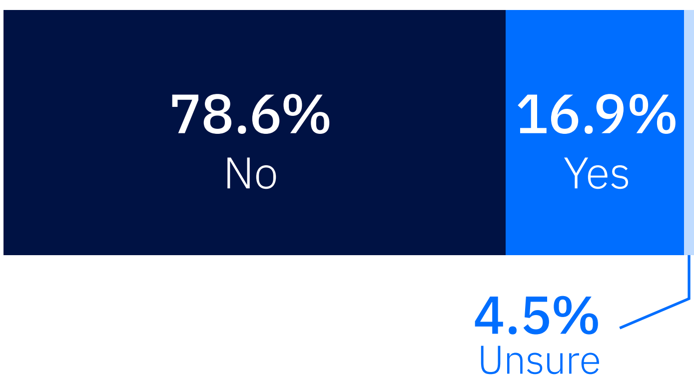
16-24 Yrs Old



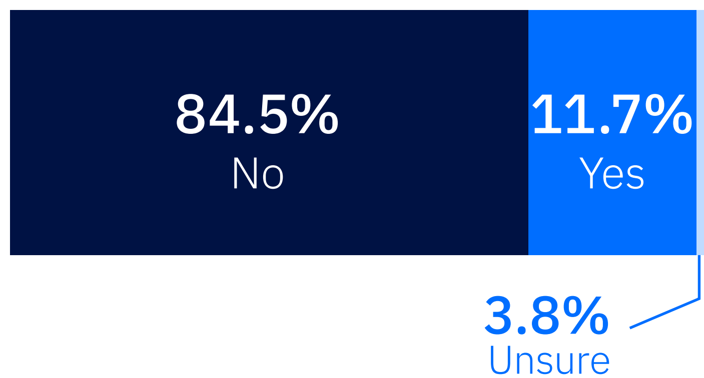
25-34 Yrs Old



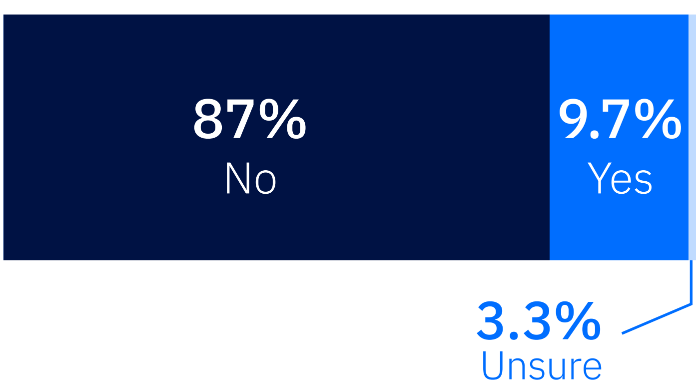
35-44 Yrs Old



45-54 Yrs Old



55+ Yrs Old

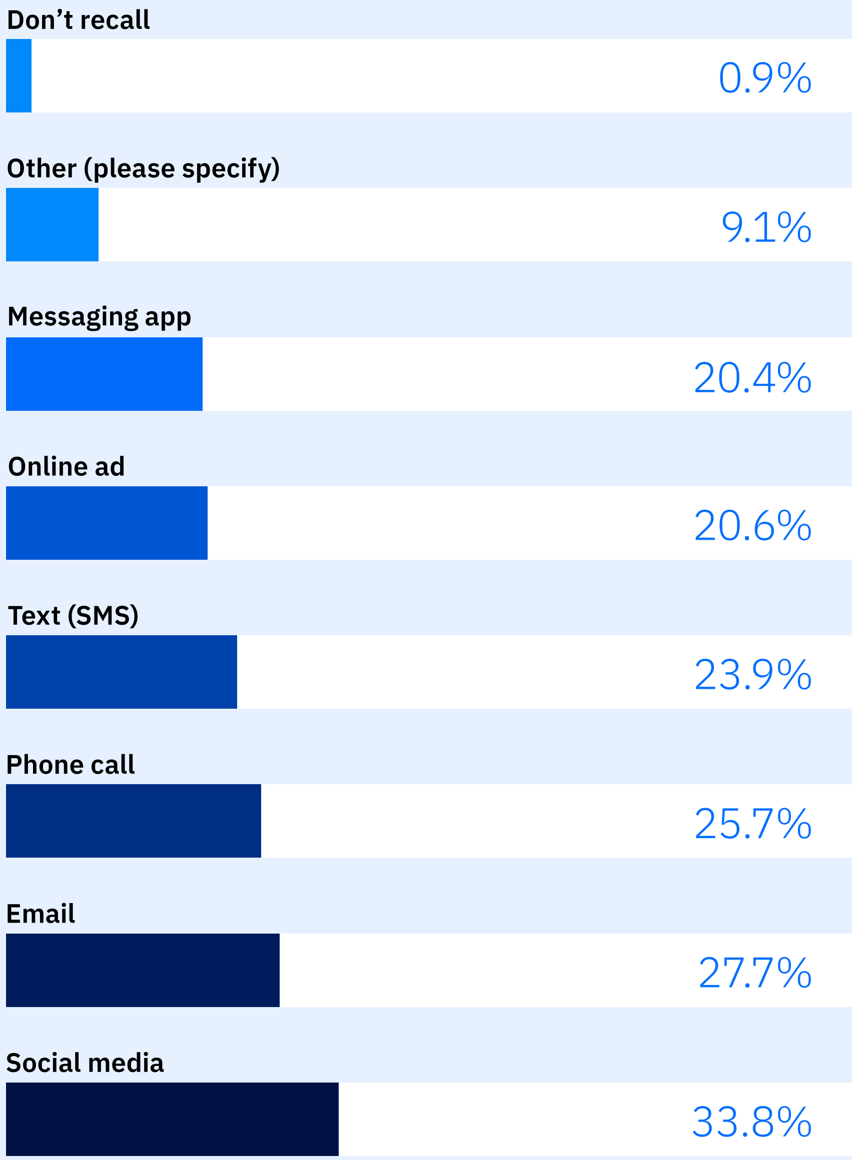


Question

How did you receive the scam(s)?

Respondents selected all that applied.

Survey Results



Perhaps unsurprisingly for a generation that has grown up with social media, youths are fueling scam risk by oversharing online — primarily TikTok, Instagram, and WhatsApp. Younger generations are also avid posters of life milestones and selfies and are daily TikTok users.

Question

What do you post to social media (by age)?

