



Online Scam in Sweden

August, 2024

Main insights

Cyber crime prevalence. Over the last two years, two-thirds of respondents reported being targeted by cybercrime. The most common scams reported include fake login pages, delivery scams, and fraudulent calls from fake service centers or banks.

Perceived online scam harm differs from the real time occurrences. Perceived as the most harmful cybercrimes, cloning bank cards and stealing personal or business data have a relatively low incidence among internet users in real life.

Cyber criminals follow the trends. The more popular an online communication channel is, the more likely it is to encounter cyber scams.

People react to the cyber scam attempts. Two-thirds of people took action after a scam attempt by reporting the incident, informing others, or taking steps to prevent further cybercrime attempts.

Reliance on common sense. General vigilance and common-sense actions are frequently mentioned as effective measures against cyber scams.

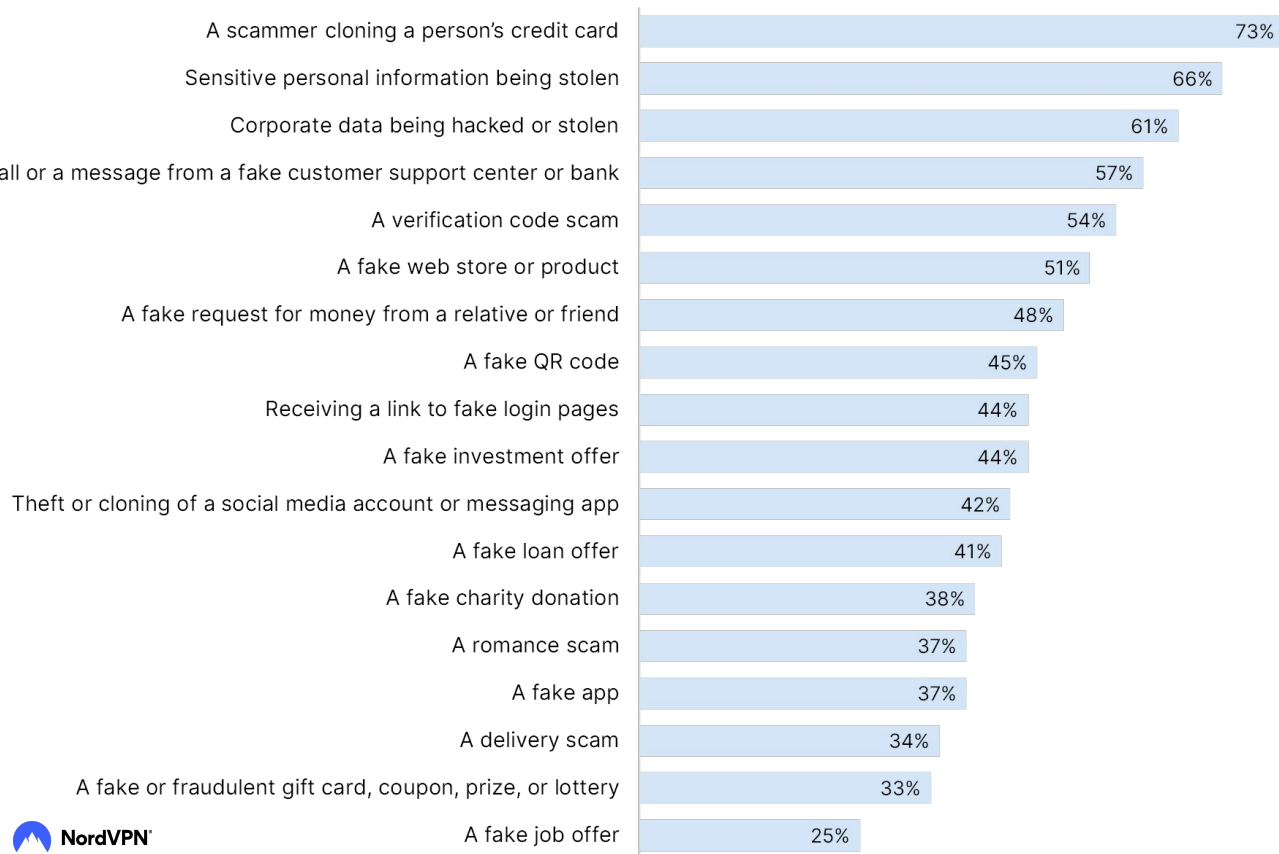
Incidence and perceived harm of online scam

- The top online scams in Sweden during the past two years are fake login pages, delivery scams, and fraudulent customer support calls
- Perceived as the most harmful cybercrimes, cloning bank cards and stealing personal or business data have a relatively low incidence among internet users in real life.



