European Commission

Special Eurobarometer 464a

Summary

Europeans' attitudes towards cyber security

Fieldwork
June 2017
Publication
September 2017

Survey requested by the European Commission,
Directorate-General for Migration and Home Affairs
and co-ordinated by the Directorate-General for Communication

Special Eurobarometer 464a – Wave EB87.4 – TNS opinion & social

Special Eurobarometer 464a

Summary

Europeans' attitudes towards cyber security

Survey conducted by TNS opinion & political at the request of the European Commission,
Directorate-General for Migration and Home Affairs

Survey co-ordinated by the European Commission, Directorate-General for Communication
(DG COMM "Media monitoring and analysis" Unit)

TABLE OF CONTENTS

INTRODUCTION

This report brings together the results of the Special Eurobarometer public opinion survey towards 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. The main types of crimes that are committed in this way include attacks on information systems that can hinder or disable their functioning, forms of online fraud and forgery such as identity theft and malicious code, and the dissemination of illegal online content such as child pornography.

Cybercrime is estimated to cause the loss of billions of euros per year, and is placing an increasing strain on law enforcement response capability. With rising use of the Internet, the proliferation of different kinds of Internet-enabled devices, and an increasing amount of personal data being transmitted online, the problem of cybercrime will only get worse unless concerted steps are taken by the authorities to eradicate it.

In response to this mounting problem, the European Commission has designed a coordinated policy in close co-operation with European Union (EU) Member States and the other EU institutions.[1] 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' awareness, experiences and perceptions of cyber security issues.

This survey was carried out by TNS Political & Social network in the 28 Member States of the European Union (EU) between 13 and 26 June 2017. Some 28,093 EU citizens from different social and demographic categories were interviewed face-to-face at home and in their native language on behalf of the Directorate-General for Communication.

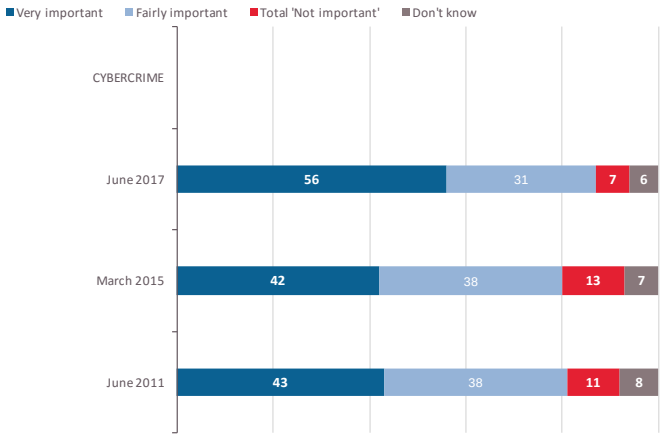
[1] More information on the fight against cybercrime in the EU can be found here: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm

I. OVERALL PERCEPTION OF CYBERCRIME AS A THREAT TO SECURITY

- A large majority of respondents consider cybercrime an important challenge to the internal security of the EU -

In the EU, over eight in ten (87%) respondents see cybercrime as important and this is the case for a majority of respondents in every country. This proportion has increased by seven percentage points since March 2015.

QB2 In your opinion, how important are the following challenges to the internal security of the EU? (% - EU)

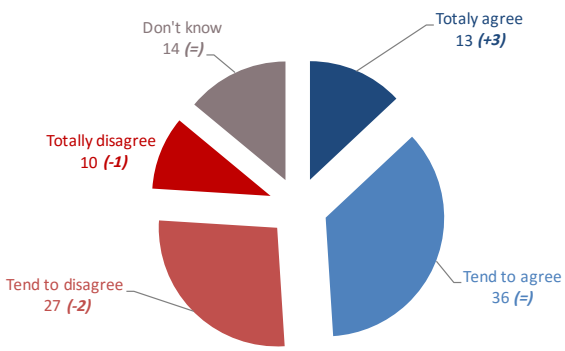


Base: All respondents (N=28,093)

- Less than half of the respondents think enough is being done by law enforcement authorities to tackle cybercrime -

Nearly half of respondents (49%) think enough is being done by the police and other law enforcement authorities to combat cybercrime, although only 13% agree completely and a significant proportion (14%) say they do not know.