16-24 | 25-34 | 35-44 | 45-54 | 55+

Survey Results

Life events photos

16-24	25-34	35-44	45-54	55+
49.8%	55.9%	50.1%	45.9%	31.1%

Personal videos

16-24	25-34	35-44	45-54	55+
51.1%	46.8%	39.4%	32%	16.8%

Selfie photos

16-24	25-34	35-44	45-54	55+
45.5%	44%	31.2%	25.6%	10.6%

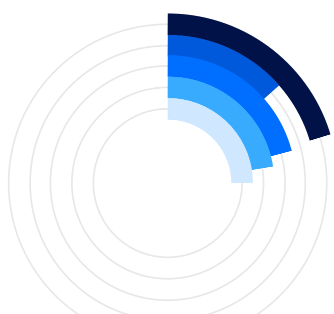
Personal milestones

16-24	25-34	35-44	45-54	55+
30.2%	39%	32.6%	25.7%	12%

News stories

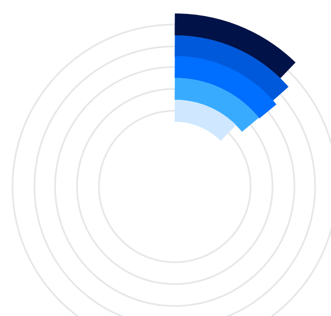
16-24	25-34	35-44	45-54	55+
19.2%	27.9%	29.3%	28.4%	19%

I don’t post, I only react



16-24	25-34	35-44	45-54	55+
17.4%	13.2%	17.6%	20%	26.9%

Political views

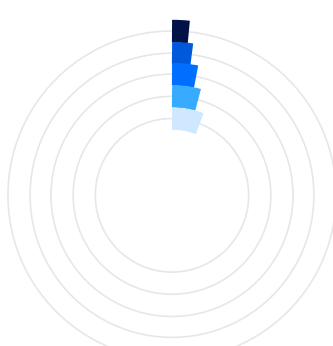


16-24	25-34	35-44	45-54	55+
14.1%	15.4%	17.3%	16%	12.4%

I don’t post, or interact with anything

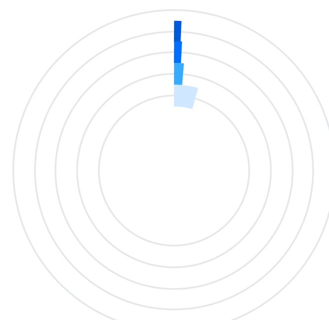
16-24	25-34	35-44	45-54	55+
3.9%	4.6%	8%	11.7%	20.4%

Other



16-24	25-34	35-44	45-54	55+
0.5%	1.5%	2.1%	2.7%	3.1%

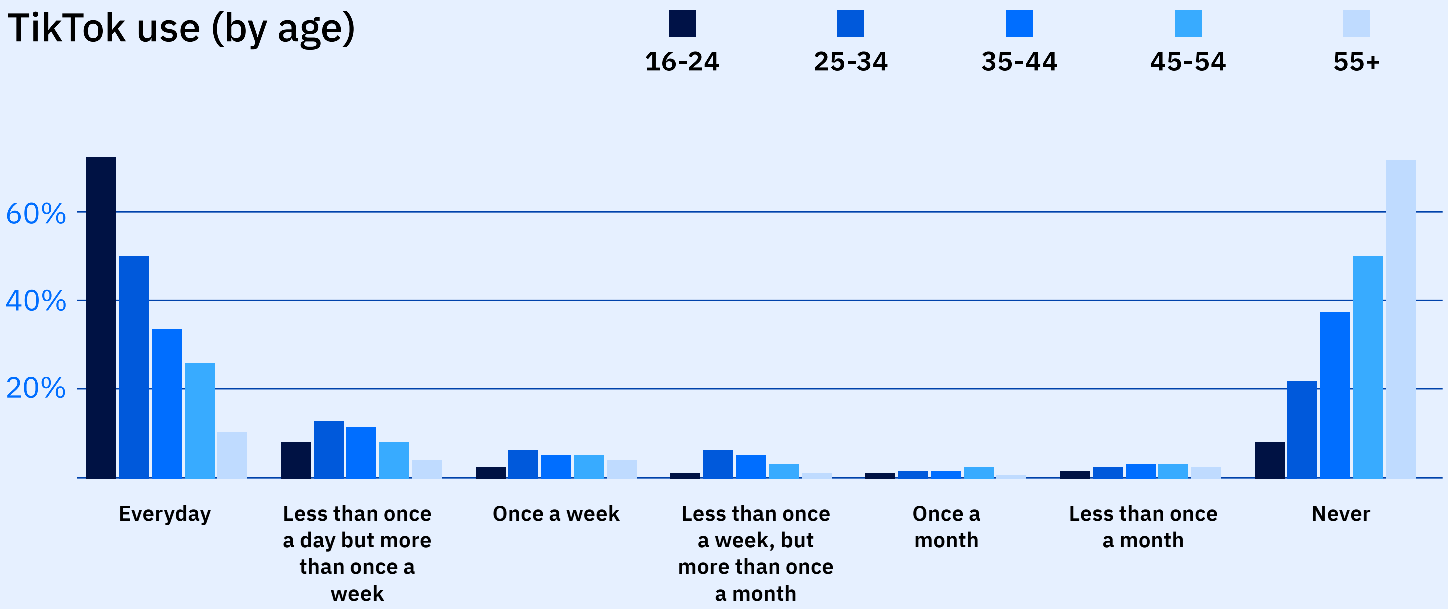
I don’t use social media



16-24	25-34	35-44	45-54	55+
0.0%	0.3%	0.4%	0.6%	3.6%

Survey Results

TikTok use (by age)

