



DIGITAL AND
POPULATION DATA
SERVICES AGENCY

Digital trust is beginning to recover

– for the first time in the history of the Barometer



Digital Security Barometer 2026

Contents

Executive summary.....	3
Study design and use of the results.....	8
Trust in the digital world is strengthening.....	9
Digital services and devices have boosted trust	10
Public authorities, the financial sector and Finnish origin form the foundation of trust.....	11
Use of AI is growing faster than trust in it.....	12
Digital services are widely used and their importance is well recognized.....	13
People's perception of their security skills does not match their actual behaviour.....	14
Concern about scams is increasing, but resilience is improving	15
Finns believe they can recognise scams.....	16
Cooperation and user vigilance in the fight against cybercrime.....	18
The consequences of successful scams remain significant.....	19
Digital scams are rarely reported to those who could act on them	20
Communication and clear operating models are the most important protective measures	21
Digital security is beginning to improve.....	22
12 key indicators to monitor.....	23
Ten guidelines for digital users	
- how to avoid digital scams and what to do if you are scammed.....	24
12 recommendations for organisations and associations.....	26

The Digital Security Barometer is an annual study on digital security conducted by the Digital and Population Data Services Agency.

The study has been published annually since 2020.

The target group consists of adults living in Finland.

A total of 1,250 people responded to the 2026 survey, which was conducted in July 2026.

FOR MORE INFORMATION

Kimmo Rousku

General Secretary of VAHTI, Chief Senior Specialist
 firstname.lastname@dvv.fi or digiturva@dvv.fi
 Tel. +358 295 536 000 (switchboard)



Executive summary

The 2026 Digital Security Barometer shows that, from citizens' perspective, digital security has reached a significant turning point. For the first time in the history of the Barometer, several key indicators are improving simultaneously:

- the long streak of decline in trust has stopped,
- society's sense of security has increased, and
- citizens are taking concrete protective measures more often than before.

The change is not due to the disappearance of threats, but to an improvement in Finns' ability to operate in an environment where those threats are present.

Trust in the security of digital services and devices has begun to recover. The trust index improved by seven points in one year to -20 and is already close to the 2023 level. The proportion of respondents who felt their trust had weakened fell from 38% to 29%.

The change is greatest in the oldest age groups, where trust in the security of digital services and devices improved the most: among 65–74-year-olds, the index rose by 22 points and among 75–99-year-olds, it rose by 18 points.

A total of 86% of respondents consider their everyday activities in the digital environment to be safe, four percentage points more than a year earlier.

Finnish origin is an advantage

Familiarity and Finnish origin increase trust in the digital world. Overall, 70% consider Finland's digital operating environment safe, and 54% believe that cyber and digital security are implemented better in Finland than in most EU countries.

Eighty-seven per cent of respondents trust public authorities and financial-sector organisations to handle their data securely. The difference between domestic and foreign providers is stark: 70% trust Finnish online shops, compared to only 20% who trust foreign online shops.

Trust in content produced by public authorities is also strong in Finland: 88% of respondents trust official content. This figure has remained unchanged since 2023. Sixty-six per cent of Finns trust Finnish news media, while 50% trust foreign news media.

Trust is concentrated among actors whose responsibilities are clear and who are perceived as part of Finnish society.



There is strong trust in content produced by public authorities in Finland.

Trust in AI is lagging behind its use

AI is becoming widespread faster than trust in it is growing. The share of people using AI at least monthly has risen in two years from 20% to 47%, while the share of daily users has risen from 4% to 16%. Use is no longer concentrated among young people.

Trust in AI services is clearly lagging behind: only 23% express a high level of trust in the information security of AI services or in the content they produce. AI literacy is therefore becoming a core digital-security skill.

Finns rate their own digital-security competence more highly than their behaviour would suggest.

Eighty-nine per cent of Finns rate their digital-security skills as good. Nevertheless, 12% would log in to their online bank during a phone call at the request of someone claiming to represent a bank, 6% would click a login link sent in the name of a bank or public authority, and 22% have reacted during the past year to something that later proved to be a scam attempt.

The direction of development is nevertheless positive: several competence indicators improved by 6-8 percentage points, and 48% have improved the security of their payment instruments.



*AI literacy is becoming
a core digital security skill.*

Scams are common, but their impact is declining

Scams are common in Finland, but their impact is decreasing. Eighty-one per cent of Finns have encountered a digital scam or scam attempt, and one in five encounters them at least weekly. At the same time, the average of comparable threat indicators fell in one year from 34% to 30%.

The decline is visible across all major channels, most prominently in text messages. One contributing factor is that Finland has been able to limit cybercriminal activity through technical measures developed in broad cooperation between public authorities and the private sector.

The financial sector, telecommunications operators and public authorities have developed solutions that can, for example, block access to scam websites set up by criminals and make it more difficult to spoof and misuse sender IDs in SMS scams.