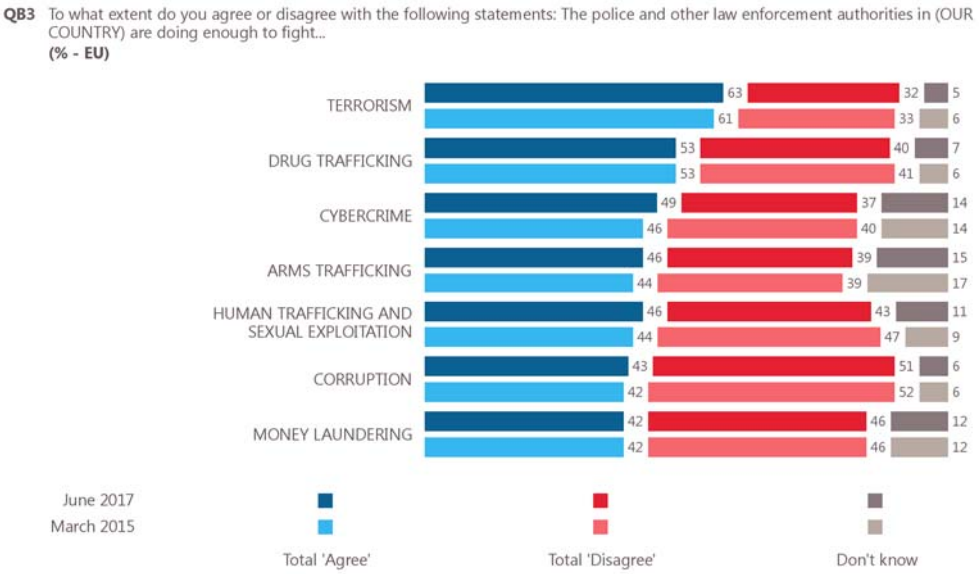
QB3.4 To what extent do you agree or disagree with the following statements:
The police and other law enforcement authorities in (OUR COUNTRY) are doing enough to fight... (% - EU)



(June 2017 - March 2015)

Base: All respondents (N=28,093)

When compared to different threats to national security perceived as important, these results place cybercrime in the middle range:



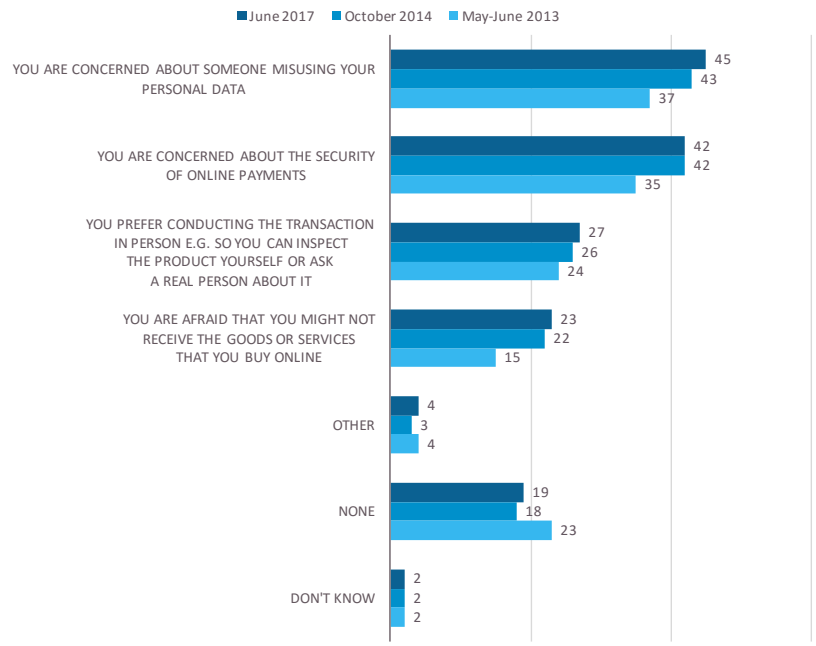
Base: All respondents (N=28,093)

II. CONCERNS ABOUT INTERNET TRANSACTIONS

- Misuse of personal data and the security of online payments continue to be the most significant concerns of Internet users -

In comparison to 2013 and 2014, users' concerns about online transactions have increased. The two most common concerns when using the Internet for online banking or purchases are about the misuse of personal data (45%) and the security of online payments (42%). However, nearly a fifth (19%) have no concerns about the security of Internet transactions.