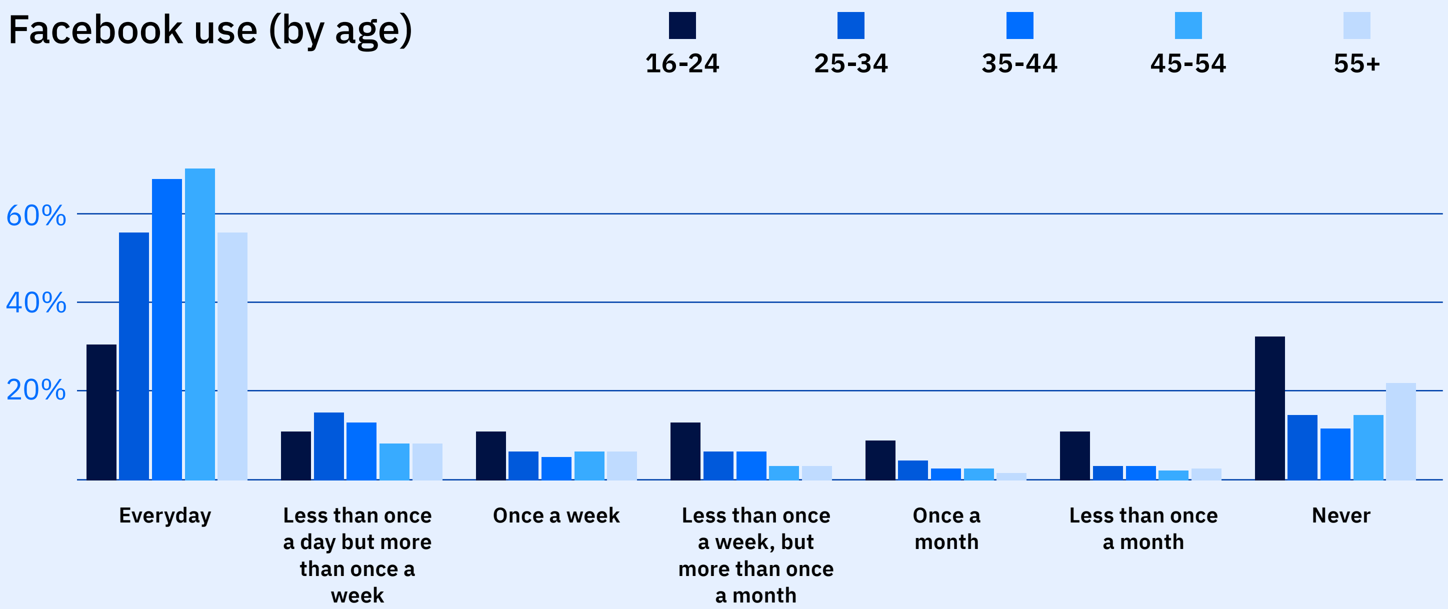


Meanwhile, Facebook and WhatsApp remain dominant among older users, creating a broad attack surface across all age groups.

Scammers are increasingly using AI to quickly adapt their campaigns to any demographic.

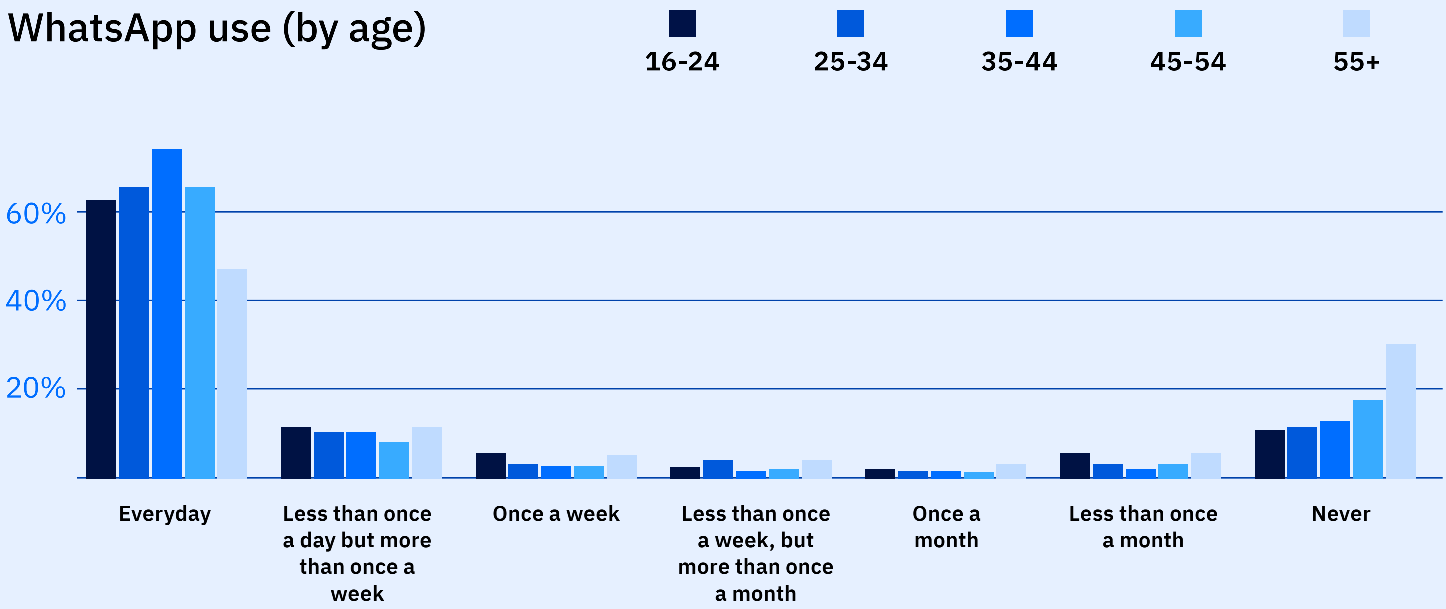
Survey Results

Facebook use (by age)



Survey Results

WhatsApp use (by age)



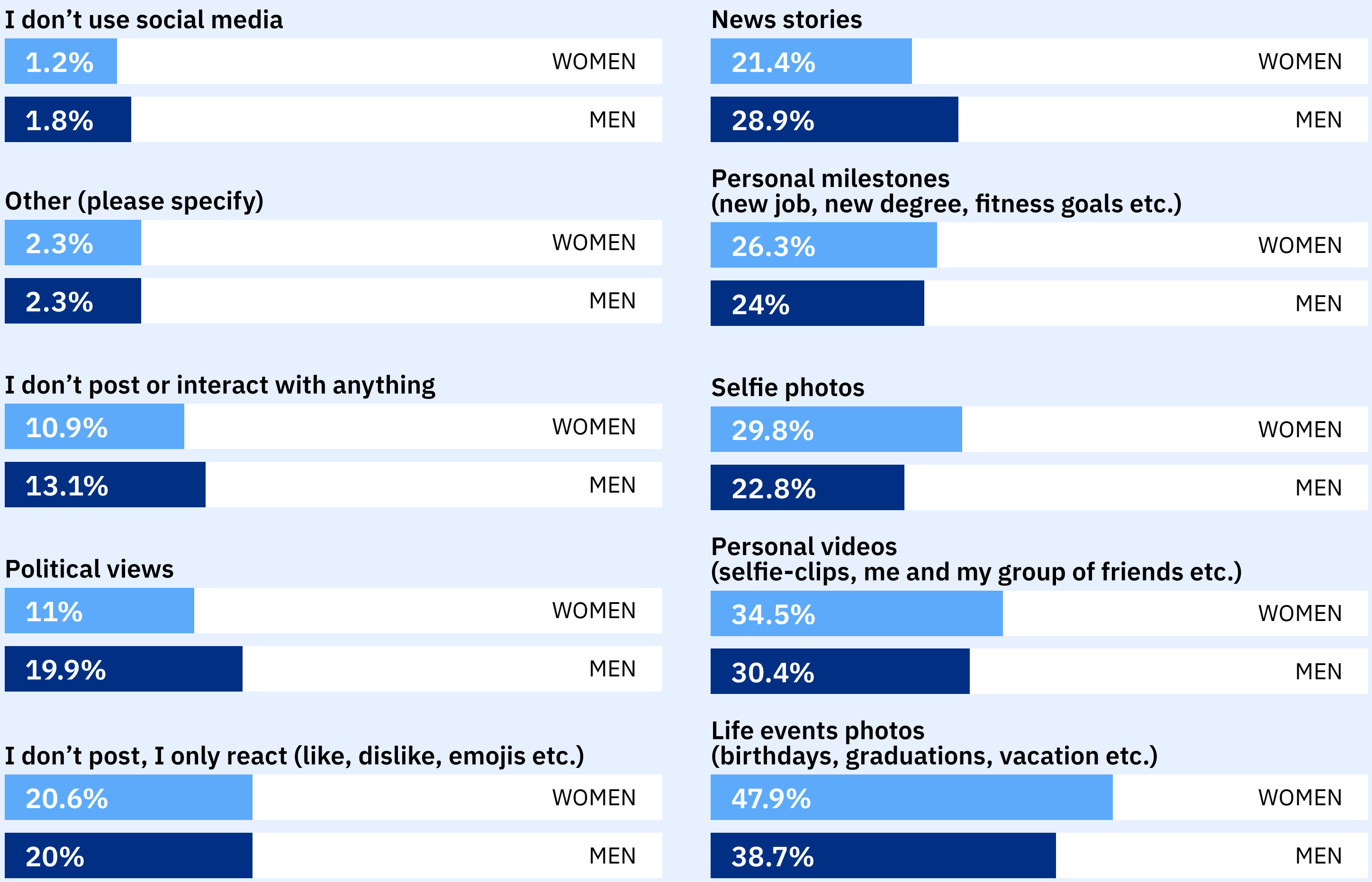
Gender splits also play a role: Women post more visual content like live events (48% vs 39%) and selfies (30% vs 23%), while men are more inclined to post news stories (29% vs 21%) and political views (20% vs 11%). Across all demographics, social platforms have become the number one attack avenue for scams.