Perceived harm of online scam

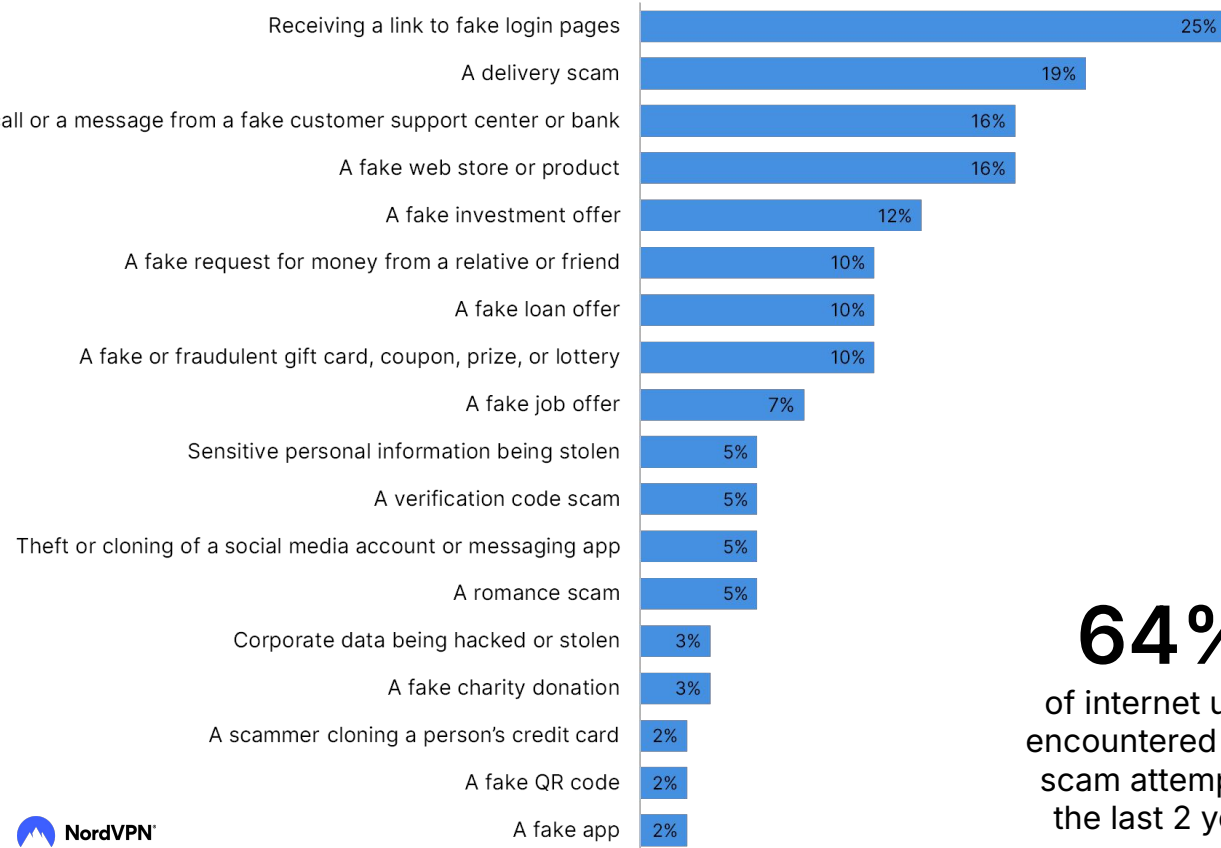
% from all respondents N=1000



Bank card scams personal and corporate information losses are perceived as the most dangerous online scams.

Internet users exposed to the online scam in the last 2 years

% from all respondents N=1000

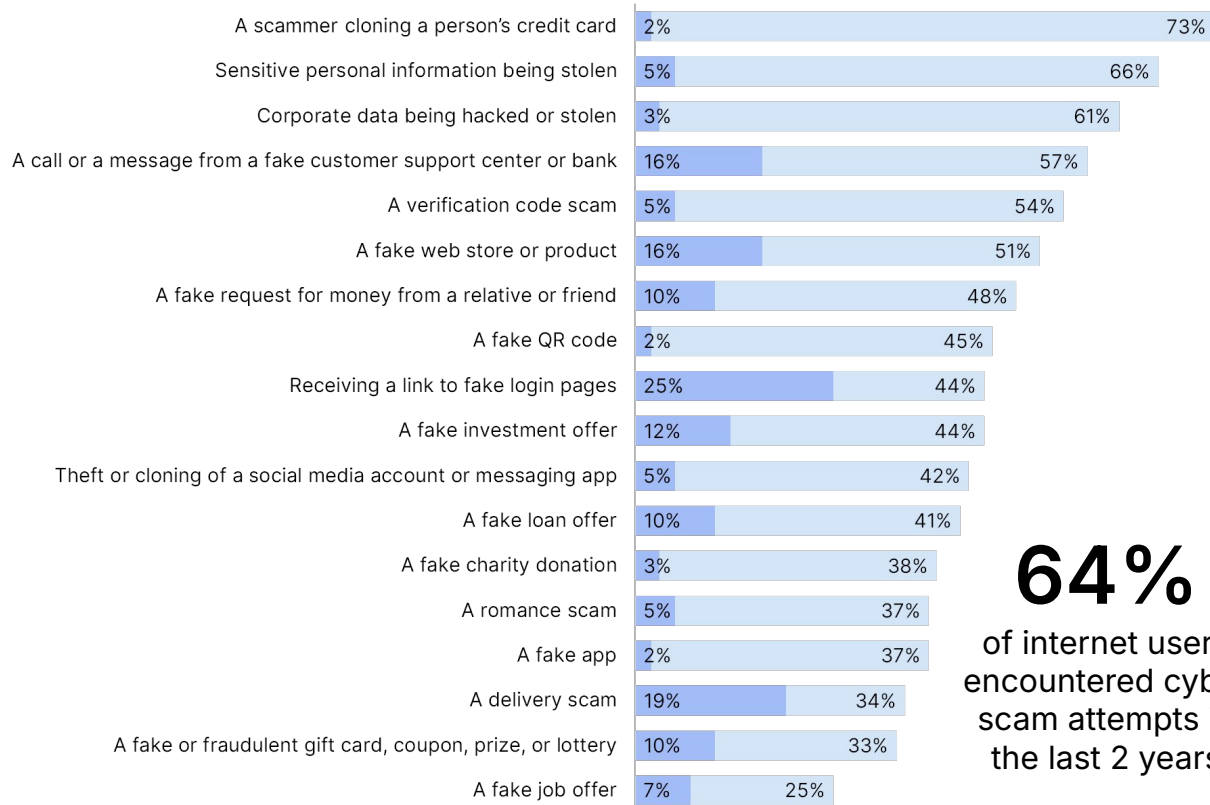


The most common online scams in Sweden over the past two years include fake login page scams, delivery scams, and calls from fake customer support centers.