QB8 What concerns do you have, if any, about using the Internet for things like online banking or buying things online? (MULTIPLE ANSWERS POSSIBLE)
(% - EU)

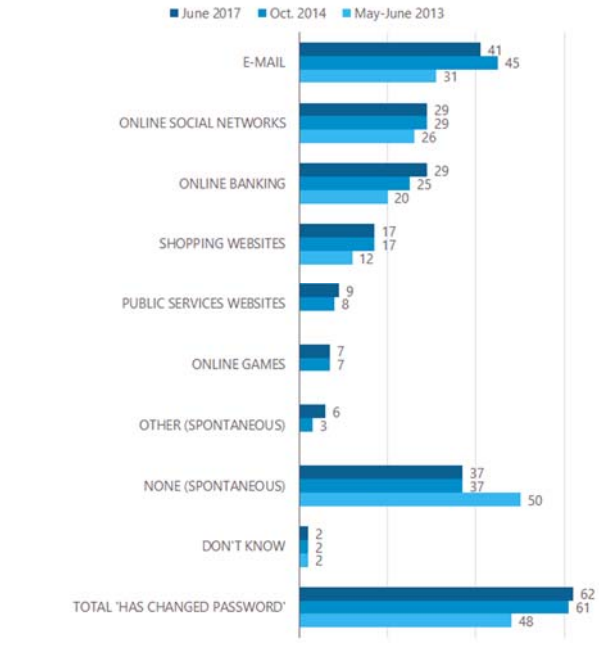


Base: Respondents who are Internet users (N=22,236)

– Over six in ten Internet users have changed their access password of at least one online service during the last 12 months –

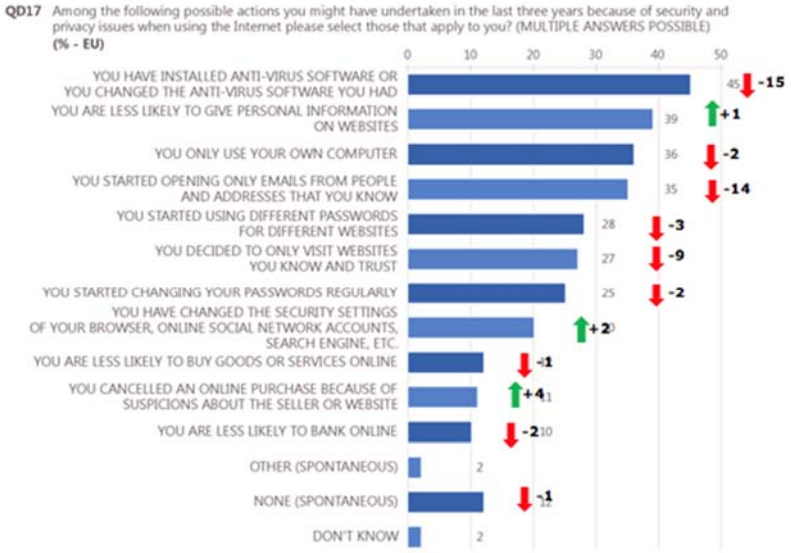
An increasing proportion of respondents have changed their passwords on online accounts during the last 12 months (62%). Changing email passwords is the most common action in the majority of countries.

QB15 Have you changed your password to access your account(s) for any of the following online services during the last 12 months? (MULTIPLE ANSWERS POSSIBLE)
(% - EU)



Base: Respondents who are Internet users (N=22,236)

Nearly half (45%) have installed or changed anti-virus software, and nearly four in ten (39%) have reduced the personal information they give out on website. A significant minority of users are opting out of conducting online transactions through, for example, reducing the goods and services they buy online (12%) or opting out of online banking (10%)[2]. The number of respondents who have cancelled transactions because of suspicions has risen significantly, to 11% from 7% in 2014.



