

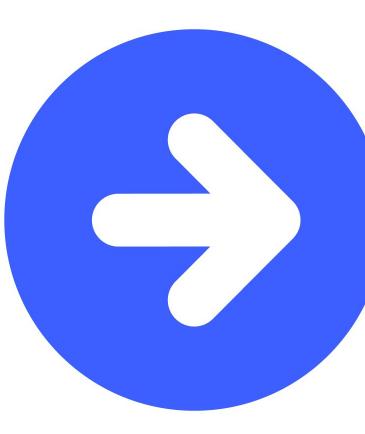
## Online Scam in Sweden, Norway, and Denmark

October, 2024

### Main insights

Cybercrime prevalence	Over the last two years, over two-thirds of respondents in Scandinavian countries 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.
Cybercriminals follow the trends	Popular online communication channels like email, SMS, Facebook, and Messenger are common targets for cyber scams.
People react to 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.
NordVPN'	

- The overall incidence of cyber crime is high in the Scandinavian countries, with more than two thirds of people being exposed to cyber scam attempts in the past 2 years. Danish internet users are more likely to be exposed to cyber scams than Swedes.
- There is a discrepancy between the perceived cyber threats and the actual risks associated with them.





Encounters with cyber scam attempts in the last 2 years



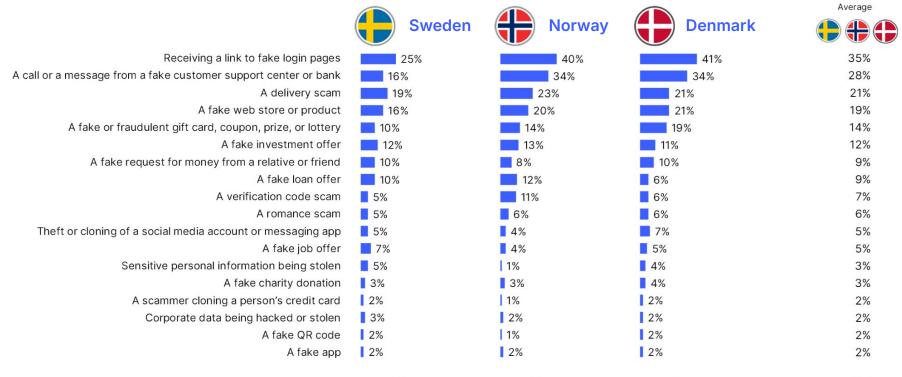


from all respondents: SE N=1000, NO N=1005, DK N=1005

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

from all respondents: SE N=1000, NO N=1005, DK N=1005

The most common online scams in all three Scandinavian countries over the past two years include fake login page scams, delivery scams, and calls from fake customer support centers. In Sweden, however, cybercrimes are less frequent.



N=1005

N=1005

N=3010

#### Perceived harm of online scam

from all respondents: SE N=1000, NO N=1005, DK N=1005

Bank card clones are considered the most perilous online scams in Sweden, while Danes and Norwegians perceive the compromise of personal information as an even greater threat than credit card fraud.

				Average
	Sweden	Norway	Denmark	
A scammer cloning a person's credit card	73%	80%	76%	76%
Sensitive personal information being stolen	66%	80%	80%	75%
Corporate data being hacked or stolen	61%	74%	62%	66%
A verification code scam	54%	56%	57%	56%
A fake request for money from a relative or friend	48%	51%	50%	51%
Receiving a link to fake login pages	44%	54%	45%	49%
A call or a message from a fake customer support center or bank	57%	41%	47%	48%
A fake investment offer	44%	47%	40%	44%
Theft or cloning of a social media account or messaging app	42%	44%	46%	44%
A fake loan offer	41%	47%	39%	42%
A fake web store or product	51%	43%	40%	42%
A fake QR code	45%	38%	38%	40%
A fake charity donation	38%	40%	38%	39%
A fake app	37%	41%	35%	38%
A romance scam	37%	42%	26%	35%
A delivery scam	34%	31%	30%	32%
A fake or fraudulent gift card, coupon, prize, or lottery	33%	27%	22%	27%
A fake job offer	25%	28%	19%	24%

N=1000 N=1005
\* incidents perceived as the most harmful on the 5-items grading scale