> *Social media has overtaken email as the top scam delivery channel. Youth are fueling scam risk by oversharing online — primarily TikTok, Instagram, and WhatsApp, while Facebook and WhatsApp are dominant among older users, creating a broad attack surface across all age groups.*

Question

What do you post to social media (by gender)?

Survey Results



66% of consumers post personal content (photos, videos, milestones).

Younger users post more and are twice as likely to be scammed (20%) as older users (9.7%).

Social media is the top scam vector (34%), ahead of email (28%) and phone calls (25%).

Women post more visual content while men are more inclined to post news stories and political views.

Bitdefender

SECTION 4

Convenience Kills Security

Consumers consistently trade online safety for speed and convenience. Password reuse, blind cookie acceptance, and lax attitudes toward terms and conditions all contribute to unnecessary risk. Despite years of repeated warnings, 37% of consumers still write down their passwords and 17% reuse them across multiple accounts — essentially leaving a master key for attackers.

Only a quarter have embraced password managers. Standard cybersecurity advice is to use long, unique passwords for individual accounts, but remembering them is hard – hence why many opt to write them down. A password manager eliminates this hassle and can generate, store and constantly renew passwords so complex that they are nearly impossible to crack.

Question

How do you manage your passwords?

Respondents selected all that applied.

Survey Results

I use Apple's password autofill

13.6%

I use my browser's autofill feature

16.9%

I use a password manager

27.3%

Other, please specify

4%

I use the same password for 3 or more accounts

15.2%

I use the same password for at least 2 accounts

17.1%

I write them down

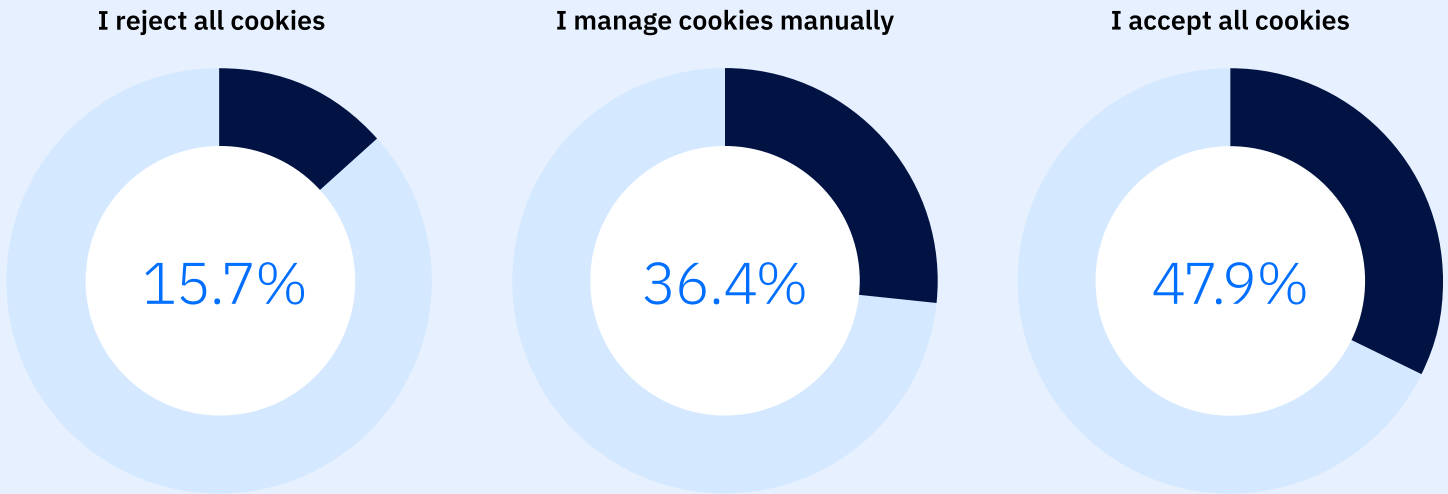
37.1%

The same pattern repeats with cookies: nearly half accept all without review, and three-quarters barely skim or ignore terms altogether. Younger generations are the most likely to blindly accept, while older groups at least attempt to manage settings.

Question

How do you manage cookies while browsing the web?

