



Flash Eurobarometer 496

SMEs and cybercrime

Report

Fieldwork:

November-December 2021

Publication:

May 2022

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

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.

Flash Eurobarometer 496 – Ipsos European Public Affairs

Flash Eurobarometer 496

Report

SMEs and cybercrime

November-December 2021

Survey conducted by Ipsos European Public Affairs at the request of the European Commission,
Directorate-General for Migration and Home Affairs

Survey coordinated by the European Commission, Directorate-General for Communication
(DG COMM “Media Monitoring and Eurobarometer” Unit)

Project title	Flash Eurobarometer 496 SMEs and cybercrime – November-December 2021 Report
Linguistic version	EN
Catalogue number	DR-01-22-164-EN-N
ISBN	978-92-76-49352-5 doi:10.2837/14988
© European Union, 2022	

<https://europa.eu/eurobarometer>

Table of contents

Introduction	1
Key findings.....	3
Section 1. Level of digitalisation of SMEs.....	5
1.1. Online tools used in SMEs	5
1.2. Personally-owned devices for business-related activities.....	10
Section 2. Level of awareness of risks of cybercrime	12
2.1. Managers' awareness about risks of cybercrime.....	12
2.2. Employees' awareness about risks of cybercrime.....	15
2.3. Training or awareness raising about the risks of cybercrime	18
Section 3. Concern about cybercrime	20
Section 4. Experience with cybercrime.....	32
4.1. Types of cybercrime experienced.....	32
4.2. Characteristics of the most serious cybercrime incident.....	43
4.3. Impact on business from the most serious cybercrime incident.....	46
Section 5. Reporting of cybercrime incidents.....	51
5.1. Reporting cybercrime (actual experience)	51
5.2. Reporting cybercrime (hypothetical question)	54
5.3. Reasons for not reporting cybercrime to the police	59
Technical specifications.....	65
Questionnaire	67
Data annex.....	72

Introduction

Europe's 25 million small and medium enterprises (SMEs)¹ are the backbone of the EU economy. They employ around 100 million people, account for more than half of Europe's GDP and play a key role in adding value in every sector of the economy. SMEs serve as **enablers for the digital transformation**. Data and information are core to the digital transformation, which unfortunately, increasingly attracts cybercriminal activity. **'Cybercrime'** refers to instances when someone uses the internet or other online technologies to access or tamper with a company's information systems or the data it holds, in order to harm or inconvenience the company.

The **COVID-19 crisis** showed how important the Internet and computers, in general, are for SMEs to maintain their business. In order to survive the pandemic and to continue in business, many SMEs had to take business continuity measures such as adopting cloud services, upgrading their internet services, improving their websites, and enabling staff to work remotely.² For these reasons, the pandemic posed additional cybersecurity challenges.

On behalf of the European Commission, Directorate-General for Migration and Home Affairs, Ipsos European Public Affairs conducted a survey exploring SMEs' experiences with cybercrime and their awareness about cybersecurity risk.

Key topics covered by the survey include:

- the extent to which SMEs' staff are aware about cybercrime risks and the level of training and awareness raising of staff about cybersecurity risks;
- level of concern about cybercrime among SMEs;
- experiences of SMEs with cybercrime over the last 12 months, including the types of cybercrime encountered, the most serious incident experienced, and the impact this had on business;
- SMEs' preferred channels for reporting cybercrime incidents, both in general and for actually experienced cybercrime incidents, and SMEs' reasons for not reporting cybercrime incidents to the police.

For this Flash Eurobarometer, a representative sample of SMEs in the manufacturing (NACE category C), retail (NACE category G), services (NACE categories, H, I, J, K, L, M, N, P, Q, R) and industry (NACE categories B, D, E, F) sectors was interviewed. Interviews took place with someone with decision-making responsibilities (managing director, general manager, CEO, financial director), someone leading the commercial activities (commercial manager, sales manager, marketing manager) or a legal officer. All interviews were carried via Computer-Assisted Telephone Interviewing (CATI).

¹ The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises that employ fewer than 250 persons and that have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million. (Extract of Article 2 of the annex to Recommendation 2003/361/EC)

² Source: European Union Agency for Cybersecurity (ENISA) (2021), Cybersecurity for SMEs. Challenges and Recommendations.

Between 26 November and 17 December 2021, 12 863 interviews were conducted by Ipsos European Public Affairs.

Results are presented from an EU, country and business-demographic perspective. Survey data are weighted to known business population proportions. The EU27 averages are weighted according to the size of the SME population of each Member State. A technical note on the methods applied to conduct the survey is appended as an annex to this report.

Notes:

- 1) Survey results are subject to sampling tolerances meaning that not all apparent differences between groups may be statistically significant. Thus, only differences that are statistically significant (at the 5% level) – i.e. where it can be reasonably certain that they are unlikely to have occurred by chance – are highlighted in the text.
- 2) Due to rounding, the percentages shown in the charts and tables do not always exactly add up to the totals mentioned in the text.
- 3) In this report, countries are referred to by their official abbreviation. The abbreviations used in this report correspond to:

BE		Belgium	LT		Lithuania
BG		Bulgaria	LU		Luxembourg
CZ		Czechia	HU		Hungary
DK		Denmark	MT		Malta
DE		Germany	NL		Netherlands
EE		Estonia	AT		Austria
IE		Ireland	PL		Poland
EL		Greece	PT		Portugal
ES		Spain	RO		Romania
FR		France	SI		Slovenia
HR		Croatia	SK		Slovakia
IT		Italy	FI		Finland
CY		Rep. of Cyprus*	SE		Sweden
LV		Latvia			

* Cyprus as a whole is one of the 27 EU MS. 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.

Key findings

Level of digitalisation of SMEs

- About three-quarters of SMEs surveyed (76%) currently use an **online bank account**, followed by 71% who have a **website for their business** and 55% that use **internet-connected 'smart' devices**. Not more than a handful of SMEs surveyed (3%) reply that they currently **do not use any of the nine online tools** listed in the survey. In 14 Member States, a majority of SMEs currently use **five or more of the online tools listed** in the survey.
- Among the SMEs surveyed, **48% report that their employees use personally owned devices to carry out business-related activities**. This figure ranges from 32% in France and 35% in Sweden to 74% in Cyprus. In total, in 12 Member States, more than six in ten SMEs answer that they apply a 'BYOD' practice.

Awareness about the risks of cybercrime

- **About seven in ten respondents (with a leading role in their SME) feel well informed about the risks of cybercrime**: 21% feel 'very well informed' and 50% 'fairly well informed'. The proportion of managers feeling well informed about the risks of cybercrime ranges from less than six in ten respondents in Hungary to nearly nine in ten respondents in Ireland and Malta.
- **15% of respondents feel that the employees in their SME are 'very well informed' about the risks of cybercrime and 41% find their employees 'fairly well informed'**. The proportion of respondents saying their employees are either very well or fairly well informed about the risks of cybercrime is the highest in Ireland (80%) and the lowest in Romania (46%).
- **19% of SMEs have provided their employees with training or awareness raising about the risks of cybercrime** in the last 12 months. In Ireland, 40% of SMEs say so; in Romania and France, this applies to less than one in ten SMEs (8%-9%).

Concerns about cybercrime

- SMEs are the most likely to be concerned about **hacking (or attempts to hack) online bank accounts** (32% are 'very concerned') and **phishing, account takeover or impersonation attacks** (31%), and **viruses and spyware or malware** (excluding ransomware) (29%).
- A quarter of SMEs are very concerned about unauthorised accessing of files or networks and 14% about unauthorised listening in to video conferences or instant messages. 22% of SMEs are very concerned about ransomware and 18% about denial-of-service attacks (DoS).
- Concern about the various types of cybercrime tends to be **higher in Portugal and Spain, but is lower in Denmark, Estonia and Sweden**. In line with the EU average results, in 12 Member States, the largest share of 'very concerned' responses is observed for hacking (or attempts to hack) online bank accounts (from 22% in Romania to 72% in Spain). Viruses, spyware or malware (excluding ransomware) receive the highest rate of 'very concerned' responses in seven Member States (from 9% in Denmark to 26% in Poland).

Experience with cybercrime

- The most prevalent type of cybercrime is **viruses, spyware or malware** (experienced by 14% of SMEs in the last 12 months), followed by **phishing, account takeover or impersonation attacks** (11%). The other types of cybercrime listed in the survey have incidence rates (for the past 12 months) of less than 5%.
- **28% of SMEs have experienced at least one of the listed types of cybercrime in the last 12 months.** This proportion ranges from 15% in Sweden and 16% in both Denmark and Germany, to 48% in Portugal.
- Three in ten SMEs say that **the most serious of the cybercrime attacks** experienced in the past 12 months was carried out by means of **malicious software**, while a similar share (28%) say it was carried out using **scams and fraud**. Slightly fewer say the most serious incident was executed by exploiting software, hardware or network vulnerabilities (23%), or by password cracking (19%).
- 58% of SMEs that have experienced at least one type of cybercrime also suffered from some kind of **impact on their business**. The most prevalent types of impact mentioned are 'additional time required to respond to the cybercrime incident(s)' (35%) and 'repair or recovery costs' (24%).
- The proportion of SMEs saying that the most serious incident they have experienced in the last 12 months **did not have any impact their business** ranges from 9% in Ireland to 60% in Estonia and 61% in Cyprus.

Reporting of cybercrime incidents

- **SMEs are most likely not to have reported the cybercrime incidents they have experienced** – 44% of cybercrimes experienced were not reported to anyone. When cybercrimes were reported, they were most often reported to the police (18% of all incidents) or the seller or service provider (17%). A further 12% of cybercrimes were reported to the Internet service provider, 7% to another official authority, 4% to a business representative body or trade body and 3% to a consumer protection organisation. Slightly less than one in ten cybercrimes (7%) were reported to 'someone else'.
- In Ireland, for 87% of cybercrime incidents reported during the survey, respondents reply that they reported the incident to someone – e.g. the police, their service provider or official authority etc. In Hungary and Poland, this applies to 30% of incidents.
- **Answering question about hypothetical incidents of cybercrime, SMEs are by far most likely to say that they would report these to the police.** This is especially the case with regard to phishing, account takeover or impersonation attacks and the hacking (or attempts to hack) online bank accounts.
- SMEs that have experienced at least one type of cybercrime in the last 12 months and did not report the incident to the police are most likely to say that they did not report the incident because they **dealt with it internally** (52%). Slightly fewer (44%) felt the incident was **too trivial / not worth reporting to the police**.

Section 1. Level of digitalisation of SMEs

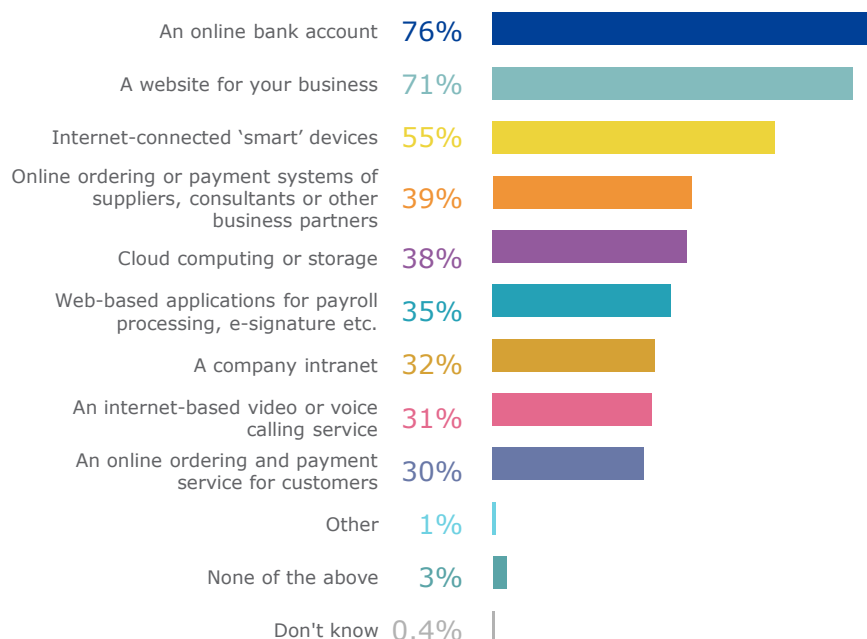
The move to 'digital business' is associated with an increase in the risk to be exposed to cybercrime. In the first section of this chapter, an analysis is presented of the **number and type of digital and online tools** being used by SMEs across the EU. The second section analyses the proportion of SMEs with a **Bring Your Own Device (BYOD)** practice where employees use their own personal laptops, smartphones, tablets or other devices for work. The practice of BYOD comes with risks with respect to security and data protection.

1.1. Online tools used in SMEs

About three-quarters of SMEs surveyed (76%) currently use an **online bank account**, followed by 71% who have **a website for their business** and 55% that use **internet-connected 'smart' devices**. About four in ten SMEs (39%) use online ordering and payment systems of suppliers or other business partners and 30% have their own online ordering and payment services for customers. Close to four in ten SMEs (38%) use cloud computing or storage, 35% have web-based applications for payroll processing, e-signature etc. and 32% have a company intranet. Finally, 31% of SMEs use an Internet-based video or voice calling service.

A handful of SMEs surveyed (3%) reply that they currently **do not use any of the online tools** listed in the survey.

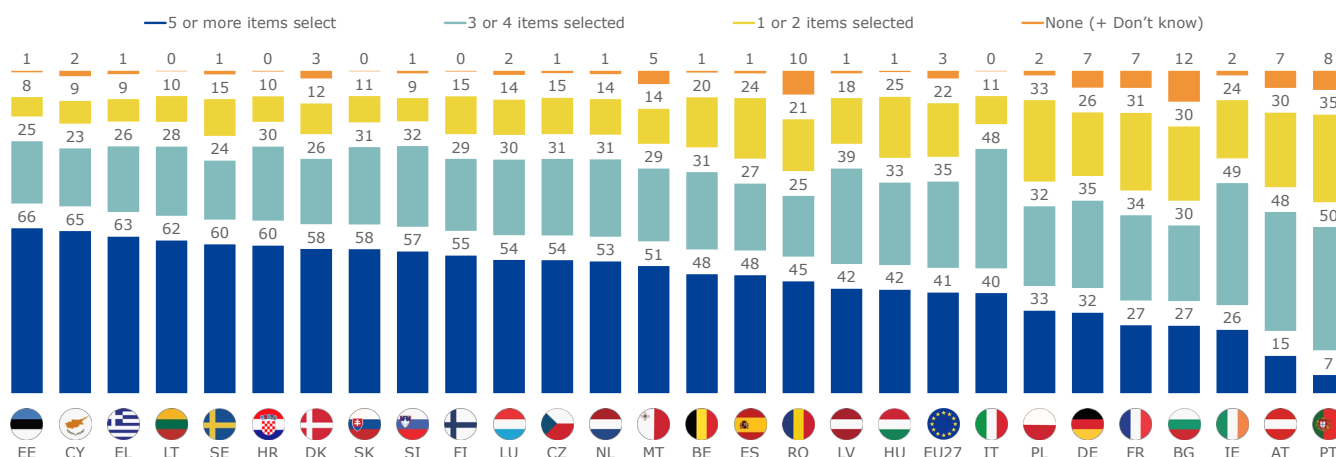
Q1 Which of the following does your company currently have or use? Multiple answers possible (% EU27)



Base: all SMEs (n=12 863)

In 14 Member States, a majority of SMEs currently use **five or more of the online tools listed** in the survey; the highest figures are seen in Lithuania (62%), Greece (63%), Cyprus (65%) and Estonia (66%). In Portugal, on the other hand, 7% of SMEs use five or more online tools, while 35% reply that they use just **one or two of the tools listed**. In Austria, Bulgaria, France and Poland, between 30% and 33% of SMEs use one or two online tools.

Q1 Which of the following does your company currently have or use? **Number of tools used**
(% by country)



Base: all SMEs (n=12 863)

The table on the following page presents, on a **country-by-country** basis, the proportion of SMEs that currently have or use each of the online tools listed in the survey. The higher the proportion of SMEs that use the online tool, the darker blue the cell in the table. For each country, there is also one cell shaded green; this is the response that is selected most frequently by SMEs in the country.

In 19 Member States, the largest share of SMEs say they currently use **on online bank account**. Moreover, in all but one of the countries, a majority of SMEs reply that they use an online bank account – from 49% in Portugal (the only country with a figure less than 50%) to 97% in Estonia.

In seven Member States, **a website for their business** is the most frequently mentioned response – this is the case, for example, in France, Germany and Italy. Across most countries, this response is given by a majority of respondents, with the largest figures seen in Luxembourg, Czechia, the Netherlands, Denmark and Slovakia (all 82%-84%).

In Croatia, the largest share of respondents say they use **Internet-connected 'smart' devices** (89%); this proportion is also higher than 80% in Estonia, Finland and Slovenia (between 83% and 89%). In Portugal, Poland, Ireland and France, however, this response is selected by less than 40% of SMEs (between 27% and 37%).

Q1 Which of the following does your company currently have or use? Multiple answers possible
(% by country)

		An online bank account	A website for your business	Internet-connected 'smart' devices	Online ordering or payment systems of suppliers, consultants or other business partners	Cloud computing or storage	Web-based applications for payroll processing, e-signature etc.	A company intranet	An internet-based video or voice calling service	An online ordering and payment service for customers	Other	None of the above	Don't know
EU27		76	71	55	39	38	35	32	31	30	1	3	0
BE		87	74	57	44	50	45	29	39	30	0	1	0
BG		65	39	56	21	17	48	31	22	19	2	11	2
CZ		94	83	71	34	42	37	34	44	31	0	1	0
DK		88	83	56	47	62	55	26	30	33	1	3	0
DE		72	76	53	35	32	23	26	22	19	0	6	1
EE		97	60	83	63	52	72	15	33	62	2	1	0
IE		62	77	36	34	29	37	24	30	30	1	1	1
EL		88	78	48	54	46	54	51	52	49	0	1	0
ES		79	67	66	31	48	43	33	32	30	1	1	1
FR		58	66	37	37	36	25	32	21	26	0	7	0
HR		82	67	89	39	43	56	29	61	42	0	0	0
IT		70	79	66	50	29	27	48	31	31	1	0	0
CY		94	75	51	57	51	40	54	60	52	0	2	1
LV		95	52	71	23	33	60	27	36	31	0	1	0
LT		96	62	78	43	42	90	23	35	41	0	0	0
LU		72	82	59	42	45	44	36	45	36	0	1	1
HU		86	65	75	38	38	26	23	33	33	0	1	0
MT		72	77	71	40	49	32	40	36	36	2	4	2
NL		90	83	55	40	61	41	27	40	32	1	1	0
AT		62	60	53	26	23	14	19	17	21	3	5	2
PL		89	67	28	36	30	34	23	28	29	0	2	0
PT		49	50	27	33	27	22	19	16	26	6	4	4
RO		78	36	67	50	31	50	23	19	42	0	10	0
SI		93	67	89	38	53	46	25	51	36	0	1	0
SK		90	84	80	32	39	53	23	53	32	0	0	0
FI		93	70	85	33	53	57	19	42	38	0	0	0
SE		82	74	66	50	57	48	29	52	35	0	1	0

The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: all SMEs (n=12 863)

A majority of SMEs in Greece (54%), Cyprus (57%) and Estonia (63%) use online ordering and payment systems of suppliers or business partners; in all other countries, this proportion ranges from 21% and 50%. SMEs in Greece, Cyprus and Estonia are also more likely than SMEs in other countries to have their own online ordering and payment services for customers (between 49% and 62%).

The proportion of SMEs that use cloud computing or storage ranges from 17% in Bulgaria to 62% in Denmark. Between 14% of SMEs in Austria and 90% in Lithuania have web-based applications for payroll processing, e-signature etc. and between 15% of SMEs in Estonia and 54% in Cyprus have a company intranet. Finally, 16% of SMEs in Portugal use an Internet-based video or voice calling service, compared to 61% in Croatia.

Larger SMEs, both in terms of **number of employees** and **turnover**, are more likely to use more online tools. For example, 38% of SMEs with less than 10 employees use five or more of the online tools listed in the survey; this proportion increases to 56% for SMEs with between 10 and 49 employees and to 67% for SMEs with between 50 and 249 employees. Similarly, 35% of SMEs with a turnover of up to 100 000 euros use five or more of the online tools listed in the survey; this proportion gradually increases to 60% for SMEs with a turnover of more than 2 000 000 euros.

At the **sector level**, SMEs active in industry (NACE sectors B, D, E and F)³ are less likely than SMEs in other sector groups to use five or more of the online tools listed in the survey and they are more likely to use just one or two online tools. For example, 35% of SMEs in industry use five or more tools, compared to 41% in services (NACE sectors H, I, J, K, L, M, N, P, Q and R). Among SMEs in industry, however, 27% use one or two online tools; this compared to 19% for SMEs in retail (NACE sector G).

Older SMEs, with more **years of activity**, on average, are slightly more likely to use more online tools than SMEs that have been in operation for a shorter period of time. The largest differences are seen compared to SMEs with less than one year of activity. Among the latter type of SMEs, 25% use five or more of the online tools listed in the survey, while almost twice as many (49%) use three or four tools.

³ Statistical classification of economic activities in the European Community, abbreviated as NACE, is the classification of economic activities in the European Union. For more information, see: <https://ec.europa.eu/eurostat/web/nacerev2/overview>

Q1 Which of the following does your company currently have or use? **Number of tools used**
(% by business demographics)

	5 or more items select	3 or 4 items selected	1 or 2 items selected	None (+ Don't know)
EU27	41	35	22	3
Company size				
<10 employees	38	36	23	3
10-49 employees	56	29	13	1
50-249 employees	67	25	8	1
Company turnover in 2020				
Up to €100,000	35	34	28	4
€100,001-€500,000	41	39	18	2
€500,001-€2,000,000	47	35	16	2
More than €2,000,000	60	29	10	1
Sector of activity				
Manufacturing	42	34	23	2
Industry	34	36	27	3
Retail	42	35	19	4
Services	41	34	21	3
Company age (years of activity)				
Less than one year	25	49	20	6
One to five years	37	37	23	3
Six to ten years	39	33	24	4
More than 10 years	42	35	21	3

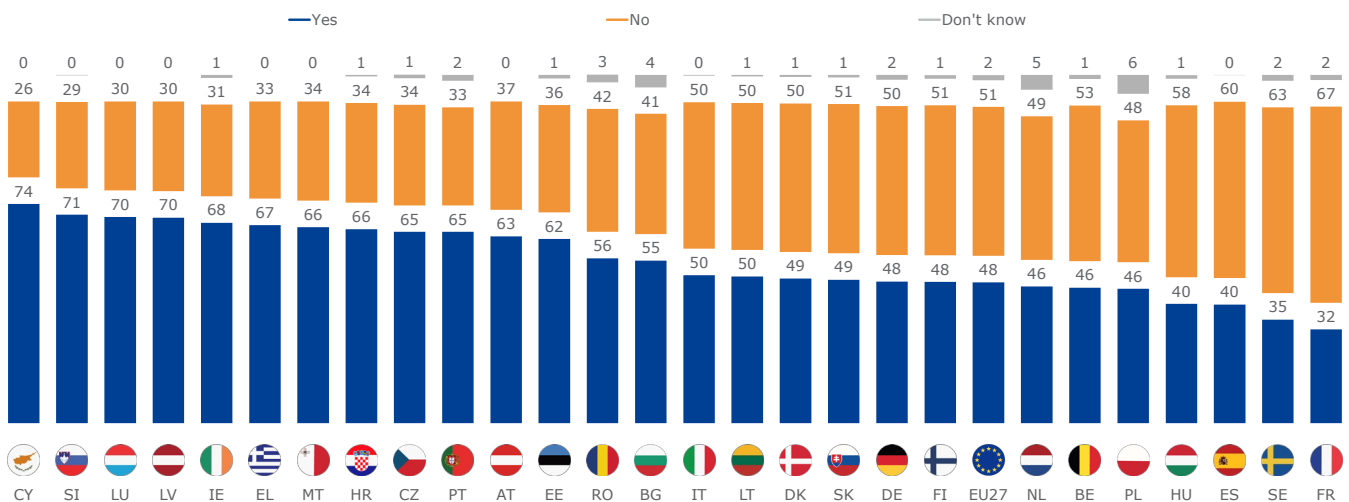
Base: all SMEs (n=12 863)

1.2. Personally owned devices for business-related activities

Bring Your Own Device (BYOD) is a practice of allowing employees to use their own personal laptops, smartphones, tablets or other devices to carry out regular business-related activities. It has become increasingly popular in recent years (and especially during the COVID-19 pandemic) as a way to enable employees to work remotely, accessing their business' network and data from home or on the go. The practice of BYOD offers many benefits, but it also entails some risks, especially when it comes to security and data protection. BYOD raises a number of data protection concerns and can lead to vulnerabilities in information security. For example, personal devices may contain malicious apps or malware or be more vulnerable to attack from online threats.

Among the SMEs surveyed, 48% report that their employees use personally owned devices to carry out regular business-related activities. This figure ranges from 32% in France and 35% in Sweden to 74% in Cyprus. In total, in 12 Member States, more than six in ten SMEs answer that they apply a 'BYOD' practice.

Q2 Do employees in your company use personally owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities? This includes devices that are subsidized by your company. (% by country)



Base: all SMEs (n=12 863)

Across all types of SMEs, between 43% and 57% of respondents reply that their employees use personally owned devices to carry out regular business-related activities. The variation in these proportion is not statistically significant, except for the difference in proportions for SMEs with different level of turnover. SMEs with lower level of turnover are more likely than SMEs with a turnover of more than 2 000 000 euros to apply a BYOD policy (48%-49% vs 43%).

