European Commission

Special Eurobarometer 423

CYBER SECURITY

SUMMARY

Fieldwork: October 2014

Publication: February 2015

This survey has been requested by the European Commission, Directorate-General for Home Affairs and co-ordinated by Directorate-General for Communication.

http://ec.europa.eu/public_opinion/index_en.htm

This document does not represent the point of view of the European Commission.
The interpretations and opinions contained in it are solely those of the authors.

Special Eurobarometer 423 / Wave EB82.2 – TNS Opinion & Social

Eurobarometer

Special Eurobarometer 423

Cyber security

Conducted by TNS Opinion & Social
at the request of the
Directorate-General for Home Affairs

Survey co-ordinated by the
Directorate-General for Communication
(DG COMM "Strategy, Corporate Communication Actions
and Eurobarometer" Unit)

TABLE OF CONTENTS

INTRODUCTION

This summary brings together the results of the Special Eurobarometer public opinion survey on "Cyber security" in the 28 European Union countries.

Cybercrime is a borderless problem, consisting of criminal acts that are committed online by using electronic communications networks and information systems, including crimes specific to the Internet, online fraud and forgery, and illegal online content.[1]

Whilst the value of the cybercriminal economy as a whole is not precisely known, the losses are thought to represent billions of euros per year. The scale of the problem is itself a threat to law enforcement response capability – with more than 150,000 viruses and other types of malicious code in circulation and a million people victims of cybercrime every day.

Given the development of cybercrime in recent years, the European Commission has designed a coordinated policy in close co-operation with European Union (EU) Member States and the other EU institutions.

EU legislative actions contributing to the fight against cybercrime address issues such as attacks against information systems, online offensive material and child pornography, online privacy, and online fraud and counterfeiting.

The aim of this survey is to understand EU citizens' experiences and perceptions of cyber security issues. The survey examines the nature and frequency of Internet usage; their awareness and experience of cybercrime; and the level of concern that they feel about this type of crime.

The findings from this survey update a previous study which was carried out in May-June 2013 (Special Eurobarometer 404). The 2014 survey repeats most of the questions asked in 2013 in order to provide insight into the evolution of knowledge, behaviour and attitudes towards cyber security in the European Union.

[1] More information on the fight against cybercrime in the EU can be found here: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

This survey was carried out by TNS Opinion & Social network in the 28 Member States of the European Union between 11 and 20 October 2014. Some 27.868 respondents from different social and demographic groups were interviewed face-to-face at home in their mother tongue on behalf of the Directorate-General for Home Affairs. The methodology used is that of Eurobarometer surveys as carried out by the Directorate-General for Communication ("Strategy, Corporate Communication Actions and Eurobarometer" Unit)[2]. A technical note on the manner in which interviews were conducted by the Institutes within the TNS Opinion & Social network is appended as an annex to this summary. Also included are the interview methods and confidence intervals[3].

Note: In this summary, countries are referred to by their official abbreviation. The abbreviations used in this summary correspond to:

ABBREVIATIONS			
BE	Belgium	LV	Latvia
BG	Bulgaria	LU	Luxembourg
CZ	Czech Republic	HU	Hungary
DK	Denmark	MT	Malta
DE	Germany	NL	The Netherlands
EE	Estonia	AT	Austria
EL	Greece	PL	Poland
ES	Spain	PT	Portugal
FR	France	RO	Romania
HR	Croatia	SI	Slovenia
IE	Ireland	SK	Slovakia
IT	Italy	FI	Finland
CY	Republic of Cyprus*	SE	Sweden
LT	Lithuania	UK	The United Kingdom
		EU28	European Union – 28 Member States

* Cyprus as a whole is one of the 28 European Union Member States. However, the 'acquis communautaire' has been suspended in the part of the country which is not controlled by the government of the Republic of Cyprus. For practical reasons, only the interviews carried out in the part of the country controlled by the government of the Republic of Cyprus are included in the 'CY' category and in the EU28 average.

* * * * *

We wish to thank the people throughout the European Union
who have given their time to take part in this survey.
Without their active participation, this study would not have been possible.

[2] http://ec.europa.eu/public_opinion/index_en.htm
[3] The results tables are included in the annex. It should be noted that the total of the percentages in the tables of this summary may exceed 100% when the respondent has the possibility of giving several answers to the question.

EXECUTIVE SUMMARY

- The survey shows that the levels of Internet use still vary widely: while more than half of EU citizens access the Internet every day (63%), a substantial minority (24%) say that they never use the Internet or do not have access.
- Besides accessing the Internet from a computer (92%), 61% of Internet users access the Internet through a smartphone, and 30% use a touchscreen tablet. The use of smartphones and touchscreen tablets has increased dramatically compared with 2013.
- More than half of Internet users in the EU say they use the Internet to access their e-mail (86%), read news online (63%), access online social networks (60%), buy goods or services online (57%) or do online banking (54%), while 23% sell goods or services. Levels of use of all of these activities have increased since 2013. There is considerable variation in the online activities that respondents undertake in different countries.
- When using the Internet for online banking or shopping, the two most common concerns are about someone misusing personal data (mentioned by 43% of Internet users in the EU) and security of online payments (42%). EU citizens are more concerned about these issues than they were in 2013.
- Internet users are more likely to have changed their online behaviour because of security concerns since 2013: 61% have installed anti-virus software, 49% do not open emails from people they do not know, while 38% say that they are less likely to give personal information on websites. Three in five Internet users (61%) have changed at least one of their online passwords during the past year.
- Just under half (47%) of EU citizens feel well informed about the risks of cybercrime, a slight increase on the 2013 figure (44%).
- Internet users express high levels of concern about cyber security:
    - 89% agree that they avoid disclosing personal information online;
    - 85% agree that the risk of becoming a victim of cybercrime is increasing;
    - 73% agree that they are concerned that their online personal information is not kept secure by websites;
    - 67% agree that they are concerned that this information is not kept secure by public authorities.
- Around two in three Internet users in the EU are concerned about experiencing identity theft (68%) and about discovering malicious software on their device (66%). More than half are concerned about being the victim of bank card or online banking fraud (63%); having their social media or email account hacked (60%); scam emails or phone calls (57%); online fraud (56%);

and accidentally discovering child pornography online (52%). Similar proportions are concerned about not being able to access online services because of cyber-attacks (50%); cyber extortion (47%); and accidentally encountering material which promotes racial hatred or religious extremism (46%).

- These levels of concern about specific types of cybercrimes are considerably higher than in 2013, with the largest increase in relation to identity theft (up 16 percentage points).
- Despite the high levels of concern, three in four Internet users (74%) agree that they are able to protect themselves sufficiently against cybercrime, although 23% disagree.
- The two most common situations experienced by respondents are discovering malicious software on their device (47%) and receiving an email or phone call fraudulently asking for access to their computer, logins or personal details (31%). In each case, 7% of Internet users say that this has happened to them often. Experience of the various types of cybercrime has remained at a similar level, in comparison with the 2013 survey.
- If they experienced or were the victim of cybercrime, most respondents say they would contact the police, especially if the crime was identity theft (84%) or online banking fraud (79%), or if they accidentally encountered child pornography online (76%).
- Various steps are taken to protect children aged under 16 while they are online, such as monitoring their Internet usage (22%), talking to children about risks on the Internet (21%), limiting the time spent online (18%) and adjusting security settings on browser (13%).
- There are differences between countries that can be seen throughout the findings:
    - Respondents in Sweden, the Netherlands and Denmark are more likely to be frequent Internet users (87% or more accessing the Internet at least once a day), and to use the Internet for buying things (80%, 83% and 80% of Internet users respectively) or for online banking (91%, 89% and 94%). They are also more likely to be well informed about the risks of cybercrime (66%, 67% and 67% feeling either very or fairly well informed), and to have taken steps to address security concerns (69%, 65% and 61% say they are less likely to give personal information on websites).
    - By contrast, lower levels of Internet use can be seen in a number of countries such as Romania, Portugal, Greece and Bulgaria (with 54%, 56%, 58% and 60% of respondents using the Internet). In Romania and Bulgaria in particular, respondents feel less well informed about the risks of cybercrime (31% and 34% feeling either very or fairly well informed in these countries).