64%
of internet users
encountered cyber
scam attempts in
the last 2 years

Incidence vs. perceived harm of online scam

% from all respondents N=1000



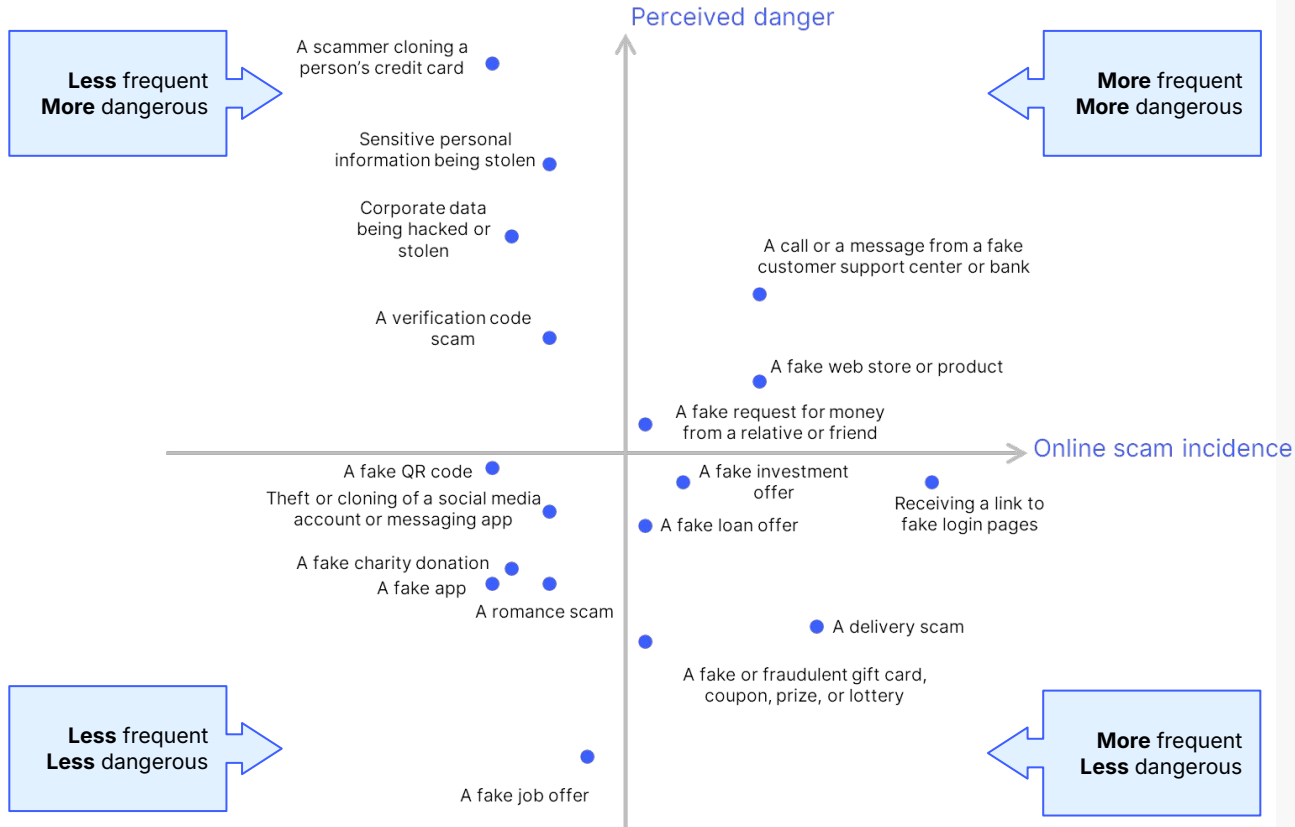
64%
of internet users
encountered cyber
scam attempts in
the last 2 years

The most common online scams in Sweden over the past two years include fake login page scams, delivery scams, and calls from fake customer support centers.

Among the top three "real-life" online scam incidents, fraudulent calls from fake customer service centers are considered the most dangerous.

The level of perceived threat varies based on the gender and age of the respondents. Females and elderly individuals tend to perceive online scams as more dangerous.

Incidence vs. perceived harm of online scam



The most dangerous cyber scams involve financial losses and complex social engineering tactics.

Allegedly the least harmful online scams include fake loan or job offers, delivery scams, or romance scams.

Reasons for vulnerability to cyber scams

- People often blame cyber criminals' advanced technical and psychological knowledge when they fall victim to cybercrime
- The more popular a communication channel is, the more likely it is that cyber criminals will try to exploit it for online scams