Q2 Do employees in your company use personally owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities? This includes devices that are subsidized by your company. (% 'yes' by business characteristics)

	Yes
EU27	48
Company size	
<10 employees	48
10-49 employees	49
50-249 employees	47
Company turnover in 2020	
Up to €100,000	49
€100,001-€500,000	48
€500,001-€2,000,000	48
More than €2,000,000	43

Sector of activity	
Manufacturing	48
Industry	49
Retail	45
Services	49
Company age (years of activity)	
Less than one year	57
One to five years	48
Six to ten years	51
More than 10 years	47

Base: all SMEs (n=12 863)

Section 2. Level of awareness of risks of cybercrime

Research conducted by the European Union Agency for Cybersecurity (ENISA) in 2021 concluded that SMEs within the European Union appear to understand that cybersecurity is an important issue; nonetheless, **low awareness of the threats posed to their business by poor cybersecurity was identified as one of the greatest challenges to SMEs.**⁴ The second chapter of this report looks at managers' self-assessed level of awareness about the risks of cybercrime and their assessment of their employees level of awareness. The last section presents the proportion of SMEs that have organised training or awareness raising about the risks of cybercrime.

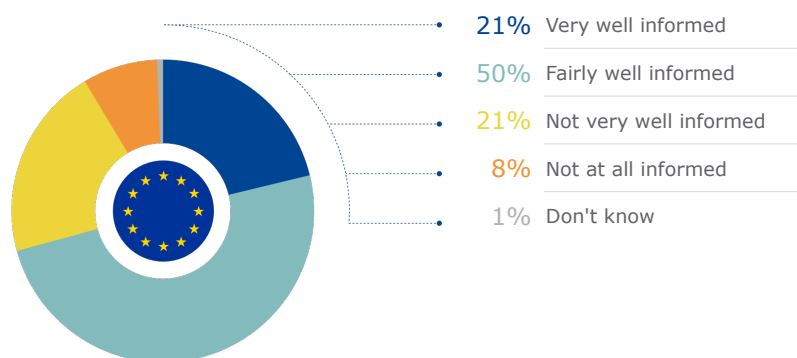
2.1. Managers' awareness about risks of cybercrime

Across all SMEs surveyed, the interview took place with someone with decision-making responsibilities (managing director, general manager, CEO, financial director) someone leading the commercial activities (commercial manager, sales manager, marketing manager) or a legal officer. These respondents were asked to evaluate how informed they feel about the risks of cybercrime. The following definition of cybercrime was read out to them:

For the purpose of this survey, 'cybercrime' refers to instances when someone uses the internet or other online technologies to access or tamper with your company's information systems or the data it holds, in order to harm or inconvenience your company.

About seven in ten respondents feel they are well informed about the risks of cybercrime: 21% feel 'very well informed' and 50% 'fairly well informed'. About one in five (21%) respondents feel 'not very well informed' and 8% feel 'not at all informed'.

Q3 How well informed do you feel about the risks of cybercrime? (% EU27)



Base: all SMEs (n=12 863)

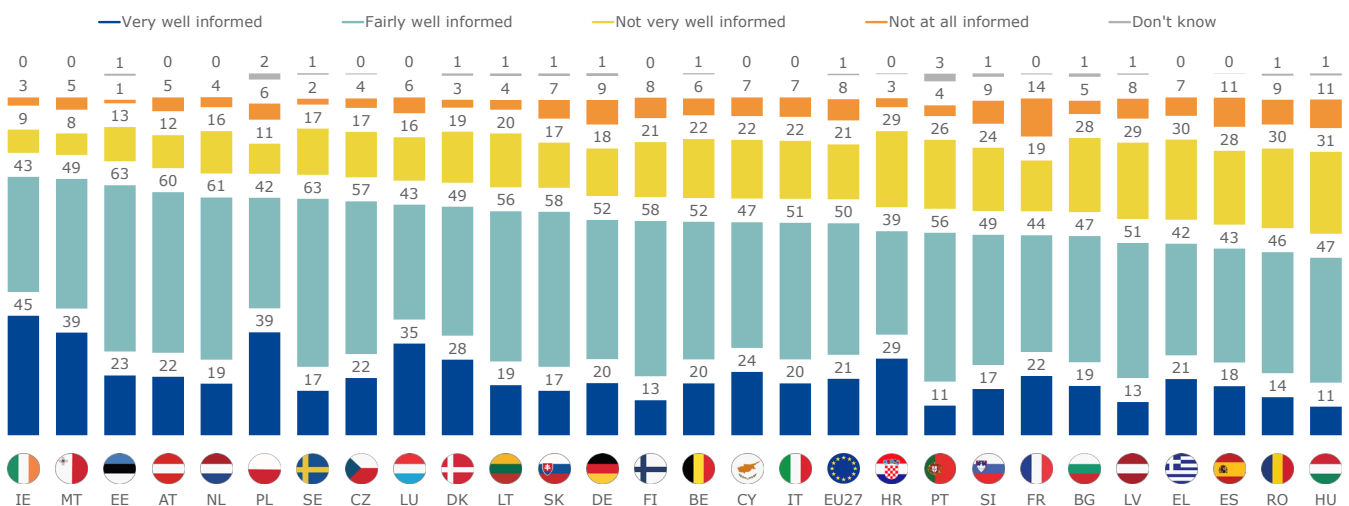
⁴ Other challenges identified in the study are the costs of implementing cybersecurity measures often combined with a lack of dedicated budget, the availability of ICT cybersecurity specialists, a lack of suitable guidelines aimed at the SME sector, and low management support. Source: ENISA (2021), Cybersecurity for SMEs. Challenges and Recommendations.

In Special Eurobarometer 499 ‘Europeans’ attitudes towards cyber security’ (conducted in October 2019), EU citizens were asked the same question. In that survey, 52% answered that they felt well informed compared to 47% who felt not well informed. The respondents in the current survey – all **individuals with a managing role in an SME – are more likely than EU citizens, on average, to report feeling well informed about the risks of cybercrime** (71% vs 52%).

At **country level**, the proportion of managers **feeling either very or fairly well informed about the risks of cybercrime** ranges from less than six in ten respondents in Hungary to nearly nine in ten respondents in Ireland and Malta. In Ireland, 45% of managers say they feel ‘very well informed’ about the risks of cybercrime; in Poland and Malta, this response is given by 39% of respondents. In Hungary and Portugal, on the other hand, just 11% of managers feel very well informed about the risks of cybercrime. The largest share of respondents who say they feel not well informed, nonetheless, is observed in Hungary (42% ‘not very well’ and ‘not at all informed’ responses); in Romania and Spain, this applies to 39% of respondents.

In Special Eurobarometer 499 ‘Europeans’ attitudes towards cyber security’, the proportion of EU citizens that felt well informed about the risk of cybercrime varied between 30% in Bulgaria and 80% in Denmark. Some of the countries found at the higher end of the country ranking in Special Eurobarometer 499 are also found in this position in the current survey – such as Sweden and the Netherlands. Similarities can also be observed at the lower end of the country ranking – for example, Romania and Hungary are found in this position in both surveys.

Q3 How well informed do you feel about the risks of cybercrime? (% EU27)



Base: all SMEs (n=12 863)

Respondents with a leading role in larger SMEs are more likely than those in smaller SMEs to say that they feel well informed about the risks of cybercrime – 86% of managers in SMEs with 50 to 249 employees and 79% of those in SMEs with 10 to 49 employees feel this way, compared to 69% of those in SMEs with less than 10 employees.

Managers' self-assessed level of information about cybercrime is similar across SMEs from different **grouped NACE sectors**. At the level of **specific NACE sectors**, some managers are more likely to feel well informed; this includes those working in the NACE sectors J (Information and communication), K (Financial and insurance activities), N (Administrative and support service activities) and P (Education), in which 82%-86% feel well informed about cybercrime risks.

Managers working in SMEs with a **turnover** of more than 2 million euros most often self-assess to be well informed about cybersecurity risks. Eight in ten managers in the latter type of SMEs feel well informed, compared to 69%-71% in SMEs with turnovers of up to 100 000 euros, 100 000 to 500 000 euros, or 500 000 to 2 million euros.

The more **online tools** SMEs use, the more likely it is that their managers feel well informed about the risks of cybercrime; 76% of those using five or more of the online tools listed in the survey find themselves well informed, compared to 70% of those in SMEs using three to four online tools and 64% of those in SMEs using one to two online tools.

Q3 How well informed do you feel about the risks of cybercrime?
(% **Total 'Informed'** by business characteristics)

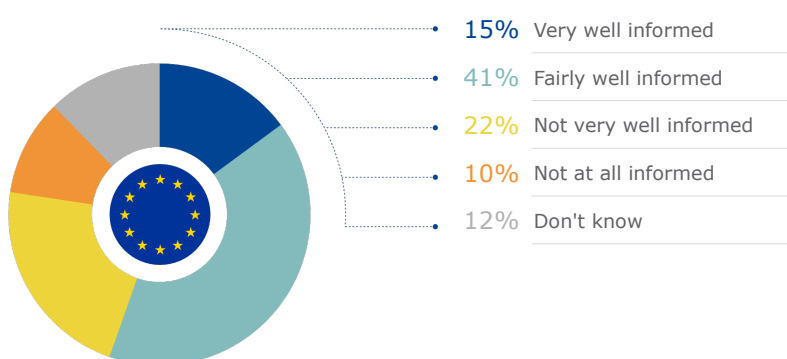
Total 'Informed'	
EU27	71
Company size	
<10 employees	69
10-49 employees	79
50-249 employees	86
Company turnover in 2020	
Up to €100,000	71
€100,001-€500,000	69
€500,001-€2,000,000	71
More than €2,000,000	80
Sector of activity	
Manufacturing	71
Industry	68
Retail	68
Services	73
Company age (years of activity)	
Less than one year	61
One to five years	72
Six to ten years	72
More than 10 years	71
Online tools being used in the SME	
None	53
One or two tools	64
Three or four tools	70
Five or more tools	76
Personally owned devices for business activities	
No	72
Yes	69

Base: all SMEs (n=12 863)

2.2. Employees' awareness about risks of cybercrime

Respondents were also asked whether, in their opinion, the employees in their SME are well informed about the risks of cybercrime. **15% of respondents feel that the employees in their SME are 'very well informed' about the risks of cybercrime and 41% find their employees 'fairly well informed'** about these risks. About one third of respondents find their staff not well informed about the risks of cybercrime: 10% think their employees are 'not at all informed' about the risks of cybercrime and 22% who feel that their staff is 'not very well informed' about these risks. 12% do not know how well informed their employees are about the risks of cybercrime.

Q4 How well informed do you feel your employees are about the risks of cybercrime? (% EU27)

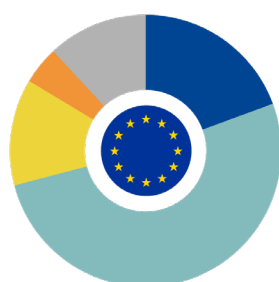


Base: all SMEs (n=12 863)

Among **managers who feel well informed** about cybercrime, 19% report that their employees are 'very well informed' and 52% say they are 'fairly well informed'. The responses of **managers who do not feel well informed** about the risks of cybercrime are close to a mirror image with 25% saying that their employees are 'not at all informed' and 45% that they are 'not very well informed'.

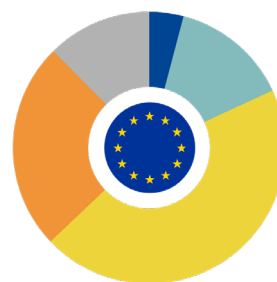
Q4 How well informed do you feel your employees are about the risks of cybercrime? (% EU27)

Respondents who feel well informed about cybercrime



19%	Very well informed
52%	Fairly well informed
13%	Not very well informed
5%	Not at all informed
12%	Don't know

Respondents who feel NOT well informed about cybercrime

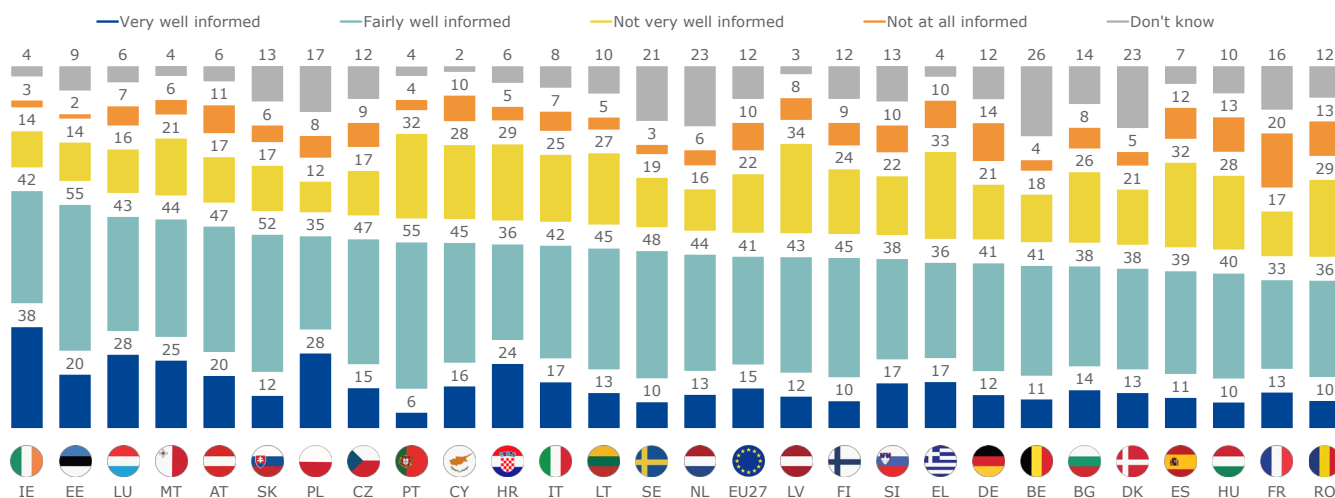


4%	Very well informed
14%	Fairly well informed
45%	Not very well informed
25%	Not at all informed
12%	Don't know

Base: well-informed respondents (n=9 621) and not well-informed respondents (n=3 168)

At the country level, the proportion of respondents who feel **their employees are either very well or fairly well informed** about the risks of cybercrime is the highest in Ireland (80%) and the lowest in Romania (46%). Apart from in Romania, less than half of managers surveyed find their staff well informed about the risks of cybercrime in France (47%) and Hungary (49%). Like in Ireland, at least seven in ten respondents find their employees well informed about the risks of cybercrime in Estonia (75%) and Luxembourg (71%).

Q4 How well informed do you feel your employees are about the risks of cybercrime? (% by country)



Base: all SMEs (n=12 863)

Larger SMEs are more likely than their smaller counterparts to say that their staff are well informed about the risks of cybercrime – 68% of SMEs with 50 to 249 employees and 62% of those with 10 to 49 employees claim this is the case, compared to 54% of SMEs with less than 10 employees.

SMEs active in the retail and services **NACE sectors** are more likely than those active in the manufacturing and (especially) industry sectors to say that their staff are well informed about the risks of cybercrime. The proportion saying their staff are well informed ranges from 48% in the industry sector and 52% in the manufacturing sector, to 56% in the retail sector and 58% in the services sector.

How long SMEs are in business does not appear to have an impact on their likelihood to say their staff are well informed about the risks of cybercrime. The company's **turnover**, however, does make an important difference: SMEs with a turnover of more than 2 million euros are much more likely than those with a lower turnover to say their staff are well informed about the risks of cybercrime (68% say so, compared to 51%-58% of SMEs with turnovers of up to 100 000 euros, 100 000 to 500 000 euros, or 500 000 to 2 million euros).

The more **online tools** SMEs use, the more likely they are to say that their employees are well informed about the risks of cybercrime; 62% of those using five or more of the online tools find their staff well informed, compared to 56% of SMEs using three to four online tools and 46% of those using one to two online tools. SMEs that are not using any of the online tools are clearly least likely to say their staff well informed about the risks of cybercrime (32% say their staff is well informed, while 41% of these SMEs say their staff are not well informed).

Q4 How well informed do you feel your employees are about the risks of cybercrime?
(% **Total 'Informed'** by business characteristics)

	Total 'Informed' ⁵
EU27	55
Company size	
<10 employees	54
10-49 employees	62
50-249 employees	68
Company turnover in 2020	
Up to €100,000	51
€100,001-€500,000	58
€500,001-€2,000,000	56
More than €2,000,000	68
Sector of activity	
Manufacturing	52
Industry	48
Retail	56
Services	58

Company age (years of activity)	
Less than one year	56
One to five years	55
Six to ten years	56
More than 10 years	56
Online tools being used in the SME	
None	32
One or two tools	46
Three or four tools	56
Five or more tools	62
Personally owned devices for business activities	
No	59
Yes	53

Base: all SMEs (n=12 863)

⁵ Due to rounding, the percentages for specific response options shown in the charts do not always add up to the totals mentioned in the tables and text.

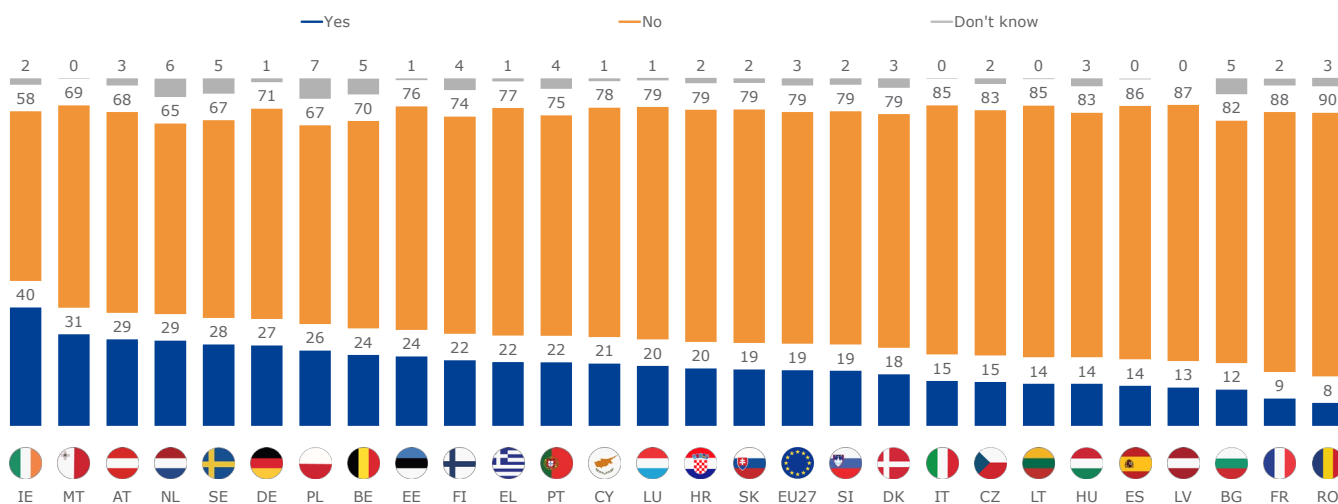
2.3. Training or awareness raising about the risks of cybercrime

About one in five SMEs surveyed (19%) have provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months.

In Ireland, 40% of SMEs reply that they have provided employees with training or awareness raising about the risks of cybercrime in the past 12 months. In another seven Member States, this reply is given by more than a quarter of respondents: Poland (26%), Germany (27%), Sweden (28%), the Netherlands and Austria (both 29%) and Malta (31%).

In Romania and France, less than one in ten SMEs have provided training or awareness raising about the risks of cybercrime (8%-9%). Other countries at the lower end of the country ranking are Bulgaria (12% 'provided training'), Latvia (13%), and Hungary, Lithuania and Spain (all 14%).

Q5 In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime? (% by country)



Base: all SMEs (n=12 863)

Larger SMEs are much more likely than their smaller counterparts to have provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months. The proportion that has provided this kind of training or awareness raising ranges from 17% of SMEs with less than 10 employees, and 29% of those with 10 to 49 employees, to 45% of those with 50 to 249 employees.

In line with the results relating to SMEs' number of employees, SMEs with a higher **turnover** are more likely to have provided their employees with training or awareness raising about the risks of cybercrime. Of SMEs with a turnover of more than 2 million euros, 33% provided this kind of training to their staff, compared to between 15% and 22% of SMEs with turnovers of up to 100 000 euros, 100 000 to 500 000 euros, or 500 000 to 2 million euros.

More than one in five SMEs in the **manufacturing and services sectors** (21% in both sectors) provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months. In the retail sector, and especially the industry sector, this proportion is notably lower (17% and 14%, respectively).

SMEs that use more **online tools** are much more likely to have provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months. Among SMEs using five or more online tools, a quarter have provided their employees with training or awareness raising about the risks of cybercrime. About one in six (17%) of SMEs using three or four online tools provide this kind of training or awareness raising. Of the SMEs using one to two online tools, this proportion is lower – at 11%.

Q5 In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime? (% 'yes', by business characteristics)

	Yes
EU27	19
Company size	
<10 employees	17
10-49 employees	29
50-249 employees	45
Company turnover in 2020	
Up to €100,000	15
€100,001-€500,000	17
€500,001-€2,000,000	22
More than €2,000,000	33
Sector of activity	
Manufacturing	21
Industry	14
Retail	17
Services	21

Company age (years of activity)	
Less than one year	14
One to five years	16
Six to ten years	18
More than 10 years	20
Online tools being used in the SME	
None	9
One or two tools	11
Three or four tools	17
Five or more tools	25
Personally owned devices for business activities	
No	20
Yes	18

Base: all SMEs (n=12 863)

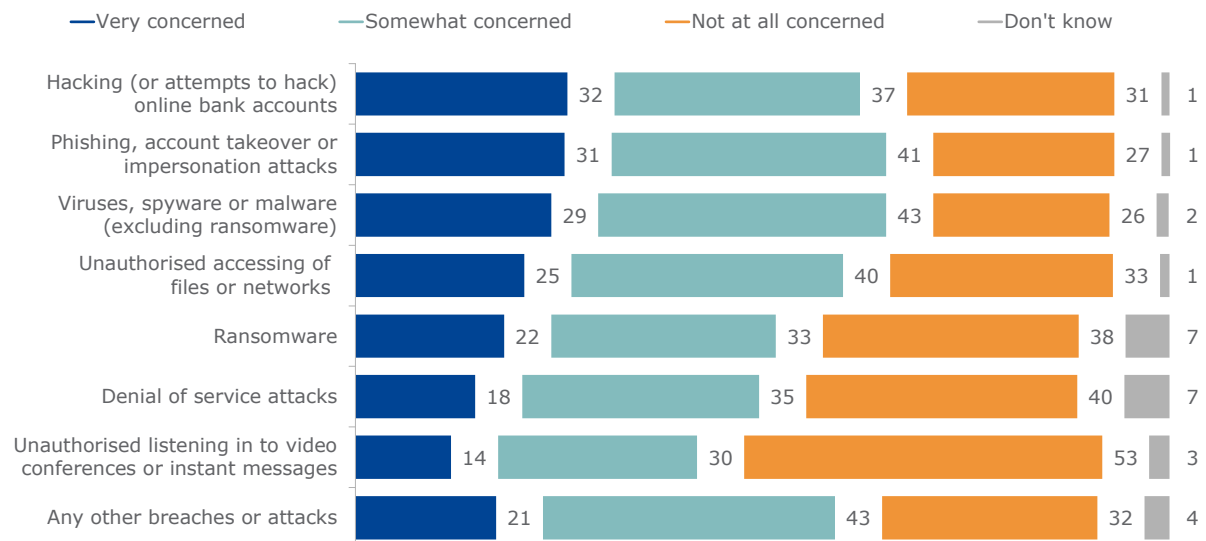
Section 3. Concern about cybercrime

To measure **SMEs' level of concern about cybercrime**, respondents in the SMEs surveyed were asked how concerned they are about a number of key cybercrime-related risks. The results show that **SMEs are the most likely to be concerned** about **hacking (or attempts to hack) online bank accounts** (32% are 'very concerned') and **phishing, account takeover or impersonation attacks** (31%), and **viruses and spyware or malware** (excluding ransomware) (29%). Between 37% and 43% of SMEs are somewhat concerned about these risks, and between 26% and 31% report not being concerned at all.

A quarter of SMEs are very concerned about **unauthorised accessing of files or networks** and 40% say they are somewhat concerned about this threat. One in three SMEs is not concerned at all about unauthorised accessing.