I. INTERNET USE

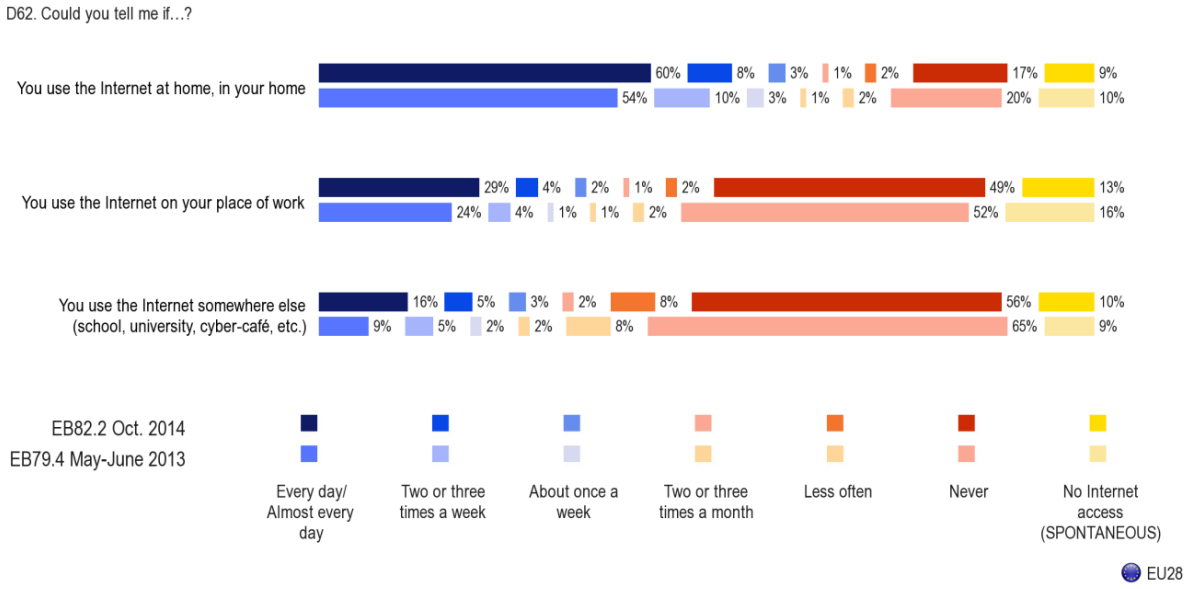
1. FREQUENCY OF INTERNET ACCESS

A significant majority of Europeans have Internet access and they are most likely to use it from home on a daily basis.[4] However, a substantial minority of EU citizens (24%) do not access the Internet at all; this includes 18% who never access the Internet and 6% who say they do not have any Internet access.

More than half of EU citizens (60%) use the Internet at home every day or almost every day. In addition, more than one in three EU citizens (38%) use the Internet at their place of work and around one in three respondents (34%) use the Internet somewhere else.

There has been an increase in usage at home, work and elsewhere. This is not only seen in the reduced proportion of people who say they never access the Internet or have no access, but also in the increased frequency of Internet usage on a daily basis.

Although not strictly comparable as the question wording is different, the proportion is in line with the 79% of Europeans who use the Internet reported by Eurostat in the most recent EU wide data available[5].



Base: all respondents (n=27,868 in EU28)

[4] EB82.2: D62 'Could you tell me if ….? 1. You use the Internet at home, in your home. 2. You use the Internet on your place of work. 3. You use the Internet somewhere else (school, university, cyber-café, etc.).' Possible answers: Every day/Almost every day; Two or three times a week; About once a week; Two or three times a month; Less often; Never; No Internet access (SPONTANEOUS).

EB82.1: D62 'Could you tell me if ….? 1. You use the Internet at home, in your home. 2. You use the Internet on your place of work. 3. You use the Internet somewhere else (school, university, cyber-café, etc.).' Possible answers: Every day/Almost every day; Two or three times a week; About once a week; Two or three times a month; Less often; Never; No Internet access (SPONTANEOUS).

[5] Internet use and frequency of use by individuals, 2013 (% of individuals), Eurostat

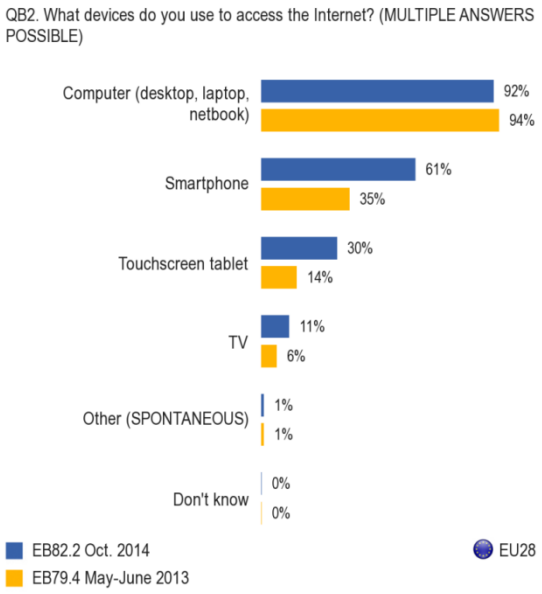
Respondents in every Member State are most likely to use the Internet at home. However, there are large variations between individual Member States in levels of Internet use.

Overall levels of Internet use can be assessed by combining the findings for use at different locations. People who use the Internet are likely to do so frequently: 63% of EU citizens use the Internet every day (or almost every day), while a smaller proportion (13%) uses the Internet often or sometimes.

The highest levels of Internet use can be seen in Sweden (96%), the Netherlands (95%) and Denmark (94%). The lowest proportions that use the Internet can be found in Romania (54%), Portugal (56%), Greece (58%) and Bulgaria (60%).

2. MEANS OF INTERNET ACCESS

Use of smartphones and tablets is increasing rapidly, although computers remain the most common means of accessing the Internet.[6] The vast majority of Internet users (92%) access the Internet from a desktop computer, laptop or netbook, while over half (61%) access the Internet through a smartphone. In addition, 30% use a touchscreen tablet, while 11% access the Internet from a TV.



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

Looking at the findings for individual countries, access through a computer (desktop, laptop or netbook) is the most common method in all countries.

[6] EB82.2: QB2 'What devices do you use to access the Internet?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Computer (desktop, laptop, netbook); Touchscreen tablet; Smartphone; TV; Other (SPONTANEOUS); Don't know.

EB79.4: QC2 'What devices do you use to access the Internet?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Desktop computer; Laptop computer/Netbook; Tablet computer/Touchscreen; Smartphone; TV; Other (SPONTANEOUS); Don't know.

The use of smartphones and touchscreen tablets has increased substantially in the last year. The proportion that accesses the Internet through a smartphone has increased by 26 percentage points (from 35% to 61%), while there has been an increase in the use of touchscreen tablets of 16 points (from 14% to 30%). Furthermore, this increase can be seen in all of the countries surveyed.

The largest increases in Internet access via smartphones can be seen in Spain (up 41 percentage points since 2013)[7], Italy (up 41 points), Croatia (up 36 points) and Hungary (up 36 points), while in the case of touchscreen tablets, the largest increases can be seen in the UK (up 26 percentage points since 2013), Finland (up 25 points), Ireland (up 24 points) and Cyprus (up 23 points).

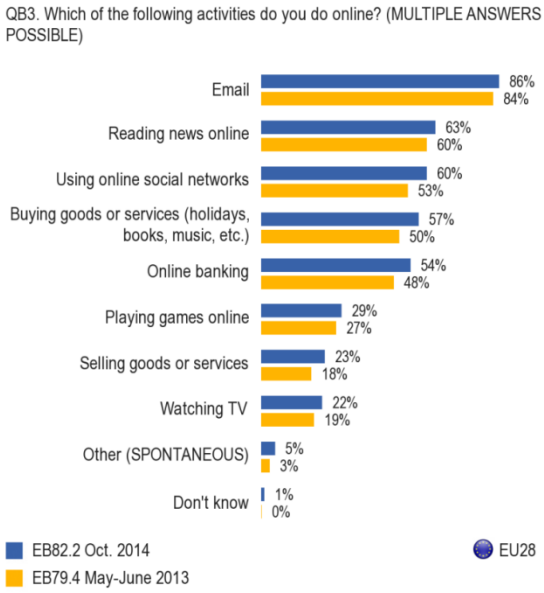
[7] This corresponds with the large increase in mobile access seen in Spain in the 2014 (which now stands at the 3rd highest mobile access in the EU) and the highest increase in mobile Internet usage (the biggest increase seen in the EU). http://ec.europa.eu/public_opinion/archives/ebs/ebs_414_en.pdf (pages 23, 54)

3. ONLINE ACTIVITIES

The vast majority of respondents across the EU use the Internet to access their email (86%), while more than half of respondents do each of the following activities: read news online (63%), use online social networks (60%), buy goods or services (57%), and do online banking (54%). Internet users in the EU are less likely to say that they play games online (29%), sell goods or services (23%) or watch TV (22%).[8]

In total, seven in ten respondents (70%) conduct any kind of online financial transactions, either buying or selling goods or services or online banking. This compares with 66% of Internet users conducting any kind of financial transactions in 2013, an increase of four percentage points.