The main reasons people fall victim to online criminals

% from all respondents N=1000



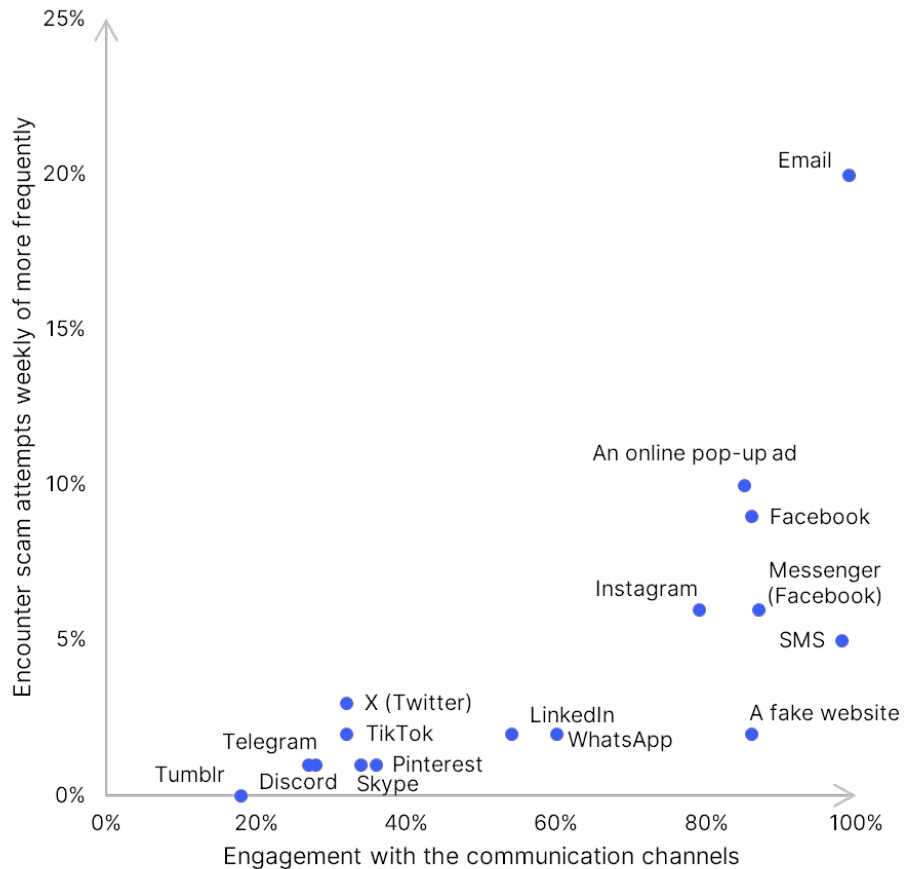
When falling victim to cybercrime, people commonly attribute it to the advanced technological and psychological knowledge of cyber criminals.

Fewer respondents acknowledge that scammers exploit people's weaknesses, such as greed or overconfidence, to recognize the cyber risks.

Male and female respondents have different perspectives on why people fall victim to online scammers. Females highlighted the increasing professionalism of scammers and their advanced methods, while males pointed out scam victims' vulnerabilities such as greed, lack of knowledge, and overconfidence.

Cyber scam delivery channels

% of those who encountered cyber scam in the last 2 years, N=629



Frequency of encounters with the cyber scam over the last two years are directly related to the overall popularity of communication channels.

Consequences of cyber crime

- After experiencing cybercrime, 40% of respondents reported consequences
- The main consequences of cybercrime encounters are primarily related to financial losses and negative psychological effects



Consequences of the cyber crime

% of those who encountered cyber scam in the last 2 years, N=629

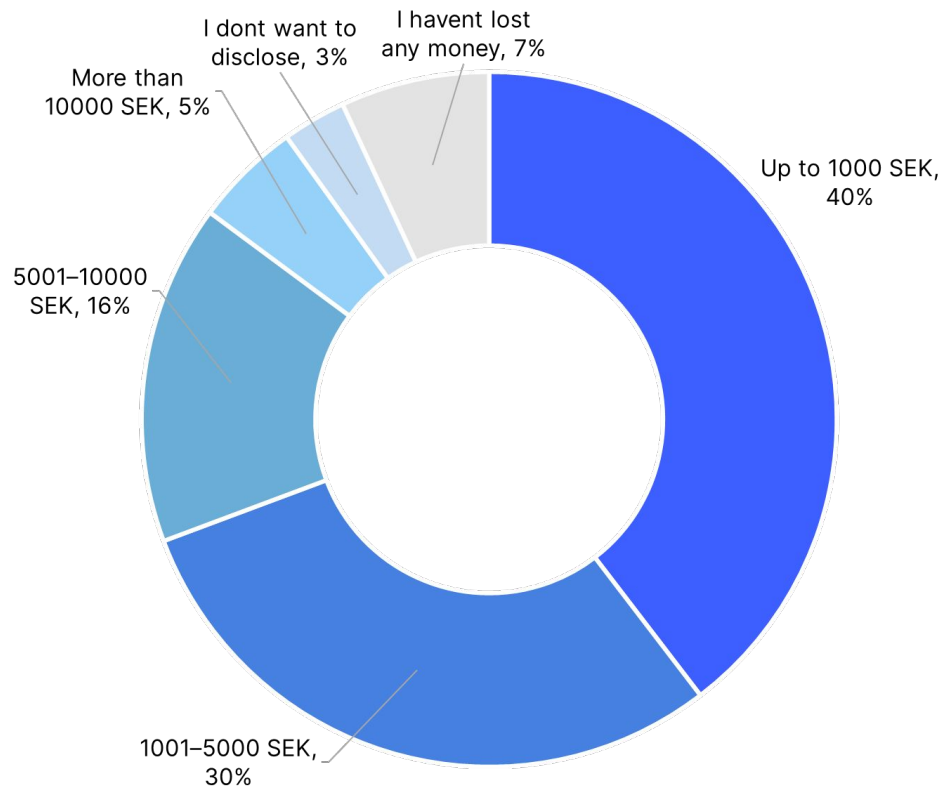


40% of people who experienced cybercrime in the last 2 years reported suffering from the consequences of cyber-attacks.

The majority of the consequences were associated with financial losses and adverse psychological effects.

Financial losses due to the cyber crime

% of those who lost money due to cyber scam, N=77



The most common financial losses from cybercrime were up to 1000 SEK in 40% of cases, and 1000 - 5000 SEK in 30% of cases.