Although concern about scams has increased, people feel that scams have a slightly smaller effect than before on their everyday lives and on their trust in the digital world. This suggests that Finns' digital crisis resilience is strengthening. The cost of successful scams nevertheless remains high. Ten per cent report having lost money during the year, and 9% of those lost more than 1 000 €. In order-of-magnitude terms, this corresponds to around 450 000 people and estimated annual losses of EUR 128 million among private individuals alone. In addition, 30% believe that scams cause significant financial concerns. Losses suffered by organisations come on top of this.

In addition to financial losses, scams make people more cautious and undermine trust in digital services.



Ten per cent report having lost money over the past year, and 9 percent of them lost more than one thousand euros.

Reporting needs to increase

According to the Barometer results, the area in which Finns have the greatest room for improvement is reporting digital scams.

Of those who recognised a scam, 43% did not tell anyone about it; 17% reported it to the service provider, 12% to their bank and 7% to the police. Even in cases that resulted in a criminal offence, 42% did not file a police report. However, being scammed online is nothing to be ashamed of, as even leading experts in the field fall victim to scams and lose money.

Failure to report scams weakens the situational awareness of public authorities, banks and telecommunications operators and slows down prevention efforts.

Finland's strength is not a low number of scams, but a growing ability to function despite them.

Citizens' digital-security competence has improved, and it remains important to continue developing it. However, security cannot be based on the assumption that every user should be able to recognise increasingly convincing and technically sophisticated scams. The next development step is to strengthen security further in service structures, processes and technical safeguards. Users should be able to verify the authenticity of a contact easily, report suspicious activity and receive protection even when they do not personally recognise a scam.

At the same time, closer cooperation and a clearer division of responsibilities are needed between public authorities, the financial sector, telecommunications operators, digital platforms and service providers. The aim is an environment in which the secure course of action is also the easiest and the default option for the user.



Security must work even when people make mistakes.

Study design and use of the results

The Digital Security Barometer study of the Digital and Population Data Services Agency examines cybersecurity and digital security competence, attitudes and experiences of adult residents of Finland concerning the safety of the digital operating environment.

The aim is to build an overall picture of how Finns use digital services, how they perceive their own competence and security, and how they view current phenomena and threats in the digital world. The Digital Security Barometer has been conducted since 2020. The study concept was renewed in autumn 2022, when research company Vastakaiku Oy was selected to carry out the study. The survey data are collected through the M3 panel maintained by Bilendi Oy.

This report presents the results of the 2026 Digital Security Barometer. Some of the results are compared with earlier Digital Barometer results from 2023-2025.

The target population consists of adults residing in Finland. A total of 1250 people responded to the 2026 survey in July 2026. The results have been weighted so that the data form a nationally representative sample by gender, age and region

of residence. The margin of error for the 2026 study is approximately +/-3.0 percentage points at a 95% confidence level.

The study makes it possible to examine, among other things, how significant a role the digital world plays in Finns' everyday lives and how actively different digital services and devices are used. The Barometer also provides information on citizens' use of AI and their trust in it, as well as on how Finns assess the state of cyber and digital security in Finland.

The study also examines Finns' own assessments of their digital-security competence, their sense of security in everyday life and the digital threats they encounter. It also explores the extent to which Finns trust different actors and digital services to handle personal data and other important information securely.

In 2026, new questions were also added to the study to enable comparisons, for example, of Finland's international position.

At the end of the report, we provide ten guidelines for digital users on how to avoid digital scams and what to do if they are scammed themselves. We

also provide recommendations for organisations and associations on improving security in digital transactions and services.

The Digital and Population Data Services Agency uses the results of the Digital Security Barometer in developing cyber and digital security, in the work of the Public Administration Digital Security Steering Group (VAHTI), and in the agency's own projects and services.

The Barometer's longitudinal data also make it possible to monitor year-to-year changes in attitudes, competence, behaviour and trust relating to digital security.

More information on VAHTI activities

<https://dvv.fi/vahti>

We also maintain and continuously develop the My personal data has been stolen or leaked guide for citizens:

<https://www.suomi.fi/guides/data-leak>

Trust in the digital world is improving

The most significant message of the 2026 Digital Security Barometer is a positive change. For the first time in the history of the Barometer, several important indicators have simultaneously turned in a better direction.

Trust in the digital world is no longer declining as it did in previous years. Instead, the sense of security has strengthened and Finns are taking concrete measures to improve their own security more often than before.

Trust has started to improve, but there is still much work to be done.

The consequences of digital scams can be significant and have a serious impact on the victim's finances.

Organizations should develop and regularly practise their processes for responding to digital scams.



Digital services and devices have boosted trust

The clearest change is seen in trust in the security of digital services and devices.

The trust index improved by seven points from 2025 to 2026, from -27 to -20. The index is calculated as the difference between the share of respondents who feel their trust has strengthened and the share who feel it has weakened.

The proportion of respondents who felt their trust had weakened fell from 38% to 29%. Sixty-two per cent said their trust had remained unchanged and 9% said it had strengthened.

The 2026 result is already very close to the 2023 level, when the index stood at -19.

Respondents attribute the strengthening of trust to improvements in protective measures, identification and authentication, monitoring and scam prevention; increased digital-security communication; and actions taken by banks, telecommunications operators and public authorities. People also feel that their own competence and caution have increased.