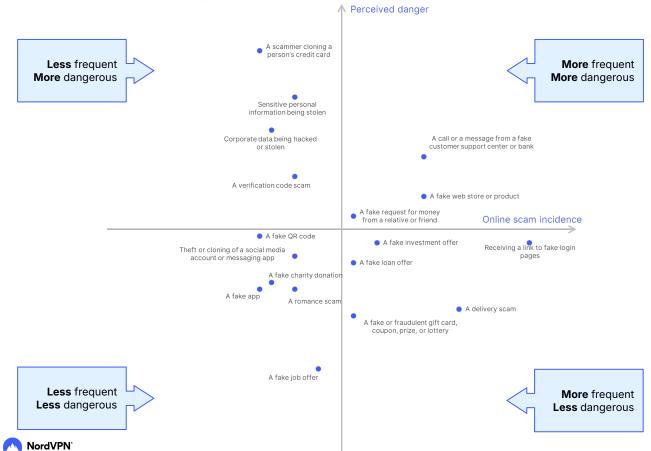
N=3010

N=1005

from all respondents: SE N=1000, NO N=1005, DK N=1005

Generally, there is a disparity between the perceived cyber threats and actual exposure to them. The closest correlation exists between personal exposure to online scams and the level of threat posed by scams involving fake login pages and fraudulent calls from support centers or banks. These types of scams are most prevalent in Denmark and Norway.

		Swede	en	Norway		Denmark
A scammer cloning a person's credit card		73%	1%	80%	2%	76%
Sensitive personal information being stolen		66%	1%	80%	4%	80%
Corporate data being hacked or stolen		61%	2%	74%	2%	62%
A verification code scam		54%	11%	56%	6%	57%
A fake request for money from a relative or friend	10%	48%	8%	51%	10%	50%
Receiving a link to fake login pages	25%	44%	40%	54%	41%	45%
A call or a message from a fake customer support center or bank	16%	57%	34%	41%	34%	47%
A fake investment offer		44%	13%	47%	11%	40%
Theft or cloning of a social media account or messaging app		42%	4%	44%	7%	46%
A fake web store or product		51%	20%	43%	21%	40%
A fake loan offer	10%	41%	12%	47%	6%	39%
A fake QR code		45%	1%	38%	2%	38%
A fake charity donation		38%	3%	40%	4%	38%
A fake app		37%	2%	41%	2%	35%
A romance scam		37%	6%	42%	6%	26%
A delivery scam		34%	23%	31%	21%	30%
A fake or fraudulent gift card, coupon, prize, or lottery		33%	14%	27%	19%	22%
A fake job offer		25%	4%	28%	5%	19%
	N=1000			N=1005		N=3010
incidents perceived as the most harmful				nally encounter in the last 2	years	

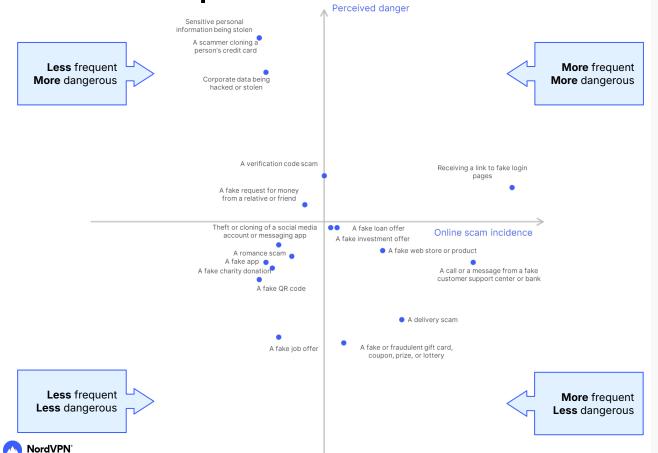


The most dangerous cyber scams involve financial losses and complex social engineering tactics.