There have been increases in the use of Internet for various online activities at the EU level and across different Member States since 2013. The largest increases can be seen for using online social networks (from 53% to 60%), buying goods or services (from 50% to 57%) and online banking (from 48% to 54%).



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

[8] EB82.2: QB3 'Which of the following activities do you do online?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Online banking; Buying goods or services (holidays, books, music, etc.); Selling goods or services; Using online social networks; Email; Reading news online; Playing games online; Watching TV; Other (SPONTANEOUS); Don't know.

EB79.4: QC3 'Which of the following activities do you do online?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Online banking; Buying goods or services (holidays, books, music, etc.); Selling goods or services; Using online social networks; Email; Reading news online; Playing games online; Watching TV; Other (SPONTANEOUS); None (SPONTANEOUS); Don't know.

There is considerable variation in the online activities that respondents undertake in different countries.

In almost all Member States, most respondents use the Internet to access e-mail. In Finland online banking is as frequently used as email (93%).

In five Member States, most respondents use the Internet to read online news: Lithuania (89%), Poland (82%), Croatia (81%), Greece (76%), and Cyprus (74%). In Romania, most respondents (64%) use the Internet to access online social networks.

II. CONCERNS ABOUT INTERNET TRANSACTIONS

1. CONCERNS

Misuse of personal data (43%) and security of online payments (42%) remain the two biggest concerns about using the Internet for things like online banking or buying things online.[9] Some respondents also express a preference for conducting transactions in person (26%), while 22% are concerned about not receiving goods or services that they buy online.

Around one in six Internet users (18%) say they have no concerns about using the Internet for things like online banking or buying things online.

Overall, levels of concern have increased across the EU since the 2013 survey. Specifically, larger proportions are concerned about someone misusing personal data (43% compared with 37%), security of online payments (42% compared with 35%), and not receiving goods or services that they buy online (22% compared with 15%).

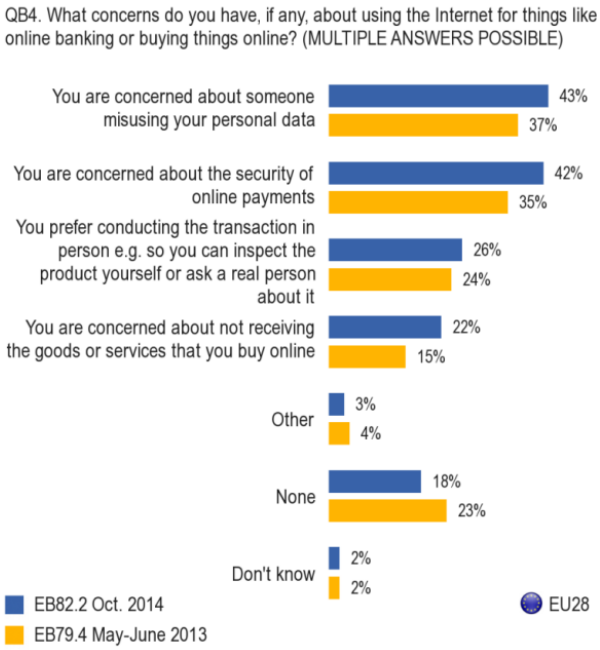
The proportions that say they have no concerns have decreased in most Member States. The largest decreases can be seen in Finland (down 18 percentage points), Czech Republic (down 16 points) and Slovakia (down 16 points).

The increase in the level of concern may also reflect the media landscape shortly before and during the time that fieldwork was taking place. Interviewing took place within the context of widespread reporting of the Shellshock virus and the publication of a UN report on mass internet surveillance, amongst other stories of the time[10].

[9] EB82.2: QB4 'What concerns do you have, if any, about using the Internet for things like online banking or buying things online?' (DO NOT SHOW CARD – DO NOT READ OUT – MULTIPLE ANSWERS POSSIBLE). Possible answers: You prefer conducting the transaction in person e.g. so you can inspect the product yourself or ask a real person about them; You are concerned about the security of online payments; You are concerned about someone misusing your personal data; You are concerned about not receiving the goods or services that you buy online; Other; None; Don't know.

EB79.4: QC5 'What concerns do you have, if any, about using the Internet for things like online banking or buying things online?' (DO NOT SHOW CARD – DO NOT READ OUT – MULTIPLE ANSWERS POSSIBLE). Possible answers: You prefer conducting the transaction in person e.g. so you can inspect the product yourself or ask a real person about them; You are concerned about the security of online payments; You are concerned about someone taking/ misusing your personal data; You are concerned about not receiving the goods or services that you buy online; Other; None; Don't know.

[10] http://www.theguardian.com/technology/2014/sep/25/shellshock-bug-heartbleed
http://www.theguardian.com/world/2014/oct/15/internet-surveillance-report-edward-snowden-leaks



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

2. IMPACT ON BEHAVIOUR

The actions that respondents are most likely to take because of concerns about online security issues are installing anti-virus software (61%) and not opening emails from people they do not know (49%).[11]

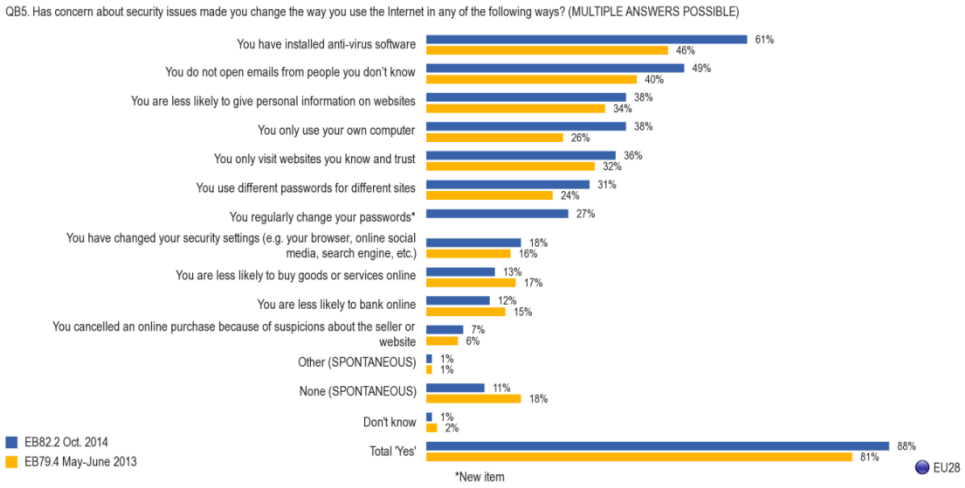
Other changes include being less likely to give personal information on websites (38%), only using their own computer (38%), only visiting websites that they know and trust (36%), using different passwords for different sites (31%), and regularly changing their passwords (27%).

Other actions are mentioned less frequently: 18% have changed their security settings on browser, 13% say they are less likely to buy goods online and 12% are less likely to bank online. In addition, 7% have cancelled an online purchase because of suspicions about the seller or website. However, 11% of respondents say they have not made any changes because of concerns about security issues.

[11] EB82.2: QB5 'Has concern about security issues made you change the way you use the Internet in any of the following ways?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: You are less likely to buy goods or services online; You are less likely to bank online; You are less likely to give personal information on websites; You have changed your security settings (e.g. your browser, online social media, search engine, etc.); You only visit websites you know and trust; You use different passwords for different sites; You do not open emails from people you don't know; You only use your own computer; You have installed anti-virus software; You cancelled an online purchase because of suspicions about the seller or website; You regularly change your passwords; Other (SPONTANEOUS); None (SPONTANEOUS); Don't know.

EB79.4: QC6 'Has concern about security issues made you change the way you use the Internet in any of the following ways?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Less likely to buy goods online; Less likely to bank online; Less likely to give personal information on websites; Changing security settings (e.g. your browser, online social media, search engine, etc.); Only visit websites you know and trust; Use different passwords for different sites; Do not open emails from people you don't know; Only use your own computer; Have installed anti-virus software; Cancelled an online purchase because of suspicions about the seller or website; Other (SPONTANEOUS); None (SPONTANEOUS); Don't know.

Overall, respondents are more likely to have changed their online behaviour due to security issues (an increase of 7 points) since 2013. The largest increases can be seen for installing anti-virus software (up 15 percentage points), only using the respondent's own computer (up 12 points), not opening emails from people they do not know (up 9 points), and using different passwords for different sites (up 7 points).