Around one in five (22%) SMEs are very concerned about **ransomware** and a somewhat lower proportion (18%) are very concerned about **denial-of-service attacks**. For these threats, about twice as many respondents say they are not concerned at all (38% and 40%, respectively). The proportion being 'not concerned at all' is the highest for **unauthorised listening in to video conferences or instant messages** (53% vs 14% who are 'very concerned'). 'Any other breaches or attacks' are a reason to be very concerned for 21% of SMEs.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? (% EU27)

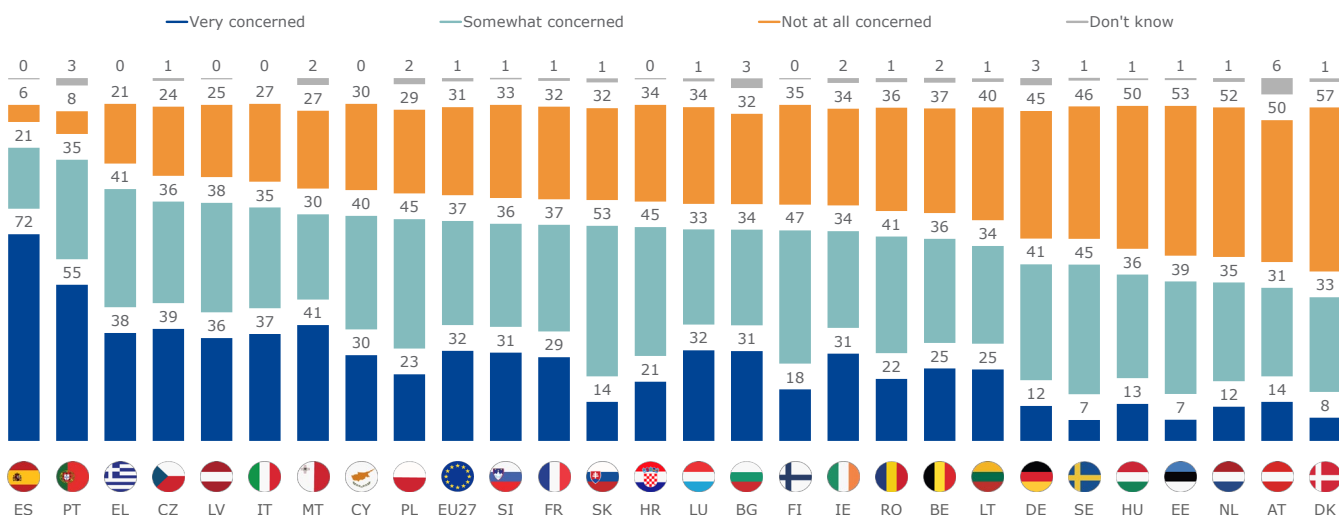


Base: all SMEs (n=12 863)

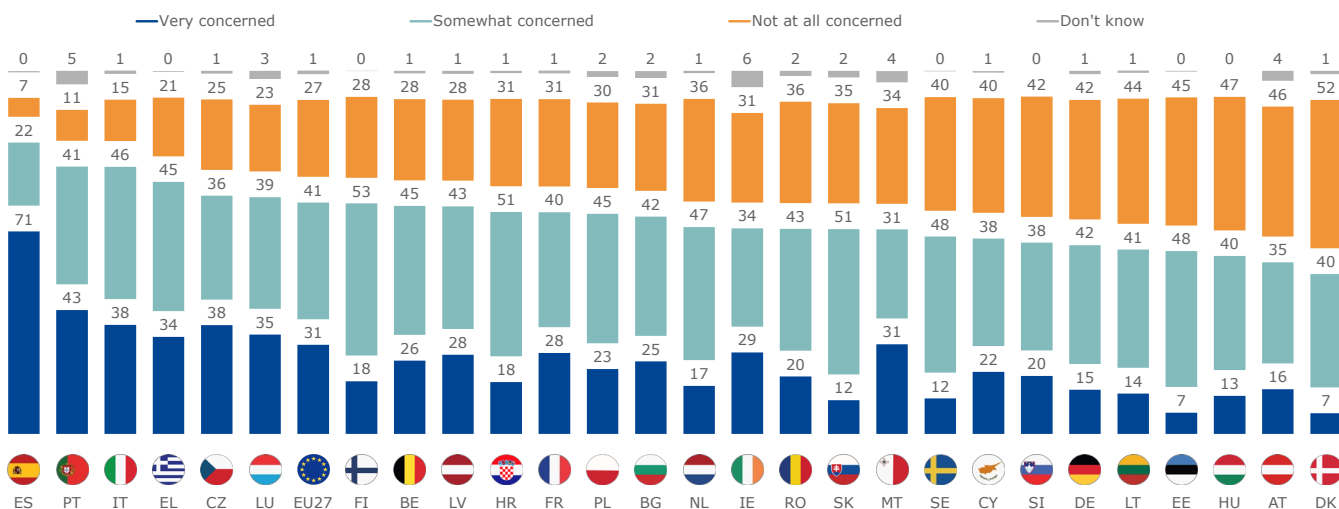
In Portugal and Spain, about nine in ten SMEs surveyed report being very or somewhat concerned about **hacking (or attempts to hack) online bank accounts**; in Denmark, Austria, the Netherlands, Estonia and Hungary, less than half of respondents are concerned about this type of cybercrime (between 41% and 49%). The proportion of SMEs being 'very concerned' about hacking (or attempts to hack) online bank accounts ranges from 7% in Estonia and Sweden, to 72% in Spain.

More than eight in ten SMEs in Italy, Portugal and Spain (between 84% and 93%) reply that they are very or somewhat concerned about **phishing, account takeover or impersonation attacks**; in Denmark, on the other hand, 47% report being concerned, while 52% say they are not concerned at all about this type of attacks. The proportion of SMEs being 'very concerned' about phishing, account takeover or impersonation attacks ranges from 7% in Denmark and Estonia, to 71% in Spain.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
Hacking (or attempts to hack) online bank accounts (% by country)



Phishing, account takeover or impersonation attacks (% by country)

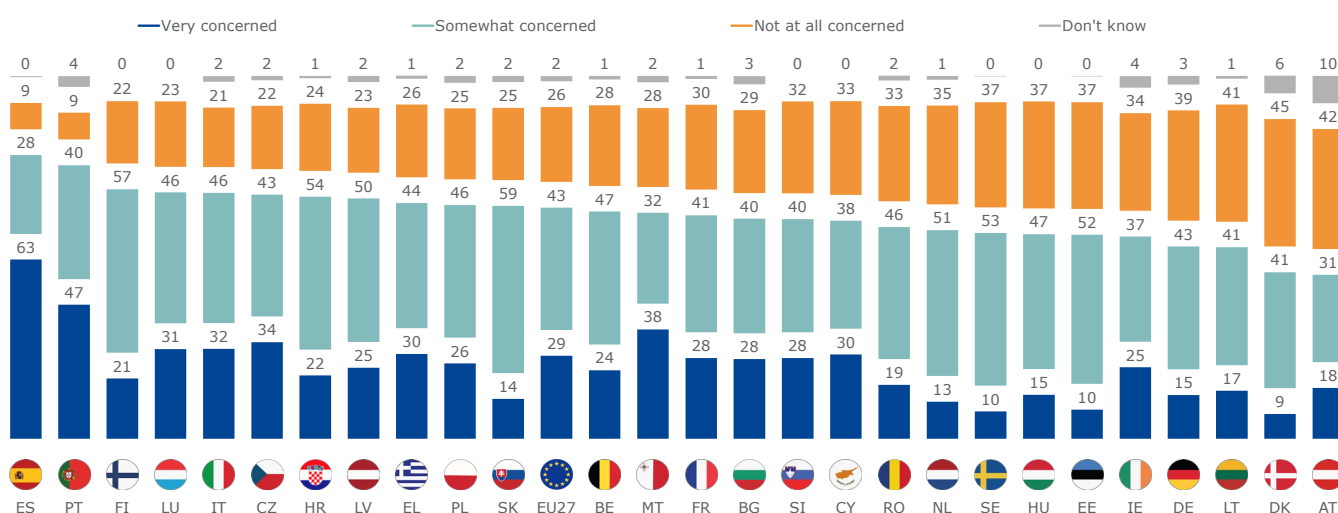


Base: all SMEs (n=12 863)

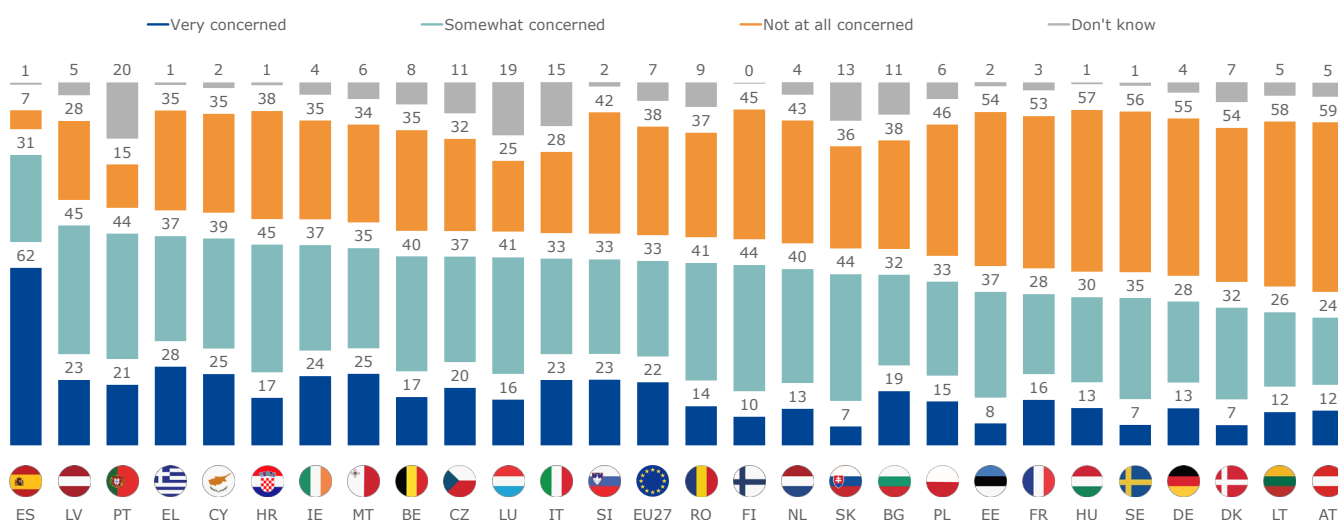
About half of SMEs surveyed in Austria and Poland say they are very or somewhat concerned about **viruses, spyware or malware (excluding ransomware)**. Across all other countries, a majority of SMEs is concerned about this type of cybercrime, with respondents Portugal and Spain – once again – being the most likely to express concern. In these two countries, respondents are also the most likely to say they are ‘very concerned’ (47% and 63%, respectively). In Denmark, Estonia and Sweden, in contrast, about one in ten SMEs is ‘very concerned’.

Across most countries, a smaller share of SMEs say they are very or somewhat concerned about **ransomware**, with the proportion being concerned ranging from 36% in Austria to 68% in Latvia; Spain stands out with 93% of concerned SMEs. The proportion of SMEs being ‘very concerned’ about ransomware remains below a quarter in 23 of the 27 Member States.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
Viruses, spyware or malware (excluding ransomware) (% by country)



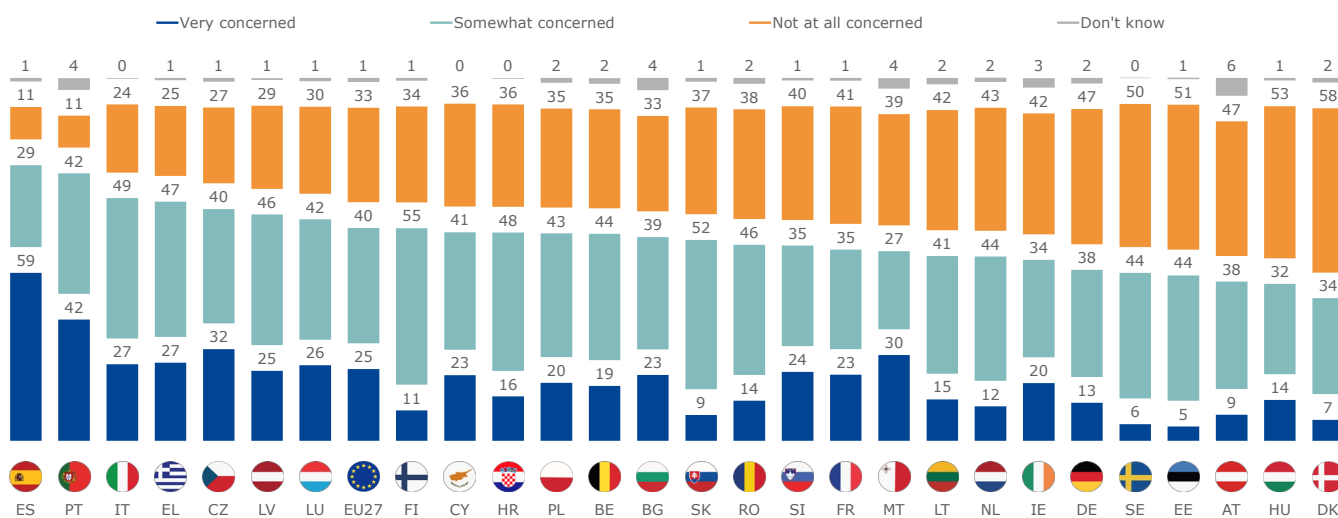
Ransomware (% by country)



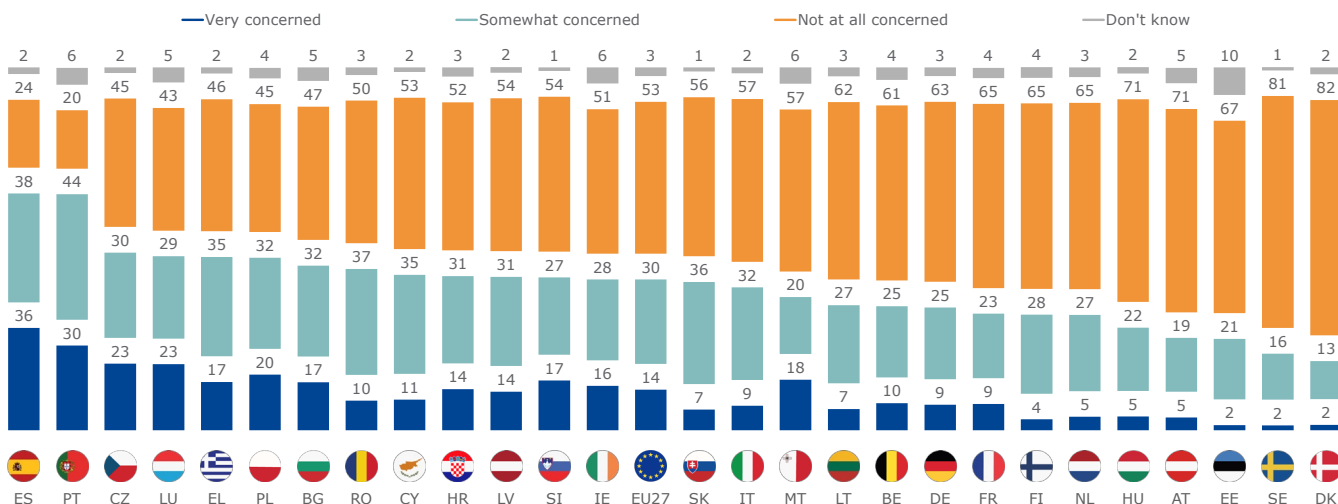
Base: all SMEs (n=12 863)

Between 41% of SMEs in Denmark and 88% in Spain are very or somewhat concerned about **unauthorised accessing of files or networks**. Portugal is again found close to Spain with more than eight in ten SMEs being concerned about this type of cybercrime. In Spain, respondents are also the most likely to say they are 'very concerned' (59%), while in Estonia, Sweden, Denmark and Slovakia, about one in ten SMEs is 'very concerned'. Across all countries, a smaller share of SMEs say they are very or somewhat concerned about **unauthorised listening in to video conferences or instant messages**. For example, in Croatia, 64% of SMEs are concerned about unauthorised accessing of files or networks and 45% about unauthorised listening in to video conferences or instant messages. Spain and Portugal stand out with 74% of SMEs that are concerned about unauthorised listening in to video conferences or instant messages.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
Unauthorised accessing of files or networks (% by country)



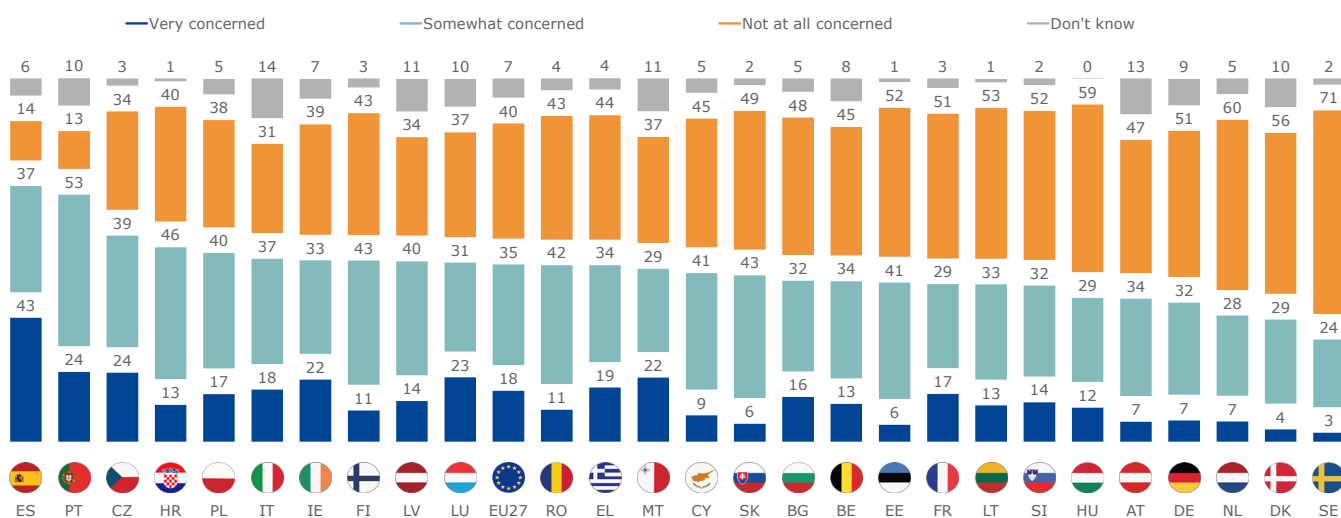
Unauthorised listening in to video conferences or instant messages (% by country)



Base: all SMEs (n=12 863)

In about 14 Member States, at least half of SMEs surveyed say they are very or somewhat concerned about **denial of service (DoS) attacks**. This concern is again most frequently voiced in Portugal (77%) and Spain (80%). In Sweden, on the other hand, about a quarter (27%) of SMEs are concerned about DoS attacks; in Denmark and the Netherlands, this applies to about a third of SMEs. The proportion of SMEs being very concerned about this type of attacks is the lowest in Sweden (3%), and then increases to 24% in Czechia and Portugal, and to 43% in Spain.

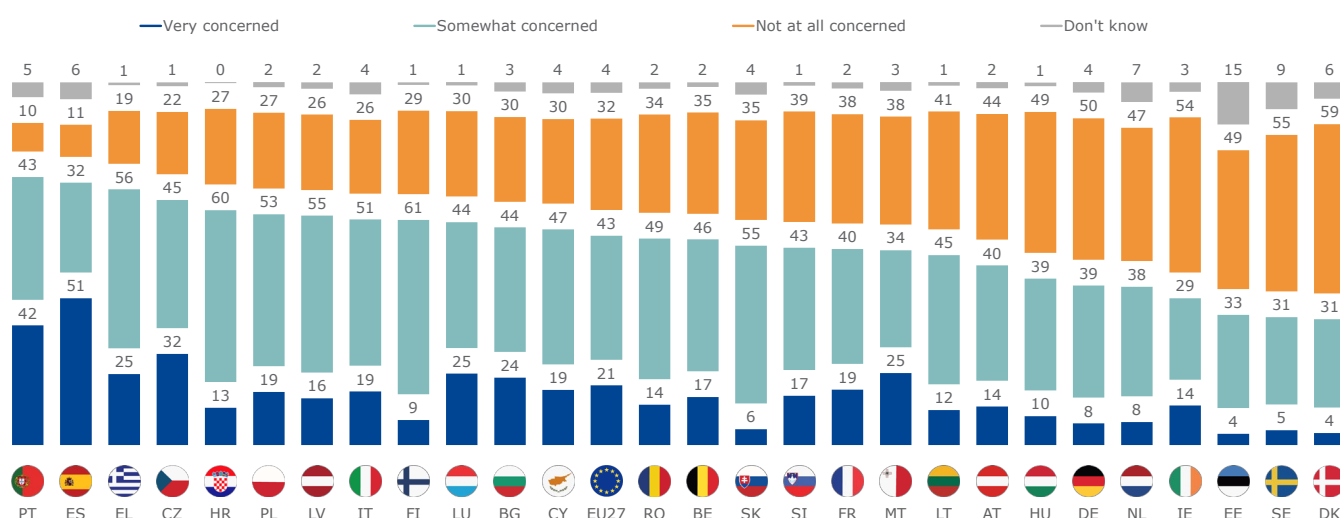
Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
Denial of service attacks (% by country)



Base: all SMEs (n=12 863)

In the survey, seven types of cybercrime were specifically named, but respondents were also asked if there are **any other types of breaches of attacks** that they are concerned about. In the countries at the lower end of the country ranking, less than four in ten SMEs are very or somewhat concerned about other types of cybercrime: 35% in Denmark, 36% in Sweden and 37% in Estonia. In the countries at the higher end of the country ranking, the proportion of SMEs being concerned is about 80%: Greece (81%), Spain (83%), Portugal (85%). The proportion of SMEs who report being 'very concerned' about another type of breach of attack ranges from 4%-5% in Denmark, Estonia and Sweden to 51% in Spain.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
Any other breaches or attacks (% by country)































Base: all SMEs (n=12 863)

The table on the following page presents, **on a country-by-country basis, the proportion of SMEs that report being ‘very concerned’** for each of the types of cybercrime listed in the survey. The higher the proportion of ‘very concerned’ SMEs, the darker blue the cell in the table. For each country, there is also one cell shaded green; this is the response that is selected most frequently by SMEs in the country.

Concern about the various types of cybercrime tends to be **higher in Portugal and (especially) Spain, but is lower in Denmark, Estonia and Sweden**. By way of example, the share of SMEs that are ‘very concerned’ about hacking (or attempts to hack) online bank accounts ranges from 7% in both Estonia and Sweden, and 8% in Denmark, to 55% in Portugal and 72% in Spain. Likewise, the proportion of SMEs that are ‘very concerned’ about phishing, account takeover or impersonation attacks is highest in Spain (71%), followed by Portugal (43%), and is the lowest in Denmark and Estonia (both 7%), and Sweden (12%), which are this time joined by Slovakia (also 12%).

The table on the next page also identifies for each country **the type of cybercrime with the highest proportion of SMEs that report being ‘very concerned’**. In line with the EU average results, in 12 Member States, the largest share of ‘very concerned’ responses is observed for hacking (or attempts to hack) online bank accounts (from 22% in Romania to 72% in Spain). In Cyprus and Slovakia, an equal proportion of SMEs report being ‘very concerned’ about hacking (or attempts to hack) online bank accounts and viruses, spyware or malware (excluding ransomware) (30% in Cyprus and 14% in Slovakia). The latter type of cybercrime receives the highest rate of ‘very concerned’ responses in seven Member States (from 9% in Denmark to 26% in Poland). In Germany, SMEs are as likely to be very concerned about viruses, spyware or malware (excluding ransomware) as they are very concerned about phishing, account takeover or impersonation attacks (both 15%). The latter type of cybercrime is ranking the highest in five Member States (from 12% in Sweden to 38% in Italy).

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
(% **'very concerned'** by country)

		Hacking (or attempts to hack) online bank accounts	Phishing, account takeover or impersonation attacks	Viruses, spyware or malware (excluding ransomware)	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27		32	31	29	25	22	18	14	21
BE		25	26	24	19	17	13	10	17
BG		31	25	28	23	19	16	17	24
CZ		39	38	34	32	20	24	23	32
DK		8	7	9	7	7	4	2	4
DE		12	15	15	13	13	7	9	8
EE		7	7	10	5	8	6	2	4
IE		31	29	25	20	24	22	16	14
EL		38	34	30	27	28	19	17	25
ES		72	71	63	59	62	43	36	51
FR		29	28	28	23	16	17	9	19
HR		21	18	22	16	17	13	14	13
IT		37	38	32	27	23	18	9	19
CY		30	22	30	23	25	9	11	19
LV		36	28	25	25	23	14	14	16
LT		25	14	17	15	12	13	7	12
LU		32	35	31	26	16	23	23	25
HU		13	13	15	14	13	12	5	10
MT		41	31	38	30	25	22	18	25
NL		12	17	13	12	13	7	5	8
AT		14	16	18	9	12	7	5	14
PL		23	23	26	20	15	17	20	19
PT		55	43	47	42	21	24	30	42
RO		22	20	19	14	14	11	10	14
SI		31	20	28	24	23	14	17	17
SK		14	12	14	9	7	6	7	6
FI		18	18	21	11	10	11	4	9
SE		7	12	10	6	7	3	2	5

The higher the proportion of 'very concerned' SMEs, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: all SMEs (n=12 863)

Respondents who consider themselves to be **well informed** about cybercrime are less concerned about each of the types of cybercrime listed in the survey than those who do not feel informed. For example, 38% of those who do *not* feel informed are 'very concerned' about hacking (or attempts to hack) online bank accounts, compared to 29% of those who consider themselves informed. A similar observation can be made when looking at how well **employees are informed about cybercrime**: respondents that indicate that their employees are well informed about cybercrime are less likely to be very concerned about most of the types of cybercrime. For example, 35% of respondents who think that the employees in their SMEs are not well informed about the risks of cybercrime say they are very concerned about phishing, account takeover or impersonation attacks; compared to 30% of respondents who feel that their employees are well informed about cybercrime.

Concern about cybercrime tends to be higher among SMEs that use more **online tools**. For example, 20% of SMEs that use five or more online tools are 'very concerned' about denial of service (DoS) attacks, compared to 12% of those that do not use any of these tools or don't know if they use these. The corresponding figure for SMEs that use one or two tools is 16% and it is 17% for those that use three to four tools. A similar observation can be made for SMEs that have employees who use **personally owned devices**, such as smartphones, tablets, laptops or desktop computers, **to carry out regular business-related activities**. For example, among these SMEs, 32% report being very concerned about viruses, spyware or malware (excluding ransomware); this figure is 27% for SMEs with no employees using personally owned devices.