Sweden

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

Axes intersect at the average values of perception of harm from cyber scams and incidents of cyber scams

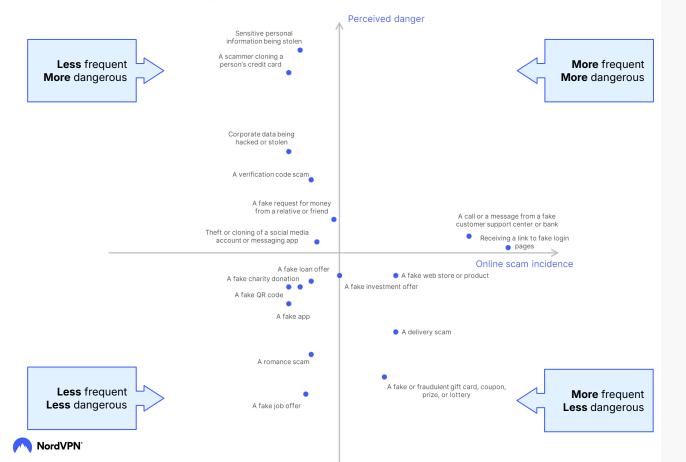


The most common and potentially dangerous cybercrime involves receiving links to fake login pages.

Norway

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

Axes intersect at the average values of perception of harm from cyber scams and incidents of cyber scams



The most common and potentially dangerous cybercrime involves receiving links to fake login pages.

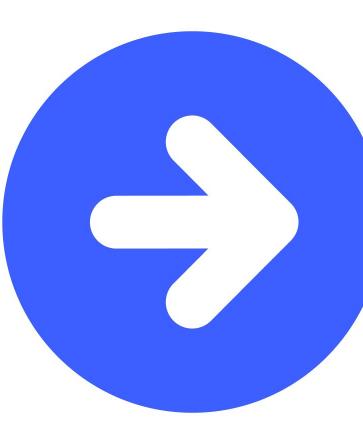
**Denmark** 

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

Axes intersect at the average values of perception of harm from cyber scams and incidents of cyber scams

# Reasons for vulnerability to cyber scams

- Scandinavian internet users blame cyber criminals' advanced technical and psychological knowledge when they fall victim to cybercrime
- Swedes are very concerned about the ability of cybercriminals to impersonate technical support center representatives. Danish respondents stated the lack of awareness and education concerning the operation of cyber scams
- 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: SE N=1000, NO N=1005, DK N=1005

Sweden Norway Denmark Scammers often pretend to be banks, government agencies, 64% 55% 54% tech support, or other trusted organizations Scammers use clever tricks like phishing emails, fake websites, 51% 53% 58% and pretending to be someone the victim trusts Scammers use high-tech methods to make fake websites, 52% 47% 56% emails, and messages look real Scammers manipulate victims using emotions to appeal to them 50% 45% 46% People lack awareness and education about how scams operate 34% 39% 48% Loneliness or isolation may make people fall for romance or 40% 45% 35% friendship scams Scammers pressure their victims to act quickly without thinking 45% 25% 37% by using tactics like threatening consequences Scammers gather personal information through data breaches 35% 38% 33% and social media to make their communication seem authentic Online shopping is becoming more popular, which makes 19% 30% 27% shoppers an easier target for cybercriminals Some people overestimate their ability to recognize scams and 25% 26% 24% therefore do not take the necessary precautions Scammers exploit people's greed for easy money by promising 24% 24% 23% profitable investments or luxurious prizes N=1000 N=1005 N=1005 N=3010

Average Swedes are very concerned about the ability of cybercriminals to 58% impersonate call center representatives. Danish 54% respondents stated the lack of 52% awareness and education concerning the operation of cyber 47% scams. 40%

Fewer respondents acknowledge 40% that scammers exploit people's 36% weaknesses, such as greed or overconfidence, to recognize the 35% cvber risks. 25%