Factors weakening trust include the increasing number and credibility of scams, more sophisticated scams enabled by AI, and the feeling that too much responsibility for security is left to users themselves.

	Trust index	Change from previous
2023	-19	
2024	-26	-7
2025	-27	-1
2026	-20	+7

Trust declined sharply between 2023 and 2024. One possible contributing factor was the widely publicised data breach targeting the City of Helsinki’s Education Division in spring 2024. However, the Barometer data themselves do not demonstrate a causal relationship between any single event and the change in trust.

Major change in the oldest age groups

Trust in the security of digital services and devices has increased particularly among 25–34-year-olds and people aged over 64. For example, among 65–74-year-olds, the trust index rose in one year from -42 to -20, an increase of 22 points, while among 75–99-year-olds it rose from -49 to -31, an increase of 18 points.

Eighty-six per cent of Finns consider their daily activities in the digital operating environment either fairly or very safe. This is four percentage points more than a year earlier. Ten per cent feel that their activities are unsafe.

Among 18–24-year-olds, the sense of security increased by eight percentage points in one year, and among 75–99-year-olds, it increased by nine percentage points.

Public authorities, the financial sector and Finnish origin form the foundation of trust

In 2026, new questions were added to the Barometer. The responses reinforce the picture of Finland as a safe digital society.

Seventy per cent of respondents consider Finland's digital operating environment safe, and only 3% strongly disagree. In addition, 54% believe that cyber and digital security are implemented better in Finland than in most other EU countries. Seventeen per cent disagree with the statement, while almost one-third cannot form an opinion, reflecting in part the difficulty of the question. This partly reflects the complexity of the question.

Trust in key societal institutions is particularly strong.

Eighty-seven per cent of Finns trust financial-sector actors and public authorities to handle personal data and other important information securely. The result for both has remained at the same high level as a year earlier. Similarly, 81% of respondents trust their employer.

Finnish online shops and content are trusted

Finnish origin also appears to increase trust. As a new question, we asked about trust in the Suomi.fi service. Eighty-two per cent of respondents express a high level of trust in Suomi.fi. Overall, 70% trust Finnish online shops, while only 20% trust foreign online shops.

Trust in online shops has nevertheless declined: from 75% to 70% for Finnish shops and from 23% to 20% for foreign shops. This is probably due to fake online shops and other payment-related scams.

It is noteworthy that, at the same time, the proportion of people who lost money in a fake online shop decreased from 10% to 7%. Trust has therefore declined even though actual losses have decreased.

The significance of Finnish origin is also visible in content. Eighty-eight per cent of Finns express a high level of trust in content produced by public authorities, exactly the same share as a year earlier. Sixty-six per cent trust well-known Finnish news media, compared with 50% for well-known foreign news media.

Overall, trust in the digital world is therefore not evenly distributed. Trust is strongest where the actor is familiar, its responsibilities are clear, and it is perceived as part of Finnish society.

Use of AI is growing faster than trust in it

The adoption of AI services is one of the strongest changes measured in the Barometer.

When AI was first included in the survey in 2024, 20% of Finns used AI at least monthly. The share was 31% in 2025 and already 47% in 2026. Regular use of AI services has therefore more than doubled in two years.

The proportion of people using AI daily or almost daily has risen in two years from 4% to 16%.

At the same time, the proportion of people who do not use AI at all has fallen from 55% to 27%.

Growth is no longer limited to young people. AI is used monthly or more often by 66% of 18–24-year-olds, 59% of 25–49-year-olds, 43% of 50–64-year-olds, 31% of 65–74-year-olds and 26% of 75–99-year-olds. The largest year-on-year changes are seen among 25–49-year-olds and 65–74-year-olds.

AI-generated content is trusted more than social media content

Trust in AI is nevertheless growing considerably more slowly than its use. Only 23% express a high level of trust that AI services handle personal data and other important information securely. A year

earlier, the figure was 20%. Likewise, only 23% of Finns express a high level of trust in AI-generated content.

AI-generated content is now trusted more than social media content, which 21% of respondents trust to a high degree. Trust in AI-generated content rose by two percentage points in one year, while trust in social media content fell by four percentage points.

The picture in 2026 is therefore two-sided: the use of AI is rapidly becoming normal, but trust in it is not growing at the same pace. This will make AI literacy and the secure use of AI some of the key digital security skills in the coming years.

AI literacy and the secure use of AI will be key digital security skills in the coming years.



Digital services are widely used, and their importance is well recognized

Digital services are firmly established as part of Finns' everyday lives: 77% consider digital services and applications important. The result has remained practically unchanged for five years. Among people under 35, their perceived importance is at its highest level in 2026, with 88–93% considering such services important.

Use of digital services is also extensive. Seventy-two per cent of Finns use digital services a great deal during the day, and among people under 50, the share is as high as 81–91%. Even in the oldest age group, 75–99-year-olds, half use digital services a great deal.

Finns' average leisure-time screen time is 21 hours per week. This is around one hour more than a year earlier. Among people under 35, screen time totals 27–30 hours per week. People aged 75–99 spend the least time in front of screens, but even for them the figure is 14 hours, or an average of two hours per day.