Base: Respondents who are Internet users (N=22,472)

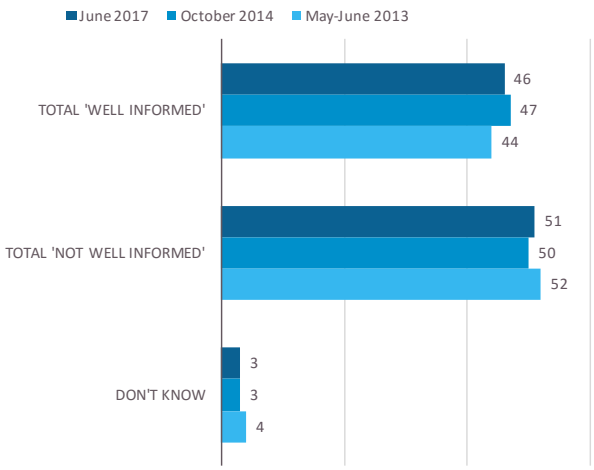
[2] QD17 was asked in EBS460.

III. AWARENESS AND EXPERIENCE OF CYBERCRIMES

- Nearly half of respondents consider themselves to be well informed about cybercrime, but this varies significantly across Member States –

Respondents were asked how well informed they felt themselves to be about the risks of cybercrime activity.[3] As in previous surveys, responses on this issue are fairly evenly divided. 46% of respondents say they are 'well informed', while 51% say they are 'not well informed'.

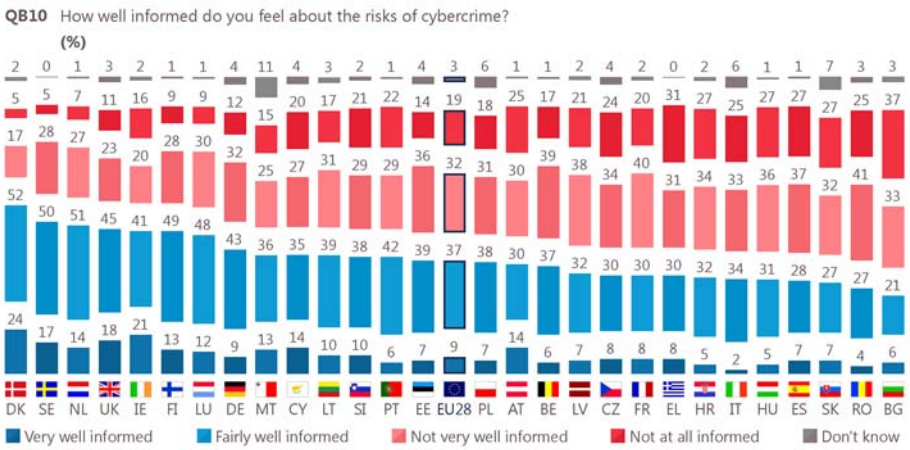
QB10 How well informed do you feel about the risks of cybercrime?
(% - EU)



Base: All respondents (N=28,093)

Results vary significantly across Member States. In 11 of the 28 Member States, a relative majority of respondents consider themselves to be 'well informed' about cybercrime, ranging from 76% of respondents in Denmark to 49% in Lithuania. In the remaining countries, the proportion of respondents who feel 'not well informed' outweighs the proportion of those who feel 'well informed'.