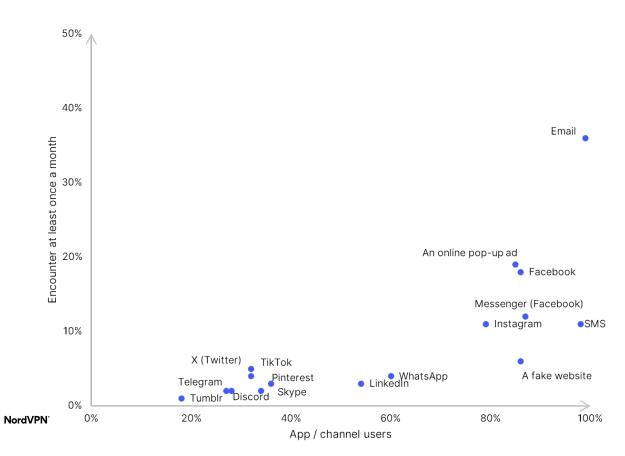
25%

24%



#### Cyber scam delivery channels

% of those who encountered cyber scam in the last 2 years, N=639

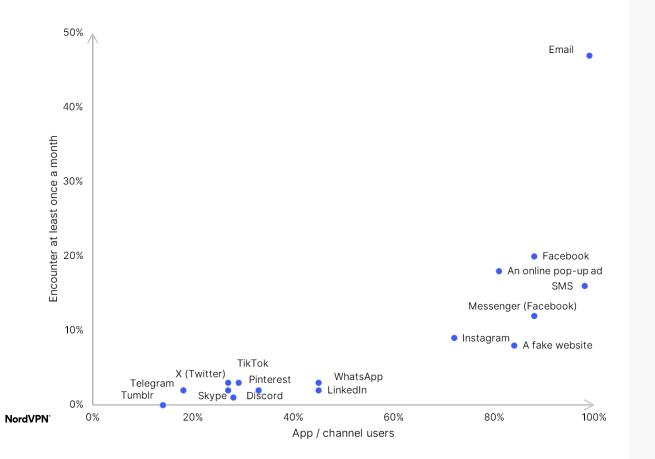


Frequency of encounters with the cyber scam over the last two years are directly related to the overall popularity of communication channels.



#### Cyber scam delivery channels

% of those who encountered cyber scam in the last 2 years, N=700

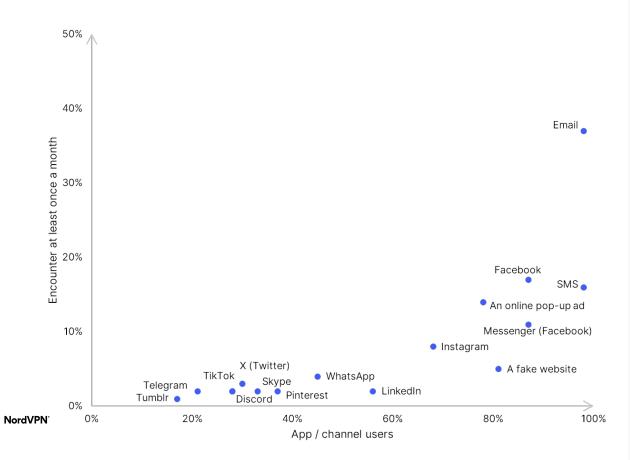


Norway

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

#### Cyber scam delivery channels

% of those who encountered cyber scam in the last 2 years, N=786

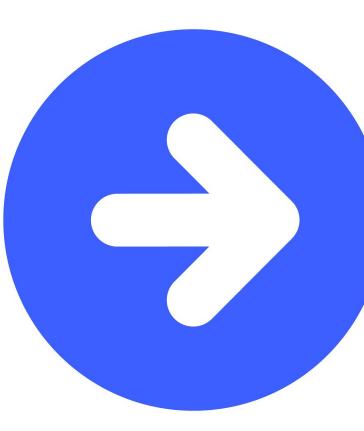


Denmark

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**

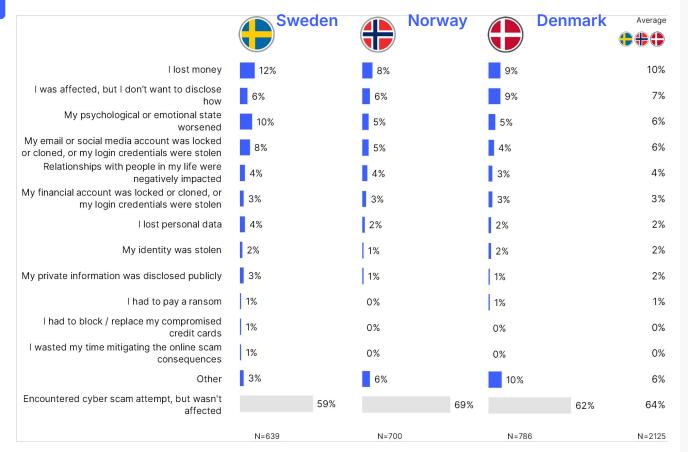
- Around 40% of Swedes and Danes who experienced cybercrime in the last 2 years reported suffering from the consequences of cyber-attacks. In Norway, the proportion of reporting actual harm after experiencing a cyber scam attempt is lower, at around 30%.