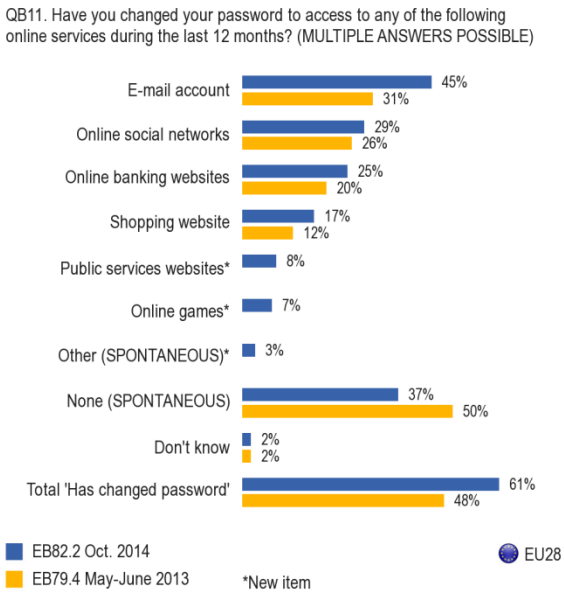
Base: respondents who use the Internet (D62) (n=21,015 in EU28)

Looking at individual countries, respondents are most likely to say that they have changed the way they use the Internet because of concerns about security issues in the Netherlands (98%), Sweden (96%), Denmark (95%) and Austria (95%). The lowest proportions can be observed in Poland (78%), Romania (80%) and the UK (80%).

In every Member State, except Bulgaria and Cyprus, most respondents have installed anti-virus software. In Bulgaria, one in four (38%) do not open emails from unknown people instead, while in Cyprus, around half (46%) only use their own computer.

Across the EU as a whole, the largest increase since 2013 has been in the proportion that have installed anti-virus software (up 15 percentage points). Looking at the findings for individual countries, the largest increases in the proportions that have installed anti-virus software can be seen in Ireland (up 31 percentage points), Hungary (up 27 points), Italy (up 27 points) and Portugal (up 26 points). On the other hand, respondents in Slovenia are less likely to have installed anti-virus software.

More than half of Internet users across the EU (61%) have changed their password to access an online service. [12] Respondents are most likely to have changed their password to access an email account (45%), while 29% have changed their password to access online social networks, 25% to access online banking websites and 17% for shopping websites. Internet users are less likely to have changed their password to access public services websites (8%) or online games (7%).



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

[12] EB82.2: QB11 'Have you changed your password to access to any of the following online services during the last 12 months?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: E-mail account; Online social networks; Shopping website; Online banking websites; Online games; Public services websites; Other (SPONTANEOUS); None (SPONTANEOUS); Don't know.

EB79.4: QC13 'Have you changed your password to access to any of the following online services during the past 12 months?' (MULTIPLE ANSWERS POSSIBLE) Possible answers: Web-based e-mail; Online social networks; Shopping website (e.g. travel agents); Online banking websites; None (SPONTANEOUS); Don't know.

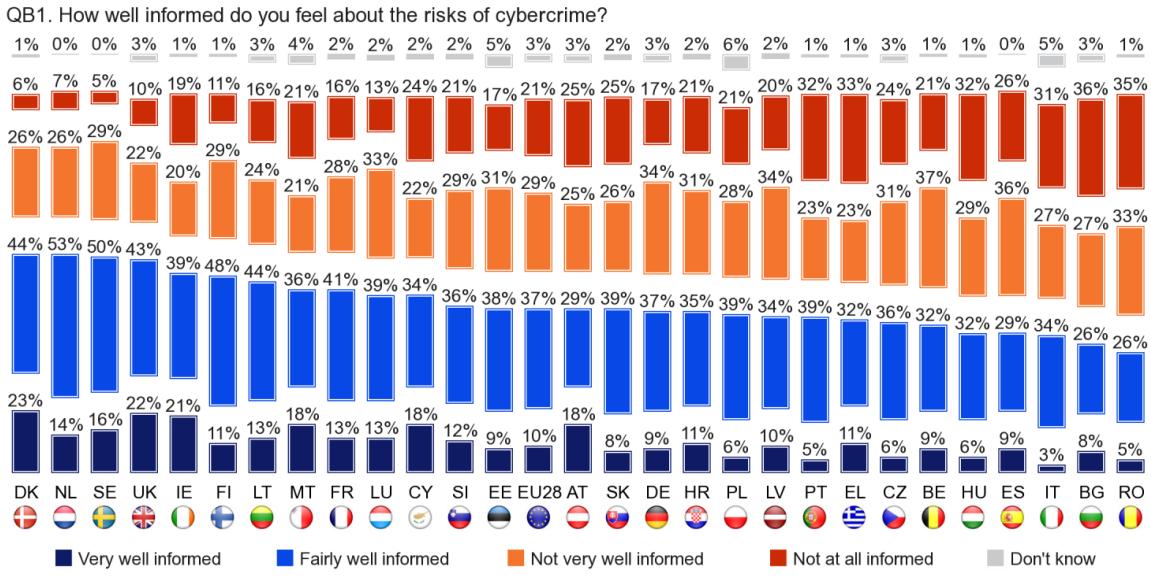
III. AWARENESS AND EXPERIENCE OF CYBERCRIMES

1. LEVEL OF KNOWLEDGE

Just under half of EU citizens (47%) say that they feel well informed about the risks of cybercrime; specifically, 10% feel very well informed and 37% feel fairly well informed. However, 29% do not feel very well informed and 21% say they do not feel informed at all about the risks of cybercrime[13].

Compared with the 2013 survey, there has been a slight increase in the proportion of EU citizens who feel well informed about the risks of cybercrime. In this survey, 47% feel very or fairly well informed, compared with 44% in 2013. There has been a corresponding decrease in the proportion that say they are not at all informed (from 23% in 2013 to 21% in this survey).

There is some variation by country in the extent to which respondents feel well informed about cybercrime. Respondents in Denmark (67%), the Netherlands (67%), Sweden (66%) and the UK (65%) are most likely to feel very or fairly well informed. People are least likely to feel well informed in Romania (31%) and Bulgaria (34%).



Base: all respondents (n=27,868 in EU28)

In most countries, respondents are more likely now than they were in 2013 to feel well informed about the risks of cybercrime, reflecting the overall increase across the EU. The largest increases can be seen in Austria (up 14 percentage points), Portugal (up 13 points) and Slovakia (up 10 points). In some countries, there has been a decrease in the proportion of respondents who feel well informed, most notably Luxembourg (down 10 percentage points) and Denmark (down 7 points).

[13] EB82.2: QB1 'How well informed do you feel about the risks of cybercrime?' Possible answers: Very well informed; Fairly well informed; Not very well informed; Not at all informed; Don't know.

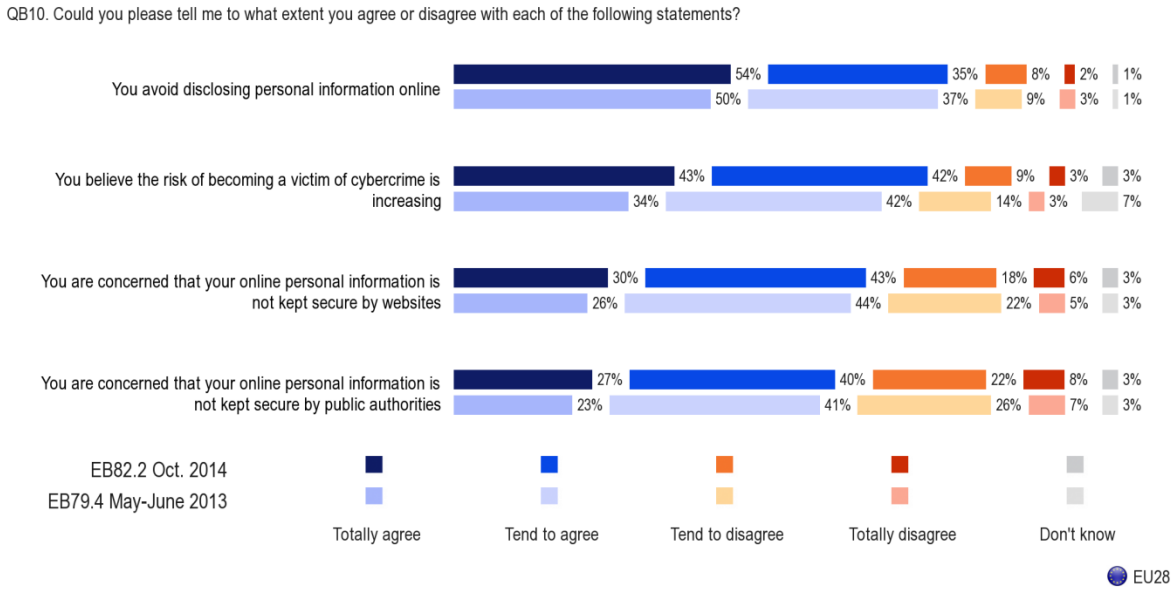
EB79.4: QC8 'How well informed do you feel about the risks of cybercrime?' Possible answers: Very well informed; Fairly well informed; Not very well informed; Not at all informed; Don't know.