Response to the cyber crime attempts

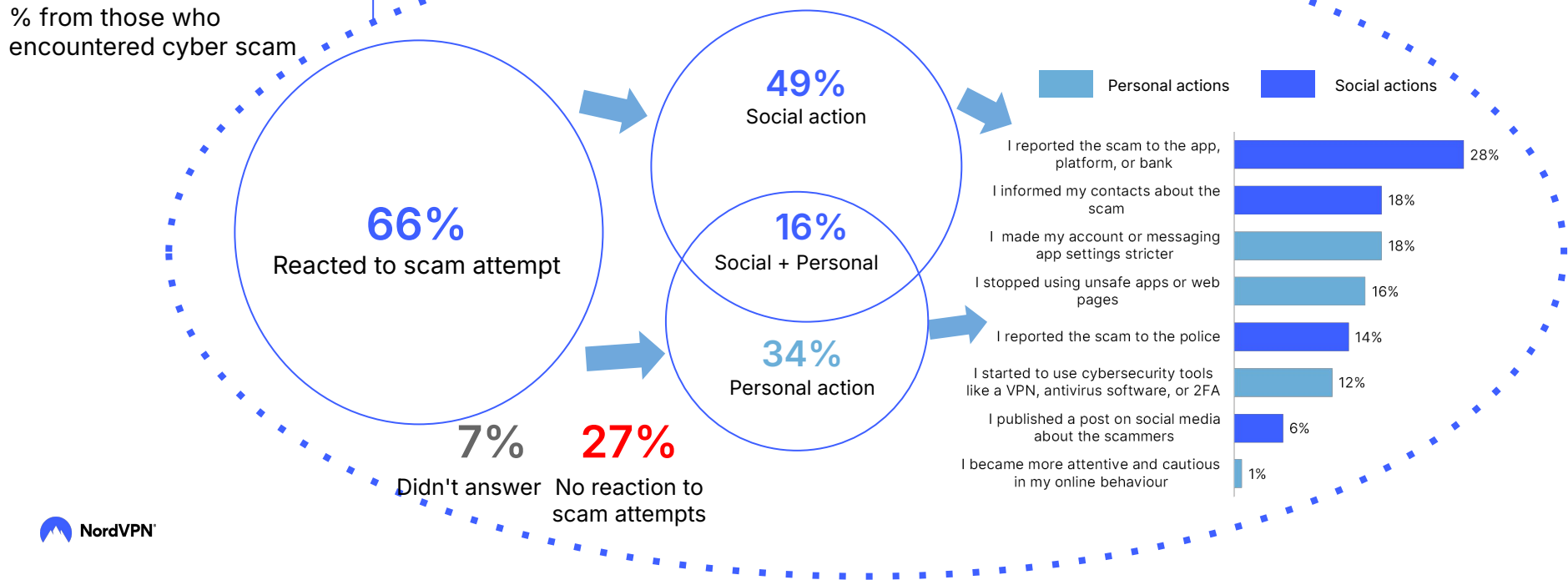
- Following a scam attempt, two-thirds of people either reported the incident, informed others, or took steps to prevent further cybercrime attempts
- Confidence to handle the cyber incident independently is the primary reason for not reporting the situation



Reactions to the cyber scam attempts

% of those who encountered cyber scam in the last 2 years, N=629

After experiencing a scam attempt, two-thirds of people either reported or informed others about the incident or took personal actions to prevent further cybercrime attempts. Male respondents more frequently than females, chose not to report or inform others about online scam incidents.



Reactions to the cyber scam attempts

% of those who encountered cyber scam in the last 2 years, N=629

After experiencing a scam attempt, two-thirds of people either reported or informed others about the incident or took personal actions to prevent further cybercrime attempts. Male respondents more frequently than females, chose not to report or inform others about online scam incidents.