#### **Consequences of the cyber crime**

% of those who encountered cyber scam in the last 2 years



Around 40% of Swedes and Danes who experienced cybercrime in the last 2 years reported suffering from the consequences of cyber-attacks. In Norway, the proportion of reporting actual harm after experiencing a cyber scam attempt is lower, at around 30%.

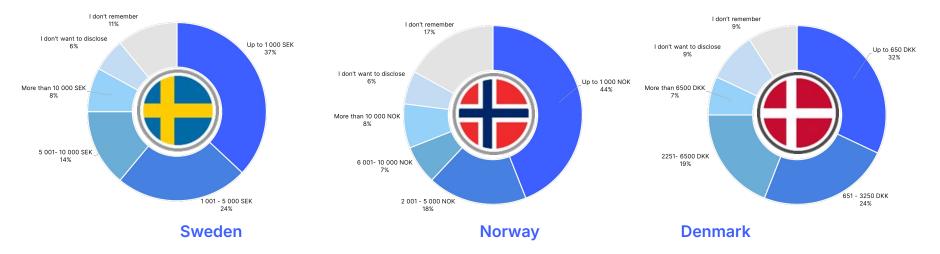
The majority of the consequences were associated with financial losses and adverse psychological effects.

#### Financial losses due to the cyber crime

% of those who suffered financial losses due to cyber scam. SE N=125, NO N=104, DK N=124

The financial loss due to cyber crimes in all countries is typically less than 90 EUR.

NordVPN<sup>®</sup>



\* Exchange rates of SEK and NOK are nearly identical (1=1.04). The SEK and DKK exchange rate 1=0.66.

For reference: 1000 SEK, 1000 NOK or 650 DKK estimate around 90 EUR.

# Response to the cyber crime attempts

- 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. Danes in comparison with Swedes and Norwegians are less likely to report the incident.
- The main reason Swedish internet users choose not to report cyber incidents is their confidence in handling the situation independently. Danes are more likely to avoid reporting cyber incidents because they believe it would make no difference.





#### **Reactions to the cyber scam attempts**

% of those who encountered cyber scam in the last 2 years, N=639

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.

Sweden

**Exposure** Reaction **Reaction type** % of all internet users, N=1000 % of those those who encountered cyber scam, N=639 % of those those who encountered cyber scam, N=639 Personal actions Social actions No answer / didn't remember 7% I reported the scam to the app, platform, or 28% Didn't react to scam attempt bank 27% I informed my contacts about the scam 18% I made my account or messaging app 66% 18% settings stricter 64% Of scam targets Were exposed I stopped using unsafe apps or web pages 16% reacted to cyber to cyber scam scam I reported the scam to the police 14% I started to use cybersecurity tools like a 12% VPN, antivirus software, or 2FA I published a post on social media about 6% the scammers I became more attentive and cautious in my 1% online behaviour 10% 34% 49% NordVPN Social + Personal Personal action Social action

#### **Reactions to the cyber scam attempts**

% of those who encountered cyber scam in the last 2 years, N=700

#### 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.

Norway

**Exposure** Reaction **Reaction type** % of all internet users, N=1000 % of those those who encountered cyber scam, N=700 % of those those who encountered cyber scam, N=700 Personal actions Social actions No answer / didn't remember 6% I reported the scam to the app, platform, or 34% bank Didn't react to scam attempt I stopped using unsafe apps or web pages 23% 28% I made my account or messaging app 20% 66% settings stricter 70% Of scam targets I informed my contacts about the scam 14% Were exposed reacted to cyber to cyber scam scam I started to use cybersecurity tools like a 9% VPN, antivirus software, or 2FA I reported the scam to the police 6% I published a post on social media about 5% the scammers I became more attentive and cautious in my 1% online behaviour 13% 40% 43% NordVPN Social + Personal Personal action Social action