Survey Results

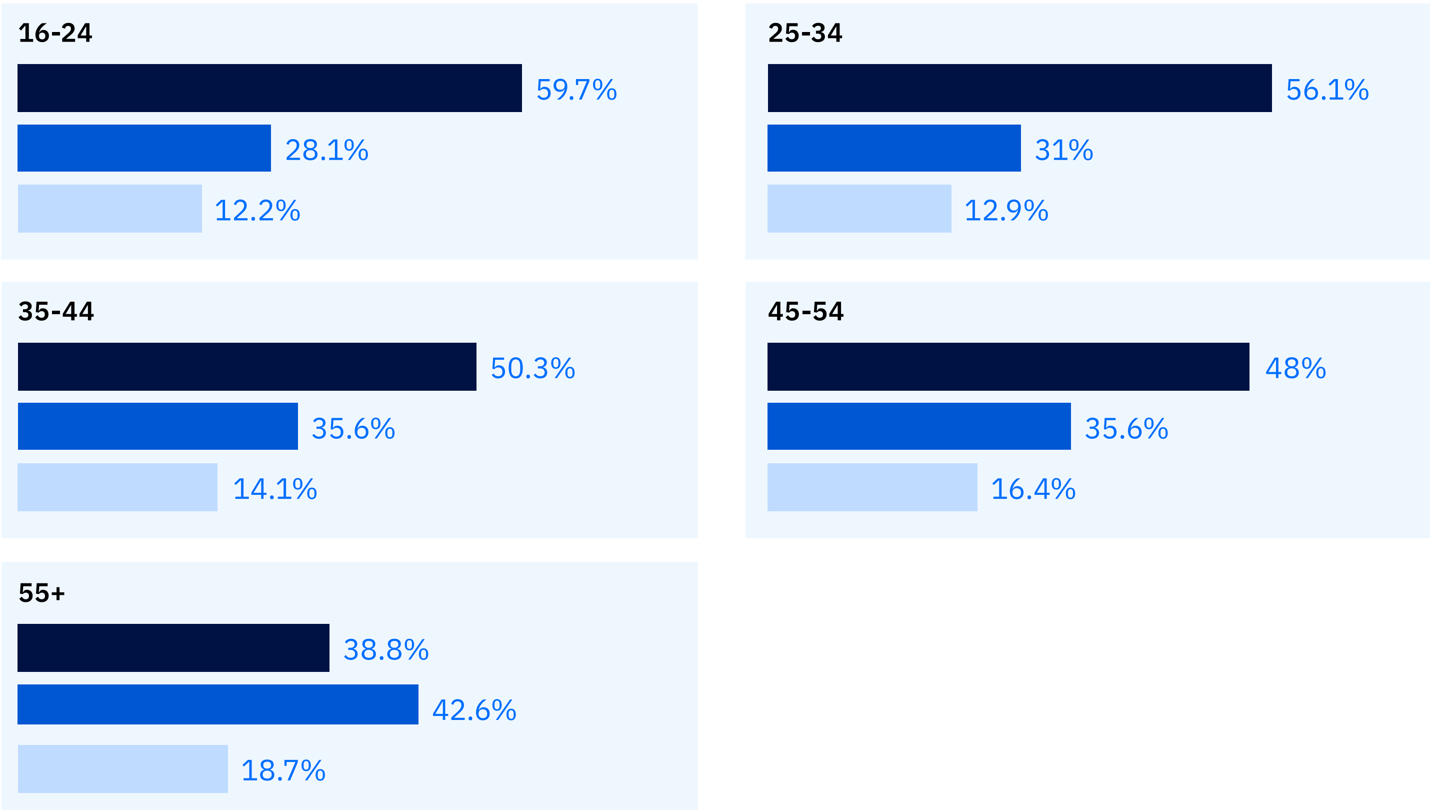


Question

How do you manage cookies while browsing the web? (by age)

I accept all cookies
I manage cookies manually
I reject all cookies

Survey Results



But across the board, speed trumps safety. Scam victims, for example, are much more likely to accept all cookies (60%) than non-victims (46%). These seemingly minor lapses—comparable to clicking on links in spam emails—add up quickly. Ironically, while consumers fear financial loss above all else (as we'll see later), it's their own shortcuts that fuel the very risks they want to avoid.

37% still write down passwords, and 17% reuse them across multiple accounts.

Only 27% use a password manager.

48% "accept all" cookies without review, and 75% don't carefully read cookie terms.

Victims of scams are more likely to accept all cookies (60%) than those who haven't been scammed (46%).

SECTION 5

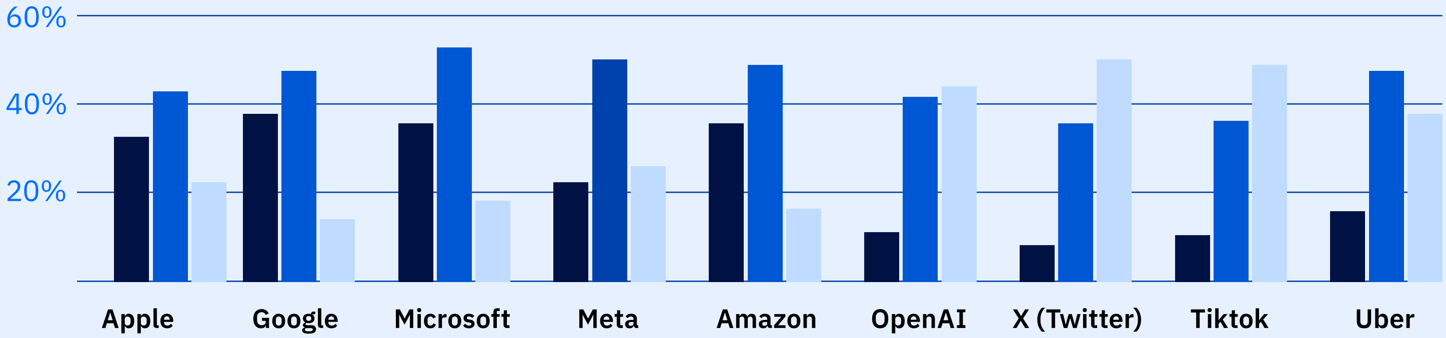
Who Do Consumers Trust?

Trust in tech giants is mixed. While people rely on their products daily, they remain deeply cautious about handing over sensitive data. Nearly nine in 10 say they trust Google (88%) or Microsoft (85%) to some extent, and over three-quarters trust Apple (77%). By contrast, skepticism runs high toward newer or more controversial platforms. More than half of respondents say they don't trust X/Twitter (52%) or TikTok (51%) at all, and almost as many view OpenAI with suspicion (45%).

Question

Do you trust tech giants with your security and privacy?