People themselves also recognise screen time as a problem. Forty-five per cent consider their leisure-time screen time too high or far too high. Among people under 50, 58–63% think so.

Digitalisation is no longer a separate operating environment but a significant part of ordinary life. At the same time, digital security is increasingly becoming part of everyday safety and security.

45% feel that they spend too much time in front of screens.

People's perception of their security skills does not match reality

As many as 89% of Finns rate themselves as good or very good at using digital services and devices securely. The result is high, although it has fallen by two percentage points after three nearly identical years.

In the oldest age group, 76% consider their competence good, while among 35–49-year-olds, the figure is as high as 95%.

However, people's perception of their competence is partly inconsistent with their actual behaviour.

Twelve per cent of respondents would begin logging in to their online bank during a phone call if the caller claimed to represent a bank or public authority. Six per cent would click a link sent by email or text message in the name of a bank or public authority, and 8% answer calls from unknown foreign numbers.

As many as 22% report having clicked a link, opened an attachment or answered a call during the past year that turned out to be a scam attempt.

This reveals one of the Barometer's most interesting contradictions: Finns consider themselves safer digital users than their behaviour suggests.

Better preparedness for scam attempts

At the same time, there are also clear positive changes in competence. More people know what to do if they suspect an online scam, know how to check the security of a website or online shop, and use different passwords for different services. These skills improved by 6–8 percentage points in one year.

The amount of training and information received on strong authentication has decreased exceptionally sharply since 2025: –10%. This may be partly related to official communications becoming primarily digital. As a result of this change, the number of Suomi.fi Messages users has increased by more than 2.4 million since spring 2025. Suomi.fi messages, like an increasing number of other digital services, requires strong authentication.

The use of concrete protective measures has also increased. Forty-eight per cent of Finns have improved the security of their payment cards and accounts during the past year, six percentage points more than in 2025. The greatest increases are among 75–99-year-olds, 18–24-year-olds and 50–64-year-olds.

We consider ourselves safer digital users than our actual behaviour suggests.

Concern about scams is increasing, but resilience is improving

Finns are clearly more concerned about digital scams than before. Sixty-nine per cent are fairly or very concerned about them, as much as ten percentage points more than a year earlier. Misuse of personal data also concerns 75% of Finns.

A key reason for such a significant increase is probably that the topic has received more attention than before in different media. People's own experiences and those of their close circle, relatives, friends and acquaintances also have an effect.

However, the increase in concern is not reflected as negative development in every indicator. Nineteen per cent of respondents say that digital scams have had a major impact on their everyday lives. This is four percentage points less than last year.

Half of respondents feel that scams have had a major impact on their trust in digital society, but here too the share has fallen by three percentage points from the previous year.

Society's preparedness is also assessed slightly more positively than before. Forty-four per cent of Finns consider Finland's preparedness for preventing and combating digital scams to be good. This is three percentage points more than

last year. A majority, 56%, nevertheless still assess it as poor.

At the same time, 91% of respondents are willing to take steps to protect themselves online. The figure has improved by two percentage points more than a year earlier.

Digital security is nevertheless not seen as being as strongly an individual responsibility as before. The share of respondents who consider digital security primarily the responsibility of the individual has fallen from 75% to 71%.

The result may indicate that a new balance is emerging in people's thinking: individuals are willing to take responsibility for their own security, but digital security is no longer seen solely as an individual task.

91% are willing to make an effort to ensure their security.

Finns believe they can recognise scams

Finns' confidence in their own ability to recognise scams is high by international standards. Eighty-six per cent say they are fairly or very confident that they can recognise a digital scam.

In the Global Anti-Scam Alliance (GASA) 2026 European comparison*, the corresponding figure is 71%, giving Finland a 11-percentage-point lead.

Strong confidence in one's ability to recognise scams does not, however, mean that people are not exposed to them. Eighty-one per cent of Finns have encountered a digital scam or scam attempt during the past 12 months, compared with the European benchmark of 75%.

One in five Finns reports encountering scams at least weekly, and 5% encounter them daily or almost daily.

The prevalence of digital scams in Finland can partly be explained by the high degree of digitalisation in society: Finland has comprehensive and well-functioning digital infrastructure, electronic services and payment systems are widely used, and almost everyone has access to some kind of smart device. The population also has strong language skills. These factors make Finland an attractive target for international cybercrime as well.

In the age of AI, language no longer provides protection

At the same time, there may still be an image of Finland as a kind of "Moominvalley" of the digital world - a safe society in the far north, protected by its geographical location and the internationally uncommon Finnish language. There is increasingly little justification for this sense of security.

Cybercrime is global, and geography provides no meaningful protection against it. Rapid advances in AI also reduce the protection once offered by language: it is now easier than before to produce high-quality scam messages, conversations, speech and videos in Finnish.

AI enables increasingly convincing audio, image and video deepfakes. This makes it more difficult to distinguish authentic content from synthetic content produced or manipulated using AI.