QB10 How well informed do you feel about the risks of cybercrime?
(%)

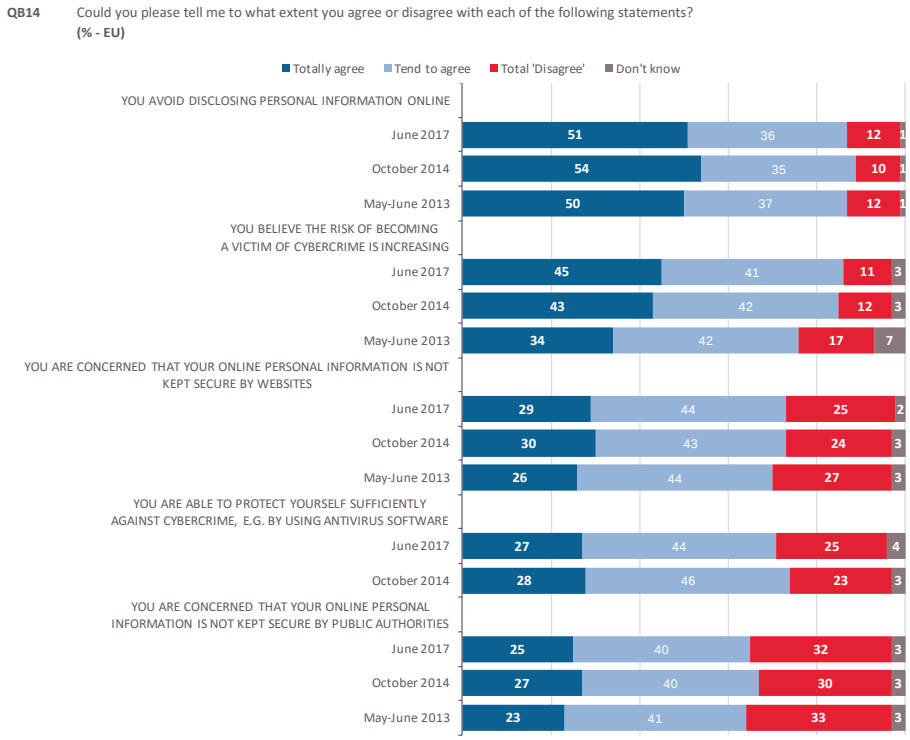


Base: All respondents (N=28,093)

[3] QB10. 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.

- A majority of people in the EU are alert to the problem of cybersecurity -

Respondents were asked about their attitudes to several statements on the topic of cybersecurity.[4] In each case, a clear majority of respondents agree, although the extent of agreement differs. For each of the statements, results have not changed significantly since 2014