Survey Results

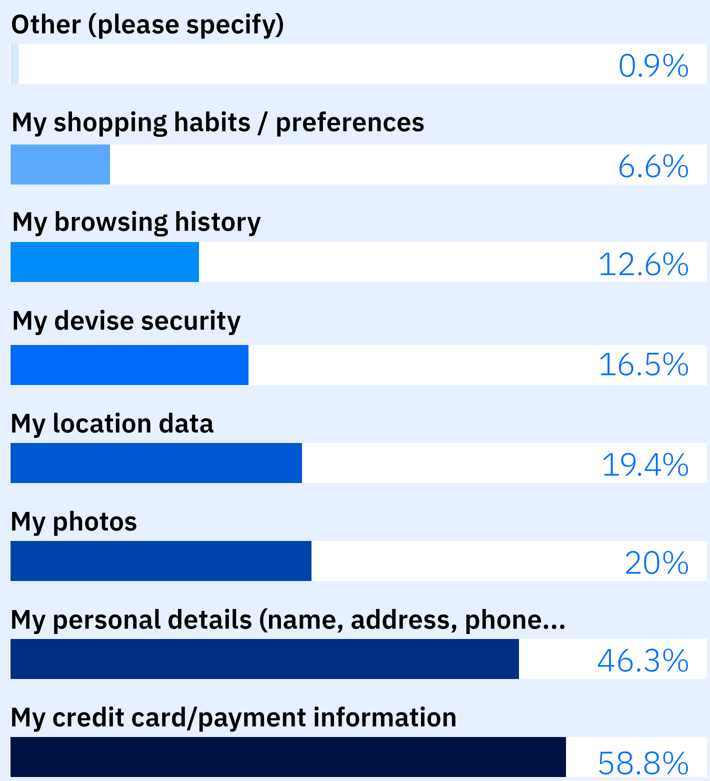


Even when trust exists, it stops short of financial and personal details. Most consumers draw the line at sharing financial information, with 59% saying they want to keep their credit card and payment data out of tech giants' reach. One in five also want to shield photos (20%) and location data (19%).

Question

What do you prefer to keep private from major tech companies?

Survey Results



The paradox is clear: consumers will continue to use platforms they mistrust, but they draw hard lines around the data they consider most sensitive — money, identity, and personal moments.

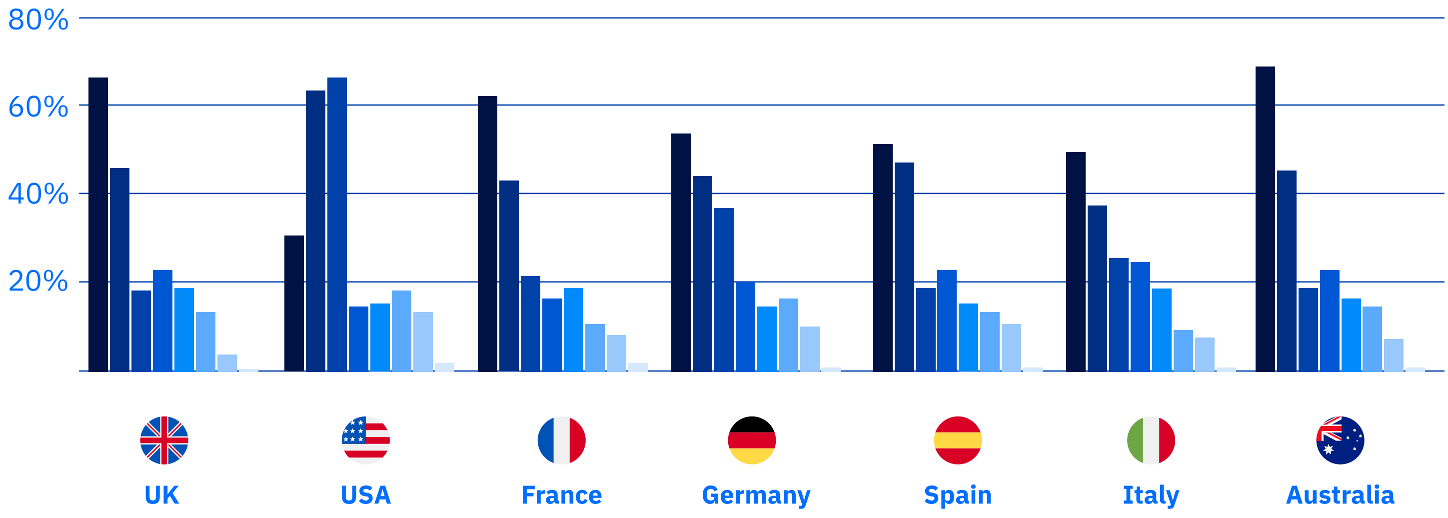
Trust in 'Big Tech' looks different in various parts of the world. U.S. consumers are less concerned about sharing certain categories like location data, with only 14% wanting to keep it private, compared to more than one in five in Spain and Italy. Europeans also tend to be stricter about safeguarding personal details, shaped by years of GDPR-driven awareness. Credit card information is the universal red line, but concern is sharper in Europe and Australia (above 60%) than in the U.S. (just over 50%). The pattern suggests that while American consumers focus on convenience, Europeans are more attuned to privacy — though both groups continue to rely on platforms they say they don't fully trust.

Question

What do you prefer to keep private from major tech companies? (by region)

- My credit card/payment info
- My personal details
- My photos
- My location data
- My device security
- My browsing history
- My shopping habits / preferences
- Other

Survey Results



Top trusted companies (trust or somewhat trust):

- Google (88%)
- Microsoft (85%)
- Apple (77%)

What consumers want to keep private from Big Tech:

- Credit card/payment info (59%)
- Personal details (46%)
- Photos (20%)
- Location data (19%)

Least trusted (not trust at all):

- X/Twitter (52%)
- TikTok (51%)
- OpenAI (45%)