The next chapter of this report looks at the proportion of SMEs that, in the past 12 months, became a victim of each of the types of cybercrime discussed in this section. The table on the next page shows that **SMEs that have experienced at least one type of cybercrime in the past 12 months** are more likely to report being 'very concerned' about the risks of cybercrime. Moreover, the proportion of SMEs reporting being very concerned increases with the number of times an SME has fallen victim of different types of cybercrime. For example, 19% of SMEs that have not experienced any type of cybercrime in the past 12 months answer that they are very concerned about ransomware; this figure increases to 25% of SMEs that have been victim to one type of cybercrime in the past 12 months and to 35% for SMEs that have been a victim of more than one type of cybercrime in this timeframe. In line with this finding, it can also be seen that, among SMEs that have become a victim of cybercrime in the past 12 months, those reporting that **their business was impacted by this crime⁶** are more likely to be very concerned about the different types of cybercrime than those that have not seen any impact. For example, 24% of the former, compared to 15% of the latter, are very concerned about unauthorised listening in to video conferences or instant messages

⁶ SMEs that have experienced at least one type of cybercrime were asked to report how their business impacted for the most serious incident; the response options included, for example, loss of revenue, repair costs and reputation damage. The results for this question are discussed in Section 4.3.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
(% **'very concerned'** by responses on various questions)

	Hacking (or attempts to hack) online bank accounts	Phishing, account takeover or impersonation attacks	Viruses, spyware or malware (excluding ransomware)	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27	32	31	29	25	22	18	14	21
Self-reported level of information about cybercrime (respondent)								
Not well informed	38	35	34	27	24	20	16	24
Well informed	29	30	27	24	21	17	14	20
Self-reported level of information about cybercrime (employees)								
Not well informed	36	36	33	27	25	19	16	23
Well informed	31	30	28	26	21	18	14	21
Online tools being used in the SME								
None	25	20	20	17	19	12	12	15
One or two tools	30	27	26	23	19	16	13	21
Three or four tools	32	33	31	25	22	17	13	21
Five or more tools	32	33	30	27	24	20	16	21
Personally owned devices for business activities								
No	30	30	27	23	21	17	13	20
Yes	34	33	32	27	23	19	16	22
Experienced at least one type of cybercrime in the past 12 month								
No	28	27	25	22	19	15	12	18
Yes, one type	38	40	35	30	25	22	19	26
Yes, more than one type	41	47	46	37	35	29	23	33
Cybercrime impact on business (among SMEs that experienced at least one type of cybercrime in the past 12 month)								
No	33	38	33	29	23	20	15	23
Yes	43	47	43	35	32	29	24	31

Base: all SMEs (n=12 863)

The analysis by company characteristics shows that the level of concern about cybercrime tends to be similar among different types of SMEs. Nevertheless, some noteworthy observations can be made.

Generally speaking, across the types of cybercrime, SMEs of **different sizes** are equally concerned about cybercrime. At the level of specific types of cybercrime, however, some significant differences are visible. SMEs with less than 10 employees are more concerned about hacking (or attempts to hack) online bank accounts – 32% of are ‘very concerned’ about this, compared to 27% of SMEs with 10 to 49 employees and 25% of those with 50 to 249 employees. On the other hand, larger SMEs are more concerned about ransomware – 26% of SMEs with 50 to 249 employees are very concerned about this, compared to 21% to 22% of SMEs with less than 10 or with 10 to 49 employees.

At the **sector level**, SMEs active in industry (NACE sectors B, D, E and F) are somewhat more concerned about cybercrime compared to SMEs active in manufacturing (NACE sector C) and, even more so, compared to SMEs in retail (NACE sector G) and services (NACE sectors H, I, J, K, L, M, N, P, Q and R). For instance, 27% of SMEs in the industry sector are ‘very concerned’ about other types of breaches or attacks versus 19% of SMEs active in services and 21% of SMEs in both the manufacturing and retail sectors.

Older SMEs, with 11 or more **years of activity**, on average, are slightly more concerned about cybercrime compared to SMEs that have been in operation for a shorter period of time, although differences are limited. For example, 24% of SMEs with 11 or more years of activity are ‘very concerned’ about ransomware, compared to 18%-19% of SMEs with less than one year, one to five years or six to ten years of activity.

SMEs with a **turnover** of between 500 000 to 2 million euros or more than 2 million euros tend to be somewhat less concerned about cybercrime than their counterparts with a lower turnover, especially when compared to those with a turnover of between 100 000 and 500 000 euros, although overall differences are again small. For example, 29% of both SMEs with a turnover of 500 000 to 2 million euros or more than 2 million euros are ‘very concerned’ about phishing, account takeover or impersonation attacks, versus 32% of SMEs with a turnover of up to 100 000 euros and 34% of those with a turnover of between 100 000 and 500 000 euros.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
(% **'very concerned'** by business characteristics)

	Hacking (or attempts to hack) online bank accounts	Phishing, account takeover or impersonation attacks	Viruses, spyware or malware (excluding ransomware)	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27	32	31	29	25	22	18	14	21
Company size								
<10 employees	32	31	29	26	22	18	15	22
10-49 employees	27	29	29	22	21	17	12	17
50-249 employees	25	32	30	25	26	16	12	19
Company turnover in 2020								
Up to €100,000	32	32	29	25	21	17	16	21
€100,001-€500,000	35	34	32	27	23	18	14	23
€500,001-€2,000,000	30	29	27	23	23	19	12	20
More than €2,000,000	31	29	28	23	22	15	11	17
Sector of activity								
Manufacturing	33	36	32	25	24	18	13	21
Industry	35	34	31	27	24	22	16	27
Retail	32	30	29	24	22	18	14	21
Services	30	30	28	25	21	17	14	19
Company age (years of activity)								
Less than one year	23	26	33	28	18	21	12	14
One to five years	30	29	25	24	19	17	18	20
Six to ten years	28	26	26	23	18	16	13	18
More than 10 years	33	32	30	26	24	18	14	22

Base: all SMEs (n=12 863)

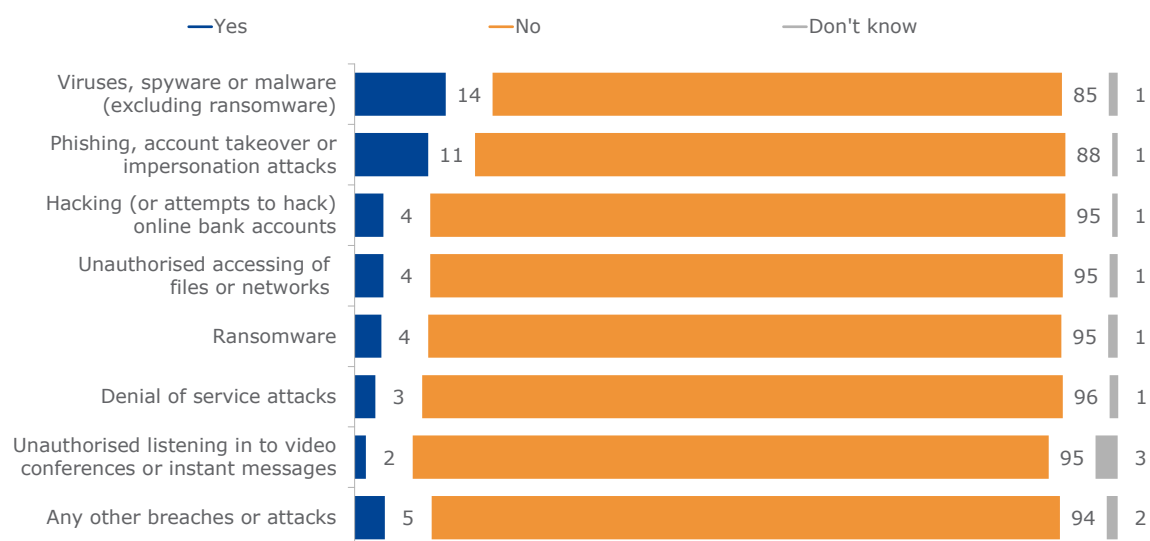
Section 4. Experience with cybercrime

4.1. Types of cybercrime experienced

The SMEs in this survey were also asked which of the listed types of cybercrime they have experienced in the last 12 months. The most prevalent type of cybercrime experienced during this timeframe is **viruses, spyware or malware** (experienced by 14% of SMEs in the last 12 months), followed by **phishing, account takeover or impersonation attacks** (11%).

The other types of cybercrime have incidence rates (for the past 12 months) of less than 5%, including hacking (or attempts to hack) online bank accounts, unauthorised accessing of files or networks and ransomware (all three experienced by 4% of SMEs in the last 12 months), denial of service (DoS) attacks (3%) and unauthorised listening in to video conferences or instant messages (2%). Lastly, 5% of SMEs surveyed have experienced 'another breach or attack' over the last 12 months.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)

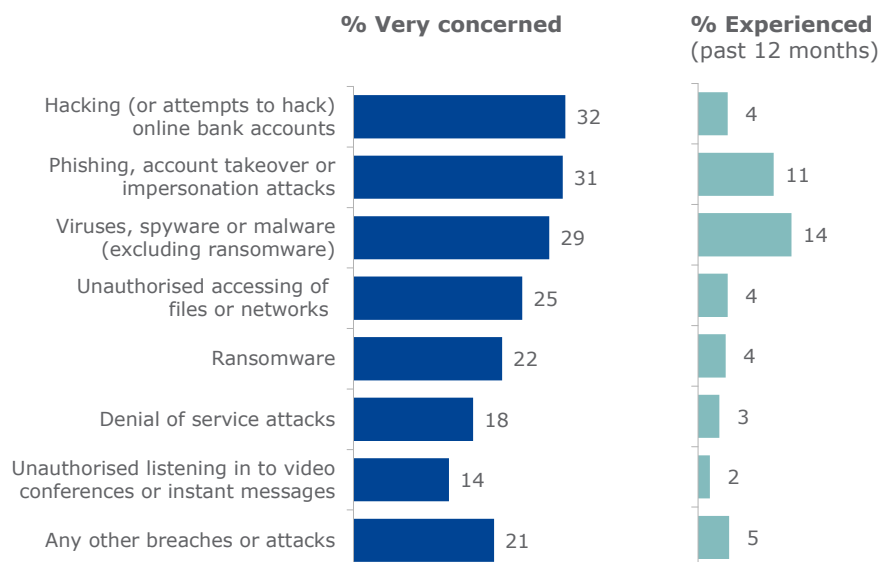


Base: all SMEs (n=12 863)

In the previous chapter, **SMEs' level of concern about different types of cybercrime** were compared. This analysis showed that approximately an equal share of SMEs are 'very concerned' about: (1) hacking (or attempts to hack) online bank accounts, (2) phishing, account takeover or impersonation attacks and (3) viruses, spyware or malware (between 29% and 32 'very concerned' responses). The latter two of these types of cybercrime are also the ones that SMEs are **most likely to have become a victim of: 11% for phishing, account takeover or impersonation attacks and 14% for viruses, spyware or malware (excluding ransomware)**. Fewer SMEs (4%) have fallen victim to hacking (or attempts to hack) online bank accounts, but the level of concern about this type of cybercrime is as high as for the other two types.

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?

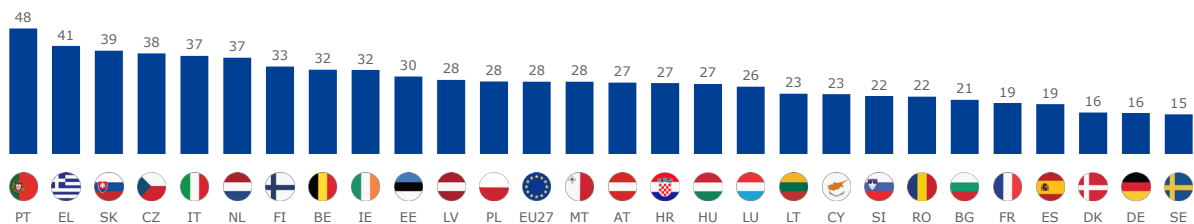
Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% EU27)



Base: all SMEs (n=12 863)

Aggregating all types of cybercrime, it is calculated that **28% of SMEs in the EU have experienced at least one of the listed types of cybercrime in the last 12 months**. At country level, the proportion of SMEs that have experienced at least one of these types of cybercrime in the last 12 months ranges from 15% in Sweden and 16% in both Denmark and Germany, to 48% in Portugal. Apart from Portugal, in five other countries, more than one in three surveyed SMEs experienced at least one type of cybercrime in the last 12 month: Greece (41%), Slovakia (39%), Czechia (38%), Italy (37%) and the Netherlands (both 37%).

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% **experienced at least one type of cybercrime**, by country)































Base: all SMEs (n=12 863)

With regard to the specific types of cybercrime experienced, **country differences are quite pronounced**. While in Czechia, 28% of SMEs surveyed have been fallen victim to viruses, spyware or malware (excluding ransomware) during the last 12 months, this applies to just 2% of their counterparts in Denmark. The share of SMEs that have experienced phishing, account takeover or impersonation attacks ranges from 4% in both Croatia and Spain, to 26% in Estonia and 27% in Greece.

There are also substantial country differences across countries for overall less prevalent types of cybercrime. For example, the proportion of SMEs that suffered from hacking (or attempt to hack) online bank accounts varies between 2% in Germany and Italy, and 12% in Greece. Unauthorised accessing of files or networks was encountered by 14% of SMEs in Portugal, compared to 1% of SMEs in Finland and Estonia. Ransomware was experienced by 11% of SMEs in Croatia, compared to 1% of those Denmark and Estonia.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% 'yes' by country)

		Viruses, spyware or malware (excluding ransomware)	Phishing, account takeover or impersonation attacks	Hacking (or attempts to hack) online bank accounts	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27		14	11	4	4	4	3	2	5
BE		16	20	4	4	5	4	0	4
BG		8	12	3	4	2	3	1	6
CZ		28	10	9	8	8	6	2	8
DK		2	10	3	2	1	1	0	2
DE		5	6	2	4	2	2	1	2
EE		6	26	4	1	1	1	0	2
IE		9	11	6	4	8	4	4	4
EL		16	27	12	4	7	3	3	8
ES		12	4	5	2	2	3	0	3
FR		12	6	3	2	3	1	1	3
HR		16	4	3	6	11	3	1	4
IT		17	15	2	5	4	2	2	4
CY		8	16	4	2	5	2	0	1
LV		13	12	6	8	6	4	1	7
LT		13	8	4	5	3	8	1	7
LU		12	7	6	8	5	3	4	3
HU		17	14	3	5	4	4	0	4
MT		10	12	4	3	3	3	4	2
NL		17	21	3	6	5	3	1	4
AT		5	6	6	3	2	6	3	4
PL		13	11	8	5	4	6	5	7
PT		21	14	9	14	9	8	6	10
RO		14	8	4	3	4	2	3	3
SI		12	8	3	5	8	2	2	4
SK		22	15	9	5	5	5	1	8
FI		11	20	3	1	6	5	0	5
SE		5	7	3	2	2	1	0	5

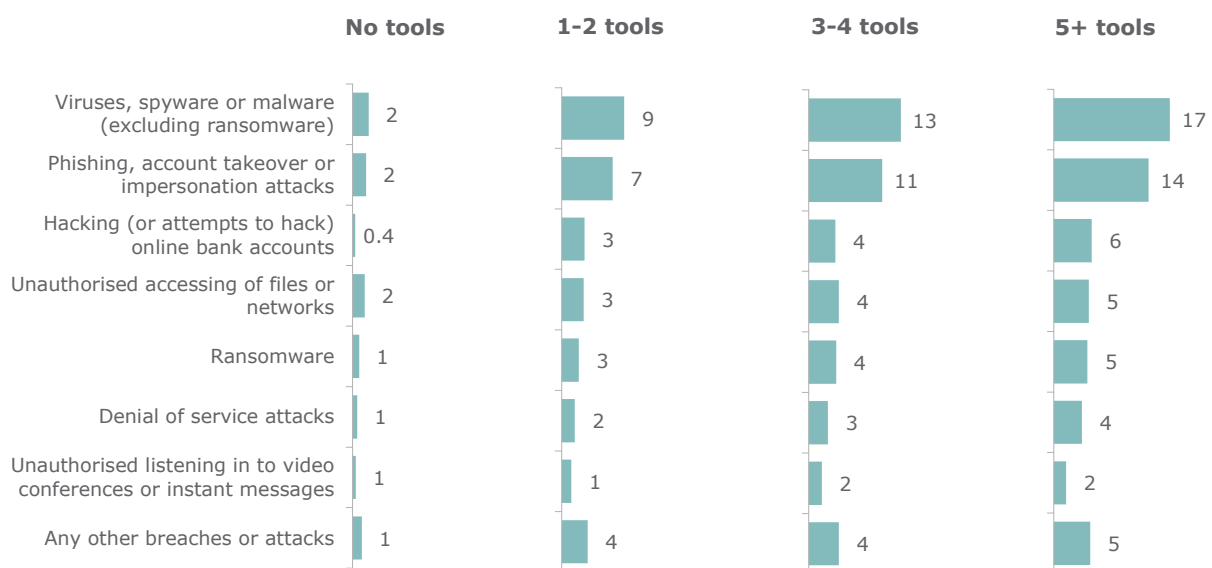
The more prevalent the type of cybercrime is, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: all SMEs (n=12 863)

SMEs that use more online tools are more likely to have experienced at least one type of cybercrime in the past 12 months. Just 6% of SMEs that use none of the online tools listed in the survey (or don't know if they use these) report having fallen victim to at least one type of cybercrime in the past 12 months. The corresponding figure for SMEs that use one or two tools is 19% and it is 29% for those that use three to four tools. Among SMEs that use five or more of the tools listed in the survey, 33% have experienced at least one of the types of cybercrime in the past 12 months.

Moreover, SMEs that use more online tools are more likely to have experienced each of the individual types of cybercrime. For example, 17% of SMEs that use five or more online tools have experienced viruses, spyware or malware in the last 12 months, compared to 13% of those that use three to four online tools and 9% of those that use one to two online tools. As may be expected, SMEs that do not use any of the listed online tools (or don't know if they use these) are by far the least likely to have experienced viruses, spyware or malware (2% of the latter say they have experienced viruses, spyware or malware).

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% by number of online tools used by the SME)



Base: all SMEs (n=12 863)

The table on the next page shows that differences in incidence for the different types of cybercrime tend to be much smaller when comparing SMEs with a **Bring Your Own Device (BYOD) practice** and those without. In total, across all types of cybercrime listed in the survey, 30% of SMEs with a BYOD policy have experienced at least one type of cybercrime in the past 12 months, compared to 25% that do not allow personally owned devices for work-related activities.

Differences in incidence rates also tend to be small for the two variables looking at self-reported level of information about cybercrime. There is a small, but significant, difference for phishing, account takeover or impersonation attacks: 9% of respondents who do *not* feel informed answer that they have been the victim of this type of attack in the past 12 months, compared to 12% for respondents who consider themselves informed.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% 'yes' by various questions)

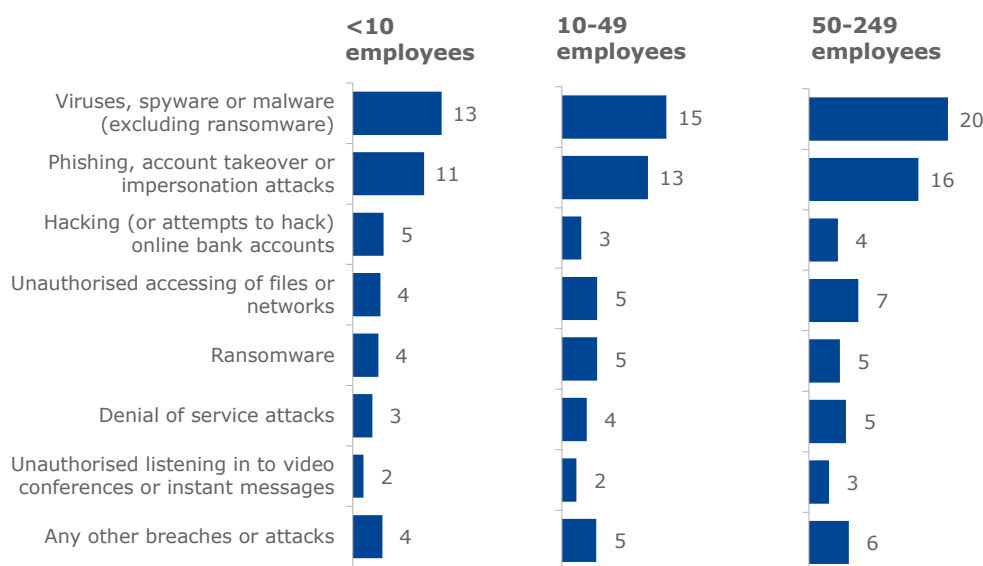
	Viruses, spyware or malware (excluding ransomware)	Phishing, account takeover or impersonation attacks	Hacking (or attempts to hack) online bank accounts	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27	14	11	4	4	4	3	2	5
Self-reported level of information about cybercrime (respondent)								
Not well informed	13	9	5	5	3	3	1	4
Well informed	14	12	4	4	4	3	2	5
Self-reported level of information about cybercrime (employees)								
Not well informed	14	9	5	4	4	3	2	4
Well informed	14	12	4	5	4	3	2	5
Personally owned devices for business activities								
No	12	10	4	3	4	2	1	4
Yes	15	12	5	6	4	4	2	5

Base: all SMEs (n=12 863)

The larger the SME (in terms of number of employees), the more likely it is to have become a victim to cybercrime in the past 12 months. Just over a quarter of SMEs with less than 10 employees have experienced at least one type of cybercrime in the past 12 months, this figure increases to 31% for SMEs with between 10 and 49 employees and to 38% for SMEs with between 50 and 249 employees.

The difference between SMEs of different sizes is particularly visible looking at the results for attacks with viruses, spyware or malware (excluding ransomware): 20% of SMEs with between 50 and 249 employees say they have experienced this in the last 12 months, compared to 13% and 15% of those with less than 10 and 10 to 49 employees, respectively. Similarly, 16% of SMEs with between 50 and 249 employees say they have experienced phishing, account takeover or impersonation attacks in the last 12 months, versus 11% of those with less than 10 employees and 13% of those with 10 to 49 employees.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% by company size)



Base: all SMEs (n=12 863)

There are also differences to be observed across **NACE sectors**. The last column in the table on the next page shows the proportion of SMEs in each NACE sector that have experienced at least one type of cybercrime in the past 12 months. The largest figure is seen for SMEs in the sector of information and communication (38%), followed by SMEs in human health and social work activities, in professional, scientific and technical activities, manufacturing, construction and water supply, sewerage, waste management and remediation (all between 29% and 33%).

There are also large differences across NACE sectors in the incidence for specific crimes; for example, while 5% of SMEs in mining and quarrying have experienced a phishing, account takeover or impersonation attack in the past 12 months, this figure is four times higher in the sector of information and communication (20%).

Across all sectors, in line with the average results, viruses, spyware or malware (excluding ransomware), and phishing, account takeover or impersonation attacks are the most common types of cybercrime. For example, in the sector of human health and social work activities, 14% of SMEs report having had issues with viruses, spyware or malware the past 12 months and 12% have experienced a phishing, account takeover or impersonation attack in that timeframe; the other types of cybercrime have been experienced by between 1% and 6% of SMEs in this sector.

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% 'Yes' by NACE sector)

	Viruses, spyware or malware (excluding ransomware)	Phishing, account takeover or impersonation attacks	Hacking (or attempts to hack) online bank accounts	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks	Experienced at least one type of crime
B - Mining and Quarrying	6	5	2	4	2	2	1	2	11
C - Manufacturing	14	13	5	6	4	3	3	7	30
D - Electricity, gas, steam and air conditioning supply	12	15	5	9	9	3	2	5	26
E - Water supply, sewerage, waste management and remediation	17	16	10	6	4	10	2	0	33
F - Construction	17	8	5	5	4	3	1	6	31
G - Wholesale and retail trade, repair of motor vehicles	14	11	4	4	4	4	2	5	27
H - Transportation and storage	11	6	4	2	2	2	2	4	22
I - Accommodation and food service activities	12	9	5	3	3	2	1	4	25
J - Information and communication	13	20	4	8	6	8	2	6	38
K - Financial and insurance activities	12	9	5	2	3	2	2	2	23
L - Real estate activities	9	11	2	2	5	2	0	1	22
M - Professional, scientific and technical activities	18	13	4	5	6	3	2	5	32
N - Administrative and support service activities	9	13	3	4	4	3	2	4	26
P - Education	9	8	2	4	4	1	4	4	23
Q - Human health and social work activities	14	12	3	6	4	2	1	3	29
R - Arts, entertainment and recreation	7	9	6	2	2	3	1	3	19

The more prevalent the type of cybercrime is, the **darker blue** the cell. The most-frequently selected response for each NACE sector is shown in **green**

Base: all SMEs (n=12 863)

Differences in incidence rates tend to be small, and non-significant, when comparing SMEs in terms **years of activity** and in terms of different amounts of **turnover**. Only one difference reaches statistical significance: while 15% of SMEs that have been active for more than 10 years report having had issues with viruses, spyware or malware (excluding ransomware) in the past 12 months, this figure is lower among SMEs active for less than 10 years (between 8% and 11%).

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months? (% 'yes' by business characteristics)

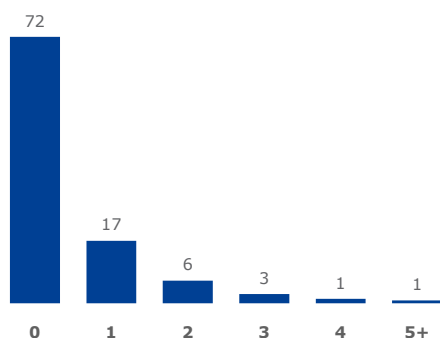
	Viruses, spyware or malware (excluding ransomware)	Phishing, account takeover or impersonation attacks	Hacking (or attempts to hack) online bank accounts	Unauthorised accessing of files or networks	Ransomware	Denial of service attacks	Unauthorised listening in to video conferences or instant messages	Any other breaches or attacks
EU27	14	11	4	4	4	3	2	5
Company turnover in 2020								
Up to €100,000	15	11	6	5	4	3	2	5
€100,001-€500,000	15	11	5	5	4	3	2	5
€500,001-€2,000,000	12	13	4	5	5	4	2	4
More than €2,000,000	16	14	4	4	4	3	1	4
Company age (years of activity)								
Less than one year	8	16	2	3	4	6	6	5
One to five years	11	10	4	6	3	2	3	3
Six to ten years	11	11	5	4	3	4	1	4
More than 10 years	15	11	4	4	4	3	2	5

Base: all SMEs (n=12 863)

Analysis focussing on all cybercrimes reported

It was noted above that 28% of SMEs report having experienced at least one of the types of cybercrime listed in the survey in the past 12 months. Considering also the number of different types of crime experienced, it can be seen that 17% of SMEs have experienced one type of cybercrime in the past 12 months, 6% have experienced two types of cybercrime, 3% three types of cybercrime, 1% four types and 1% five or more types (see chart below).