Exposure

% of all internet users, N=1000



Reaction

% of those **those who encountered** cyber scam, N=629



Reaction type

% of those **those who encountered** cyber scam, N=629



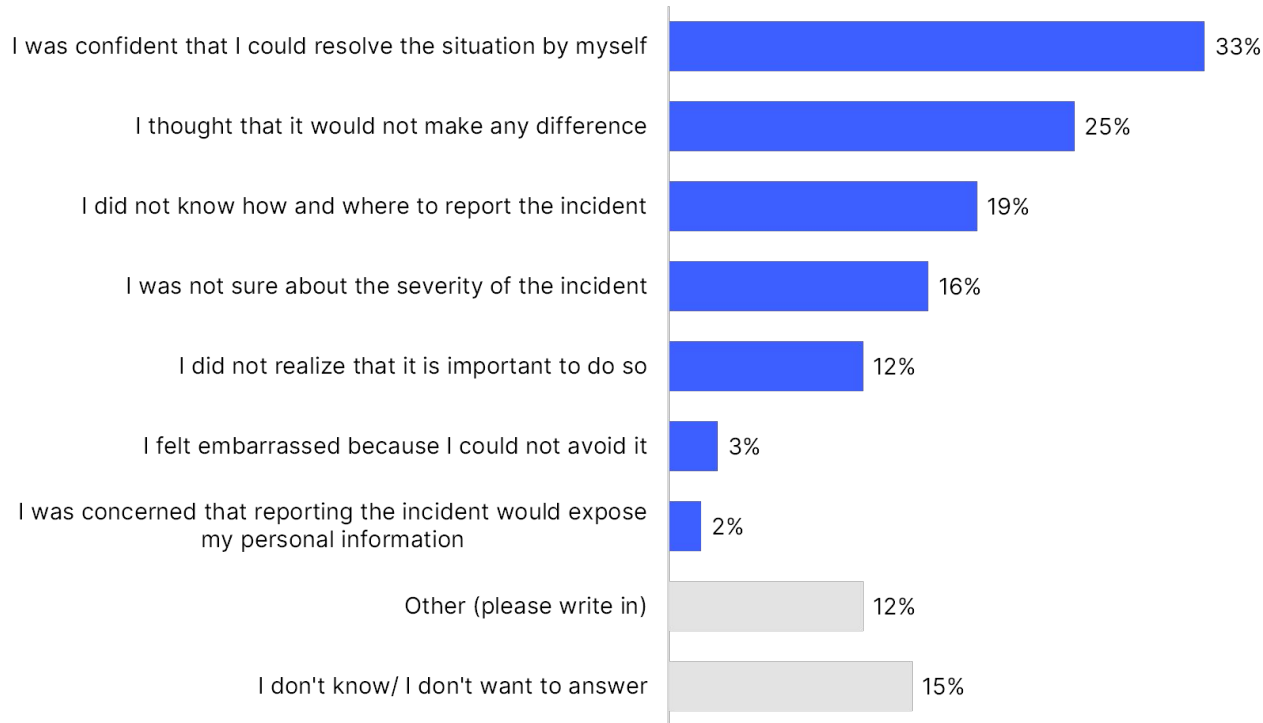
49%
Social action

34%
Personal action

16%
Social + Personal

Reasons for not informing about the cyber incident

from respondents who didn't inform anyone about the cyber incident, N=344



Confidence to handle the cyber incident independently is the primary reason for not reporting the situation.

Lack of awareness about the severity of cybercrime consequences and uncertainty about whom to report cyber incidents to are significant reasons for not reporting the incidents.

Attitudes towards cyber security and preventive measures against cyber scam

- People generally acknowledge the threats and consequences of cybercrime and critically assess their preparedness and knowledge to prevent cyber incidents
- General vigilance and common-sense actions are frequently mentioned as effective measures against cyber scams.



Attitudes towards cyber security

from all respondents N=1000

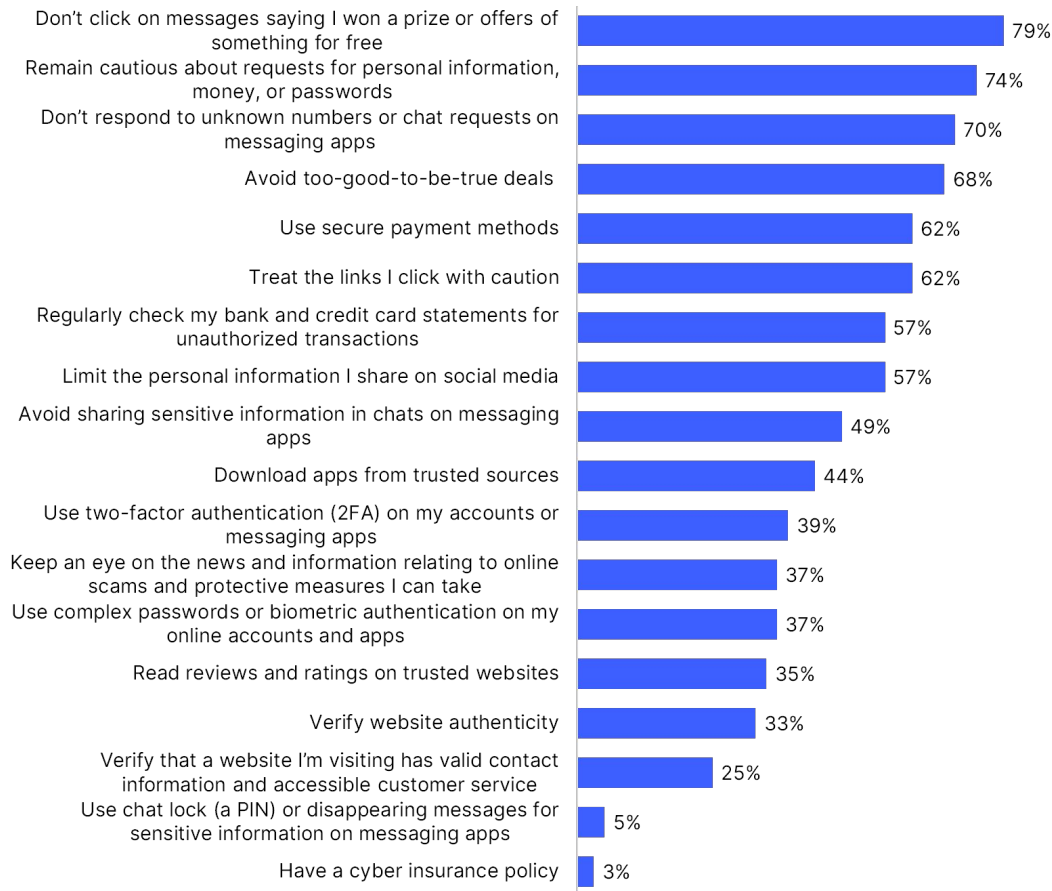


People generally recognize the threats and consequences of cybercrime.

They also critically evaluate their preparedness and knowledge to prevent cyber incidents.