SECTION 6

What Consumers Fear Most

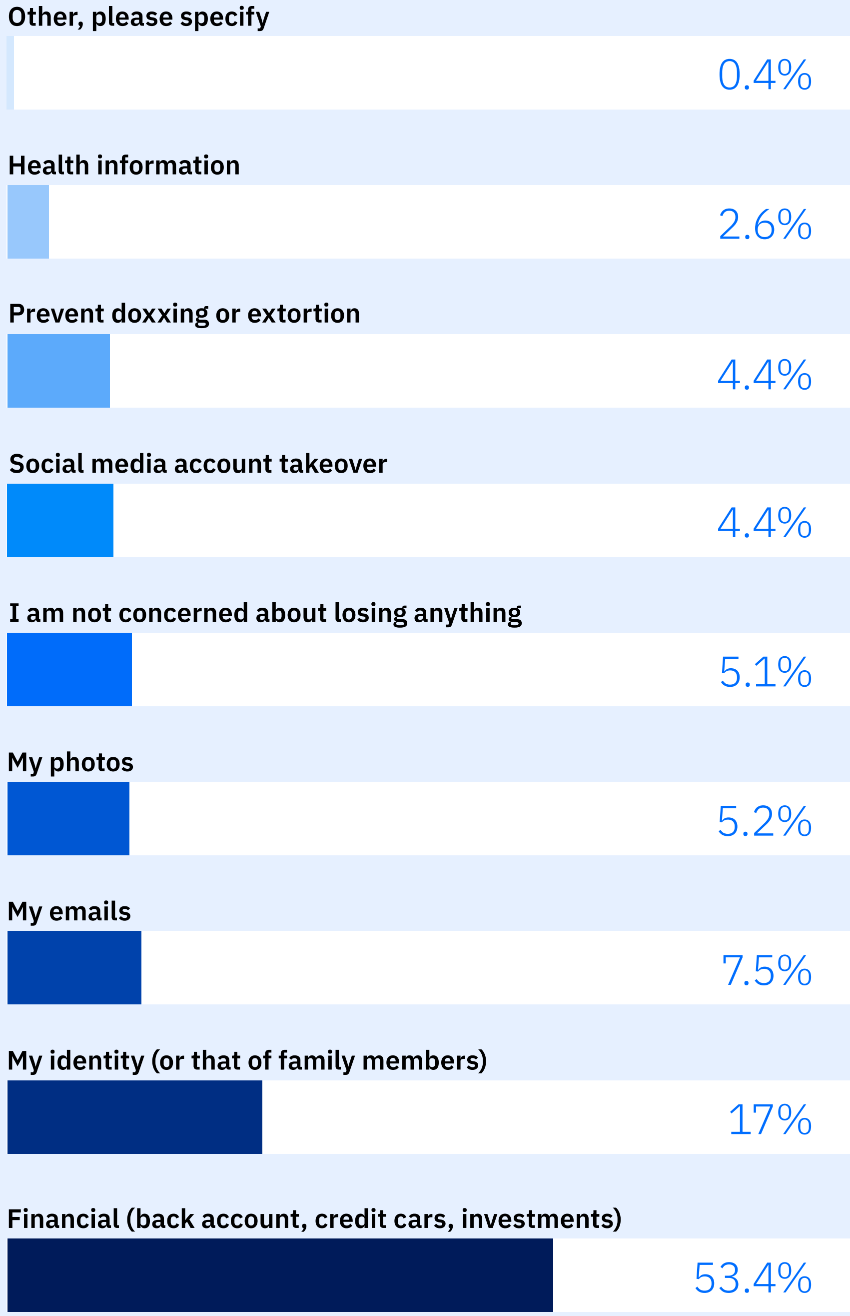
When consumers imagine the worst possible outcome of a hack, it is no suprise money dominates the picture. The majority (53%) selected financial loss as their top fear, far outpacing identity theft (17%) or the compromise of email (7%) and personal photos (5%).

Notably, 5% of respondents said they were not afraid of losing anything at all — a striking sign of complacency given the scale of scams and fraud reported annually.

Question

When it comes to what matters most to you online – what are you most concerned about protecting from a hacker, if anything?

Survey Results

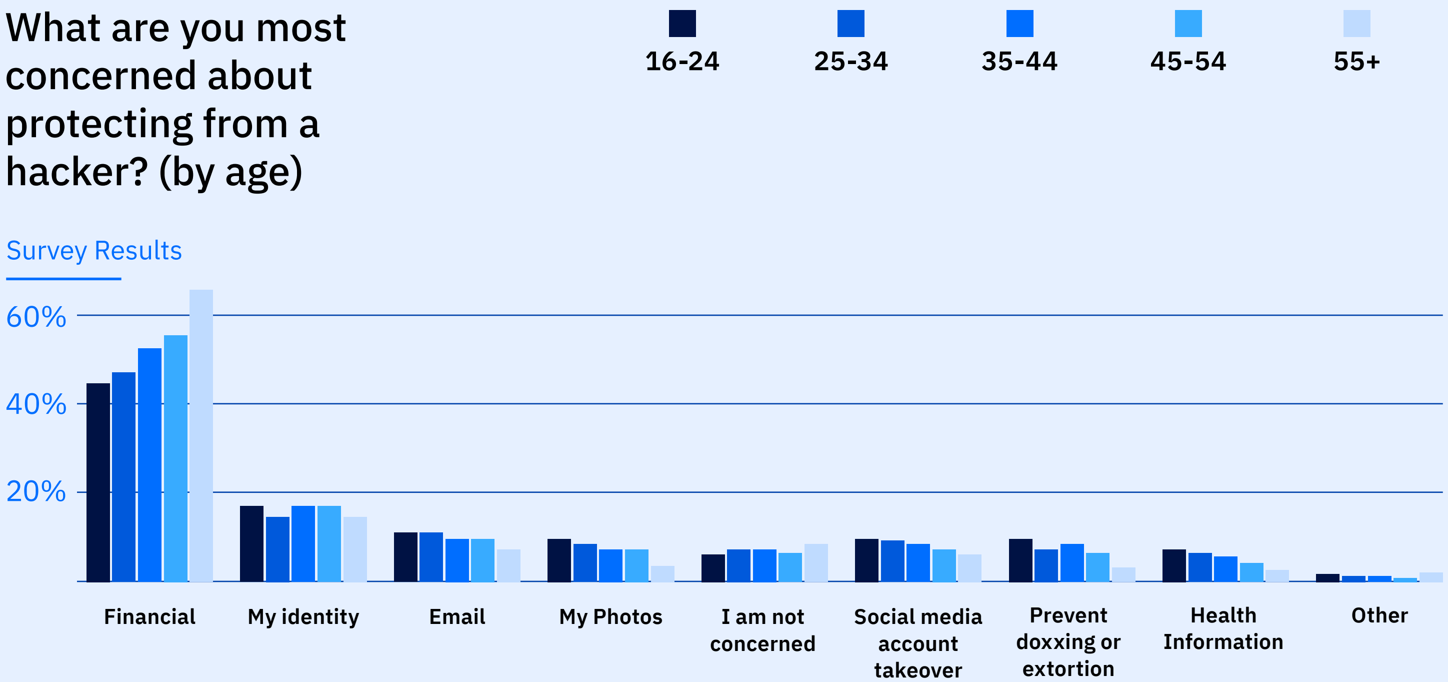


Age plays a major role in shaping these anxieties: older generations, particularly those 55+, overwhelmingly fear financial loss (63%), while younger groups express more concern about identity theft and exposure of personal photos.

Question

What are you most concerned about protecting from a hacker? (by age)