The EU AI Act, which became applicable on 2 August 2026, introduced new obligations, including requirements to disclose the use of AI and to label deepfakes and other AI-generated or AI-manipulated content.

* Global Anti Scam Alliance (GASA):
State of Scams in Europe 2026



Scam and phishing messages are encountered less frequently than before.

Several threats are trending downward

Another significant positive signal in 2026 is the development of realised threats. The overall average of comparable threat indicators fell in one year from 34% to 30%.

Email remains the most common scam channel: 71% of respondents have received scam or phishing messages. Forty-eight per cent have encoun-

tered text-message scams, 47% have received scam calls, 42% have come across scam attempts on social media and 33% have run into scams in instant-messaging applications.

Several major types of scam have declined. The share encountering scam and phishing emails fell from 78% to 71%, text-message scams from 62% to 48%, and scam calls from 54% to 47%. In instant-messaging applications, the share fell from 42% to 33%.



The change in text-message scams is therefore as much as -14 percentage points, and in instant-messaging scams -9 percentage points.

Disruptions and outages in digital services affect people's ability to handle their affairs digitally: 36 percent of respondents say that disruptions have prevented them from doing so. The figure has increased by three percentage points since 2025.

The share of people who lost money in a fake online shop fell from 10% to 7%, losses due to extortion or digital scams from 7% to 6%, and losses due to identity theft from 6% to 5%.

Finland's strength is therefore not that scams are rare. Rather, the strength appears to be that citizens recognise them relatively well and learn how to operate in an environment where they are common.

Scams remain widespread in Finland, but their number has decreased and people are getting better at recognizing them.

Cooperation and vigilance in the fight against cybercrime

Several new technical measures to combat digital scams have been introduced in Finland during the past year.

A blocklist restricts access to malicious addresses

One way to combat digital scams is the so-called blocklist service implemented jointly by the financial sector, telecommunications operators and public authorities. It can be used to restrict access quickly to malicious web addresses used by cybercriminals.

When a new scam website or other malicious address is identified and reported to the service, blocking can take place within minutes in the best cases and typically within a few hours.

The blocklist is an effective tool, but it depends on malicious web addresses being detected and reported quickly. Reporting new scam websites and malicious links therefore remains important.

Text-message sender IDs must be approved in advance

Finland made text-message scams significantly more difficult in May 2026, when new sender-identification obligations entered into force (Traficom's revised Regulation 28 L/2025 M on the interoperability of communications networks and services).

Finnish telephone numbers and alphanumeric sender IDs used by organisations in their text messages must be approved in advance. In addition to SMS, the requirement also applies to MMS and RCS messages. As a result of the authorisation requirement, faking the sender ID of a bank, public authority or other well-known organisation is, as a rule, prevented in Finland.

Messages sent without authorisation are displayed to recipients with the sender label "Unknown", and from 2 November 2026 with the label "Spam", or are blocked entirely.

Technical solutions do not eliminate text-message scams entirely. Cybercriminals can still send scam messages from their own numbers or other numbers available to them and direct recipients, for example, to malicious websites.

User vigilance and the ability to recognise scam attempts are therefore still needed alongside technical safeguards.

The consequences of successful scams remain significant

Of those who encountered a scam, 8% disclosed some form of protected information as a result. Most commonly, this involved personal data or bank and payment-card details, which were disclosed by 4% of those who encountered a scam.

In practice, criminals typically also obtain other personal information in the same incident, depending on the digital scam channel used.

Ten per cent of Finns report having lost money during the past 12 months because of a digital scam, extortion or a purchase from a fake online shop.

Particularly concerning is the fact that approximately one in six of them (16%) have lost money more than once.

Of those who lost money, 69% lost 1–100 €, 19% lost 101–500 €, 3% lost EUR 501–1 000 € and 9% lost more than 1 000 €.

If Finland has approximately 4,5 million active digital users according to Statistics Finland's estimate, and 10% of them have lost money as a result of a digital scam, this would correspond to around 450 000 Finns.

Using conservative average euro amounts for each loss category, total financial losses can be

estimated at approximately EUR 128 million per year. The order of magnitude is consistent, for example, with annual figures published by the police and Finance Finland.

It is important to note that the estimate only covers losses suffered by private individuals. Additional financial losses are caused by, among other things, digital scams targeting companies and other organisations, payment-transaction fraud and extortion, and debit- and credit-card fraud.

The total direct financial losses caused by digital crime in Finland are therefore significantly higher. For this reason, reporting the incident is particularly important, especially in cases where the crime results in financial loss.

When a criminal gains access to a person's bank account, credit card or other identity-related assets, in just over one third (34%) of digital scams, the scammer obtained the money through a bank transfer. In around one quarter (22%) of such scams, the money was transferred using a debit or credit card, and in 15% of these cases, through so-called instant-payment services.

It is worth noting that gift cards and vouchers purchased from shops were used in 5% of scams, while cryptocurrency was used in only 3%.