Q7 Number of types of cybercrime experienced in the past 12 months (%)



Base: all SMEs (n=12 863)

In this survey, 12 863 SMEs have been interviewed, out of which 3 916 report having experienced at least one type of cybercrime.

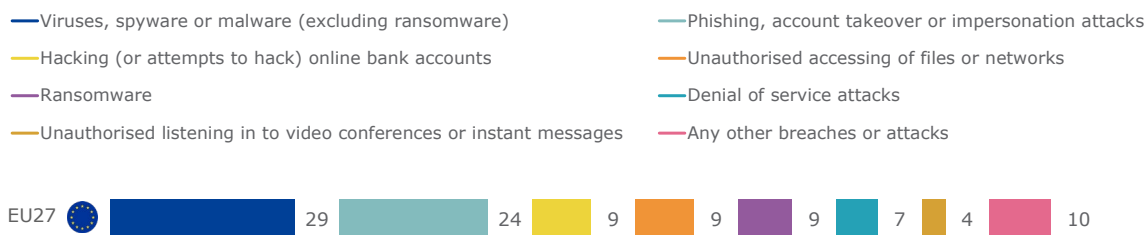
The **total number of cybercrimes reported** in the survey, however, is higher (given that a proportion of SMEs report more than one type). In the following analysis, the total number of crimes reported (n=5 971) is used as the basis for reporting. The analysis shows, out of all types of cybercrimes reported, which types have been experienced most frequently by SMEs.

Two types of cybercrime represent more than half of all cybercrime incidents experienced by SMEs:

- **viruses, spyware or malware** – accounting for 29% of the total number of crimes reported in the survey; and
- **phishing, account takeover or impersonation attacks** – accounting for 24% of crimes.

The other types of cybercrime individually account for less than a tenth of the cybercrimes reported in the survey. This includes 'hacking (or attempts to hack) online bank accounts', 'unauthorised accessing of files or networks' and 'ransomware' (which each account for 9% of all cybercrimes experienced), denial of service attacks (7%) and unauthorised listening in to video conferences or instant messages (4%). 'Any other breaches or attacks' make up 10% of all cybercrimes experienced.

Q7 Distribution of type of cybercrimes experienced by SMEs (% EU27)



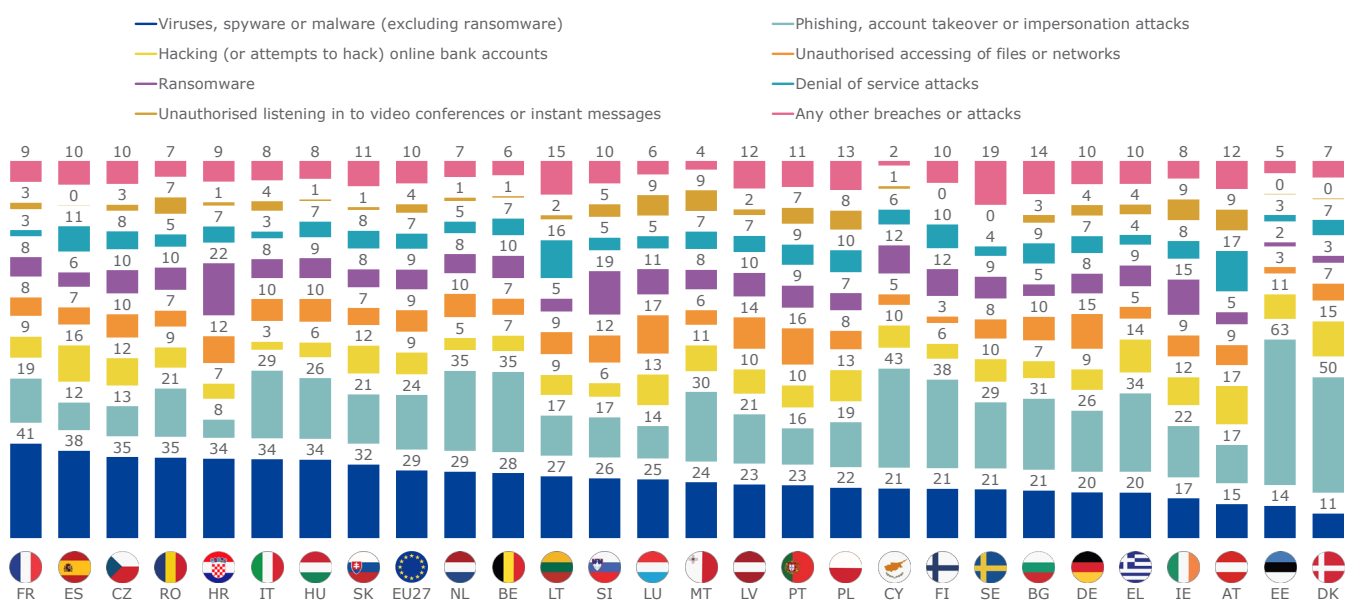
Base: all cybercrimes reported in the survey (n=5 971)

At the individual country level, one of the two most common types of cybercrime at EU level tends to predominate. In 14 out of 27 countries, **viruses, spyware or malware** are the most prevalent type of cybercrime encountered by SMEs over the past 12 months. In all but one of the remaining countries (12 out of 27), **phishing, account takeover or impersonation attacks** is the most encountered type of cybercrime over the last 12 months. The exception is Austria, where phishing, account takeover or impersonation comes in shared first place with hacking (or attempts to hack) online bank accounts and denial of service attacks.

Nonetheless, the relative weight of the two overall most prevalent types of cybercrime varies markedly across countries. Viruses, spyware or malware account for between 11% of crimes encountered in Denmark and 41% of crimes in France. The share of phishing, account takeover or impersonation attacks in the total number of cybercrimes experienced varies between 8% in Croatia and 63% in Estonia.

The relative weight of the other types of cybercrime also tends to diverge substantially across countries, in particular, the share of ransomware in the total of cybercrimes experienced. Ransomware accounts for 2% of the total in Estonia, but this proportion goes up to 19% in Slovenia and 22% in Croatia. The share of denial-of-service attacks in the total of cybercrimes experienced ranges from 3% in Estonia, France and Italy, to 16% in Lithuania and 17% in Austria.

Q7 Distribution of type of cybercrimes experienced by SMEs (% by country)

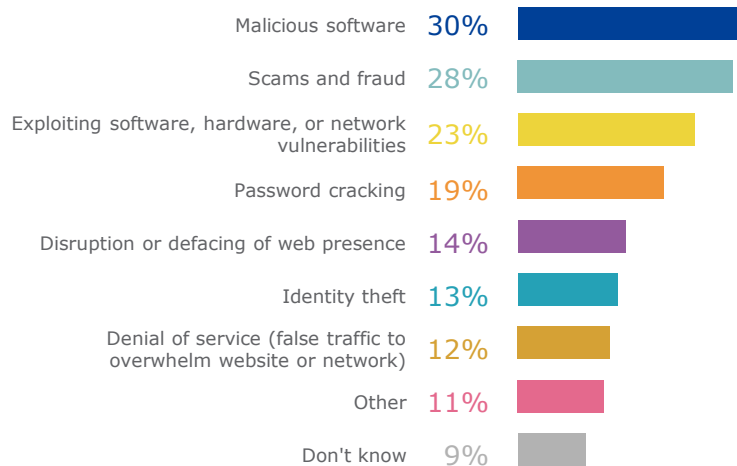


Base: all cybercrimes reported in the survey (n=5 971)

4.2. Characteristics of the most serious cybercrime incident

SMEs that have experienced at least one type of cybercrime in the last 12 months were asked **how the most serious of these cybercrime attacks was carried out**. Three in ten of these SMEs say this attack was carried out by means of **malicious software**, while a similar share (28%) say it was carried out using **scams and fraud**. Slightly fewer of these SMEs say the most serious incident was executed by exploiting software, hardware or network vulnerabilities (23%), or by password cracking (19%). Less frequently mentioned are disruption or defacing of web presence (14%), identity theft (13%), denial of service (12%) or other forms of attacks (11%).

Q8 Thinking about the most serious incident, how was this attack carried out? Multiple answers possible (% EU27)



Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

In 13 Member States, SMEs are most likely to mention **scams and fraud** as the method used for the most serious cybercrime attack they have experienced in the past 12 months; in 12 Member States, this is **malicious software**. In Italy, Hungary and Slovenia, the most commonly used method is 'exploiting software, hardware, or network vulnerabilities'. In Lithuania, 'denial of service' (false traffic to overwhelm website or network) is mentioned most frequently.

The proportion of SMEs reporting that the most serious cybersecurity attack they have experienced over the last 12 months was carried out using malicious software ranges from 10% in Denmark and 12% in Cyprus, to 52% in Spain. For scams and fraud, this figure ranges from 16% in France to 52% in Cyprus and 57% in Czechia. The share of SMEs reporting the most serious cybersecurity attack experienced over the last 12 months as being carried out by means of exploitation of software, hardware, or network vulnerabilities ranges from 3% in Cyprus to 42% in Slovenia.

Q8 Thinking about the most serious incident, how was this attack carried out? Multiple answers possible (% by country)

		Malicious software	Scams and fraud	Exploiting software, hardware, or network vulnerabilities	Password cracking	Disruption or defacing of web presence	Identity theft	Denial of service (false traffic to overwhelm website or network)	Other	Don't know
EU27		30	28	23	19	14	13	12	11	9
BE		31	33	19	17	12	22	14	18	8
BG		23	25	14	20	7	7	10	12	12
CZ		41	57	26	24	16	12	17	4	7
DK		10	39	18	14	5	17	12	19	13
DE		29	26	28	19	11	17	20	12	14
EE		19	34	22	3	4	4	9	18	20
IE		28	37	19	35	13	19	12	6	9
EL		36	26	15	20	13	5	14	16	1
ES		52	27	35	17	21	19	21	9	8
FR		24	16	8	9	15	13	4	7	20
HR		37	27	21	19	8	7	9	16	9
IT		20	21	35	26	15	10	5	11	4
CY		12	52	3	24	8	11	11	14	7
LV		24	30	23	16	16	11	17	12	10
LT		27	32	26	14	18	7	32	8	6
LU		34	27	25	22	21	14	13	12	15
HU		18	25	28	21	12	6	5	14	13
MT		15	45	12	29	11	24	15	9	4
NL		21	34	12	12	8	14	9	21	10
AT		33	21	15	15	3	23	22	10	0
PL		35	28	13	17	10	13	15	11	9
PT		37	22	21	21	15	19	14	2	8
RO		38	26	29	28	24	16	21	15	8
SI		19	34	42	8	22	16	9	9	4
SK		35	34	15	15	15	14	20	9	12
FI		22	37	15	9	5	12	9	17	13
SE		29	38	17	12	9	24	9	28	2

The higher the proportion of SMEs selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

Analysis by company characteristics shows that the characteristics of the most serious cybercrime attack experienced are similar for different types of SMEs. One difference, however, is noteworthy: large SMEs, both in terms of number of employees and turnover, are more likely than smaller SMEs to reply that the most serious cybercrime incidence they have experienced in the past 12 months involved identity theft. This response is given by 18% of SMEs with between 50 and 249 employees and/or with a turnover of more than 2 million euros, compared to between 11% and 16% of smaller SMEs.

Q8 Thinking about the most serious incident, how was this attack carried out? Multiple answers possible (% by business characteristics)

	Malicious software	Scams and fraud	Exploiting software, hardware, or network vulnerabilities	Password cracking	Disruption or defacing of web presence	Identity theft	Denial of service (false traffic to overwhelm website or network)	Other	Don't know
EU27	30	28	23	19	14	13	12	11	9
Company size									
<10 employees	30	28	23	20	14	13	12	11	9
10-49 employees	31	27	22	17	12	15	10	12	6
50-249 employees	33	24	21	16	9	18	11	11	10
Company turnover in 2020									
Up to €100,000	32	26	26	22	14	11	12	9	10
€100,001-€500,000	32	30	24	20	18	14	10	11	7
€500,001-€2,000,000	24	34	17	15	10	16	12	13	8
More than €2,000,000	32	27	22	15	11	18	9	10	9
Sector of activity									
Manufacturing	27	30	21	14	13	16	9	15	8
Industry	35	28	19	21	16	13	13	6	11
Retail	28	26	21	20	14	13	11	13	8
Services	30	28	25	19	13	13	13	11	9
Company age (years of activity)									
Less than one year*	15	32	48	22	17	29	23	5	4
One to five years	29	22	21	21	22	17	13	14	8
Six to ten years	27	35	23	24	15	12	16	9	8
More than 10 years	31	27	23	18	12	13	11	12	9

Note: * results based on less than 50 interviews

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

4.3. Impact on business from the most serious cybercrime incident

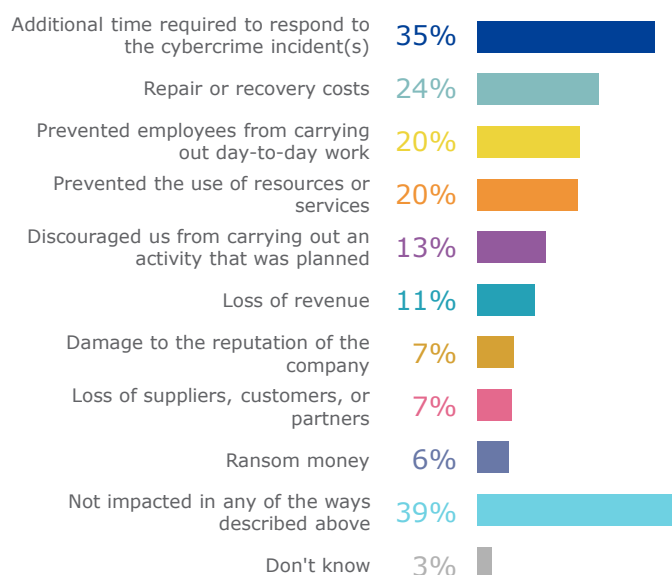
SMEs that indicated to have been the victim of at least one type of cybercrime in the last 12 months were asked how the most serious incident they have experienced affected their business; they were presented with a list of nine possible way that that their business could have been impacted.

The results of this question show that, overall, **more than half (58%) of SMEs that have experienced at least one type of cybercrime also suffered from some kind of impact on their business.** The most prevalent impact mentioned is 'additional time required to respond to the cybercrime incident(s)' – 35% of SMEs that have experienced cybercrime had to deal with this. About a quarter (24%) incurred repair or recovery costs. One in five (20%) note that the incident prevented employees from carrying out day-to-day work or prevented the use of resources or services. Slightly more than one in ten note that the most serious cybersecurity incident they have experienced discouraged them from carrying out an activity that was planned (13%); a similar share refers to a loss of revenue (11%).

Other potential effects were experienced by less than 10% of SMEs that experienced cybercrime in the last 12 months, including damage to the reputation of the company, and loss of suppliers, customers or partners (both 7%), and (the payment of) ransom money (6%).

Almost four in ten (39%) SMEs that had fallen victim to at least one type of cybercrime in the last 12 months answer that their **business was not impacted in any of the ways described in the survey.**

Q9 Still thinking about the most serious incident, how was your business impacted? Multiple answer possible (% EU27)



Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

At the country level, the proportions mentioning specific impacts vary significantly. The overall most prevalent impact, 'additional time required to respond to the cybercrime incident(s)', is mentioned, at the low end of the country ranking, by 14% of surveyed SMEs in Portugal and 15% in Hungary; in comparison, at the high end of the country ranking, 57% of surveyed SMEs in Sweden mention they have experienced this effect. The proportion of SMEs saying they incurred in repair or recovery costs because of the most serious cybercrime incident they have experienced in the last 12 months ranges from 9% of SMEs in Estonia and 10% of SMEs in Cyprus, to 33% of SMEs in Hungary, 34% in Ireland and 37% in Spain.

The proportion of SMEs saying that the most serious incident they have experienced in the last 12 months **did not impact their business** in any of the ways described ranges from 9% in Ireland to 60% in Estonia and 61% in Cyprus.

Q9 Still thinking about the most serious incident, how was your business impacted? Multiple answer possible (% by country)

		Additional time required to respond to the cybercrime incident(s)	Repair or recovery costs	Prevented employees from carrying out day-to-day work	Prevented the use of resources or services	Discouraged us from carrying out an activity that was planned	Loss of revenue	Damage to the reputation of the company	Loss of suppliers, customers, or partners	Ransom money	Not impacted in any of the ways described above	Don't know
EU27		35	24	20	20	13	11	7	7	6	39	3
BE		38	24	19	25	16	5	7	6	3	46	5
BG		28	14	15	12	6	7	2	6	0	42	5
CZ		51	31	23	20	15	16	11	11	7	31	2
DK		39	14	8	10	9	13	6	5	1	47	6
DE		41	27	15	15	21	9	1	5	0	40	8
EE		36	9	9	10	6	2	2	1	1	60	2
IE		32	34	23	14	23	19	15	18	12	9	5
EL		47	29	23	9	18	11	3	1	6	35	0
ES		32	37	30	35	19	26	14	7	7	24	5
FR		33	13	20	20	11	8	13	10	5	40	2
HR		22	27	21	18	25	11	13	4	13	33	5
IT		30	25	18	18	16	7	3	9	11	50	1
CY		23	10	13	6	6	7	8	3	1	61	3
LV		51	23	27	28	19	10	10	4	3	32	2
LT		54	31	38	23	42	15	12	12	1	24	2
LU		31	29	31	21	31	13	21	10	4	41	7
HU		15	33	28	18	5	10	2	2	2	39	3
MT		31	24	20	29	15	22	18	22	18	49	1
NL		34	17	13	14	3	6	5	2	2	46	4
AT		34	30	20	16	12	18	6	3	3	44	0
PL		35	14	14	11	4	9	8	3	2	44	5
PT		14	21	27	32	11	16	11	8	12	18	5
RO		50	24	21	31	11	16	9	18	1	28	3
SI		21	20	21	12	1	12	5	6	3	44	2
SK		45	29	24	25	21	14	9	6	11	39	1
FI		42	16	14	17	4	8	7	2	2	45	0
SE		57	13	33	31	13	21	10	4	0	35	5

The higher the proportion of SMEs selecting the type of impact, the **darker blue** the cell. The most-frequently selected impact for each country is shown in **orange**. For the response 'Not impacted', the darker shaded cells (**green**) are those of countries with a higher proportion of SMEs not having been impacted.

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

Analysis by company characteristics shows that generally different types of SMEs tend to be impacted by cybercrime to similar degrees. However, there are some important differences:

When focussing at the surveyed **SMEs' size**, it can be noted that SMEs with 50 to 249 employees are more likely than their smaller counterparts to say the most serious cybercrime incident they have experienced in the last 12 months had an impact: 28% of the latter say this incident did not impact them in any of the ways described, compared to 37% of those with 10 to 49 employees and 40% of those with less than 10 staff members. SMEs with 50 to 249 employees are particularly likely to say that the most serious incident prevented the use of resources or services (31% say so, versus 18% of SMEs with less than 10 employees and 25% in those with 10 to 49 employees), prevented employees from carrying out day-to-day work (34% vs 19% and 24%), or led to additional time required to respond to the cybercrime incident (45% vs 34% and 39%).

The differences between the **grouped sectors** tend to be minimal. An exception is the impact 'additional time required to respond to the cybercrime incident(s)', which is often reported by SMEs in the manufacturing sector (43% in this sector mention this, compared to 32% in the retail sector, 35% in the services sector and 31% in the industrial sector). 'Damage to the reputation of the company' is more likely to affect SMEs in the services sector (9% of the latter sector mention they have experienced this impact, versus 4% to 6% in the other sectors).

There is no noteworthy link between SMEs' **years of activity** and the impact on business of the most serious cybercrime incident experienced in the last 12 months. SMEs' **turnover** does seem to make a difference: SMEs with a large turnover are more likely to say that the most serious incident they have experienced prevented employees from carrying out day-to-day work (29% of SMEs with a turnover of more than 2 million euros say they suffered this impact, compared to 18%-20% of SMEs with a turnover of up to 100 000 euros, 100 000 to 500 000 euros, or 500 000 to 2 million euros).

Q9 Still thinking about the most serious incident, how was your business impacted? Multiple answer possible (% by business characteristics)

	Additional time required to respond to the cybercrime incident(s)	Repair or recovery costs	Prevented employees from carrying out day-to-day work	Prevented the use of resources or services	Discouraged us from carrying out an activity that was planned	Loss of revenue	Damage to the reputation of the company	Loss of suppliers, customers, or partners	Ransom money	Not impacted in any of the ways described above	Don't know
EU27	35	24	20	20	13	11	7	7	6	39	3
Company size											
<10 employees	34	23	19	18	13	11	7	7	6	40	3
10-49 employees	39	26	24	25	14	12	7	7	6	37	3
50-249 employees	45	28	34	31	13	12	8	5	7	28	2
Company turnover in 2020											
Up to €100,000	36	21	18	17	16	12	7	7	7	38	2
€100,001-€500,000	32	30	20	22	14	12	9	8	6	37	3
€500,001-€2,000,000	36	17	19	18	10	10	4	7	5	42	3
More than €2,000,000	36	24	29	22	11	9	7	4	6	35	4
Sector of activity											
Manufacturing	43	25	22	16	16	12	6	5	9	36	3
Industry	31	24	13	19	11	12	4	6	8	42	4
Retail	32	23	20	23	14	12	6	7	5	36	3
Services	35	23	22	19	13	10	9	7	6	41	2
Company age (years of activity)											
Less than one year*	41	33	26	10	20	14	16	17	1	44	0
One to five years	29	24	22	21	19	12	12	9	9	37	3
Six to ten years	37	21	17	17	11	11	9	8	7	38	2
More than 10 years	35	24	20	20	13	11	6	6	6	39	3

Note: * results based on less than 50 interviews

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months (n=3 916)

Section 5. Reporting of cybercrime incidents

This chapter looks at channels for cybercrime reporting and is divided in two sections. The first section presents the results of a question presented to SMEs that had experienced at least one type of cybercrime in the past 12 months. For each type of cybercrime experienced, respondents were asked **who, if anyone, they have reported the incident to**. The second section presents the results of **a similar – but hypothetical – question** presented to SMEs that had not experienced any type of cybercrime in the past 12 months. For each type of cybercrime, respondents in this group were asked who they would report the incident to if they were to experience the crime.

5.1. Reporting cybercrime (actual experience)

When analysing across all crimes experienced by the SMEs surveyed, it can be observed that SMEs **are most likely not to have reported these incidents** – 44% of cybercrimes experienced were not reported to anyone. When cybercrimes were reported, they were most often reported to the police (18% of all incidents) or the seller or service provider (17%). A further 12% of cybercrimes were reported to the Internet service provider, 7% to another official authority, 4% to a business representative body or trade body and 3% to a consumer protection organisation. Slightly less than one in ten cybercrimes (7%) were reported to ‘someone else’.

Q10a Who, if anyone, did you report this incident to? Multiple responses possible (% EU27)

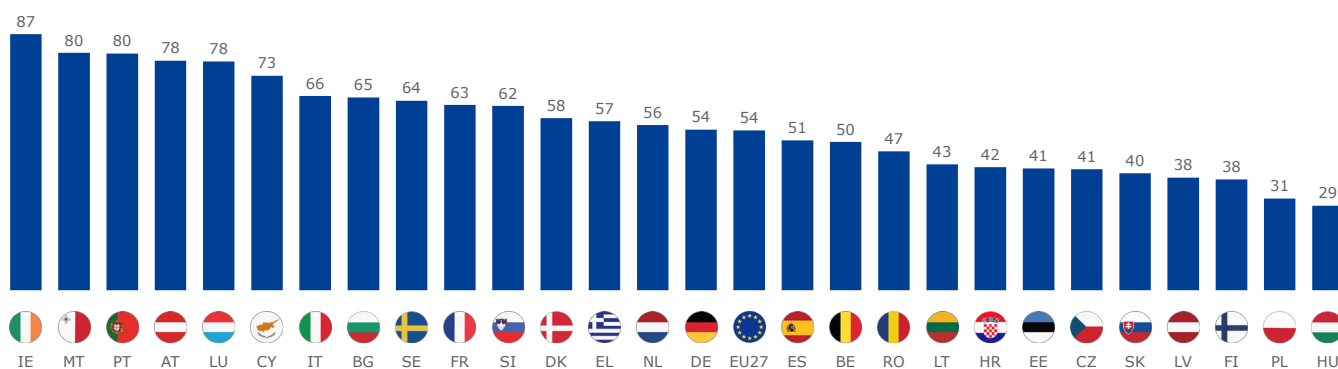
	Did not report to anyone	Total 'Reported to someone'	The police	Seller or service provider	Your Internet service provider	Another official authority	A business representative body or trade body	A consumer protection organisation	Someone else	Don't know
Total	44	54	18	17	12	7	4	3	7	2
Viruses, spyware or malware (excl. ransomware)	52	46	11	17	13	4	3	1	7	2
Denial of service attacks	35	60	21	14	21	9	7	5	8	5
Hacking (or attempts to hack) online bank accounts	38	60	21	21	12	10	4	3	10	2
Phishing, account takeover or impersonation attacks	40	56	19	17	9	9	4	2	8	3
Ransomware	44	54	23	12	8	7	4	2	10	2
Unauthorised accessing of files or networks	40	58	20	16	14	7	5	8	6	2
Unauthorised listening in to video conferences or IM	37	60	21	10	20	7	9	6	5	3
Any other breaches or attacks	41	57	24	18	13	4	4	3	7	2

*The higher the proportion selecting a response option, the **darker blue** the cell*
Base (Total): all cybercrimes reported in the survey (n=5 971)

Across most types of cybercrime, between 54% and 60% of incidents were reported to someone – the police, a seller or service provider etc. This proportion, however, is lower for **viruses, spyware or malware (excl. ransomware)** – of these incidents **46% was reported to someone**.