2. ATTITUDES TO CYBER SECURITY

Internet users express high levels of concern about cyber security and the risks of cybercrime.[14] The vast majority of Internet users agree that they avoid disclosing personal information online (89%, including 54% who totally agree), while 85% agree that the risk of becoming a victim of cybercrime is increasing.

A majority also agree that they are concerned that their online personal information is not kept secure by websites (73%). Most respondents are also concerned that this information is not kept secure by public authorities (67%).

Comparisons with the 2013 survey indicate that respondents have become slightly more concerned about cybercrime in the last year.



Base: respondents who use the Internet (D62) (n=21,015 in EU28)

Despite these concerns, around three in four Internet users (74%) agree that they are able to protect themselves sufficiently against cybercrime (28% totally agree, 46% tend to agree) while 23% disagree.

[14] EB82.2: QB10 'Could you please tell me to what extent you agree or disagree with each of the following statements?' 1) You are concerned that your online personal information is not kept secure by websites. 2) You are concerned that your online personal information is not kept secure by public authorities. 3) You avoid disclosing personal information online. 4) You believe the risk of becoming a victim of cybercrime is increasing. 5) You are able to protect yourself sufficiently against cybercrime, e.g. by taking precautions or by using antivirus software. Possible answers: Totally agree; Tend to agree; Tend to disagree; Totally disagree; Don't know.

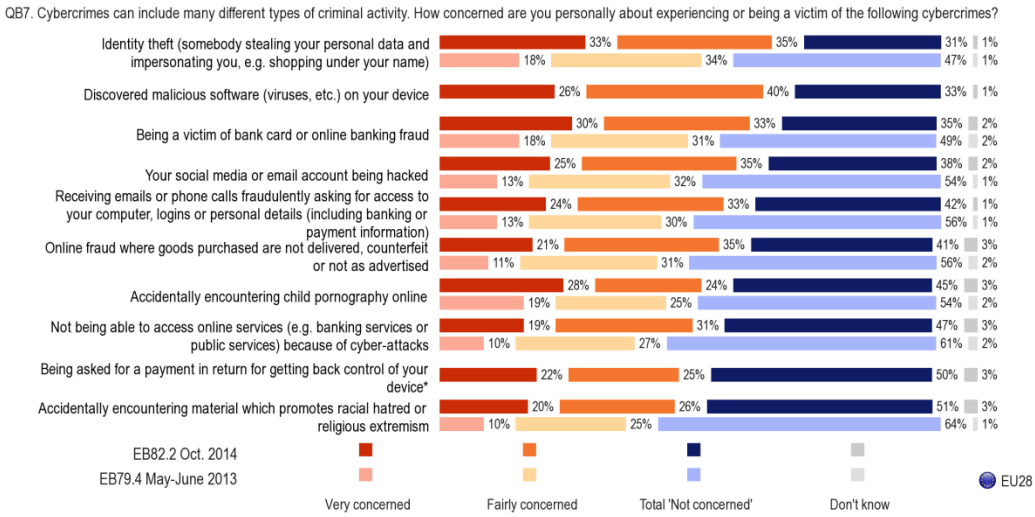
EB79.4: QC12 'Could you please tell me to what extent you agree or disagree with each of the following statements?' 1) You are concerned that your online personal information is not kept secure by websites. 2) You are concerned that your online personal information is not kept secure by public authorities. 3) You avoid disclosing personal information online. 4) You believe the risk of becoming a victim of cybercrime has increased in the past year. Possible answers: Totally agree; Tend to agree; Tend to disagree; Totally disagree; Don't know.

3. CONCERNS ABOUT AND EXPERIENCE OF SPECIFIC CYBERCRIMES

EU citizens have become increasingly concerned about becoming a victim of cybercrime.[15] When asked how concerned they are about experiencing or being a victim of different types of cybercrime, Internet users are most likely to say they are concerned about identify theft (68% are concerned about this) and discovering malicious software on their device (66%).

Internet users also express concern about being the victim of bank card or online banking fraud (63%) and about their social media or email account being hacked (60%).

More than half of Internet users are concerned about the following types of cybercrime: receiving emails or phone calls fraudulently asking for computer access or details (57%), online fraud where goods purchased are not delivered, are counterfeit or not as advertised (56%) and accidentally discovering child pornography online (52%).



*New item

Base: respondents who use the Internet (D62) (n=21,015 in EU28)

[15] EB82.2: QB7 'Cybercrimes can include many different types of criminal activity. How concerned are you personally about experiencing or being a victim of the following cybercrimes? 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Receiving emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased were not delivered, counterfeit or not as advertised. 4. Accidentally encountering child pornography online. 5. Accidentally encountering material which promotes racial hatred or religious extremism. 6. Not being able to access online services (e.g. banking services or public services) because of cyber-attacks. 7. Your social media or email account being hacked. 8. Being a victim of bank card or online banking fraud. 9. Being asked for a payment in return for getting back control of your device. 10. Discovered malicious software (viruses, etc.) on your device. Possible answers: Very concerned; Fairly concerned; Not very concerned; Not at all concerned; Don't know.

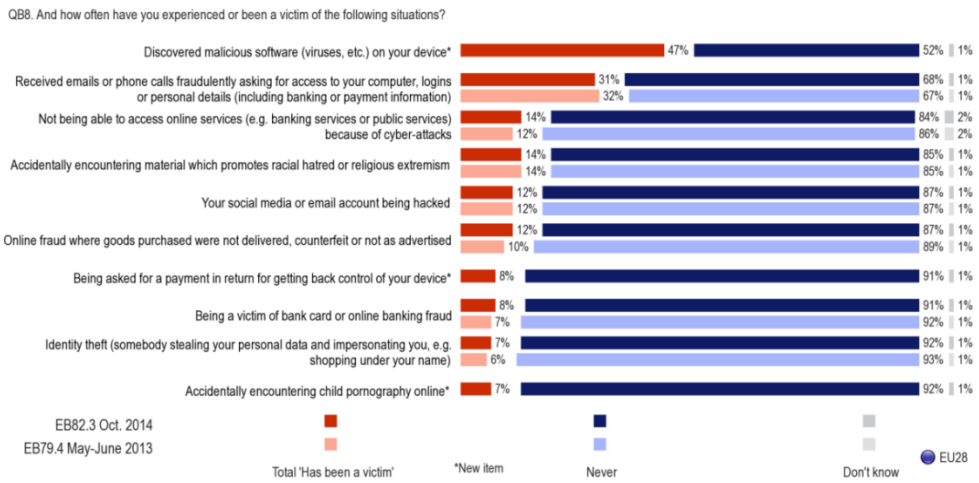
EB79.4: QC10 'And how concerned are you personally about experiencing or being a victim of the following cybercrimes? 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Receiving emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased were not delivered, counterfeit or not as advertised. 4. Accidentally encountering child pornography online. 5. Accidentally encountering material which promotes racial hatred or religious extremism. 6. Not being able to access online services (e.g. banking services) because of cyber-attacks. 7. Your social media or email account being hacked. 8. Being a victim of credit card or banking fraud online. Possible answers: Very concerned; Fairly concerned; Not very concerned; Not at all concerned; Don't know.

Slightly lower proportions are concerned about not being able to access online services because of cyber-attacks (50%), being asked for a payment in return for getting back control of your device (47%) and accidentally encountering material which promotes racial hatred or religious extremism (46%).

Internet users express greater levels of concern in 2014 than they did in 2013, with increases ranging from 8 percentage points (for encountering child pornography online) to 16 points (for identity theft).

The two **most common situations experienced** by respondents are discovering malicious software on their device (47%) and receiving an email or phone call fraudulently asking for access to their computer, logins or personal details (31%)[16].

In addition, 14% of Internet users say that they have not been able to access online services because of cyber-attacks, while the same proportion (14%) have accidentally encountered material which promotes racial hatred or religious extremism, 12% have had their social media or email account hacked, and 12% have experienced online fraud (where goods are not delivered, counterfeit or not as advertised). Furthermore, 16% of Internet users who say they buy online goods or services have experienced online fraud.