Survey Results

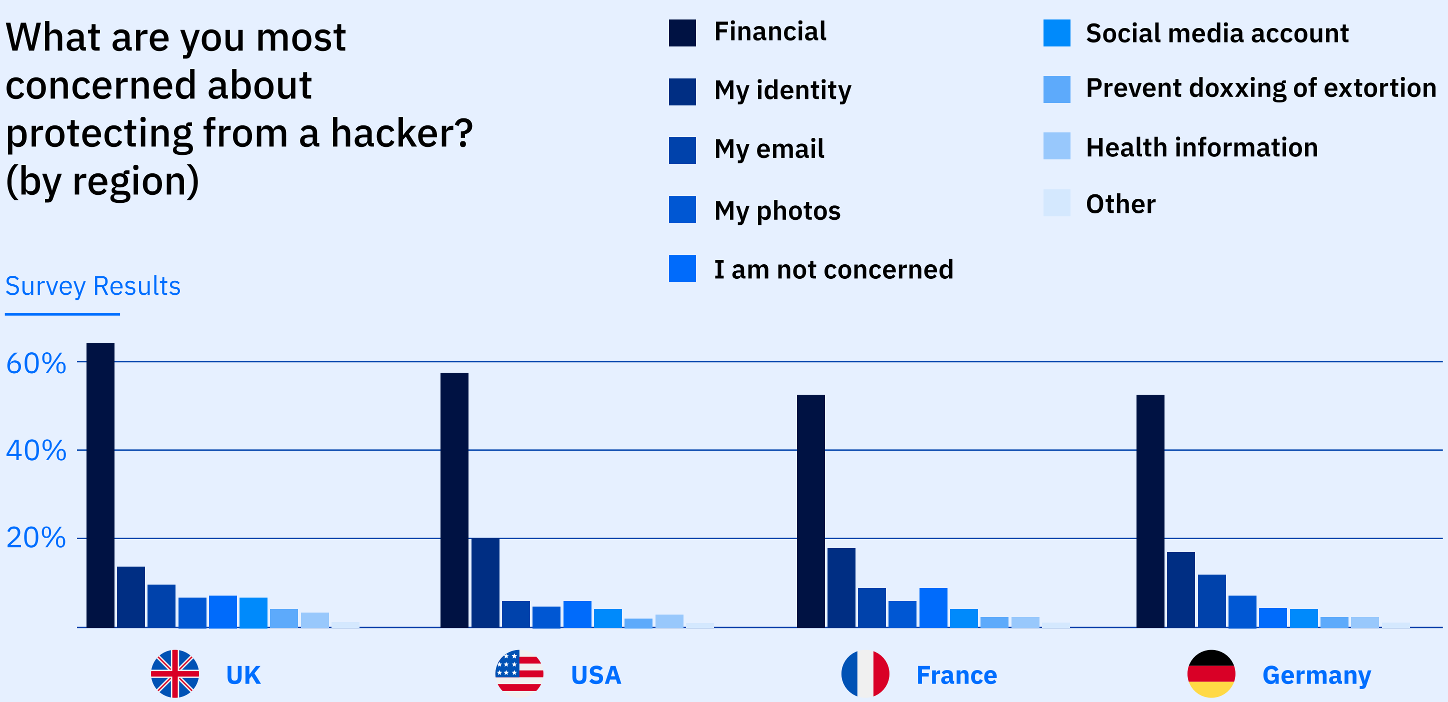


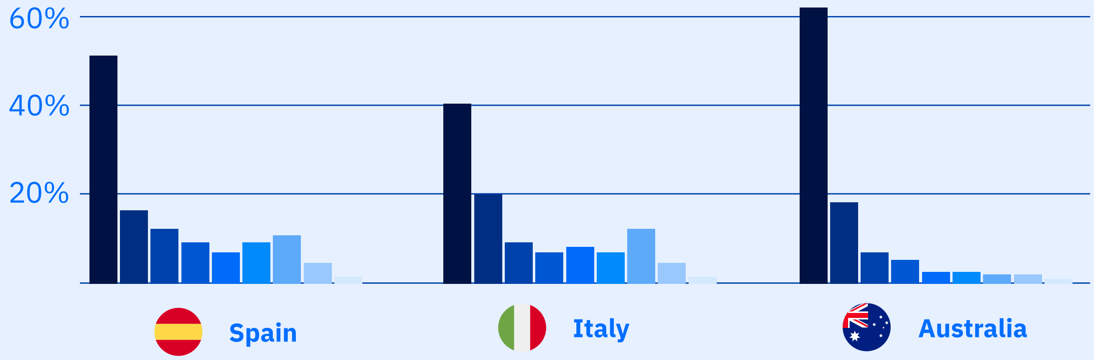
Regionally, British (63%) and Australian (62%) respondents were the most concerned about malicious attackers targeting their finances, while German respondents were most likely to worry about photos being stolen.

Question

What are you most concerned about protecting from a hacker? (by region)

Survey Results





The data underscores a consistent paradox: consumers know what they value most, but as earlier findings show (i.e. eschewing security tools), their daily behaviors often undercut their own priorities.

53% fear financial loss, far ahead of identity theft (17%).

UK (63%) and Australia (62%) are the most concerned about hackers targeting their finances.

Older generations are more concerned about finances, while younger groups worry more about stolen identity and photos.

Victims of scams are more likely to accept all cookies (60%) than those who haven't been scammed (46%).

Germany (8%) are the most likely to worry about stolen photos.

Only 3% overall worry about health data, despite its value in extortion schemes.

Spain (7%) and Italy (11%) show higher concern about doxxing/ extortion than other regions.

5% fear nothing at all — a sign of complacency despite clear risks.

Bitdefender

CONCLUSION

Conclusion And Advice For Consumers

Consumers live in a mobile-first, convenience-first world. But their daily habits — oversharing, reusing passwords, blindly clicking "Accept All," and leaving phones unprotected — are widening the gap between exposure and protection.

The rise of AI scams means that spotting fraud with "common sense" is no longer enough. Scammers now deploy sophisticated decoys capable of tricking even a trained eye.

The survey shows a consistent gap between what people fear most and how they behave online. An attitude of "it won't happen to me"—combined with the lure of convenience—continues to drive risky shortcuts. Oversharing and misplaced trust only deepen these vulnerabilities, which scammers are now exploiting at scale.

Advice for Consumers

Harden your logins:
Use a password manager, unique passphrases, and two-factor authentication to reduce the risk of account takeover.

Protect your phone first:
Install a reputable mobile security solution; keep operating systems and apps updated; and enable anti-phishing and anti-fraud protections where possible.

Think before you share:
Limit personal posts and be cautious with your voice, video, and location online – all of which can be cloned or misused for scams.

Don't accept cookies blindly:
Manage cookies manually wherever possible to minimize tracking and profiling (which can fuel targeted fraud and scams).

Assume AI is in the loop:
Treat unexpected calls, DMs, or "urgent" requests as suspect, and always verify through a trusted channel before acting.

Let good AI work for you:
Just as criminals are using AI to refine scams, Bitdefender applies advanced AI to detect, block, and stay ahead of threats – safeguarding not just devices, but your entire digital life.

About the Survey

The Bitdefender 2025 Consumer Cybersecurity Assessment Report is based on an independent survey conducted and analyzed from June–September 2025 polling more than 7,000 internet users across the United States, United Kingdom, Germany, France, Spain, Italy, and Australia. Respondents ranged from ages 16 to 65+, with quotas applied to ensure balanced representation by age, gender, and geography. The survey explored consumer attitudes and behaviors around scams, AI, mobile and social media usage, trust in technology companies, and the perceived consequences of cyberattacks. Findings provide a snapshot of global consumer risk awareness and digital life protection needs at a time when AI is rapidly reshaping the threat landscape.