#### **Reactions to the cyber scam attempts**

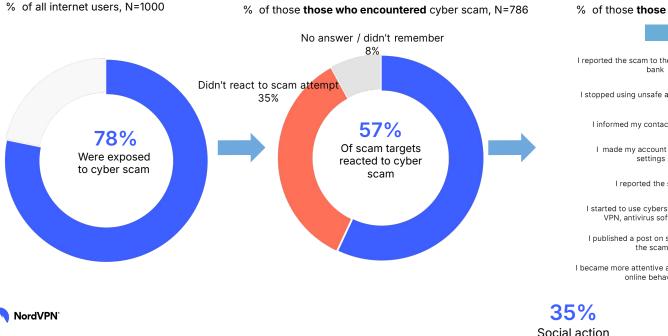
% of those who encountered cyber scam in the last 2 years, N=786

After experiencing a scam attempt, 57% of Danes either reported or informed others about the incident or took personal actions to prevent further cybercrime attempts. Danes in comparison with Swedes and Norwegians are less likely to report the incident.

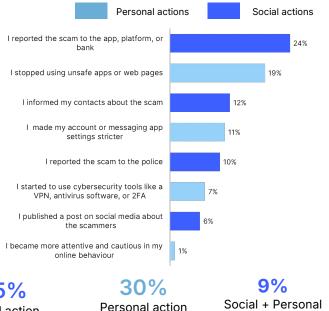
**Exposure** 







%~ of those those who encountered cyber scam, N=786  $\,$ 

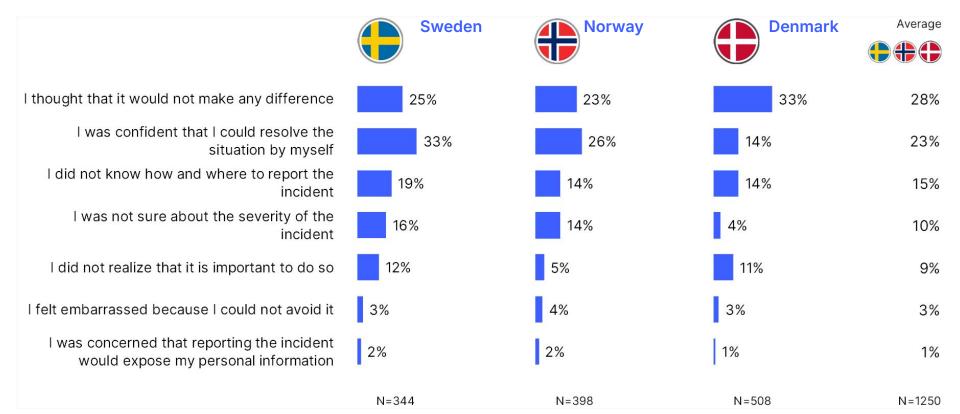




#### Reasons for not informing about the cyber incident

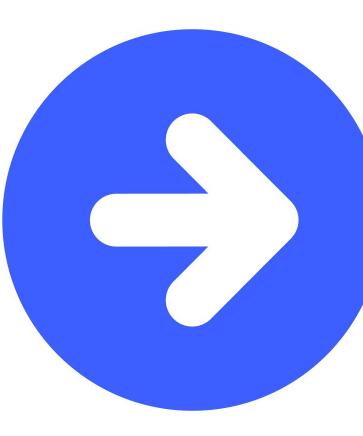
from the respondents who were exposed to cyber crime but did not report it

The main reason Swedish internet users choose not to report cyber incidents is their confidence in handling the situation independently. Danes are more likely to avoid reporting cyber incidents because they believe it would make no difference.



# Attitudes towards cyber security and preventive measures against cyber scam

- Scandinavian internet users 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. 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.