Base: respondents who use the Internet (D62) (n=21,015 in EU28)

[16] EB82.2: QB8 'And how often have you experienced or been a victim of the following situations?' 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Received emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased were not delivered, counterfeit or not as advertised. 4. Accidentally encountering child pornography online. 5. Accidentally encountering material which promotes racial hatred or religious extremism. 6. Not being able to access online services (e.g. banking services or public services) because of cyber-attacks. 7. Your social media or email account being hacked. 8. Being a victim of bank card or online banking fraud. 9. Being asked for a payment in return for getting back control of your device. 10. Discovered malicious software (viruses, etc.) on your device. Possible answers: Often; Occasionally; Never; Don't know.

EB79.4: QC9 'Cybercrimes can include many different types of criminal activity. How often have you experienced or been a victim of the following situations?' 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Received emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased were not delivered, counterfeit or not as advertised. 4. Accidentally encountering material which promotes racial hatred or religious extremism. 5. Not being able to access online services (e.g. banking services) because of cyber-attacks. 6. Your social media or email account being hacked. 7. Being a victim of credit card or banking fraud online. Possible answers: Often; Occasionally; Never; Don't know.

Across the EU, 8% of Internet users say they have been asked for payment in return for getting back control of their device, 8% say they have been a victim of credit card or banking fraud online, 7% say they have experienced identity theft, and 7% say they have accidentally encountered child pornography online.

The **level of concern** that Internet users have about the various types of cybercrime is generally similar across socio-demographic groups, although there are some differences by gender and age.

Daily Internet users are more likely to be concerned about a number of types of crime. For example, 65% of daily Internet users are concerned about being the victim of bank card or online banking fraud, compared with 56% of less frequent users. On the other hand, respondents who feel well informed about the risks of cybercrime are less likely to be concerned about experiencing various types of problem.

Daily Internet users are more likely than less frequent users to have **experienced or been a victim** of most of the various types of cybercrime. The difference is greatest in relation to scam emails or phone calls (34% of daily Internet users have experienced this problem, compared with 16% of less frequent users) and discovering malicious software (50% compared with 29%).

The proportion of Internet users that have experienced various types of cybercrime is generally consistent across socio-demographic groups. However, there are some differences by gender, age and level of education. These differences generally reflect frequency of Internet use (i.e. groups that are more frequent Internet users are more likely to experience the various types of cybercrime).

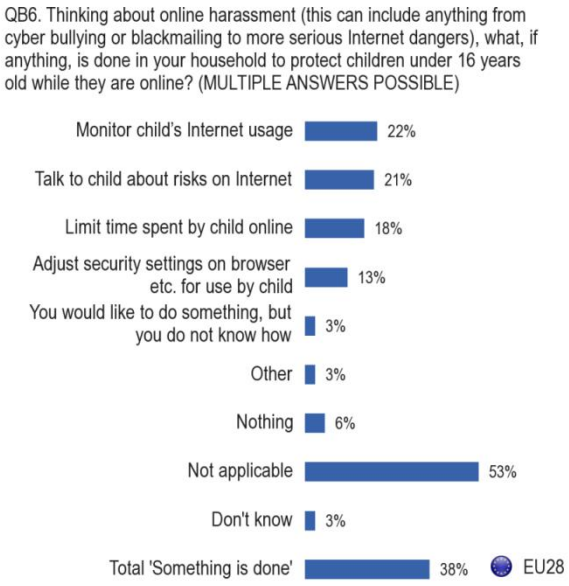
4. FIGHTING CYBERCRIME

Children are protected from online harassment by monitoring and limiting Internet usage or discussing the risks.[17] All respondents were asked what, if anything, is done in their household to protect children under 16 years old from online harassment. Respondents answered in their own words and were not prompted with possible options.

Overall, around four in ten EU citizens (38%) try to protect children under 16 years old while they are online in some way.

Around one in five respondents say that they monitor children's Internet usage (22%), while similar proportions say they talk to children about risks on the Internet (21%) and limit the time spent by children online (18%). Respondents are less likely to say that they adjust the security settings for use by children (13%).

More than half of respondents (53%) say that the question does not apply to them (e.g. because they do not have children under 16).



Base: all respondents (n=27,868 in EU28)

Daily Internet users and those who feel well informed about the risks of cybercrime are more likely to say that measures are taken to protect children while they are online. For example, 26% of daily Internet users talk to their children about risks on the Internet, compared with 22% of less frequent users and 9% of those who do not personally use the Internet.

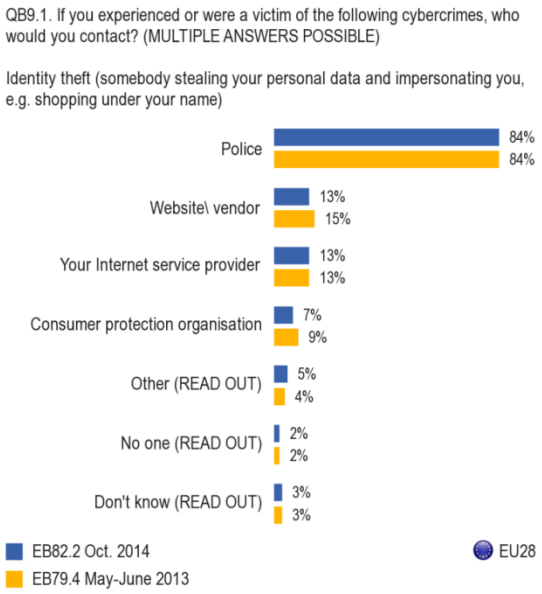
[17] EB82.2: QB6: 'Thinking about online harassment (this can include anything from cyber bullying or blackmailing to more serious Internet dangers), what, if anything, is done in your household to protect children under 16 years old when they are online?' (DO NOT SHOW SCREEN – DO NOT READ OUT – MULTIPLE ANSWERS POSSIBLE) Possible answers: Monitor child's Internet usage; Adjust security settings on browser, etc, for use by child; Limit time spent by child online; Talk to child about risks on Internet; You would like to do something, but you do not know how; Other; Nothing; Not applicable; Don't know.

On the same question, 25% of respondents who feel well informed about the risks of cybercrime say that they talk to their children about risks on the Internet, compared with 17% of those who do not feel well informed.

At least half of respondents in four countries say that something is done to protect children when they are online: Italy (58%), Luxembourg (53%), Croatia (52%), and Malta (52%). This compares with fewer than three in ten respondents in Estonia (29%), Lithuania (27%) and Germany (26%).

If they experienced or were the victim of cybercrime, most respondents say they would contact the police, especially if the crime was identity theft (84%) or online banking fraud (79%), or if they accidentally encountered child pornography online (76%)[18].

The vast majority of respondents say that they would contact the police (84%) if they were the victim of **identity theft**, while some respondents say that they would contact the relevant website or vendor (13%), their Internet service provider (13%) or a consumer protection organisation (7%).



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

If they experienced a **scam email or phone call**, 53% of Internet users across the EU say they would contact the police. Smaller proportions of respondents say they would contact their Internet service provider (19%), the website or vendor (14%) or a consumer protection organisation (8%), while 15% say they would not contact anyone.

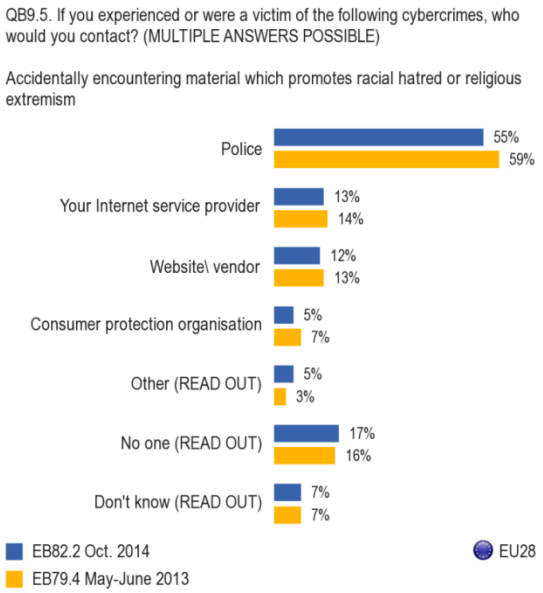
[18] EB82.2: QB9 'If you experienced or were a victim of the following cybercrimes, who would you contact?' 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Receiving emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased were not delivered, counterfeit or not as advertised. 4. Accidentally encountering child pornography online. 5. Accidentally encountering material which promotes racial hatred or religious extremism. 6. Not being able to access online services (e.g. banking services or public services) because of cyber-attacks. 7. Your social media or email account being hacked. 8. Being a victim of bank card or online banking fraud. 9. Being asked for a payment in return for getting back control of your device. 10. Discovered malicious software (viruses, etc.) on your device. (MULTIPLE ANSWERS POSSIBLE) Possible answers: Police; Website/vendor; Your Internet service provider; Consumer protection organisation; Other (READ OUT); No-one (READ OUT); Don't know (READ OUT).