Finland differs significantly from the results of the GASA Europe survey in several respects. Across Europe, it is considerably more common than in Finland for fraudsters to obtain money through gift cards or vouchers, via a digital wallet (such as PayPal, Apple Pay or Google Pay), through cryptocurrency or crypto services, or in cash. The results highlight that payment transactions in Finland are concentrated in the services of traditional financial-sector providers and that the use of cash is limited.

Digital scams are rarely reported to those who could act on them

One of the 2026 findings stands out particularly prominently as an area for development: scams are reported too rarely.

Of those who encountered a scam or scam attempt, 43% did not report it to anyone. Thirty-four per cent told a family member or friend, while 17% reported it to the service or platform provider, 12% to a bank or other financial service, and only 7% to the police.

The situation changes substantially when money is lost. In those cases, 37% say they report the incident to their bank or payment service provider and 30% to the police. Even so, 13% of those who lost money do not report the incident to anyone. Finland also stands out positively in this respect compared with Europe as a whole: such incidents are reported less frequently elsewhere in Europe than in Finland.

The reporting gap is even clearer in cases where an offence actually occurred. For 6% of scam victims, the case resulted in a criminal offence, such as fraud or the loss of money or personal data. Of these victims, 58% filed a police report and 42% did not.

This is a system-level problem. If scams are not reported, public authorities, banks, telecommunications operators and service platforms cannot build an adequate situational picture of the number, methods and development of scams. At the same time, it becomes more difficult to identify criminal activity, apprehend offenders and disrupt their operations.

Making reporting easy, understandable and worthwhile should be elevated to one of the next key development priorities in digital security.

When a scam attempt is detected in time, the key warning signs are usually related to human judgement. A sender who appears untrustworthy raises suspicion among 56% of respondents, a suspicious link or website among 54%, and inconsistencies or illogical elements in the message among 51%. An offer that seems too good to be true is recognized as a warning sign in 43% of cases.

Reporting scams must be made easy, understandable and useful.

Communication and clear operating models are the most important protective measures

The Barometer's most important qualitative finding concerns why scams succeed or fail.

Of those who lost money, 36% say the scam succeeded because the situation seemed credible and genuine. Twenty-four per cent trusted the sender or person contacting them, and 22% believed the payment to be safe. A lack of time and an offer that seemed too good to be true influenced 20 percent of respondents, while the scammer posing as a trusted organization influenced 19 percent.

Age influences where people obtain information. Communication from banks, payment service providers, and public authorities is particularly important among respondents aged over 64. Social media, in contrast, is a more significant source of information for younger respondents, and its importance declines steadily with age.

The results also show what helps citizens in practice. Communication from banks and payment services is the single most important factor supporting the recognition or avoidance of scams, cited by 47%. This is followed by news media at 43%, communication and websites of public authorities at 43%, and personal experience of scams at 41%.

These issues are communicated very extensively in Finland, and Finland's figures are in many respects significantly higher than the European average.

Scams can also have serious consequences even when no money or personal data is lost. Among those who have encountered a scam, 49% have become more cautious users of digital services, while 30% trust digital services less than before. In addition, 15% share more warnings with others, 14% are afraid of becoming a victim of a scam again, and 8% report that scams have caused them stress or anxiety.

For those who have lost money, the consequences can be considerably more serious: 15% have had difficulty paying for essential expenses, 12% have had to reduce their normal spending, 10% have needed financial support from family or friends, and 6% have had to take out a loan or incur debt.

One of Finland's strengths is the extensive communication provided to citizens and the cooperation between different stakeholders.

Just under one third trust digital services and online environments less than before.

Digital security is beginning to improve

Positive development can be seen in digital security, but in practice, security is built into people's everyday lives. The 2026 Digital Security Barometer does not portray a risk-free digital Finland - quite the opposite: four out of five Finns encounter scam attempts, one in five encounters them at least weekly, and concern about digital scams has increased sharply.

The decisive difference in 2026 compared with earlier years, however, is that an increase in threats no longer automatically means a decline in trust.

- The trust index has turned in a better direction.
- The sense of security has increased.
- Exposure to several types of scams has decreased.
- Citizens are taking concrete protective measures more often than before.
- People are willing to make a greater effort for digital security.
- Trust in public authorities, the financial sector and key Finnish digital services is strong.

AI is changing the operating environment at unprecedented speed. Its use is growing much faster than trust in it. At the same time, AI strengthens citizens' ability to protect themselves while also enabling increasingly convincing scams and other forms of cybercrime.

Security must be built into services

The Barometer's key message is that in 2026, Finnish digital society is showing the first signs of strengthening digital crisis resilience. Trust is no longer declining and the sense of security has increased, even though threats have not disappeared and trust has not yet fully recovered.

The next step is not simply better technology or better-informed citizens, but security built into services: an easy way to verify the authenticity of contacts, a low threshold for reporting problems, and a clear division of responsibilities between banks, public authorities, telecommunications operators and platforms.

Citizen competence is one part of the overall system, not a substitute for it.