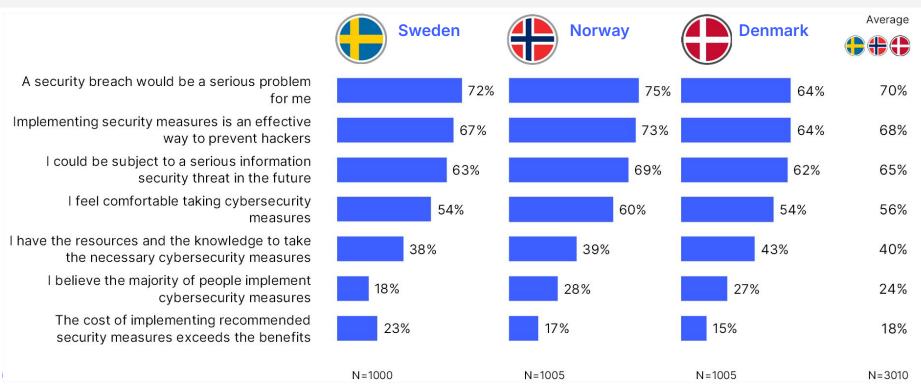




#### Attitudes towards cyber security

from all respondents: SE N=1000, NO N=1005, DK N=1005

People generally recognize the threats and consequences of cybercrime. They also critically evaluate their preparedness and knowledge to prevent cyber incidents.



% of agreement with the statement (agree + completely agree)

#### Preventive actions against online scams

from all respondents: SE N=1000, NO N=1005, DK N=1005

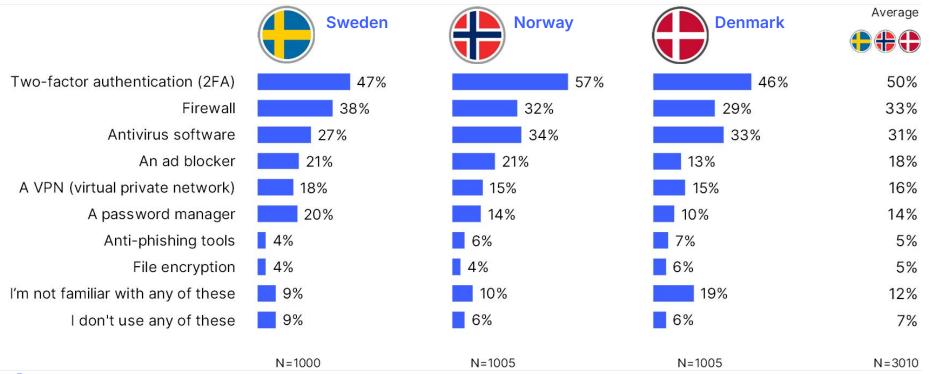
Vigilance and common-sense actions are often cited as effective measures against cyber scams, but more advanced measures like verifying website authenticity, using strong passwords, and staying informed about cyber threats are less recognized as important preventive steps.

Sweden		Norway		Denmark			Average
Don't click on messages saying I won a prize or offers of something for free		79%	6	80%	6	73%	77%
Remain cautious about requests for personal information, money, or passwords		74%		76%		64%	71%
Avoid too-good-to-be-true deals		68%		71%		65%	68%
Don't respond to unknown numbers or chat requests on messaging apps		70%		72%		60%	67%
Use secure payment methods		62%		68%		52%	61%
Limit the personal information I share on social media		57%		62%		48%	56%
Treat the links I click with caution		62%		59%		46%	56%
Regularly check my bank and credit card statements for unauthorized transactions		57%		47%		53%	52%
Avoid sharing sensitive information in chats on messaging apps		49%		58%		48%	52%
Use two-factor authentication (2FA) on my accounts or messaging apps		39%		49%		38%	42%
Download apps from trusted sources		44%		49%	3	3%	42%
Use complex passwords or biometric authentication on my online accounts and apps		37%		51%		37%	42%
Keep an eye on the news and information relating to online scams and protective measures I can take		37%		39%	3	2%	36%
Verify website authenticity		33%		40%	3	2%	35%
Read reviews and ratings on trusted websites		35%	3	32%	:	36%	34%
Verify that a website I'm visiting has valid contact information and accessible customer service	2	25%	3	32%		38%	32%
Use chat lock (a PIN) or disappearing messages for sensitive information on messaging apps	5%		14%		7%		9%
Have a cyber insurance policy	3%		5%		7%		5%
Other	2%		2%		2%		2%
None of the above	2%		1%		2%		2%
	N=1000	i.	N=1005		N=1005		N=3010

#### Perceived effectiveness of cybersecurity tools

from all respondents: SE N=1000, NO N=1005, DK N=1005

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

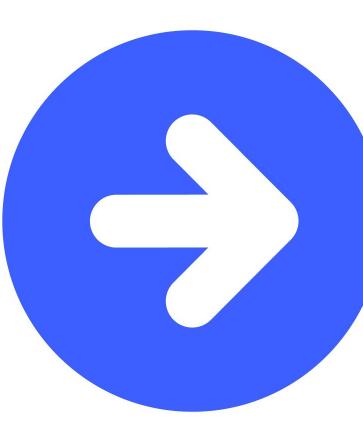


Which of the cybersecurity tools that you currently use do you find the most effective?