The chart below shows the **variation across countries** in the proportion of incidents reported to someone. In Ireland, for 87% of cybercrime incidents reported during the survey, respondents reply that they reported the incident to someone – e.g. the police, their service provider or official authority etc. This also applies to about 80% of incidents in Luxembourg, Austria, Portugal and Malta. In Hungary and Poland, on the other hand, for about 30% of incidents reported during the survey, respondents reply that they reported the incident to someone.

Q10a Who, if anyone, did you report this incident to? Multiple responses possible
(% **Total 'Reported to someone'**, by country)































Base: all cybercrimes reported in the survey (n=5 971)

In 21 Member States, the **most frequently given response is that the incident experienced was not reported to anyone**. This includes, for example, Hungary and Poland, where 71% and 64%, respectively, of cybercrimes were not reported to anyone. At the other end of the country ranking, in Ireland, just 7% of cybercrimes were not reported to anyone.

The share of cybercrimes **reported to the police** ranges from 4% in Slovakia, 6% in Finland and 7% in Latvia, to 36% in Slovenia and 38% in Ireland. The share of cybercrimes reported to an **Internet service provider** also differs substantially across countries, ranging from 4% in Denmark, 5% in Hungary and 6% in Latvia, Poland and Spain, to 34% in Ireland and 35% in Luxembourg. Between 8% of incidents in Poland and Germany and 25% in France, Romania and Sweden have been reported to a **seller or service provider**.

Q10a Who, if anyone, did you report this incident to? Multiple responses possible
(% 'yes' by country)

		Did not report to anyone	Total 'Reported to someone'	The police	Seller or service provider	Your Internet service provider	Another official authority	A business representative body or trade body	A consumer protection organisation	Someone else	Don't know
EU27		44	54	18	17	12	7	4	3	7	2
BE		45	50	18	11	14	12	2	1	10	5
BG		30	65	9	15	23	3	25	3	3	4
CZ		58	41	11	13	11	2	1	1	9	1
DK		39	58	19	11	4	11	15	5	9	2
DE		43	54	27	8	12	2	9	4	5	2
EE		57	41	12	11	11	15	1	0	4	1
IE		7	87	38	18	34	19	10	13	8	6
EL		43	57	18	15	23	9	3	3	6	0
ES		49	51	25	14	6	2	3	3	15	0
FR		33	63	14	25	10	7	4	0	18	4
HR		57	42	19	11	17	4	1	1	1	1
IT		34	66	22	22	14	11	3	3	3	0
CY		25	73	29	23	25	15	2	0	6	2
LV		57	38	7	15	6	6	4	0	3	5
LT		56	43	8	12	13	5	1	0	13	1
LU		20	78	32	18	35	20	17	13	4	2
HU		71	29	6	9	5	3	4	0	6	0
MT		18	80	32	21	16	9	8	4	21	2
NL		40	56	17	21	11	5	6	0	10	4
AT		17	78	33	16	7	23	6	11	2	5
PL		64	31	14	8	6	2	1	0	6	5
PT		13	80	24	18	17	15	13	14	2	6
RO		52	47	10	25	9	9	6	4	5	1
SI		37	62	36	21	16	6	3	1	8	1
SK		59	40	4	15	16	6	0	0	8	2
FI		60	38	6	18	9	2	1	0	7	2
SE		33	64	29	25	20	0	3	0	8	3

The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: all cybercrimes reported in the survey (n=5 971)

5.2. Reporting cybercrime (hypothetical question)

SMEs that did not experience any type of cybercrime in the last 12 months were asked if, in case they were to experience or be a victim of a specific incident, to whom they would report the incident.

For all types of (hypothetical) cybercrime incidents, SMEs are by far most likely to say that they would report these to the police. This is especially the case with regard to phishing, account takeover or impersonation attacks and the hacking (or attempts to hack) online bank accounts, which more than seven in ten of these SMEs (73% and 72%, respectively) say they would report to the police. Apart from the police, SMEs are relatively likely to say they would report incidents to the seller or service provider or their internet service provider. For example, 31% say they would report the hacking (or attempts to hack) online bank accounts to their seller or service provider, while 25% say they would report viruses, spyware or malware (excluding ransomware) to their internet service provider. The other potential reporting channels are mentioned much less frequently.

The share saying that they would not report the incidents to anyone is at 10% or below for all types of incidents. For example, just 2% say they would not report hacking (or attempts to hack) online bank accounts to anyone, while 38% of SMEs that actually experienced such a hacking attempt did not report this to anyone (see section above).

Q10b If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Multiple responses possible (% EU27)

	Would not report to anyone	The police	Seller or service provider	Your Internet service provider	Another official authority	A business representative body or trade body	A consumer protection organisation	Someone else	Don't know
Viruses, spyware or malware (excl. ransomware)	10	50	27	25	11	8	6	8	4
Denial of service attacks	7	56	23	22	11	7	5	6	8
Hacking (or attempts to hack) online bank accounts	2	72	31	18	16	9	7	11	3
Phishing, account takeover or impersonation attacks	4	73	23	19	14	8	7	7	3
Ransomware	6	69	20	19	12	8	6	5	5
Unauthorised accessing of files or networks	6	62	25	21	12	9	7	6	5
Unauthorised listening in to video conferences or IM	9	62	20	18	11	7	6	5	8
Any other breaches or attacks	7	66	21	18	11	7	6	6	7

*The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for type of cybercrime is shown in **green***





























Base (per row): SMEs that have not experienced any type of cybercrime in the last 12 months (n=8 947)

At the country level, the police are the preferred entity to report cybercrime incidents to in almost all countries for almost all types of cybercrime (it should be stressed again that this refers to hypothetical incidents, not actually experienced incidents, which are reported in Section 5.1). This is, for example, the case with regard to phishing, account takeover or impersonation attacks and the hacking (or attempts to hack) online bank accounts, the results for these types are shown in the tables overleaf.

The proportion of SMEs that would report **hypothetical hacking (or attempts to hack) online bank accounts to the police** ranges from 55% in both Ireland and Latvia and 56% in Slovakia, to 81% in both Cyprus and Spain. The share of SMEs that would **report phishing, account takeover or impersonation attacks to the police** is the smallest in Ireland (52%), Hungary and Malta (both 56%), and the largest in Croatia and Poland (both 84%).

Q10b If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Multiple responses possible

Hacking (or attempts to hack) online bank accounts (% 'yes' by country)





























		Would not report to anyone	The police	Seller or service provider	Your Internet service provider	Another official authority	A business representative body or trade body	A consumer protection organisation	Someone else	Don't know
EU27		2	72	31	18	16	9	7	11	3
BE		3	72	32	13	20	10	7	27	1
BG		3	66	24	11	17	15	7	5	5
CZ		3	59	36	14	12	3	2	7	2
DK		0	64	34	16	11	11	6	11	2
DE		4	78	29	27	27	18	13	5	5
EE		1	63	42	18	9	5	2	3	0
IE		1	55	23	15	14	18	8	4	11
EL		2	77	17	18	22	17	8	12	0
ES		2	81	24	15	15	8	8	5	2
FR		1	58	26	14	8	5	1	30	3
HR		3	73	30	18	14	6	4	2	2
IT		0	78	44	29	18	10	8	5	2
CY		1	81	25	24	25	8	5	3	2
LV		0	55	50	14	22	3	2	10	1
LT		3	73	25	13	27	6	3	5	2
LU		1	70	24	14	20	10	5	2	0
HU		3	57	43	5	22	4	1	5	2
MT		3	72	10	7	14	8	4	15	4
NL		3	63	48	9	7	10	4	16	1
AT		2	69	12	27	18	7	6	8	3
PL		2	84	25	8	6	5	3	8	1
PT		2	77	15	11	15	6	8	1	8
RO		2	76	47	24	29	22	29	4	7
SI		1	77	54	20	18	18	6	5	0
SK		2	56	38	17	19	2	4	6	2
FI		1	69	43	15	8	2	1	9	1
SE		2	69	29	16	8	10	4	23	3

The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: SMEs that have not experienced any type of cybercrime in the last 12 months (n=8 947)

Q10b If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Multiple responses possible

Phishing, account takeover or impersonation attacks (% 'yes' by country)

		Would not report to anyone	The police	Seller or service provider	Your Internet service provider	Another official authority	A business representative body or trade body	A consumer protection organisation	Someone else	Don't know
EU27		4	73	23	19	14	8	7	7	3
BE		4	73	24	14	17	11	7	14	2
BG		7	61	12	13	12	11	8	5	7
CZ		5	63	28	14	5	3	2	6	3
DK		2	59	33	19	9	11	6	11	3
DE		4	78	25	27	24	13	14	5	4
EE		7	68	14	20	9	3	2	3	0
IE		0	52	16	19	17	15	16	3	12
EL		3	79	18	20	17	10	8	5	1
ES		2	83	21	14	14	7	9	4	2
FR		3	67	17	15	8	6	1	14	3
HR		1	84	16	18	11	5	4	1	2
IT		3	72	42	31	19	12	8	4	3
CY		3	77	23	24	18	4	3	4	4
LV		7	64	26	16	19	2	2	6	3
LT		4	74	14	17	13	4	5	4	5
LU		1	71	19	23	17	11	5	1	0
HU		9	56	17	16	8	4	1	10	6
MT		2	56	10	12	11	3	7	12	7
NL		5	69	19	19	9	7	2	11	3
AT		2	69	10	33	15	7	6	8	4
PL		6	84	12	9	5	3	4	5	3
PT		3	74	15	14	11	6	7	3	7
RO		6	74	35	28	29	23	28	4	7
SI		4	78	20	21	10	10	7	7	2
SK		7	57	24	22	10	2	2	7	4
FI		4	74	26	15	8	3	0	7	1
SE		3	77	18	16	6	8	1	17	4

The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: SMEs that have not experienced any type of cybercrime in the last 12 months (n=8 947)

The **smallest SMEs**, in terms of number of employees, are more inclined than their larger counterparts to report hypothetical cybercrime to the police. For example, 74% of SMEs with less than 10 employees say they would report phishing, account takeover or impersonation attacks to the police, compared to 70% of those with 10 to 49 employees and 66% of those with 50 to 249 employees. Larger SMEs are more likely to say they would report hypothetical cybercrime to a 'business representative body or trade body' or 'someone else'. For example, whereas 12% of SMEs with 50 to 249 employees and 10% of SMEs with 11 to 49 employees would report phishing, account takeover or impersonation attacks to a business representative body or trade body, this applies to 8% of SMEs with less than 10 staff members. Similarly, 12% of SMEs with 50 to 249 employees and 9% of SMEs with 11 to 49 employees would report ransomware to someone else, compared to 5% of SMEs with less than 10 employees that would do the same.

SMEs active in the **manufacturing sector** are more prone to report hypothetical cybercrime to the seller or service provider compared to their counterparts in other sectors. For example, 38% of SMEs in the manufacturing sector would report the hacking (or attempts to hack) online bank accounts to the seller or service provider, compared to 30%-31% of SMEs in the retail, services and industry sectors that would do so.

SMEs with a **higher turnover** are more likely to report hypothetical cybercrime to the seller or service provider as well (including their internet service provider). For example, 27% of SMEs with a turnover of more than 2 million euros and 28% of SMEs with a turnover of 500 000 to 2 million euros would report phishing, account takeover or impersonation attacks to the seller or service provider, compared to 21% of those with a turnover of up to 100 000 euros and 22% of those with a turnover of 100 000 to 500 000 euros.

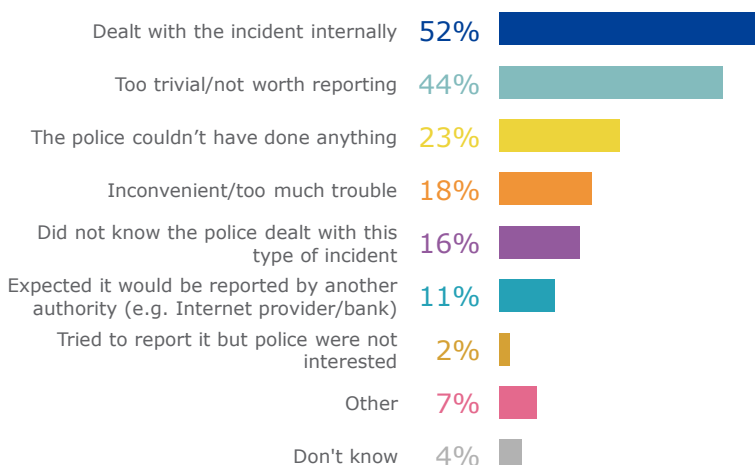
SMEs that use a larger number of **online tools** are more likely to report hypothetical cybercrime to their seller or service provider or internet service provider. By way of example, 27% of SMEs using five or more online tools and 25% of those using three to four online tools would report denial of service attacks to their seller or service provider, compared to 17% of those that use one to two online tools and 10% of those that use no online tools or that do not know which online tools they use.

5.3. Reasons for not reporting cybercrime to the police

SMEs that have experienced at least one type of cybercrime in the last 12 months and did not report the incident to the police were asked **why they did not do so**. In response, about half of these SMEs (52%) say that did not report the incident to the police because they **dealt with it internally**. Slightly fewer (44%) felt the incident was **too trivial / not worth reporting to the police**.

Other explanations for not reporting the incident to the police are mentioned less frequently: 23% felt the police could not have done anything, 18% found reporting 'inconvenient / too much trouble', 16% did not report because they did not know the police dealt with this type of incident and 11% expected it would be reported by another authority, such as an internet provider or bank. A small proportion (2%) say they tried to report the incident, but the police were not interested, while 7% say they did not report the incident to the police for 'other' reasons.

Q11 Why did you not report the incident (or incidents) to the police? Multiple answers possible (% EU27)



Base: SMEs that have experienced at least one type of cybercrime in the last 12 months, but did not report the incident to the police (n=3 183)





























In 19 Member States, the most common reason for not reporting a cybercrime incident experienced in the last 12 months to the police is that the **incident was dealt with internally**. In seven Member States, the most frequent reason given for not having reported to the police is that they felt the incident was **too trivial / not worth reporting**. In Luxembourg, SMEs that have experienced at least one type of cybercrime in the last 12 months and did not report the incident to the police are most likely not to have done so because they felt the police could not have done anything (44%).

The share of SMEs that have not reported an incident to the police because they **dealt with it internally** is the largest in Romania (76%), Lithuania and Slovakia (both 70%) and the smallest in Portugal (20%). The proportion of SMEs that feel that the incident was **too trivial to be worth reporting** ranges from 21% in Cyprus, 23% in Ireland and 25% in Austria, to 57% in Finland, 58% in Slovakia and 60% in Czechia. Between 1% of SMEs in France and 42% in Slovakia reply that reporting the incident to the police would have been **inconvenient or too much trouble**.

The proportion of SMEs that have not reported an incident to the police because, in their view, the **police could not have done anything** varies between 7% in Cyprus and 44%-45% in Luxembourg and Romania. In Luxembourg, 10% of these SMEs answer that tried to report to the police, but they were not interested; in Portugal and Ireland, this response is given by 7%-8%.

In five Member States, more than a fifth of SMEs that did not report an incident to the police because they **did not know the police dealt with this type of incident**: 28% in Romania, 22% in Czechia, Germany and Slovakia, and 21% in Greece. In Belgium, Latvia and Romania, about one in five of these SMEs expected that the incident would be reported to the police by another authority.

Q11 Why did you not report the incident (or incidents) to the police? Multiple answers possible
(% by country)

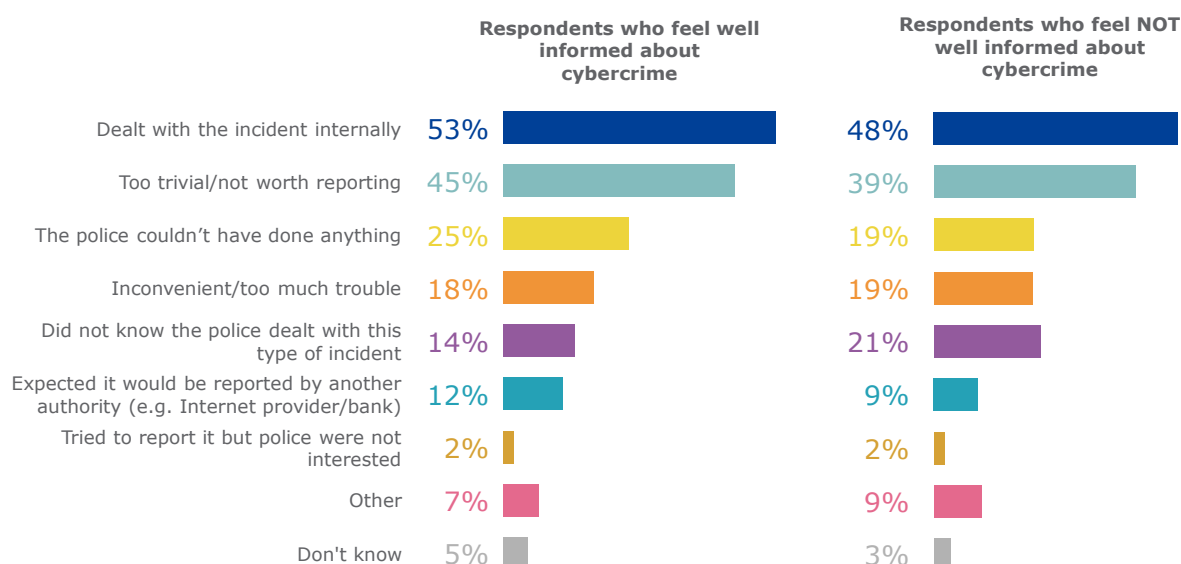
		Dealt with the incident internally	Too trivial/not worth reporting	The police couldn't have done anything	Inconvenient/too much trouble	Did not know the police dealt with this type of incident	Expected it would be reported by another authority	Tried to report it but police were not interested	Other	Don't know
EU27		52	44	23	18	16	11	2	7	4
BE		63	52	28	27	9	19	0	14	1
BG		48	27	29	8	14	5	0	13	4
CZ		68	60	35	29	22	16	0	7	1
DK		50	46	23	12	6	8	4	6	3
DE		47	52	37	24	22	16	0	14	10
EE		57	46	10	8	12	10	2	12	3
IE		38	23	25	9	17	2	7	5	8
EL		58	56	27	13	21	13	2	0	0
ES		57	33	14	12	9	18	0	19	0
FR		66	31	13	1	13	5	4	5	5
HR		32	56	28	4	17	7	2	7	0
IT		42	33	18	16	18	5	3	4	4
CY		59	21	7	5	4	5	0	16	0
LV		62	53	37	20	15	19	3	7	2
LT		70	48	25	18	16	14	2	6	3
LU		39	33	44	6	19	5	10	13	6
HU		37	52	15	9	10	13	0	3	3
MT		59	35	35	20	11	12	0	10	6
NL		41	49	31	19	13	12	3	10	7
AT		29	25	27	15	4	8	1	4	6
PL		61	56	24	31	7	10	2	9	4
PT		20	27	13	12	20	10	8	2	16
RO		76	53	45	38	28	22	3	8	5
SI		48	35	21	9	8	1	0	10	4
SK		70	58	24	42	22	18	1	7	4
FI		44	57	28	24	11	12	1	5	2
SE		48	50	39	21	19	16	0	9	8

The higher the proportion selecting a response, the **darker blue** the cell. The most-frequently selected response for each country is shown in **green**

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months, but did not report the incident to the police (n=3 183)

Respondents who **do not feel informed** about cybercrime are more likely than their counterparts who do feel informed to say they did not report a cybercrime incident because they did not know the police dealt with this type of incident (21% say so, versus 14% who feel informed).

Q11 Why did you not report the incident (or incidents) to the police? Multiple answers possible (% EU27)



Base: SMEs that have experienced at least one type of cybercrime in the last 12 months, but did not report the incident to the police - well-informed respondents (n=2 459) and not well-informed respondents (n=707)

The **largest SMEs** (in terms of employees) are more likely to mention as a reason for not reporting to the police a cybercrime incident experienced in the last 12 months the fact that 'they dealt with it internally' – 59% of SMEs with 50 to 249 employees cite this reason, compared to 51%-52% of SMEs with less than 10 or 10-49 employees. The smallest SMEs are more likely to have not reported a cybercrime incident to the police because they felt it was 'inconvenient / too much trouble' – 20% of SMEs with less than 10 employees mention this reason, compared to 11% of both those with 10 to 49 and 50 to 249 staff members.

SMEs from different **sectors** generally give similar reasons for not reporting a cybercrime incident to the police. SMEs in the services and industry sectors are, however, more likely than their counterparts in the retail sector to reply that they dealt with the incident internally (54% and 57%, respectively, of SMEs in the former two sectors say this, compared to 45% of those in the retail sector). Compared to SMEs in the manufacturing and retail sectors, SMEs in the industry sector are *unlikely* to say that they felt the incident was too trivial / not worth reporting to the police (32% of SMEs in the latter sector give this as a reason, compared to 53% of SMEs active in manufacturing sector and 48% active in retail sector).

The number of years SMEs have been active seems not to be linked to their reasons for not reporting a cybercrime incident to the police. SMEs' **turnover** does appear linked to the reasons for not reporting an incident to the police. SMEs with a lower turnover are more likely not to have reported a cybercrime incident to the police because they felt it was 'inconvenient / too much trouble'. This reply is given by 19%-21% of SMEs with a turnover of up to 100 000 euros or between 100 000 and 500 000 euros, compared to 16% of SMEs with a turnover of between 500 and 2 million euros and 11% of those with a turnover of more than 2 million euros. SMEs with a turnover of up to 100 000 euros or between 100 000 and 500 000 euros (12% and 14%, respectively) also reply that they did not report an incident to the police because they expected it would be reported by another authority (such as an internet provider/bank). In the category of SMEs with a turnover of between 500 and 2 million euros or more than 2 million euros, 6% provide this as a reason for not reporting to the police.

Q11 Why did you not report the incident (or incidents) to the police? Multiple answers possible
(% by business characteristics)

	Dealt with the incident internally	Too trivial/ not worth reporting	The police couldn't have done anything	Inconvenient / too much trouble	Did not know the police dealt with this type of incident	Expected it would be reported by another authority	Tried to report it but police were not interested	Other	Don't know
EU27	52	44	23	18	16	11	2	7	4
Company size									
<10 employees	52	43	24	20	16	12	2	8	4
10-49 employees	51	49	23	11	14	7	2	7	5
50-249 employees	59	45	20	11	15	10	3	6	8
Company turnover in 2020									
Up to €100,000	57	47	24	19	20	12	3	6	2
€100,001-€500,000	52	39	24	21	15	14	1	6	4
€500,001-€2,000,000	47	42	24	16	14	6	3	9	10
More than €2,000,000	50	49	20	11	11	6	1	5	6
Sector of activity									
Manufacturing	50	53	22	20	19	7	2	7	4
Industry	57	32	22	22	12	10	2	8	3
Retail	45	48	21	15	18	10	2	6	5
Services	54	43	26	18	15	13	3	8	5
Company age (years of activity)									
Less than one year*	25	62	39	0	10	16	0	0	9
One to five years	53	38	31	22	21	14	2	12	2
Six to ten years	56	44	20	22	16	13	2	6	7
More than 10 years	52	44	23	17	15	10	2	7	4

Note: * results based on less than 50 interviews

Base: SMEs that have experienced at least one type of cybercrime in the last 12 months, but did not report the incident to the police (n=3 183)

Technical specifications

Between 26 November and 17 December 2021, Ipsos European Public affairs carried out Flash Eurobarometer 496 at the request of the European Commission, Directorate-General for Migration and Home Affairs. It is a company survey coordinated by the Directorate-General for Communication, “Media monitoring and Eurobarometer” Unit.

Flash Eurobarometer 496 covers small and medium-sized enterprises, active in the manufacturing (NACE category C), retail (NACE category G), services (NACE categories, H, I, J, K, L, M, N, P, Q, R) and industry (NACE categories B, D, E, F) sectors within the European Union. Interviews took place with someone with decision-making responsibilities (managing director, general manager, CEO, financial director), someone leading the commercial activities (commercial manager, sales manager, marketing manager) or a legal officer. All interviews were carried via Computer-Assisted Telephone Interviewing (CATI).

The sample was selected from an international business database. Sampling targets were defined on both company size (using three different ranges: 1-9 employees, 10-49 employees and 50-249 employees) and sectors (industry, manufacturing, retail and services). These sampling targets were adjusted according to the country’s universe but were also reasoned in order to ensure that the sample was large enough in every cell.

Margin of error

Survey results are subject to sampling tolerances. The ‘margin of error’ quantifies uncertainty about (or confidence in) a survey result. As a general rule, the more interviews conducted (sample size), the smaller the margin of error. A sample of 500 will produce a margin of error of not more than 4.4 percentage points.