EB79.4: QC11 'If you experienced or were a victim of the following cybercrimes, who would you contact?' 1. Identity theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name). 2. Receiving emails or phone calls fraudulently asking for access to your computer, logins, or personal details (including banking or payment information). 3. Online fraud where goods purchased are not delivered, counterfeit or not as advertised. 4. Accidentally encountering child pornography online. 5. Accidentally encountering material which promotes racial hatred or religious extremism. 6. Not being able to access online services (e.g. banking services) because of cyber-attacks. 7. Your social media or email account being hacked. 8. Being a victim of credit card or banking fraud online. (MULTIPLE ANSWERS POSSIBLE) Possible answers: Police; Website/vendor; Your Internet service provider; Consumer protection organisation; Other (READ OUT); No-one (READ OUT); Don't know (READ OUT).

When asked who they would contact if they experienced **online fraud**, again the majority of Internet users say that they would contact the police (54%), while 36% say they would contact the website or vendor, the highest figure for any of the eight types of cybercrime included in the survey. Respondents are more likely to say they would contact a consumer protection organisation (16%) than their Internet service provider (13%).

In most cases (76%), Internet users say that they would contact the police if they accidentally encountered **child pornography** online. In addition, 11% say they would contact their Internet service provider, 8% the website or vendor and 4% a consumer protection organisation.

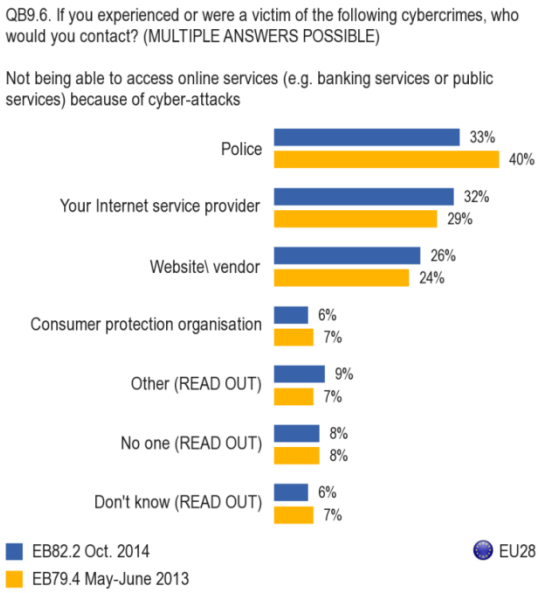
When asked who they would contact if they encountered **material which promotes racial hatred or religious extremism,** respondents again are most likely to say they would contact the police (55%), with 13% saying they would contact their Internet service provider, 12% the website or vendor, and 5% a consumer protection organisation. On this issue, a relatively high proportion of respondents say that they would contact no-one (17%) or would not know who to contact (7%).



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

If Internet users were unable to **access online services** because of cyber-attacks, 33% say they would contact the police, 32% their Internet service provider and 26% the website or vendor. Just 6% would contact a consumer protection organisation. These answers are different from those on other types of cybercrime, with a lower proportion saying they would contact the police, and relatively large proportions saying they would contact their Internet service provider, or website or vendor.

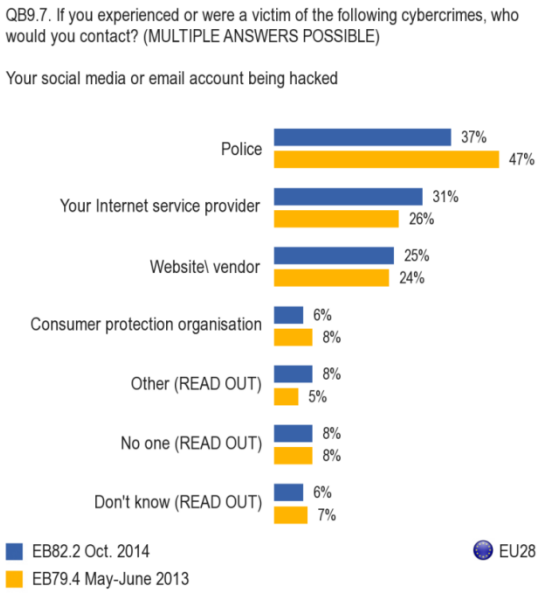
Internet users are less likely than they were in 2013 to say they would contact the police (a decrease from 40% to 33%).



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

In 37% of cases, Internet users say that they would contact the police if their **social media or email account was hacked**, while 31% say they would contact their Internet service provider, and 25% the website or vendor. Just 6% say they would contact a consumer protection organisation.

Internet users are less likely than they were in 2013 to say they would contact the police (down 10 percentage points), while there has been an increase in the proportion that say they would contact their Internet service provider (up 5 points).

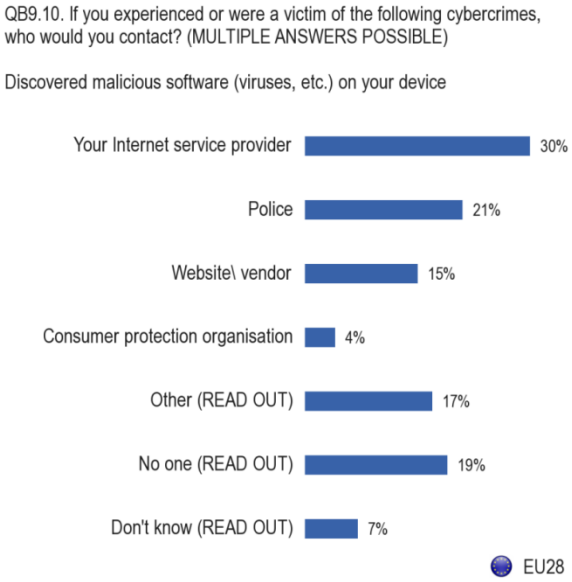


Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

In most cases (79%), Internet users say that they would contact the police if they were a victim of **bank card or online banking fraud**. In addition, 19% say they would contact the website or vendor, 11% their Internet service provider, and 7% a consumer protection organisation.

When asked who they would contact if they experienced **cyber extortion** (being asked for a payment in return for getting back control of your device)**,** respondents are most likely to say they would contact the police (65%), with 17% saying they would contact their Internet service provider, 12% the website or vendor, and 7% a consumer protection organisation.

If Internet users **discovered malicious software** on their device, 30% say they would contact their Internet service provider, 21% the police and 15% the website or vendor. Just 4% would contact a consumer protection organisation, while 19% say they would not contact anyone. The pattern of answers is different for this item than for other types of cybercrime, with a much lower proportion (21%) saying they would contact the police.



Base: respondents who use the Internet (D62)
(n=21,015 in EU28)

For a number of types of cybercrime, older respondents are more likely than younger respondents to say they would contact the police or their Internet service provider, and are less likely to say they would contact the website or vendor.

Those leaving education later are more likely to say they would contact the website or vendor, and are less likely to say they would contact the police. A similar pattern applies in terms of how well informed respondents feel about the risks of cybercrime.

Overall, these findings suggest that a greater level of knowledge of cybercrime leads to a preference to contact organisations such as the website or vendor or Internet service provider rather than the police.

CONCLUSIONS

This summary has examined EU citizens' experience and perceptions of cyber security issues, and how these have changed since the previous survey of May-June 2013.

Many respondents say they have changed their behaviour because of security concerns, for example by not giving out personal information or not opening e-mails from unknown sources.

The proportions that have taken these types of measure have increased in the past year. However, there is considerable variation in the proportions taking security measures, both by individual country, and across socio-demographic groups such as age and level of education.

EU citizens feel slightly better informed about the risks of cybercrime than they did in 2013, and most Internet users agree that they are able to protect themselves sufficiently against cybercrime. However, there remains a substantial minority who do not feel well informed, and do not feel at all able to protect themselves.

Almost half of Internet users have discovered malicious software on their device, and nearly a third say they have received a scam email or phone call, and other types of cybercrime have been experienced by a substantial number (albeit a minority) of Internet users in the EU, including online fraud, identity theft, hacking of email or social media accounts and online harassment. The proportions affected by these problems have remained similar since 2013.

Internet users express high levels of concern about cybercrime. The majority agree that the risk of becoming a victim of cybercrime is increasing; that they are concerned that their online personal information is not kept secure by websites or by public authorities.