Preventive actions against online scams

% from all respondents N=1000



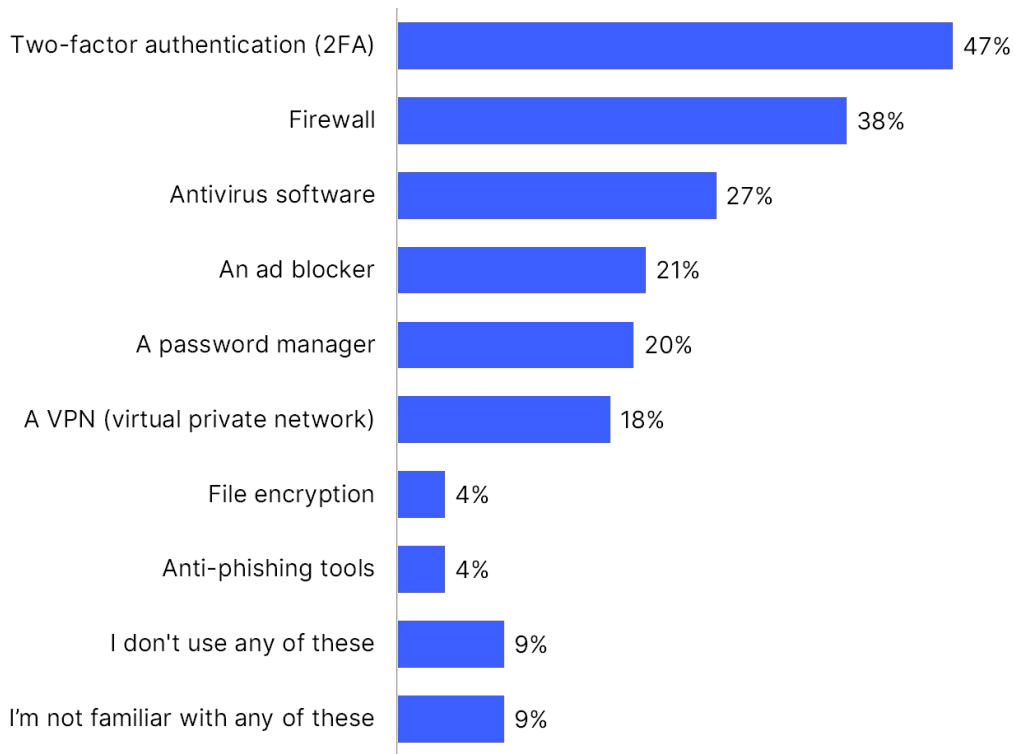
General vigilance and common-sense actions are frequently mentioned as effective measures against cyber scams.

Actions that require in-depth knowledge, such as verifying the authenticity of websites, or additional efforts like using complex passwords or staying updated with cyber news, are far less popular as preventive measures.

Cyber insurance is mentioned the least as a measure for preventing online scams.

Perceived effectiveness of cybersecurity tools

% from all respondents N=1000



Two-factor authentication, firewall, and antivirus software are believed to be the most effective tools to prevent and mitigate cyber scam risks.

Younger audiences prefer two-factor identification and ad blockers, while elderly audiences favor antivirus and firewalls.



Which of the cybersecurity tools that you currently use do you find the most effective?

Personal cyber insurance

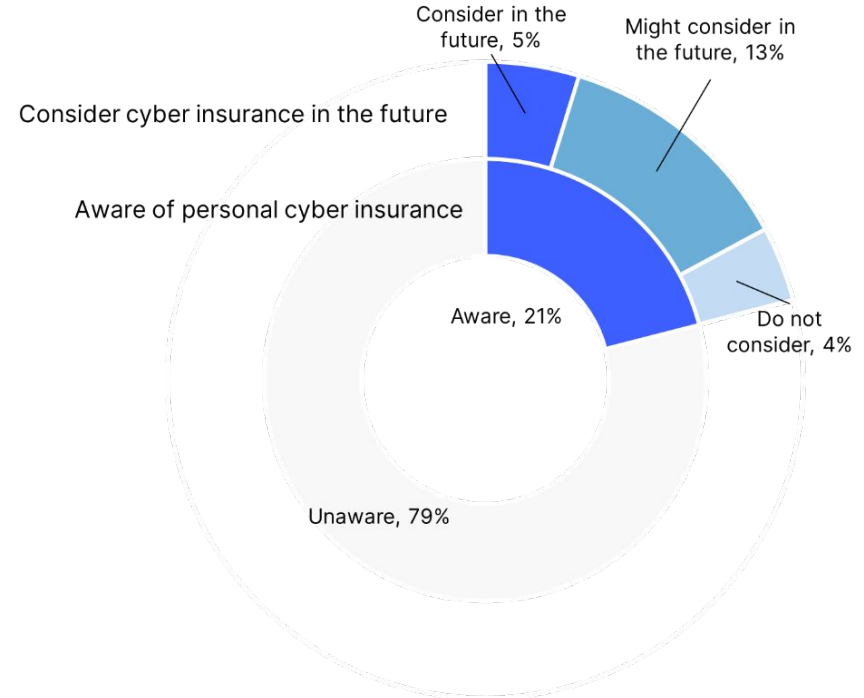
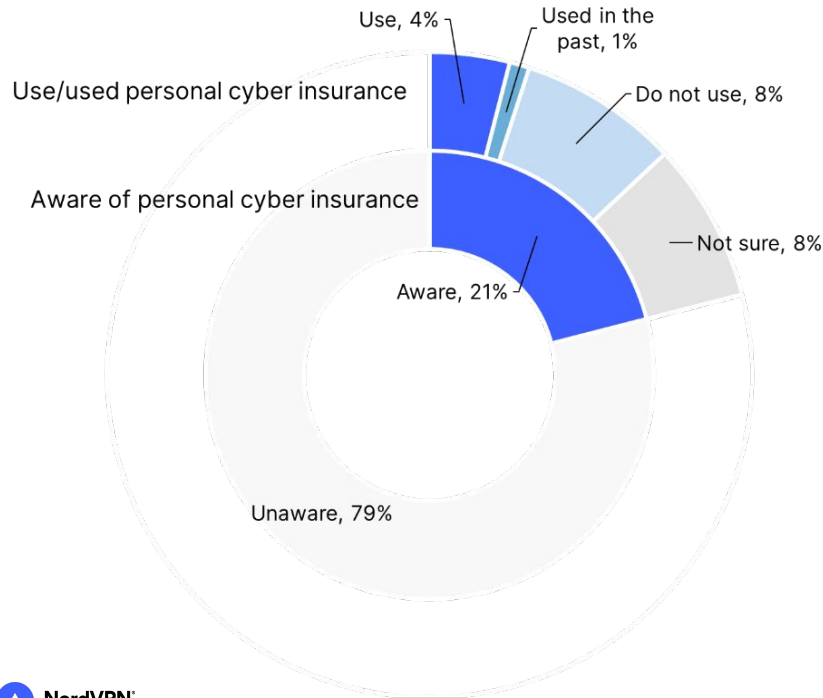
- Every fifth internet user claims to be aware of personal cyber insurance
- Cyber insurance usage is currently low, but there is higher consideration for future use