Statistical margins due to sampling tolerances (at the 95% level of confidence)

various sample sizes are in rows

various observed results are in columns

	5%	10%	25%	50%	75%	90%	95%
n=50	±6.0	±8.3	±12.0	±13.9	±12.0	±8.3	±6.0
n=100	±4.3	±5.9	±8.5	±9.8	±8.5	±5.9	±4.3
n=200	±3.0	±4.2	±6.0	±6.9	±6.0	±4.2	±3.0
n=500	±1.9	±2.6	±3.8	±4.4	±3.8	±2.6	±1.9
n=1000	±1.4	±1.9	±2.7	±3.1	±2.7	±1.9	±1.4
n=1500	±1.1	±1.5	±2.2	±2.5	±2.2	±1.5	±1.1
n=2000	±1.0	±1.3	±1.9	±2.2	±1.9	±1.3	±1.0

		Number of interviews	Fieldwork dates (start/end)	
EU27		12 863	26-Nov-21	17-Dec-21
BE		502	30-Nov-21	17-Dec-21
BG		511	02-Dec-21	15-Dec-21
CZ		504	01-Dec-21	17-Dec-21
DK		510	29-Nov-21	17-Dec-21
DE		501	30-Nov-21	17-Dec-21
EE		503	29-Nov-21	14-Dec-21
IE		507	29-Nov-21	17-Dec-21
EL		502	29-Nov-21	15-Dec-21
ES		505	29-Nov-21	15-Dec-21
FR		501	29-Nov-21	09-Dec-21
HR		501	29-Nov-21	14-Dec-21
IT		505	29-Nov-21	15-Dec-21
CY		251	29-Nov-21	08-Dec-21
LV		500	30-Nov-21	17-Dec-21
LT		504	29-Nov-21	15-Dec-21
LU		253	29-Nov-21	14-Dec-21
HU		501	29-Nov-21	10-Dec-21
MT		252	29-Nov-21	14-Dec-21
NL		528	30-Nov-21	17-Dec-21
AT		503	29-Nov-21	16-Dec-21
PL		504	26-Nov-21	17-Dec-21
PT		511	29-Nov-21	16-Dec-21
RO		502	29-Nov-21	17-Dec-21
SI		500	29-Nov-21	13-Dec-21
SK		500	30-Nov-21	16-Dec-21
FI		502	29-Nov-21	15-Dec-21
SE		500	29-Nov-21	17-Dec-21

Questionnaire

- ASK ALL
- Q1 Which of the following does your company currently have or use?**
(READ OUT, MULTIPLE ANSWERS POSSIBLE) (RANDOMISE 1-9)
- | | |
|---|-----|
| An online bank account | 1 |
| An online ordering and payment service for customers | 2 |
| Online ordering or payment systems of suppliers, consultants or other business partners | 3 |
| A website for your business | 4 |
| Web-based applications for payroll processing, e-signature etc. | 5 |
| Cloud computing or storage | 6 |
| Internet-connected 'smart' devices | 7 |
| A company intranet | 8 |
| An internet-based video or voice calling service | 9 |
| Other (DO NOT READ OUT) | 10 |
| None of the above (DO NOT READ OUT) | 11 |
| Don't know (DO NOT READ OUT) | 998 |
- ASK ALL
- Q2 Do employees in your company use personally owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities?**
This includes devices that are subsidized by your company.
- | | |
|------------------------------|-----|
| Yes | 1 |
| No | 2 |
| Don't know (DO NOT READ OUT) | 998 |
- (INTERVIEWER: READ OUT)
For the purpose of this survey, "cybercrime" refers to instances when someone uses the internet or other online technologies to access or tamper with your company's information systems or the data it holds, in order to harm or inconvenience your company.
(IF NECESSARY, ADD: Your information systems include things like your networks, devices, servers and any cloud storage you may have.)
- ASK ALL
- Q3 How well informed do you feel about the risks of cybercrime?**
(READ OUT, ONE ANSWER ONLY)
- | | |
|------------------------------|-----|
| Very well informed | 1 |
| Fairly well informed | 2 |
| Not very well informed | 3 |
| Not at all informed | 4 |
| Don't know (DO NOT READ OUT) | 998 |

ASK ALL	
Q4	How well informed do you feel your employees are about the risks of cybercrime?
(READ OUT, ONE ANSWER ONLY)	
	Very well informed 1
	Fairly well informed 2
	Not very well informed 3
	Not at all informed 4
	Don't know (DO NOT READ OUT) 998
ASK ALL	
Q5	In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?
	Yes 1
	No 2
	Don't know (DO NOT READ OUT) 998
ASK ALL	
Q6	When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
(READ OUT – ONE ANSWER PER LINE) (RANDOMISE ITEMS 1 TO 7)	
Q6_1	Viruses, spyware or malware (excluding ransomware)
Q6_2	Denial of service attacks
Q6_3	Hacking (or attempts to hack) online bank accounts
Q6_4	Phishing, account takeover or impersonation attacks
Q6_5	Ransomware
Q6_6	Unauthorised accessing of files or networks
Q6_7	Unauthorised listening in to video conferences or instant messages
Q6_8	Any other breaches or attacks
(RESPONSE SCALE)	
	Very concerned 1
	Somewhat concerned 2
	Not at all concerned 3
	Don't know (DO NOT READ OUT) 998

ASK ALL	
Q7	Has your company experienced any of the following types of cybercrime in the last 12 months?
(READ OUT – ONE ANSWER PER LINE) (ITEMS IN SAME ORDER AS IN Q6)	
Q7_1	Viruses, spyware or malware (excluding ransomware)
Q7_2	Denial of service attacks
Q7_3	Hacking (or attempts to hack) online bank accounts
Q7_4	Phishing, account takeover or impersonation attacks
Q7_5	Ransomware
Q7_6	Unauthorised accessing of files or networks
Q7_7	Unauthorised listening in to video conferences or instant messages
Q7_8	Any other breaches or attacks
(RESPONSE SCALE)	
Yes	1
No	2
Don't know (DO NOT READ OUT)	998
ASK ANY Q7_1 TO Q7_8=1	
Q8	Thinking about the most serious incident, how was this attack carried out?
(READ OUT, MULTIPLE ANSWERS POSSIBLE) (RANDOMISE 1-7)	
	Exploiting software, hardware, or network vulnerabilities 1
	Password cracking 2
	Identity theft 3
	Scams and fraud 4
	Malicious software 5
	Denial of service (false traffic to overwhelm website or network) 6
	Disruption or defacing of web presence 7
	Other (DO NOT READ OUT) 8
	Don't know (DO NOT READ OUT) 998
ASK ANY Q7_1 TO Q7_8=1	
Q9	Still thinking about the most serious incident, how was your business impacted?
(READ OUT, MULTIPLE ANSWERS POSSIBLE) (RANDOMISE 1-9)	
	Loss of revenue 1
	Loss of suppliers, customers, or partners 2
	Repair or recovery costs 3
	Ransom money 4
	Prevented the use of resources or services 5
	Prevented employees from carrying out day-to-day work 6
	Additional time required to respond to the cybercrime incident(s) 7
	Damage to the reputation of the company 8
	Discouraged us from carrying out an activity that was planned 9
	Not impacted in any of the ways described above (DO NOT READ OUT) 10
	Don't know (DO NOT READ OUT) 998

ASK ANY Q7_1 TO Q7_8=1; SHOW ONLY ITEMS FOR WHICH Q7=1

Q10a Who, if anyone, did you report this incident to?

(READ OUT – MULTIPLE ANSWER PER LINE) (ITEMS IN SAME ORDER AS IN Q6)

Q10a_1 Viruses, spyware or malware (excluding ransomware)

Q10a_2 Denial of service attacks

Q10a_3 Hacking (or attempts to hack) online bank accounts

Q10a_4 Phishing, account takeover or impersonation attacks

Q10a_5 Ransomware

Q10a_6 Unauthorised accessing of files or networks

Q10a_7 Unauthorised listening in to video conferences or instant messages

Q10a_8 Any other breaches or attacks

(RESPONSE SCALE)

Did not report to anyone	1
The police	2
Another official authority	3
Seller or service provider	4
Your Internet service provider	5
A consumer protection organisation	6
A business representative body or trade body	7
Someone else (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

ASK IF (Q7_1 =2 or 998) AND (Q7_2 =2 or 998) AND (Q7_3=2 or 998) AND (Q7_4 =2 or 998)
AND (Q7_5 =2 or 998) AND (Q7_6=2 or 998) AND (Q7_7 =2 or 998) AND (Q7_8 =2 or 998)

Q10b If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to?

(READ OUT – MULTIPLE ANSWER PER LINE) (ITEMS IN SAME ORDER AS IN Q6)

Q10b_1 Viruses, spyware or malware (excluding ransomware)

Q10b_2 Denial of service attacks

Q10b_3 Hacking (or attempts to hack) online bank accounts

Q10b_4 Phishing, account takeover or impersonation attacks

Q10b_5 Ransomware

Q10b_6 Unauthorised accessing of files or networks

Q10b_7 Unauthorised listening in to video conferences or instant messages

Q10b_8 Any other breaches or attacks

(RESPONSE SCALE)

Would not report to anyone	1
The police	2
Another official authority	3
Seller or service provider	4
Your Internet service provider	5
A consumer protection organisation	6
A business representative body or trade body	7
Someone else (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

ASK IF NONE OF THE ITEMS IN Q10a=2





























Q11 Why did you not report the incident (or incidents) to the police?

(READ OUT, MULTIPLE ANSWERS POSSIBLE) (RANDOMISE 1-7)





























Expected it would be reported by another authority (e.g. Internet provider/bank)	1
The police couldn't have done anything	2
Tried to report it but police were not interested	3
Dealt with the incident internally	4
Did not know the police dealt with this type of incident	5
Inconvenient/too much trouble	6
Too trivial/not worth reporting	7
Other (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

Data annex





























Q1 Which of the following does your company currently have or use?

		An online bank account	An online ordering and payment service for customers	Online ordering or payment systems of suppliers, consultants or other business partners	A website for your business	Web-based applications for payroll processing, e-signature etc.	Cloud computing or storage	Internet-connected 'smart' devices	A company intranet	An internet-based video or voice calling service	Other	None of the above	Don't know
EU27		76	30	39	71	35	38	55	32	31	1	3	0
BE		87	30	44	74	45	50	57	29	39	0	1	0
BG		65	19	21	39	48	17	56	31	22	2	11	2
CZ		94	31	34	83	37	42	71	34	44	0	1	0
DK		88	33	47	83	55	62	56	26	30	1	3	0
DE		72	19	35	76	23	32	53	26	22	0	6	1
EE		97	62	63	60	72	52	83	15	33	2	1	0
IE		62	30	34	77	37	29	36	24	30	1	1	1
EL		88	49	54	78	54	46	48	51	52	0	1	0
ES		79	30	31	67	43	48	66	33	32	1	1	1
FR		58	26	37	66	25	36	37	32	21	0	7	0
HR		82	42	39	67	56	43	89	29	61	0	0	0
IT		70	31	50	79	27	29	66	48	31	1	0	0
CY		94	52	57	75	40	51	51	54	60	0	2	1
LV		95	31	23	52	60	33	71	27	36	0	1	0
LT		96	41	43	62	90	42	78	23	35	0	0	0
LU		72	36	42	82	44	45	59	36	45	0	1	1
HU		86	33	38	65	26	38	75	23	33	0	1	0
MT		72	36	40	77	32	49	71	40	36	2	4	2
NL		90	32	40	83	41	61	55	27	40	1	1	0
AT		62	21	26	60	14	23	53	19	17	3	5	2
PL		89	29	36	67	34	30	28	23	28	0	2	0
PT		49	26	33	50	22	27	27	19	16	6	4	4
RO		78	42	50	36	50	31	67	23	19	0	10	0
SI		93	36	38	67	46	53	89	25	51	0	1	0
SK		90	32	32	84	53	39	80	23	53	0	0	0
FI		93	38	33	70	57	53	85	19	42	0	0	0
SE		82	35	50	74	48	57	66	29	52	0	1	0





























Q2 Do employees in your company use personally-owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities? This includes devices that are subsidized by your company.

	Yes	No	Don't know
EU27 	48	51	2
BE 	46	53	1
BG 	55	41	4
CZ 	65	34	1
DK 	49	50	1
DE 	48	50	2
EE 	62	36	1
IE 	68	31	1
EL 	67	33	0
ES 	40	60	0
FR 	32	67	2
HR 	66	34	1
IT 	50	50	0
CY 	74	26	0
LV 	70	30	0
LT 	50	50	1
LU 	70	30	0
HU 	40	58	1
MT 	66	34	0
NL 	46	49	5
AT 	63	37	0
PL 	46	48	6
PT 	65	33	2
RO 	56	42	3
SI 	71	29	0
SK 	49	51	1
FI 	48	51	1
SE 	35	63	2





























Q3 How well informed do you feel about the risks of cybercrime?

		Very well informed	Fairly well informed	Not very well informed	Not at all informed	Don't know
EU27		21	50	21	8	1
BE		20	52	22	6	1
BG		19	47	28	5	1
CZ		22	57	17	4	0
DK		28	49	19	3	1
DE		20	52	18	9	1
EE		23	63	13	1	1
IE		45	43	9	3	0
EL		21	42	30	7	0
ES		18	43	28	11	0
FR		22	44	19	14	0
HR		29	39	29	3	0
IT		20	51	22	7	0
CY		24	47	22	7	0
LV		13	51	29	8	1
LT		19	56	20	4	1
LU		35	43	16	6	0
HU		11	47	31	11	1
MT		39	49	8	5	0
NL		19	61	16	4	0
AT		22	60	12	5	0
PL		39	42	11	6	2
PT		11	56	26	4	3
RO		14	46	30	9	1
SI		17	49	24	9	1
SK		17	58	17	7	1
FI		13	58	21	8	0
SE		17	63	17	2	1





























Q4 How well informed do you feel your employees are about the risks of cybercrime?

		Very well informed	Fairly well informed	Not very well informed	Not at all informed	Don't know
EU27		15	41	22	10	12
BE		11	41	18	4	26
BG		14	38	26	8	14
CZ		15	47	17	9	12
DK		13	38	21	5	23
DE		12	41	21	14	12
EE		20	55	14	2	9
IE		38	42	14	3	4
EL		17	36	33	10	4
ES		11	39	32	12	7
FR		13	33	17	20	16
HR		24	36	29	5	6
IT		17	42	25	7	8
CY		16	45	28	10	2
LV		12	43	34	8	3
LT		13	45	27	5	10
LU		28	43	16	7	6
HU		10	40	28	13	10
MT		25	44	21	6	4
NL		13	44	16	6	23
AT		20	47	17	11	6
PL		28	35	12	8	17
PT		6	55	32	4	4
RO		10	36	29	13	12
SI		17	38	22	10	13
SK		12	52	17	6	13
FI		10	45	24	9	12
SE		10	48	19	3	21





























Q5 In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?

		Yes	No	Don't know
EU27		19	79	3
BE		24	70	5
BG		12	82	5
CZ		15	83	2
DK		18	79	3
DE		27	71	1
EE		24	76	1
IE		40	58	2
EL		22	77	1
ES		14	86	0
FR		9	88	2
HR		20	79	2
IT		15	85	0
CY		21	78	1
LV		13	87	0
LT		14	85	0
LU		20	79	1
HU		14	83	3
MT		31	69	0
NL		29	65	6
AT		29	68	3
PL		26	67	7
PT		22	75	4
RO		8	90	3
SI		19	79	2
SK		19	79	2
FI		22	74	4
SE		28	67	5


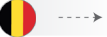
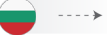
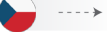
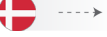
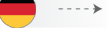
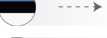
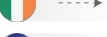
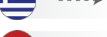
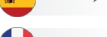
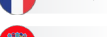
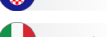
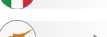
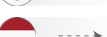
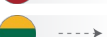
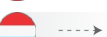
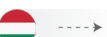

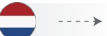
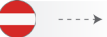
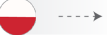

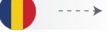

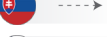
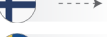
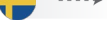

Q6_1 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Viruses, spyware or malware (excluding ransomware)

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		29	43	26	2
BE		24	47	28	1
BG		28	40	29	3
CZ		34	43	22	2
DK		9	41	45	6
DE		15	43	39	3
EE		10	52	37	0
IE		25	37	34	4
EL		30	44	26	1
ES		63	28	9	0
FR		28	41	30	1
HR		22	54	24	1
IT		32	46	21	2
CY		30	38	33	0
LV		25	50	23	2
LT		17	41	41	1
LU		31	46	23	0
HU		15	47	37	0
MT		38	32	28	2
NL		13	51	35	1
AT		18	31	42	10
PL		26	46	25	2
PT		47	40	9	4
RO		19	46	33	2
SI		28	40	32	0
SK		14	59	25	2
FI		21	57	22	0
SE		10	53	37	0


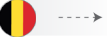
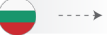
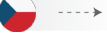
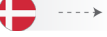
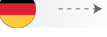
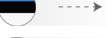
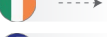
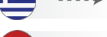
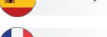
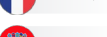
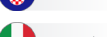
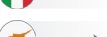
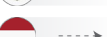
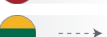
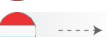
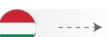

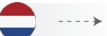
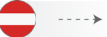
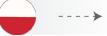

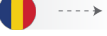

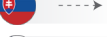
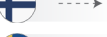
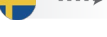

Q6_2 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Denial of service attacks

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		18	35	40	7
BE		13	34	45	8
BG		16	32	48	5
CZ		24	39	34	3
DK		4	29	56	10
DE		7	32	51	9
EE		6	41	52	1
IE		22	33	39	7
EL		19	34	44	4
ES		43	37	14	6
FR		17	29	51	3
HR		13	46	40	1
IT		18	37	31	14
CY		9	41	45	5
LV		14	40	34	11
LT		13	33	53	1
LU		23	31	37	10
HU		12	29	59	0
MT		22	29	37	11
NL		7	28	60	5
AT		7	34	47	13
PL		17	40	38	5
PT		24	53	13	10
RO		11	42	43	4
SI		14	32	52	2
SK		6	43	49	2
FI		11	43	43	3
SE		3	24	71	2





























Q6_3 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Hacking (or attempts to hack) online bank accounts

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		32	37	31	1
BE		25	36	37	2
BG		31	34	32	3
CZ		39	36	24	1
DK		8	33	57	1
DE		12	41	45	3
EE		7	39	53	1
IE		31	34	34	2
EL		38	41	21	0
ES		72	21	6	0
FR		29	37	32	1
HR		21	45	34	0
IT		37	35	27	0
CY		30	40	30	0
LV		36	38	25	0
LT		25	34	40	1
LU		32	33	34	1
HU		13	36	50	1
MT		41	30	27	2
NL		12	35	52	1
AT		14	31	50	6
PL		23	45	29	2
PT		55	35	8	3
RO		22	41	36	1
SI		31	36	33	1
SK		14	53	32	1
FI		18	47	35	0
SE		7	45	46	1





























Q6_4 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Phishing, account takeover or impersonation attacks

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		31	41	27	1
BE		26	45	28	1
BG		25	42	31	2
CZ		38	36	25	1
DK		7	40	52	1
DE		15	42	42	1
EE		7	48	45	0
IE		29	34	31	6
EL		34	45	21	0
ES		71	22	7	0
FR		28	40	31	1
HR		18	51	31	1
IT		38	46	15	1
CY		22	38	40	1
LV		28	43	28	1
LT		14	41	44	1
LU		35	39	23	3
HU		13	40	47	0
MT		31	31	34	4
NL		17	47	36	1
AT		16	35	46	4
PL		23	45	30	2
PT		43	41	11	5
RO		20	43	36	2
SI		20	38	42	0
SK		12	51	35	2
FI		18	53	28	0
SE		12	48	40	0





























Q6_5 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Ransomware

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		22	33	38	7
BE		17	40	35	8
BG		19	32	38	11
CZ		20	37	32	11
DK		7	32	54	7
DE		13	28	55	4
EE		8	37	54	2
IE		24	37	35	4
EL		28	37	35	1
ES		62	31	7	1
FR		16	28	53	3
HR		17	45	38	1
IT		23	33	28	15
CY		25	39	35	2
LV		23	45	28	5
LT		12	26	58	5
LU		16	41	25	19
HU		13	30	57	1
MT		25	35	34	6
NL		13	40	43	4
AT		12	24	59	5
PL		15	33	46	6
PT		21	44	15	20
RO		14	41	37	9
SI		23	33	42	2
SK		7	44	36	13
FI		10	44	45	0
SE		7	35	56	1





























Q6_6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Unauthorised accessing of files or networks

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		25	40	33	1
BE		19	44	35	2
BG		23	39	33	4
CZ		32	40	27	1
DK		7	34	58	2
DE		13	38	47	2
EE		5	44	51	1
IE		20	34	42	3
EL		27	47	25	1
ES		59	29	11	1
FR		23	35	41	1
HR		16	48	36	0
IT		27	49	24	0
CY		23	41	36	0
LV		25	46	29	1
LT		15	41	42	2
LU		26	42	30	1
HU		14	32	53	1
MT		30	27	39	4
NL		12	44	43	2
AT		9	38	47	6
PL		20	43	35	2
PT		42	42	11	4
RO		14	46	38	2
SI		24	35	40	1
SK		9	52	37	1
FI		11	55	34	1
SE		6	44	50	0





























Q6_7 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Unauthorised listening in to video conferences or instant messages

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		14	30	53	3
BE		10	25	61	4
BG		17	32	47	5
CZ		23	30	45	2
DK		2	13	82	2
DE		9	25	63	3
EE		2	21	67	10
IE		16	28	51	6
EL		17	35	46	2
ES		36	38	24	2
FR		9	23	65	4
HR		14	31	52	3
IT		9	32	57	2
CY		11	35	53	2
LV		14	31	54	2
LT		7	27	62	3
LU		23	29	43	5
HU		5	22	71	2
MT		18	20	57	6
NL		5	27	65	3
AT		5	19	71	5
PL		20	32	45	4
PT		30	44	20	6
RO		10	37	50	3
SI		17	27	54	1
SK		7	36	56	1
FI		4	28	65	4
SE		2	16	81	1





























Q6_8 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks? Any other breaches or attacks

		Very concerned	Somewhat concerned	Not at all concerned	Don't know
EU27		21	43	32	4
BE		17	46	35	2
BG		24	44	30	3
CZ		32	45	22	1
DK		4	31	59	6
DE		8	39	50	4
EE		4	33	49	15
IE		14	29	54	3
EL		25	56	19	1
ES		51	32	11	6
FR		19	40	38	2
HR		13	60	27	0
IT		19	51	26	4
CY		19	47	30	4
LV		16	55	26	2
LT		12	45	41	1
LU		25	44	30	1
HU		10	39	49	1
MT		25	34	38	3
NL		8	38	47	7
AT		14	40	44	2
PL		19	53	27	2
PT		42	43	10	5
RO		14	49	34	2
SI		17	43	39	1
SK		6	55	35	4
FI		9	61	29	1
SE		5	31	55	9





























Q7_1 Has your company experienced any of the following types of cybercrime in the last 12 months? Viruses, spyware or malware (excluding ransomware)

		Yes	No	Don't know
EU27		14	85	1
BE		16	83	1
BG		8	89	3
CZ		28	71	1
DK		2	97	1
DE		5	94	1
EE		6	94	0
IE		9	88	3
EL		16	84	0
ES		12	88	0
FR		12	86	2
HR		16	82	2
IT		17	81	2
CY		8	92	0
LV		13	86	1
LT		13	85	2
LU		12	85	3
HU		17	82	0
MT		10	90	0
NL		17	82	1
AT		5	92	3
PL		13	86	2
PT		21	79	0
RO		14	84	2
SI		12	87	2
SK		22	76	2
FI		11	88	1
SE		5	92	2





























Q7_2 Has your company experienced any of the following types of cybercrime in the last 12 months? Denial of service attacks

		Yes	No	Don't know
EU27		3	96	1
BE		4	93	3
BG		3	94	2
CZ		6	92	2
DK		1	97	2
DE		2	97	1
EE		1	99	0
IE		4	93	3
EL		3	96	1
ES		3	97	0
FR		1	97	2
HR		3	96	1
IT		2	98	0
CY		2	97	1
LV		4	93	3
LT		8	91	1
LU		3	92	6
HU		4	96	1
MT		3	95	2
NL		3	95	2
AT		6	90	4
PL		6	93	1
PT		8	92	0
RO		2	96	2
SI		2	94	4
SK		5	94	1
FI		5	93	1
SE		1	98	1





























Q7_3 Has your company experienced any of the following types of cybercrime in the last 12 months? Hacking (or attempts to hack) online bank accounts

		Yes	No	Don't know
EU27		4	95	1
BE		4	95	1
BG		3	95	2
CZ		9	90	1
DK		3	97	0
DE		2	97	1
EE		4	95	0
IE		6	92	2
EL		12	89	0
ES		5	95	0
FR		3	96	1
HR		3	95	2
IT		2	98	0
CY		4	96	0
LV		6	93	1
LT		4	94	1
LU		6	90	4
HU		3	96	1
MT		4	95	0
NL		3	96	1
AT		6	91	3
PL		8	91	1
PT		9	90	1
RO		4	95	1
SI		3	96	1
SK		9	91	1
FI		3	95	2
SE		3	96	2





























Q7_4 Has your company experienced any of the following types of cybercrime in the last 12 months? Phishing, account takeover or impersonation attacks

		Yes	No	Don't know
EU27		11	88	1
BE		20	79	1
BG		12	86	2
CZ		10	88	1
DK		10	89	1
DE		6	93	1
EE		26	74	0
IE		11	85	4
EL		27	72	1
ES		4	96	0
FR		6	93	1
HR		4	95	1
IT		15	85	1
CY		16	84	0
LV		12	88	0
LT		8	91	0
LU		7	85	9
HU		14	86	1
MT		12	87	1
NL		21	79	0
AT		6	94	1
PL		11	87	1
PT		14	86	0
RO		8	91	0
SI		8	91	2
SK		15	84	1
FI		20	80	1
SE		7	91	2





























Q7_5 Has your company experienced any of the following types of cybercrime in the last 12 months? Ransomware

		Yes	No	Don't know
EU27		4	95	1
BE		5	92	3
BG		2	93	5
CZ		8	88	5
DK		1	98	1
DE		2	98	1
EE		1	99	1
IE		8	90	3
EL		7	92	1
ES		2	98	0
FR		3	96	2
HR		11	89	1
IT		4	95	1
CY		5	96	0
LV		6	93	2
LT		3	97	0
LU		5	82	12
HU		4	95	1
MT		3	96	1
NL		5	93	2
AT		2	97	1
PL		4	96	0
PT		9	89	3
RO		4	92	4
SI		8	91	1
SK		5	88	7
FI		6	94	0
SE		2	96	1





























Q7_6 Has your company experienced any of the following types of cybercrime in the last 12 months? Unauthorised accessing of files or networks

		Yes	No	Don't know
EU27		4	95	1
BE		4	95	2
BG		4	94	2
CZ		8	89	3
DK		2	98	0
DE		4	96	0
EE		1	99	0
IE		4	94	2
EL		4	95	1
ES		2	97	0
FR		2	96	2
HR		6	92	3
IT		5	95	0
CY		2	98	0
LV		8	91	2
LT		5	93	2
LU		8	89	3
HU		5	94	1
MT		3	97	0
NL		6	93	1
AT		3	95	3
PL		5	93	3
PT		14	86	0
RO		3	96	2
SI		5	94	1
SK		5	92	3
FI		1	98	1
SE		2	96	2

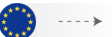
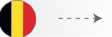
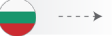
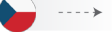
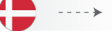
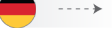
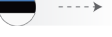
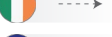
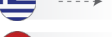
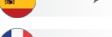
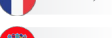
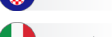
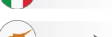
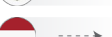
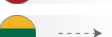
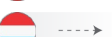
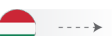
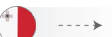
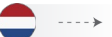
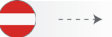
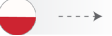
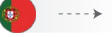
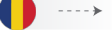
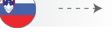
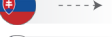
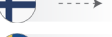
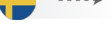

Q7_7 Has your company experienced any of the following types of cybercrime in the last 12 months? Unauthorised listening in to video conferences or instant messages

		Yes	No	Don't know
EU27		2	95	3
BE		0	94	6
BG		1	93	6
CZ		2	93	5
DK		0	99	1
DE		1	96	3
EE		0	95	5
IE		4	93	3
EL		3	96	1
ES		0	98	2
FR		1	96	3
HR		1	91	8
IT		2	97	1
CY		0	99	1
LV		1	95	4
LT		1	97	2
LU		4	92	4
HU		0	98	2
MT		4	95	2
NL		1	95	5
AT		3	92	5
PL		5	89	7
PT		6	92	2
RO		3	88	9
SI		2	94	4
SK		1	91	8
FI		0	97	3
SE		0	98	2





























Q7_8 Has your company experienced any of the following types of cybercrime in the last 12 months? Any other breaches or attacks

		Yes	No	Don't know
EU27		5	94	2
BE		4	94	3
BG		6	92	3
CZ		8	90	2
DK		2	98	0
DE		2	97	1
EE		2	88	10
IE		4	93	3
EL		8	91	1
ES		3	96	1
FR		3	96	1
HR		4	94	2
IT		4	94	2
CY		1	99	0
LV		7	93	1
LT		7	91	2
LU		3	93	4
HU		4	95	1
MT		2	98	0
NL		4	94	2
AT		4	94	2
PL		7	91	1
PT		10	88	2
RO		3	95	2
SI		4	92	3
SK		8	91	1
FI		5	94	1
SE		5	88	7

Q8 Thinking about the most serious incident, how was this attack carried out?





