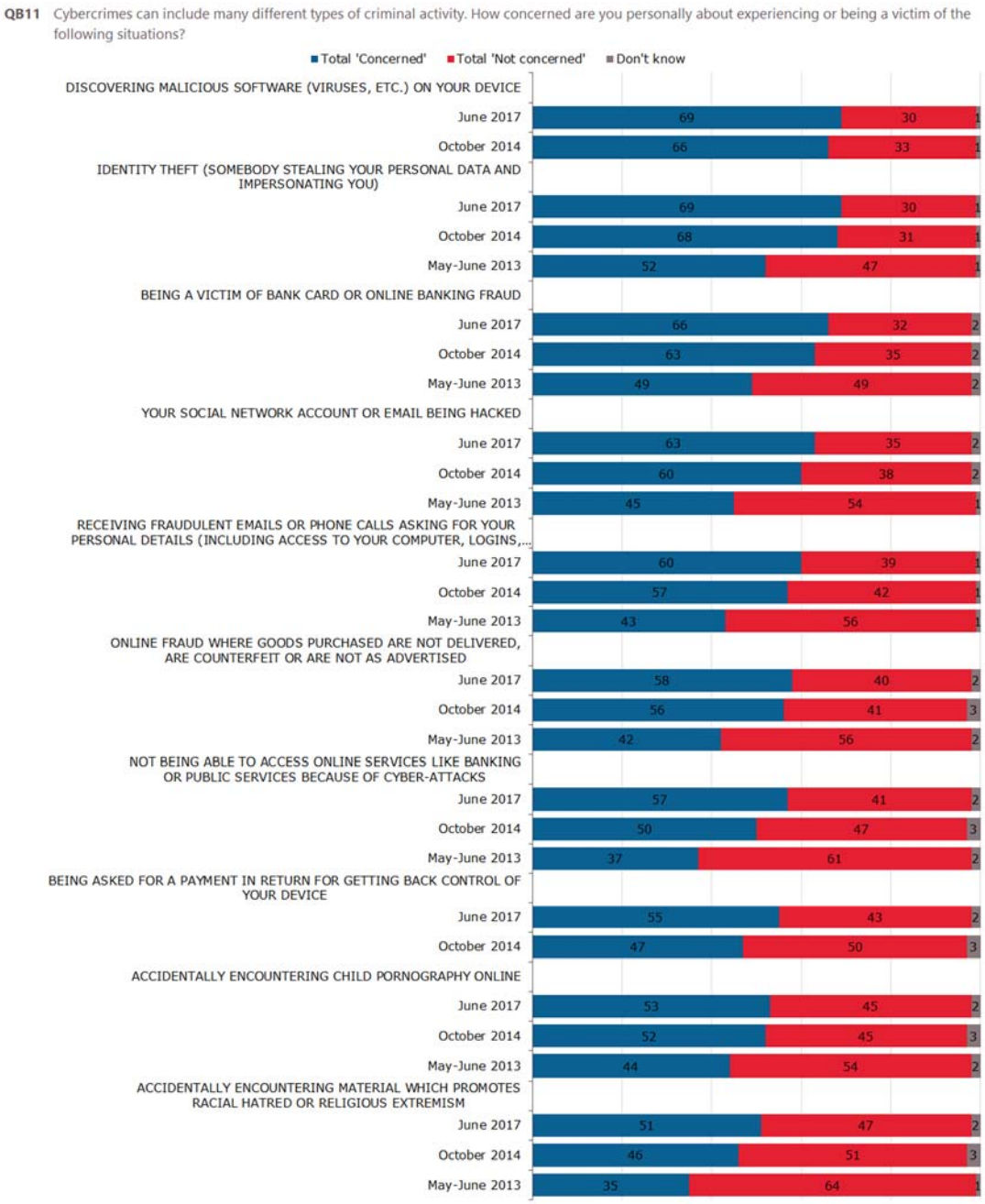


Base: Respondents who are Internet users (N=22,236)

- A rising majority of respondents are concerned about experiencing or being victims of cybercrimes -

A majority of respondents are concerned about being the victims of various forms of cybercrime, with the largest proportions concerned about discovering malicious software on their device (69%), identity theft (69%) and bank card and online banking fraud (66%). In all cases, concern about being a victim of these crimes is increasing.