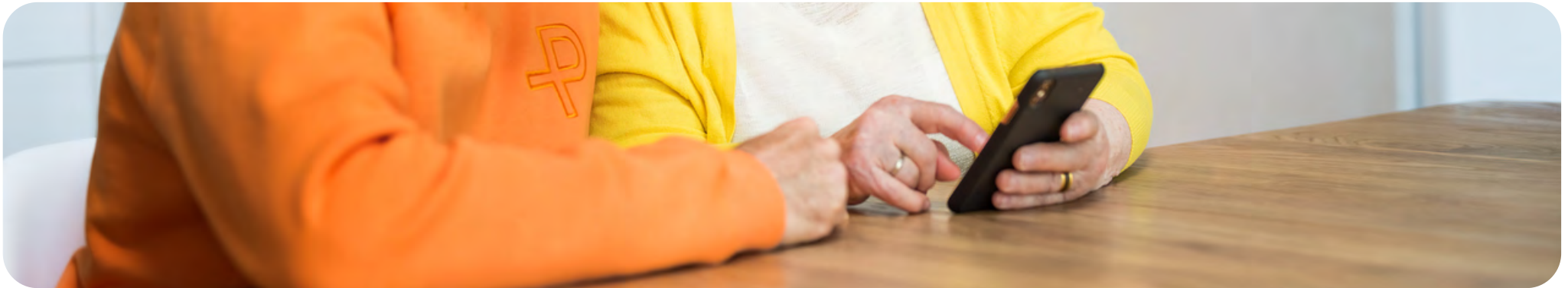
12 key indicators to monitor

Indicator	2026	Change
Trust index (strengthened - weakened)	-20	+7 points
Considers the everyday digital environment safe	86%	+4 pp
Trusts content produced by AI services	23%	+2pp
Uses AI services at least monthly	47%	+16 pp
Rates their own ability to use digital services securely as good	89%	-2 pp
Fairly or very concerned about digital scams	69%	+10 pp
Realisation of threats, overall average	30%	-4 pp
Has encountered digital scam attempts	81%	*
Has lost money due to a digital scam	10%	*
Considers Finland's digital operating environment safe	70%	*
Filed a police report concerning a digital scam, fraud or other crime	58%	*
Did not report an encountered scam to anyone	43%	*

* new question

Ten guidelines for digital users

– how to avoid digital scams and what to do if you are scammed



1. Stop whenever you are being rushed

Urgency, intimidation and pressure are common tactics used by digital scammers. If you are told to act immediately, pay quickly or keep the matter secret, stop and think before doing anything.

2. Do not trust a name, number or appearance alone

A call, message or website may appear to come from a bank, public authority, company or even someone you know. Verify the contact independently through another channel, using a phone number, application or website you already know to be genuine. Or call a friend!

3. Do not authenticate yourself or make payments by following someone else's instructions

Do not log in to your bank, approve an authentication request or make a payment based on an unexpected call or message. Always open the bank's or other service's application or website yourself. If you use a browser, type the web address into the address bar yourself. Never enter a service through a link you have received or through search-engine results.

A criminal generally cannot cause significant harm unless they obtain your credentials, authenticate to services on your behalf or hijack your identity.

4. Check before you click, buy or pay

Check the sender, the website address, the payment recipient and whether anything in the message is illogical. If an offer seems too good to be true or anything else raises doubts, do not proceed until you have verified it.

5. Protect your accounts and devices in advance

Use different passwords for different services and enable multi-factor authentication whenever possible. Keep devices and applications up to date and make use of payment, card and transaction limits offered by your bank. A small effort in advance can prevent major losses.

6. If you suspect a scam, stop the interaction immediately

Do not continue the conversation, click new links or send any more information. End the call or messaging session and calmly establish what has happened. A scam can still be stopped even if you have already taken some action.

7. If you disclosed information or sent money, act quickly

Contact your bank or payment service immediately if you have made a payment, disclosed bank or card details, or approved a suspicious transaction. If necessary, block cards and credentials and change any compromised passwords.

The faster you act, the better the chances of limiting the damage.

8. Report what happened - do not deal with it alone

Save messages, phone numbers, web addresses, receipts and other information related to the incident. Depending on the situation, report it to your bank, the service provider and the police, and where necessary, to other authorities.



9. Protect your privacy - keep your digital footprint under control

Before publishing anything online, consider what information you share about yourself, people close to you or your everyday life. Avoid unnecessarily publishing personal data, photographs, location data, travel plans and other sensitive information. Regularly review the privacy settings of applications and services and check what information about you is publicly available online.

There is no need to feel ashamed about being scammed: by reporting it, you can help prevent others from falling victim to the same scam. Even a small digital lead may help bring criminals to justice!

10. Use AI to help identify digital scams

For example, you can ask AI:

“Does this website look like a digital scam?”

Paste or enter the web address you want to check after the question.

You can also take a screenshot or photo of a message or a web page and ask AI to assess whether it shows signs of a scam.

Remember: AI can make mistakes. Even if it considers a website or message safe, always check the address, sender and other warning signs before logging in, making a payment or providing personal information. AI is a useful second pair of eyes, not the final word.

12 recommendations for organisations and associations

The positive turn in trust visible in the 2026 Digital Security Barometer can become a lasting trend if

- security is visible to the user,
- secure behaviour is made easy, and
- organisations take a more active role in preventing digital scams.