#### **Personal cyber insurance**

 In Norway and Denmark, identity protection is the most prevalent cyber insurance feature. Potential users also value protection from financial transfer fraud and cyber-attacks, while Norwegian respondents prioritize data recovery cost reimbursement.

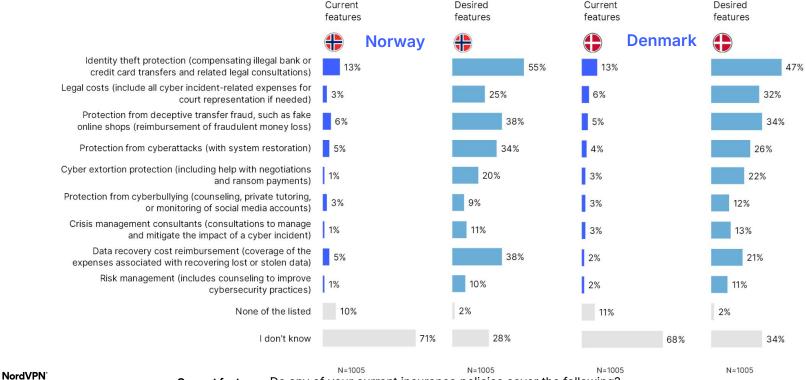




#### Use and consideration of cyber insurance features

from all respondents N=1005

In Norway and Denmark, identity protection is the most prevalent cyber insurance feature. Potential users also value protection from financial transfer fraud and cyber-attacks, while Norwegian respondents prioritize data recovery cost reimbursement.

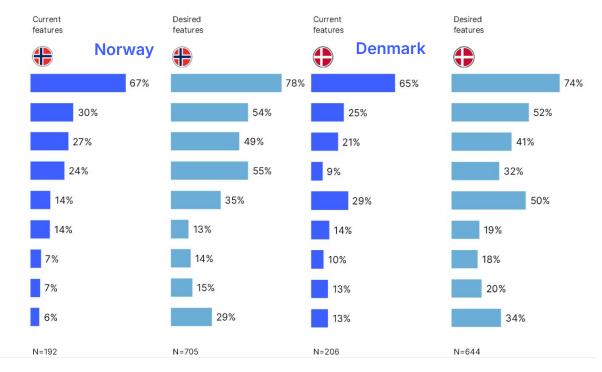


**Current features:** Do any of your current insurance policies cover the following? **Desired features:** When thinking about cyber insurance, which features would be most important to you?

#### Use and consideration of cyber insurance features

from involved respondents (those who stated at least one cyber insurance feature)

In Norway and Denmark, identity protection is the most prevalent cyber insurance feature. Potential users also value protection from financial transfer fraud and cyber-attacks, while Danish respondents prioritize data recovery cost reimbursement.



Identity theft protection (compensating illegal bank or credit card transfers and related legal consultations) Protection from deceptive transfer fraud, such as fake online shops (reimbursement of fraudulent money loss)

Protection from cyberattacks (with system restoration)

Data recovery cost reimbursement (coverage of the expenses associated with recovering lost or stolen data)

Legal costs (include all cyber incident-related expenses for court representation if needed)

Protection from cyberbullying (counseling, private tutoring, or monitoring of social media accounts)

Risk management (includes counseling to improve cybersecurity practices)

Crisis management consultants (consultations to manage and mitigate the impact of a cyber incident)

Cyber extortion protection (including help with negotiations and ransom payments)



**Current features:** Do any of your current insurance policies cover the following? **Desired features:** When thinking about cyber insurance, which features would be most important to you?

## Methodology

#### Survey target groups

18-74 y.o. Internet users of Sweden, Norway, and Denmark

#### Sampling

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

Contacts from the Cint panel

#### Sample size

1000 respondents - Sweden 1005 respondents - Norway 1005 respondents - Denmark

#### **Fieldwork dates**

July 30th - August 8th, 2024 in Sweden September 10 - 19th, 2024 in Norway and Denmark.