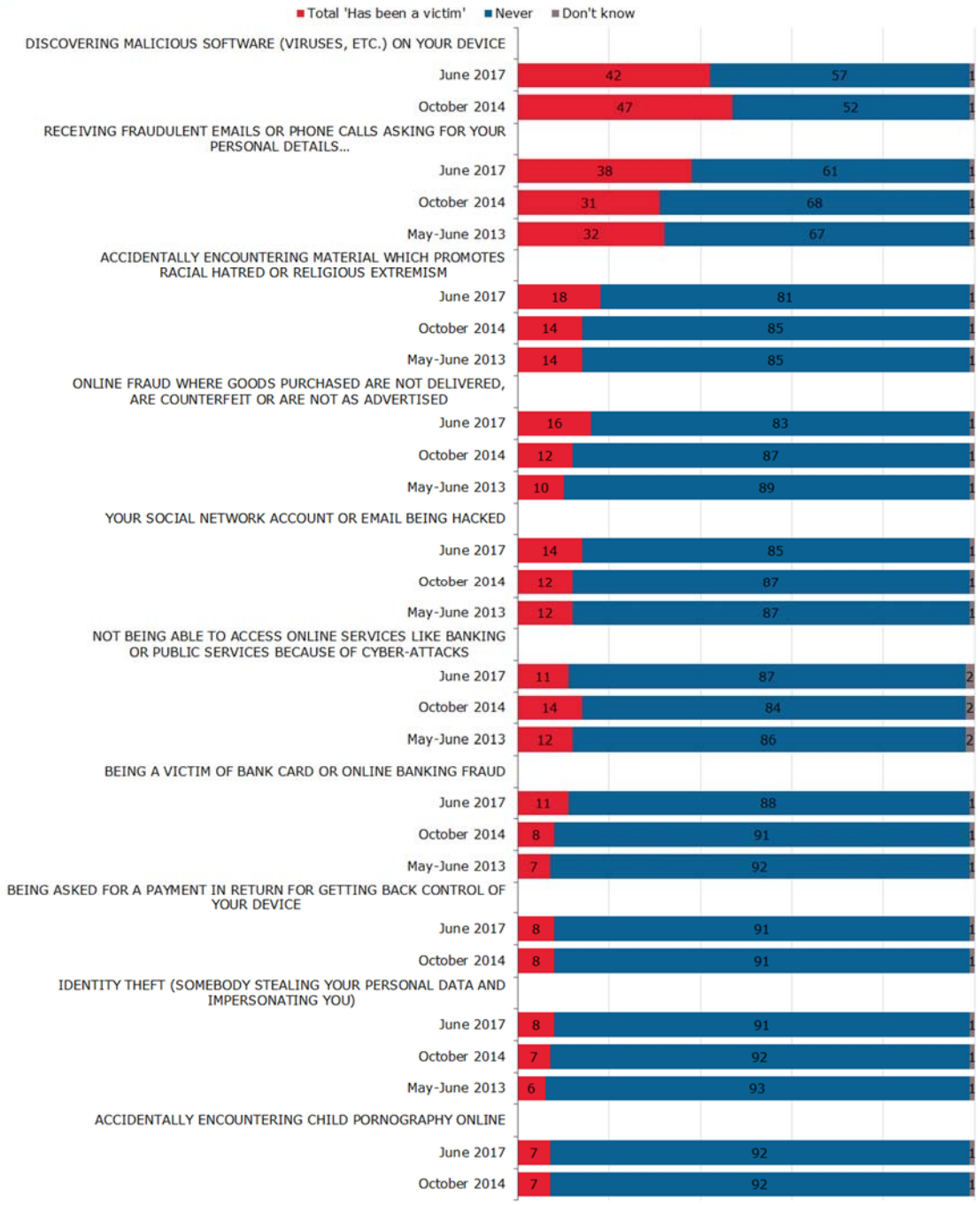
[4] QB14. Could you please tell me to what extent you agree or disagree with each of the following statements? 1. You are concerned that your online personal information is not kept secure by websites. 2. You are concerned that your online personal information is not kept secure by public authorities. 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 using antivirus software. Possible answers: Totally agree; Tend to agree; Tend to disagree; Totally disagree; Don't know.



Base: Respondents who are Internet users (N=22,236)

Less than half of respondents have actually been a victim of the various forms of cybercrime, and while there is no general trend to suggest that experiences of cybercrime overall are growing, there are increases in victimisation rates notably for phishing, online fraud and online banking fraud, as well as in encountering material which promotes racial hatred online or hacking of social media profiles. The two most common situations experienced by respondents remain discovering malicious software on their device (42%) and receiving an email or phone call fraudulently asking for access to their computer, logins or personal details (38%). These are also the types of cybercrime for which there are the most significant country-level differences.

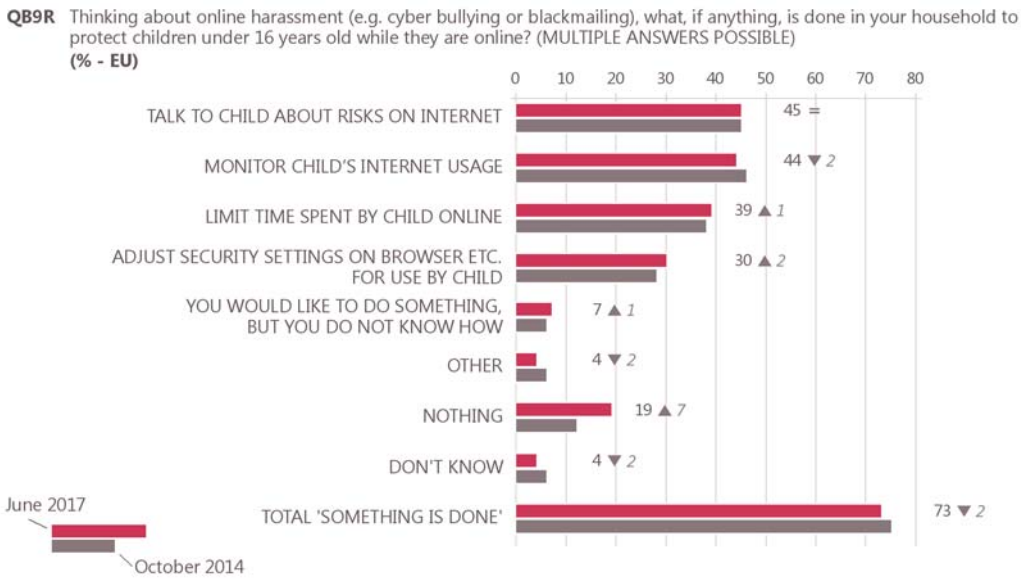
QB12 And how often have you experienced or been a victim of the following situations?
(% - EU)