1. Enable one-stop reporting of digital scams and review your own process

Create a clear reporting and service pathway for customers who suspect they have fallen victim to a digital scam. The organisation must be able to initiate its own protective measures and, where necessary, direct the customer to services provided by the police, the National Cyber Security Centre Finland, the Office of the Data Protection Ombudsman, a bank or another competent authority.

At the same time, test that your staff know the process and can act quickly.

2. Practise digital-threat scenarios that feel realistic

Do not rely on instructions and online courses alone. Run exercises involving, for example, scam calls, phishing, bank transfers, instant payments, urgency-based requests, and impersonation of a bank, public authority, manager or other trusted party.

Train people in the organisation to stop the situation, verify the contact through another channel, and report quickly. At the same time, test whether the organisation's own reporting channels work in practice.

3. Close the training gap in strong electronic identification

Strong electronic identification does not in itself prevent a scam if the user can be manipulated into approving a transaction initiated by a criminal. Teach users to routinely check what they are approving and in which service the identification or authentication is taking place.

Emphasise that people should not automatically identify themselves using online banking credentials or a mobile certificate based on an unexpected call, message or other contact. Instruct users to stop the interaction and open the correct service themselves using a known address or application.



4. Invest in the basic skills needed for safe use of AI

Teach staff what information may and may not be entered into AI services. Provide exercises on handling personal and confidential information, verifying AI-generated answers, source criticism, and recognising AI-assisted scams such as convincing messages, images, audio and video.

Direct staff to use organisation-approved and securely managed AI services for work tasks, while encouraging them to build their skills in their free time as well.

5. Use trusted messengers in communication

Digital scams cannot be prevented through the communication of a single organisation. Messages from banks, public authorities, telecommunications operators, news media, workplaces, educational institutions, associations and people close to the user can complement and reinforce one another.

Target messages to different user groups and to the channels they use. Repeat key operating practices with sufficient frequency and respond quickly to new scam phenomena.

6. Measure competence through behaviour, not only self-assessment

Do not assess digital-security competence solely by asking people how good they believe their skills are. Supplement surveys with scenario-based tasks, simulations and exercises.

Monitor, for example, whether users know how to stop a suspicious situation, verify a sender or contact through another channel, confirm a payment request and report a suspicious event. Above all, measure secure behaviour in practice.

7. Support scam victims without blaming them

Provide rapid assistance in stopping payments, securing credentials and personal data, filing a police report, and, where necessary, finding financial and debt counselling and psychological support. Listen calmly and avoid questions that may increase feelings of shame or guilt.

Scams are deliberately designed to exploit urgency, fear, trust and authority. Focus on what can still be prevented, protected, recovered and reported. Thank the person for reporting the incident - rapid reporting can prevent others from falling victim to the same scam.

8. Build scam prevention into services

Do not leave security dependent solely on users' vigilance and ability to recognise scams. Use detection of anomalous logins, payments and behaviour, risk-based additional verification, and appropriate limits and delays in services.

Design user interfaces so that exceptional or high-risk activity attracts the user's attention before approval. The secure option should also be the easiest option for the user.

Aim to make use of AI-powered security services on a 24/7 basis.

9. Make it easy to verify the authenticity of contacts from your organisation

Provide customers with a simple way to verify whether a message, call or other contact really comes from your organisation. Make routine use of established service channels, in-app messages and clear callback procedures.

Avoid practices that train customers to log in to services through links in unexpected messages. Also explain clearly what your organisation will never ask customers to do by phone, message or email.

10. Protect payments and other difficult-to-reverse actions in particular

Identify situations in your services where the consequences of a scam can quickly become significant: bank transfers, adding a new payee, changes to bank account details, granting access rights, disclosure of personal data and approval of strong electronic identification.

Depending on the risk, use independent verification, dual approval, payment limits, additional confirmation or a short delay. The aim is to create one final opportunity to stop the scam before an irreversible action is completed.

11. Actively combat scams carried out in your organisation's name

Monitor how your organisation's name, domains, logos, phone numbers and staff names are used online. Ensure that technical email protections such as SPF, DKIM and DMARC are properly configured.

Monitor lookalike domains, fake profiles and scam websites, and create an operating model for reporting and taking them down quickly. Inform customers promptly if a scam campaign is being conducted in your organisation's name.

12. Share scam intelligence rapidly across organisational boundaries

A single detected scam may be part of a campaign targeting thousands of people and multiple organisations at the same time. Create an operating model for rapidly sharing malicious domains, URLs, phone numbers, bank account numbers, payment recipients and other indicators with actors that need them.

Work with public authorities, banks, telecommunications operators, technology companies and other partners. The aim of this measure is to shorten the chain from detection to reporting, blocking and, where necessary, takedown.

We recommend that organizations:

- participate in the free annual Taisto cyber and digital security exercise:
dvv.fi/taisto
- read the “Data has been stolen or leaked from my organisation” guide:
www.suomi.fi/guides/data-breach



**DIGITAL AND
POPULATION DATA
SERVICES AGENCY**