In addition, more than half of respondents say they are concerned about experiencing various types of cybercrime, with the highest levels of concern expressed over identity theft, malicious software and online banking fraud.

Levels of concern have increased substantially since 2013, although it is worth noting that these levels of concern had previously decreased between 2012 and 2013[19].

If they experienced or were the victim of cybercrime, most respondents say they would contact the police, especially if the crime was identity theft or online banking fraud, or if they accidentally encountered child pornography online.

However, the survey findings suggest that a greater level of knowledge of cybercrime leads to a preference to contact organisations such as the website or vendor rather than the police.

[19] For example, the proportion concerned about identity theft was 61% in 2012, 52% in 2013 and is now 68% in 2014.

ANNEXES

TECHNICAL SPECIFICATIONS

SPECIAL EUROBAROMETER 423

Cyber security

TECHNICAL SPECIFICATIONS

Between the 11th and the 20th of October 2014, TNS opinion & social, a consortium created between TNS political & social, TNS UK and TNS opinion, carried out the wave 82.2 of the EUROBAROMETER survey, on request of the EUROPEAN COMMISSION, Directorate-General for Communication, "Strategy, Corporate Communication Actions and Eurobarometer" unit.

The Special Eurobarometer 423 is part of the wave 82.2 and covers the population of the respective nationalities of the European Union Member States, resident in each of the Member States and aged 15 years and over.

The basic sample design applied in all states is a multi-stage, random (probability) one. In each country, a number of sampling points was drawn with probability proportional to population size (for a total coverage of the country) and to population density.

In order to do so, the sampling points were drawn systematically from each of the "administrative regional units", after stratification by individual unit and type of area. They thus represent the whole territory of the countries surveyed according to the EUROSTAT NUTS II (or equivalent) and according to the distribution of the resident population of the respective nationalities in terms of metropolitan, urban and rural areas. In each of the selected sampling points, a starting address was drawn, at random. Further addresses (every Nth address) were selected by standard "random route" procedures, from the initial address. In each household, the respondent was drawn, at random (following the "closest birthday rule"). All interviews were conducted face-to-face in people's homes and in the appropriate national language. As far as the data capture is concerned, CAPI (*Computer Assisted Personal Interview)* was used in those countries where this technique was available.

For each country a comparison between the sample and the universe was carried out. The Universe description was derived from Eurostat population data or from national statistics offices. For all countries surveyed, a national weighting procedure, using marginal and intercellular weighting, was carried out based on this Universe description. In all countries, gender, age, region and size of locality were introduced in the iteration procedure. For international weighting (i.e. EU averages), TNS Opinion & Social applies the official population figures as provided by EUROSTAT or national statistic offices. The total population figures for input in this post-weighting procedure are listed below.

Readers are reminded that survey results are estimations, the accuracy of which, everything being equal, rests upon the sample size and upon the observed percentage. With samples of about 1,000 interviews, the real percentages vary within the following confidence limits:

Statistical Margins due to the sampling process
(at the 95% level of confidence)

various sample sizes are in rows ***various observed results are in columns***

	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	
	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	
N=50	6,0	8,3	9,9	11,1	12,0	12,7	13,2	13,6	13,8	13,9	N=50
N=500	1,9	2,6	3,1	3,5	3,8	4,0	4,2	4,3	4,4	4,4	N=500
N=1000	1,4	1,9	2,2	2,5	2,7	2,8	3,0	3,0	3,1	3,1	N=1000
N=1500	1,1	1,5	1,8	2,0	2,2	2,3	2,4	2,5	2,5	2,5	N=1500
N=2000	1,0	1,3	1,6	1,8	1,9	2,0	2,1	2,1	2,2	2,2	N=2000
N=3000	0,8	1,1	1,3	1,4	1,5	1,6	1,7	1,8	1,8	1,8	N=3000
N=4000	0,7	0,9	1,1	1,2	1,3	1,4	1,5	1,5	1,5	1,5	N=4000
N=5000	0,6	0,8	1,0	1,1	1,2	1,3	1,3	1,4	1,4	1,4	N=5000
N=6000	0,6	0,8	0,9	1,0	1,1	1,2	1,2	1,2	1,3	1,3	N=6000
N=7000	0,5	0,7	0,8	0,9	1,0	1,1	1,1	1,1	1,2	1,2	N=7000
N=7500	0,5	0,7	0,8	0,9	1,0	1,0	1,1	1,1	1,1	1,1	N=7500
N=8000	0,5	0,7	0,8	0,9	0,9	1,0	1,0	1,1	1,1	1,1	N=8000
N=9000	0,5	0,6	0,7	0,8	0,9	0,9	1,0	1,0	1,0	1,0	N=9000
N=10000	0,4	0,6	0,7	0,8	0,8	0,9	0,9	1,0	1,0	1,0	N=10000
N=11000	0,4	0,6	0,7	0,7	0,8	0,9	0,9	0,9	0,9	0,9	N=11000
N=12000	0,4	0,5	0,6	0,7	0,8	0,8	0,9	0,9	0,9	0,9	N=12000
N=13000	0,4	0,5	0,6	0,7	0,7	0,8	0,8	0,8	0,9	0,9	N=13000
N=14000	0,4	0,5	0,6	0,7	0,7	0,8	0,8	0,8	0,8	0,8	N=14000
N=15000	0,3	0,5	0,6	0,6	0,7	0,7	0,8	0,8	0,8	0,8	N=15000
	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	
	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	

ABBR.	COUNTRIES	INSTITUTES	N° INTERVIEWS	DATES FIELDWORK		POPULATION 15+	PROPORTION EU28
BE	Belgium	TNS Dimarso	1.001	11/10/14	20/10/14	9.263.570	2,18%
BG	Bulgaria	TNS BBSS	1.018	11/10/14	20/10/14	6.294.563	1,48%
CZ	Czech Rep.	TNS Aisa	1.034	11/10/14	20/10/14	8.955.829	2,11%
DK	Denmark	TNS Gallup DK	1.025	11/10/14	20/10/14	4.625.032	1,09%
DE	Germany	TNS Infratest	1.532	11/10/14	20/10/14	71.283.580	16,79%
EE	Estonia	TNS Emor	1.015	11/10/14	20/10/14	1.113.355	0,26%
IE	Ireland	Behaviour & Attitudes	1.001	11/10/14	20/10/14	3.586.829	0,84%
EL	Greece	TNS ICAP	1.015	11/10/14	20/10/14	8.791.499	2,07%
ES	Spain	TNS Spain	1.011	11/10/14	20/10/14	39.506.853	9,31%
FR	France	TNS Sofres	1.011	11/10/14	20/10/14	51.668.700	12,17%
HR	Croatia	HENDAL	1.084	11/10/14	20/10/14	3.625.601	0,85%
IT	Italy	TNS Italia	1.019	11/10/14	20/10/14	51.336.889	12,09%
CY	Rep. Of Cyprus	CYMAR	500	11/10/14	18/10/14	724.084	0,17%
LV	Latvia	TNS Latvia	1.011	11/10/14	20/10/14	1.731.509	0,41%
LT	Lithuania	TNS LT	1.013	11/10/14	20/10/14	2.535.329	0,60%
LU	Luxembourg	TNS ILReS	503	11/10/14	20/10/14	445.806	0,11%
HU	Hungary	TNS Hoffmann	1.058	11/10/14	20/10/14	8.477.933	2,00%
MT	Malta	MISCO	503	11/10/14	20/10/14	360.045	0,08%
NL	Netherlands	TNS NIPO	1.059	11/10/14	20/10/14	13.901.653	3,27%
AT	Austria	ipr Umfrageforschung	1.019	11/10/14	20/10/14	7.232.497	1,70%
PL	Poland	TNS Polska	1.010	11/10/14	20/10/14	32.736.685	7,71%
PT	Portugal	TNS Portugal	1.002	11/10/14	20/10/14	8.512.269	2,01%
RO	Romania	TNS CSOP	1.015	11/10/14	20/10/14	16.880.465	3,98%
SI	Slovenia	RM PLUS	1.055	11/10/14	20/10/14	1.760.726	0,41%
SK	Slovakia	TNS Slovakia	1.038	11/10/14	20/10/14	4.580.260	1,08%
FI	Finland	TNS Gallup Oy	1.000	11/10/14	20/10/14	4.511.446	1,06%
SE	Sweden	TNS Sifo	987	11/10/14	20/10/14	7.944.034	1,87%
UK	United Kingdom	TNS UK	1.329	11/10/14	20/10/14	52.104.731	12,27%
TOTAL EU28			27.868	11/10/14	20/10/14	424.491.772	100%*

* It should be noted that the total percentage shown in this table may exceed 100% due to rounding