Base: Respondents who are Internet users (N=22,236)

- The most common actions taken by respondents to protect children from online harassment are to monitor and limit children's Internet usage or to talk to children about Internet risks -

Various steps are taken to protect children aged under 16 while they are online, such as monitoring their Internet usage (44%), talking to children about risks on the Internet (45%), limiting the time spent online (39%) and adjusting security settings on their browser (30%).



Base: Respondents who answered 'Not applicable' are excluded (N=11,797)

- Most respondents would inform the police if they were a victim of any of the types of cybercrime considered in this study, except for discovering malicious software in their devices -

If they experienced or were the victim of cybercrime, most respondents say they would contact the police, especially if the crime was identity theft (85%), online banking fraud (76%), or if they accidentally encountered child pornography online (76%).

In 21 of the 28 Member States, the case of bank card or online banking fraud is the type of cybercrime where a largest proportion of respondents would definitively contact some institution. The cybercrime least likely to prompt a respondent to contact someone is encountering material which promotes racial hatred or religious extremism. In 19 countries, this item receives the lowest proportion of respondents.

CONCLUSION

This report has examined attitudes, perceptions and experiences of respondents in the EU regarding cybersecurity. It has confirmed many of the existing findings on this issue, and highlighted emerging trends.

Europeans remain highly alert to security threats. Prominent from the perspective of this survey, there has been a significant rise in the proportion of those who see cybercrime as an important problem. However, there appears to be some uncertainty about whether the authorities are doing enough to tackle cybercrime.

The urgency of dealing with cybercrime is amplified by three trends clearly indicated in this report: first, an increasing proportion of Europeans are making daily use of the Internet; second, they are increasingly doing so on a variety of devices; third, they are increasingly using these devices to perform tasks – such as shopping and online banking – which carry risks of exposing personal data. A majority of Internet users in the EU are aware of these threats and particularly concerned about the risks involved with exposing their personal information, with many are taking action to address these new risks. However, there is still considerable variation in the proportions of respondents taking security measures, as highlighted while analysing the results of this survey at country level and by key socio-demographic groups, such as age and level of education. These findings lend support to the rationale behind the EU's initiative to foster cyber security and combat cybercrime in a coordinated, EU-wide manner.

It is clear that there are high and increasing levels of concern about cyber security across the EU, with respondents particularly concerned about malicious software, identity theft, and online and banking fraud. However, it is worth noting that the increase in concerns about these threats is steeper than the increase in the proportion of people who have actually been victims of these various kinds of cybercrime. These figures also show that users can do more to protect themselves: the two most frequently experienced forms of cybercrime – infection with malicious software and fraudulent obtaining of personal information – are actions that a well-informed public can do much to prevent themselves.

Thus, while there is an obvious need for coordinated action to tackle large-scale organised cybercrime and impose standards of data protection on online service providers and vendors, the findings of this survey also highlight the importance of greater public education on types of cybercrime, their consequences, and ways in which their impact can be avoided or mitigated. This will allow people within the EU to come to a realistic understanding of the risks they face online, and equip them with the knowledge to deal with those risks more effectively.