Cyber insurance: awareness, usage, and consideration to use

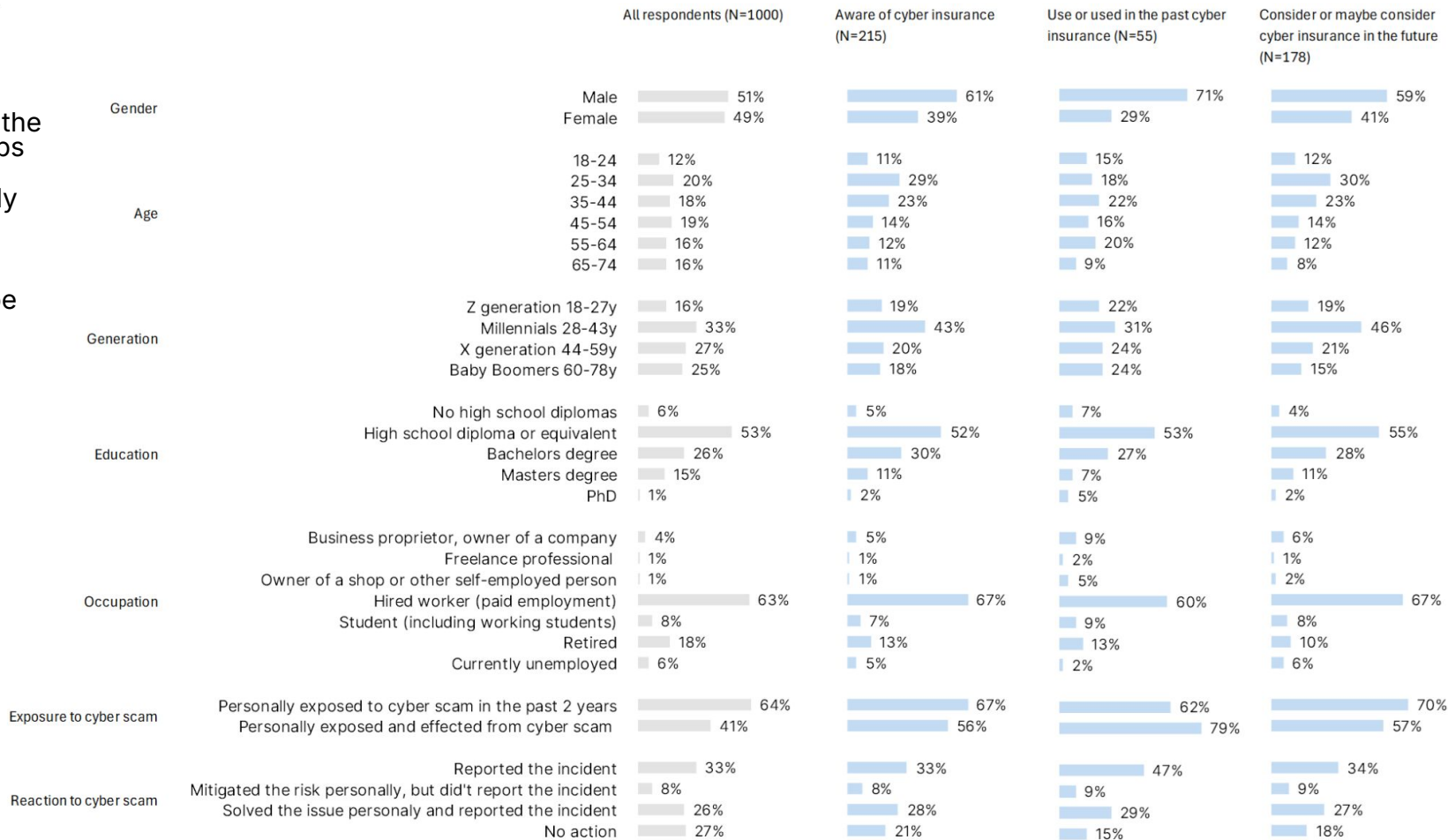
from all respondents N=1000

Every fifth internet user in Sweden is aware of personal cyber insurance. The usage of cyber insurance is rather low at 4%; therefore, the consideration to use it in the future is 18%.



Cyber insurance: awareness, usage, and consideration to use

Sizes of sub-samples in the compared groups are too small to make statistically significant inferences; therefore, the results should be considered tentative.



Methodology

Survey target group

18-74 y.o. Internet users of Sweden

Sampling

National representative sample among internet users
Quotas on age, gender, and place of residence

Contacts from the Cint panel

Sample size

1000 respondents

Fieldwork

July 30th - August 8th, 2024