		Exploiting software, hardware, or network vulnerabilities	Password cracking	Identity theft	Scams and fraud	Malicious software	Denial of service (false traffic to overwhelm website or network)	Disruption or defacing of web presence	Other	Don't know
EU27		23	19	13	28	30	12	14	11	9
BE		19	17	22	33	31	14	12	18	8
BG		14	20	7	25	23	10	7	12	12
CZ		26	24	12	57	41	17	16	4	7
DK		18	14	17	39	10	12	5	19	13
DE		28	19	17	26	29	20	11	12	14
EE		22	3	4	34	19	9	4	18	20
IE		19	35	19	37	28	12	13	6	9
EL		15	20	5	26	36	14	13	16	1
ES		35	17	19	27	52	21	21	9	8
FR		8	9	13	16	24	4	15	7	20
HR		21	19	7	27	37	9	8	16	9
IT		35	26	10	21	20	5	15	11	4
CY		3	24	11	52	12	11	8	14	7
LV		23	16	11	30	24	17	16	12	10
LT		26	14	7	32	27	32	18	8	6
LU		25	22	14	27	34	13	21	12	15
HU		28	21	6	25	18	5	12	14	13
MT		12	29	24	45	15	15	11	9	4
NL		12	12	14	34	21	9	8	21	10
AT		15	15	23	21	33	22	3	10	0
PL		13	17	13	28	35	15	10	11	9
PT		21	21	19	22	37	14	15	2	8
RO		29	28	16	26	38	21	24	15	8
SI		42	8	16	34	19	9	22	9	4
SK		15	15	14	34	35	20	15	9	12
FI		15	9	12	37	22	9	5	17	13
SE		17	12	24	38	29	9	9	28	2

Q9 Still thinking about the most serious incident, how was your business impacted?

		Loss of revenue	Loss of suppliers, or customers, or partners	Repair or recovery costs	Ransom money	Prevented the use of resources or services	Prevented employees from carrying out day-to-day work	Additional time required to respond to the cybercrime incident(s)	Damage to the reputation of the company	Discouraged us from carrying out an activity that was planned	Not impacted in any of the ways described above	Don't know
EU27		11	7	24	6	20	20	35	7	13	39	3
BE		5	6	24	3	25	19	38	7	16	46	5
BG		7	6	14	0	12	15	28	2	6	42	5
CZ		16	11	31	7	20	23	51	11	15	31	2
DK		13	5	14	1	10	8	39	6	9	47	6
DE		9	5	27	0	15	15	41	1	21	40	8
EE		2	1	9	1	10	9	36	2	6	60	2
IE		19	18	34	12	14	23	32	15	23	9	5
EL		11	1	29	6	9	23	47	3	18	35	0
ES		26	7	37	7	35	30	32	14	19	24	5
FR		8	10	13	5	20	20	33	13	11	40	2
HR		11	4	27	13	18	21	22	13	25	33	5
IT		7	9	25	11	18	18	30	3	16	50	1
CY		7	3	10	1	6	13	23	8	6	61	3
LV		10	4	23	3	28	27	51	10	19	32	2
LT		15	12	31	1	23	38	54	12	42	24	2
LU		13	10	29	4	21	31	31	21	31	41	7
HU		10	2	33	2	18	28	15	2	5	39	3
MT		22	22	24	18	29	20	31	18	15	49	1
NL		6	2	17	2	14	13	34	5	3	46	4
AT		18	3	30	3	16	20	34	6	12	44	0
PL		9	3	14	2	11	14	35	8	4	44	5
PT		16	8	21	12	32	27	14	11	11	18	5
RO		16	18	24	1	31	21	50	9	11	28	3
SI		12	6	20	3	12	21	21	5	1	44	2
SK		14	6	29	11	25	24	45	9	21	39	1
FI		8	2	16	2	17	14	42	7	4	45	0
SE		21	4	13	0	31	33	57	10	13	35	5





























Q10a_1 Who, if anyone, did you report this incident to? Viruses, spyware or malware (excluding ransomware)

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		52	11	4	17	13	1	3	7	2
BE		46	16	7	12	17	2	2	10	5
BG		42	12	5	12	27	0	14	2	0
CZ		66	6	3	10	10	0	2	8	1
DK		40	5	2	16	11	0	34	0	7
DE		65	20	1	5	16	1	2	3	0
EE		47	18	17	9	8	0	0	10	0
IE		2	40	11	25	32	12	14	7	11
EL		39	12	1	17	33	1	4	6	0
ES		63	12	1	12	5	0	2	7	0
FR		47	6	2	24	13	0	4	13	1
HR		64	8	1	9	20	0	1	3	3
IT		41	19	9	26	17	0	3	0	0
CY		19	17	11	33	21	0	0	8	11
LV		55	8	5	14	10	0	2	4	4
LT		52	8	6	13	14	1	0	18	0
LU		30	23	18	12	31	7	18	0	2
HU		73	6	0	3	2	0	7	9	0
MT		26	16	7	12	11	9	7	34	0
NL		50	5	2	19	8	1	7	15	3
AT		21	31	6	12	2	22	3	5	0
PL		80	2	1	7	6	0	0	4	3
PT		17	20	9	21	18	14	9	2	8
RO		60	3	6	20	9	2	4	8	2
SI		46	13	5	24	16	0	7	9	1
SK		64	0	3	12	14	0	0	11	0
FI		61	5	2	19	8	0	1	10	1
SE		33	12	0	23	19	0	1	22	4





























Q10a_2 Who, if anyone, did you report this incident to? Denial of service attacks

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		35	21	9	14	21	5	7	8	5
BE		60	10	11	1	30	0	9	3	0
BG		39	14	0	0	37	0	11	3	10
CZ		52	3	5	18	13	1	0	17	0
DK		74	2	0	13	2	0	13	0	0
DE		42	37	7	7	17	17	4	0	0
EE		6	8	52	33	62	0	0	0	0
IE		8	23	19	6	49	34	19	0	1
EL		31	31	29	14	5	18	2	9	2
ES		34	35	16	19	32	16	16	12	0
FR		2	14	5	9	0	0	23	61	0
HR		17	35	0	14	46	14	0	0	2
IT		5	29	5	15	75	1	0	15	0
CY		63	37	37	0	0	0	0	0	0
LV		70	3	2	10	6	0	12	0	0
LT		51	4	13	19	14	0	0	12	0
LU		28	4	10	31	23	0	10	0	0
HU		73	0	0	8	0	0	18	1	1
MT		40	24	8	26	8	0	0	19	0
NL		30	26	0	9	21	0	14	9	4
AT		10	35	32	29	0	0	2	0	8
PL		39	30	0	10	9	0	0	1	11
PT		10	6	24	22	15	6	13	0	21
RO		50	17	13	30	0	2	4	2	0
SI		19	54	27	1	0	0	0	18	0
SK		65	0	0	9	30	0	0	1	0
FI		61	8	2	17	9	0	0	0	6
SE		68	2	2	12	6	0	0	7	9





























Q10a_3 Who, if anyone, did you report this incident to? Hacking (or attempts to hack) online bank accounts

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		38	21	10	21	12	3	4	10	2
BE		42	19	12	13	11	0	0	13	3
BG		14	25	6	17	49	15	25	1	1
CZ		40	13	4	21	4	3	4	13	3
DK		15	19	7	13	0	0	37	6	10
DE		40	21	8	0	7	1	23	7	0
EE		51	10	26	10	17	0	0	0	0
IE		9	36	29	12	34	24	10	0	9
EL		28	16	18	16	27	5	5	9	0
ES		51	38	0	0	0	0	0	18	0
FR		19	25	9	46	15	0	0	25	0
HR		48	17	15	21	15	0	0	0	0
IT		25	13	25	50	25	0	13	0	0
CY		14	57	25	32	29	0	0	0	0
LV		48	16	7	26	1	0	0	0	3
LT		65	2	13	0	16	0	0	14	0
LU		2	46	25	19	44	24	13	0	7
HU		64	0	8	28	1	0	0	0	0
MT		16	54	0	28	29	0	0	23	0
NL		27	36	0	40	25	0	8	12	0
AT		21	30	41	2	10	17	0	4	6
PL		66	12	0	20	4	0	0	8	0
PT		10	27	29	15	18	14	0	0	10
RO		24	34	16	39	0	8	17	9	0
SI		20	57	2	58	44	0	2	1	0
SK		41	6	16	17	10	0	0	14	4
FI		60	0	0	35	0	0	0	4	0
SE		28	39	0	44	4	0	0	8	1


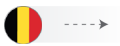






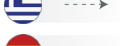






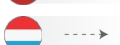












Q10a_4 Who, if anyone, did you report this incident to? Phishing, account takeover or impersonation attacks

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		40	19	9	17	9	2	4	8	3
BE		40	18	16	11	10	2	2	15	5
BG		28	4	3	24	16	3	27	7	3
CZ		58	8	0	19	8	2	0	8	1
DK		54	17	13	5	0	6	7	12	0
DE		32	20	1	11	12	1	19	2	9
EE		66	9	12	7	5	0	2	4	1
IE		20	35	13	19	38	8	11	8	2
EL		50	21	9	15	15	2	1	5	0
ES		28	39	0	22	0	7	0	26	0
FR		28	26	11	17	3	0	4	5	17
HR		54	26	0	25	17	0	0	0	0
IT		33	21	17	20	5	1	1	6	0
CY		22	26	12	19	30	0	4	10	0
LV		58	6	9	17	2	0	1	4	4
LT		45	12	0	10	19	0	5	13	3
LU		18	59	12	22	19	24	15	19	0
HU		75	2	4	15	4	0	0	4	0
MT		12	23	22	26	15	0	6	18	5
NL		32	19	6	26	14	0	3	9	4
AT		35	21	7	13	12	9	5	0	4
PL		57	18	5	6	5	0	3	11	5
PT		28	20	15	19	10	6	14	0	3
RO		30	18	13	33	18	3	7	8	2
SI		36	40	7	23	15	6	3	5	2
SK		69	3	8	14	12	0	0	5	3
FI		57	7	3	15	9	0	3	9	4
SE		29	34	0	24	18	0	8	6	2


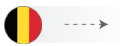






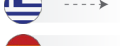






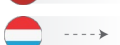












Q10a_5 Who, if anyone, did you report this incident to? Ransomware

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		44	23	7	12	8	2	4	10	2
BE		39	17	18	8	10	0	0	8	8
BG		29	6	1	5	23	0	36	5	0
CZ		75	12	0	5	7	0	0	7	0
DK		24	11	5	65	30	5	11	0	5
DE		57	33	0	0	9	0	4	0	0
EE		60	9	11	17	9	0	0	0	3
IE		0	33	19	25	20	5	0	13	7
EL		37	28	4	12	33	1	8	11	0
ES		28	50	1	1	1	13	0	21	0
FR		6	8	2	29	0	0	8	52	4
HR		55	25	2	10	16	1	1	0	1
IT		51	24	14	9	0	0	2	2	0
CY		26	43	20	11	23	0	1	0	0
LV		66	9	0	6	8	0	20	0	0
LT		62	5	0	19	11	0	1	1	8
LU		56	2	7	17	5	0	13	0	0
HU		64	28	14	1	6	0	1	15	0
MT		2	61	0	5	17	0	12	21	0
NL		43	18	5	20	10	0	9	5	6
AT		2	12	28	33	9	0	7	9	9
PL		68	16	3	10	1	0	0	0	7
PT		5	35	14	23	14	5	10	7	0
RO		67	7	7	20	2	7	3	2	0
SI		50	36	6	12	6	0	1	3	0
SK		46	8	4	19	12	0	0	16	0
FI		70	2	0	18	7	0	0	2	1
SE		6	61	0	18	37	0	0	8	4





























Q10a_6 Who, if anyone, did you report this incident to? Unauthorised accessing of files or networks

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		40	20	7	16	14	8	5	6	2
BE		57	19	15	13	10	2	0	2	1
BG		27	4	2	6	16	2	39	2	9
CZ		57	5	0	18	25	0	1	13	0
DK		0	41	38	10	21	27	11	0	0
DE		31	24	4	16	13	14	2	6	0
EE		38	2	0	20	34	0	0	0	25
IE		2	55	28	19	42	12	12	9	3
EL		41	21	4	12	33	2	2	7	0
ES		58	22	0	1	2	0	0	18	0
FR		25	9	16	49	13	0	5	14	1
HR		56	33	13	11	3	1	1	0	0
IT		42	18	3	15	3	23	1	0	0
CY		31	16	0	53	7	0	0	0	0
LV		57	3	7	15	7	0	1	5	7
LT		68	21	1	3	7	0	0	10	0
LU		0	32	28	12	56	10	13	4	0
HU		67	1	0	10	12	0	5	5	0
MT		3	54	0	18	23	0	32	16	9
NL		43	25	13	11	9	0	11	5	5
AT		1	53	20	32	22	0	22	0	4
PL		54	9	1	3	16	0	0	8	11
PT		6	39	22	19	23	14	19	0	0
RO		57	5	12	29	8	10	5	1	0
SI		29	56	0	24	22	0	0	4	0
SK		51	15	8	19	19	0	0	8	0
FI		46	10	11	16	37	0	0	0	3
SE		31	52	2	14	13	0	0	0	11





























Q10a_7 Who, if anyone, did you report this incident to? Unauthorised listening in to video conferences or instant messages

Caution should be exercised when interpreting the results due to low base sizes (<100)





























		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		37	21	7	10	20	6	9	5	3
BE		0	100	100	0	100	0	0	0	0
BG		5	9	2	0	34	0	28	0	26
CZ		31	28	19	19	37	12	2	23	0
DK		0	0	0	0	100	0	50	50	0
DE		34	47	0	16	0	0	11	0	3
EE		0	0	0	100	100	0	0	0	0
IE		5	60	44	22	21	12	13	16	2
EL		30	18	14	12	26	16	2	0	0
ES		0	100	0	0	0	0	0	0	0
FR		61	0	5	0	35	0	0	24	0
HR		91	9	0	0	0	0	0	0	0
IT		8	14	3	4	46	4	21	0	0
CY		0	0	0	100	100	0	0	0	0
LV		39	0	2	5	0	0	0	0	54
LT		86	14	0	0	0	0	0	0	0
LU		6	49	25	19	55	22	38	6	6
HU		89	11	0	0	0	0	0	0	0
MT		29	38	0	40	27	0	0	7	0
NL		95	0	0	0	0	0	0	0	5
AT		7	22	31	21	1	35	4	4	1
PL		70	16	1	8	1	0	0	6	0
PT		7	35	8	13	14	20	19	0	14
RO		58	10	0	29	10	0	10	0	3
SI		30	53	0	18	18	0	0	0	0
SK		96	4	0	0	0	0	0	0	0
FI		0	0	0	0	0	0	0	0	0
SE		0	0	0	0	0	0	0	0	0

Q10a_8 Who, if anyone, did you report this incident to? Any other breaches or attacks


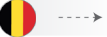
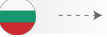
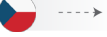
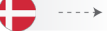
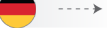
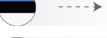
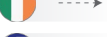
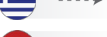
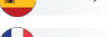
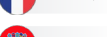
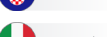
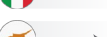
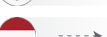
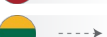
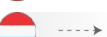
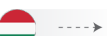

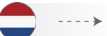
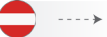
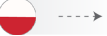

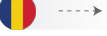

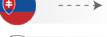
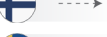
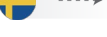

Caution should be exercised when interpreting the results due to low base sizes (<100)

		Did not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		41	24	4	18	13	3	4	7	2
BE		50	23	0	15	0	0	0	1	12
BG		30	10	0	19	16	2	34	0	6
CZ		51	41	1	7	10	0	0	0	0
DK		7	56	0	22	0	0	0	28	0
DE		45	48	1	3	10	0	3	19	0
EE		33	42	13	44	45	0	0	0	1
IE		1	26	5	8	46	10	4	15	13
EL		62	11	6	14	14	1	1	0	0
ES		43	10	0	46	0	0	0	21	0
FR		32	26	13	16	8	0	1	18	1
HR		72	18	12	4	5	2	2	4	0
IT		11	44	0	36	22	3	5	5	0
CY		78	5	5	17	22	0	0	0	0
LV		55	6	11	19	11	0	0	0	3
LT		65	3	2	14	8	0	2	10	0
LU		37	29	37	37	46	29	29	0	0
HU		72	5	0	7	16	0	1	0	0
MT		0	48	0	4	0	48	48	0	0
NL		39	29	6	18	5	1	2	7	7
AT		16	54	22	4	4	0	11	0	11
PL		66	15	4	5	3	0	0	4	5
PT		13	13	6	9	24	31	19	5	3
RO		80	0	10	10	10	0	0	0	0
SI		23	31	10	16	26	0	0	23	1
SK		46	4	4	26	29	0	0	1	7
FI		61	11	1	14	9	0	0	7	0
SE		46	15	0	31	29	0	0	0	0


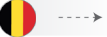
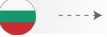
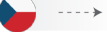
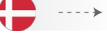
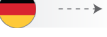
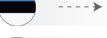
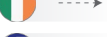
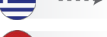
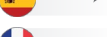
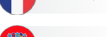
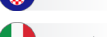
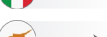
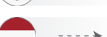
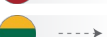
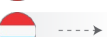
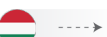

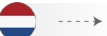
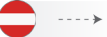
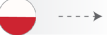

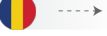

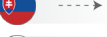
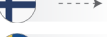
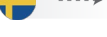

Q10b_1 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Viruses, spyware or malware (excluding ransomware)

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		10	50	11	27	25	6	8	8	4
BE		13	45	12	28	22	4	9	16	3
BG		8	56	13	14	16	7	12	6	8
CZ		19	31	3	24	21	2	3	9	5
DK		5	49	6	32	19	6	10	11	4
DE		9	59	22	24	28	12	13	6	8
EE		11	56	7	14	30	1	3	5	0
IE		2	39	10	24	23	8	10	5	13
EL		4	70	16	18	27	9	14	4	2
ES		12	47	9	32	27	5	5	8	4
FR		7	46	7	30	20	2	8	13	3
HR		8	60	11	21	24	4	4	1	4
IT		4	52	15	43	36	6	8	6	2
CY		2	66	10	33	34	4	5	3	4
LV		14	42	16	20	25	2	2	9	4
LT		9	57	11	14	26	3	3	9	5
LU		6	52	12	22	27	4	8	1	2
HU		14	42	4	18	21	2	4	13	5
MT		9	29	6	18	18	6	4	22	3
NL		16	35	6	22	25	1	7	12	4
AT		6	52	15	7	32	6	7	5	7
PL		12	65	5	15	14	3	3	8	3
PT		5	53	10	19	22	6	5	3	10
RO		24	47	22	32	29	22	18	2	7
SI		8	67	10	18	30	5	13	7	2
SK		20	17	7	32	34	4	2	8	2
FI		8	39	7	34	25	1	3	6	2
SE		14	39	4	22	31	1	7	12	8


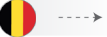
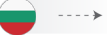
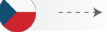
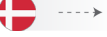
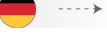
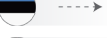
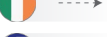
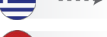
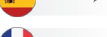
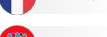
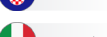
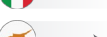
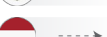
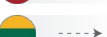
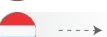
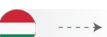

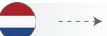
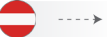
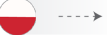

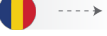

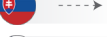
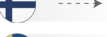
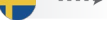

Q10b_2 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Denial of service attacks

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		7	56	11	23	22	5	7	6	8
BE		13	58	10	20	19	6	10	15	2
BG		9	51	11	15	16	8	11	7	10
CZ		14	39	2	34	19	4	2	7	7
DK		2	53	6	32	17	6	10	12	6
DE		6	65	19	20	25	11	11	5	10
EE		6	55	6	21	33	1	3	5	1
IE		2	48	11	20	21	10	10	4	12
EL		7	59	17	19	22	9	12	2	3
ES		5	58	12	28	18	5	4	4	7
FR		6	54	7	19	16	2	7	10	10
HR		6	59	10	26	22	4	4	2	2
IT		6	58	13	34	31	3	7	1	7
CY		2	44	9	27	29	7	5	7	14
LV		11	39	17	21	21	3	3	6	11
LT		6	48	11	21	27	5	5	5	5
LU		2	63	13	18	17	5	11	1	4
HU		10	39	8	19	26	2	5	5	7
MT		5	47	6	12	10	4	4	12	16
NL		7	47	7	18	32	1	7	10	6
AT		5	53	14	4	23	10	6	13	6
PL		7	71	5	14	13	3	3	6	5
PT		5	61	14	20	13	9	4	3	8
RO		19	50	22	33	25	26	19	2	9
SI		7	62	12	24	20	9	11	5	7
SK		14	25	7	33	34	4	1	5	4
FI		7	47	9	33	25	0	4	6	3
SE		8	46	3	21	28	1	6	10	8


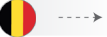
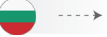
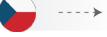
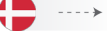
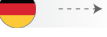
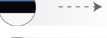
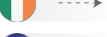
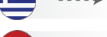
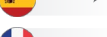
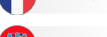
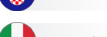
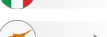
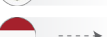
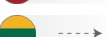
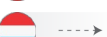
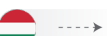

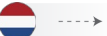
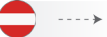
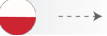

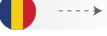

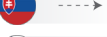
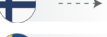
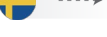

Q10b_3 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Hacking (or attempts to hack) online bank accounts

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		2	72	16	31	18	7	9	11	3
BE		3	72	20	32	13	7	10	27	1
BG		3	66	17	24	11	7	15	5	5
CZ		3	59	12	36	14	2	3	7	2
DK		0	64	11	34	16	6	11	11	2
DE		4	78	27	29	27	13	18	5	5
EE		1	63	9	42	18	2	5	3	0
IE		1	55	14	23	15	8	18	4	11
EL		2	77	22	17	18	8	17	12	0
ES		2	81	15	24	15	8	8	5	2
FR		1	58	8	26	14	1	5	30	3
HR		3	73	14	30	18	4	6	2	2
IT		0	78	18	44	29	8	10	5	2
CY		1	81	25	25	24	5	8	3	2
LV		0	55	22	50	14	2	3	10	1
LT		3	73	27	25	13	3	6	5	2
LU		1	70	20	24	14	5	10	2	0
HU		3	57	22	43	5	1	4	5	2
MT		3	72	14	10	7	4	8	15	4
NL		3	63	7	48	9	4	10	16	1
AT		2	69	18	12	27	6	7	8	3
PL		2	84	6	25	8	3	5	8	1
PT		2	77	15	15	11	8	6	1	8
RO		2	76	29	47	24	29	22	4	7
SI		1	77	18	54	20	6	18	5	0
SK		2	56	19	38	17	4	2	6	2
FI		1	69	8	43	15	1	2	9	1
SE		2	69	8	29	16	4	10	23	3





























Q10b_4 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Phishing, account takeover or impersonation attacks

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		4	73	14	23	19	7	8	7	3
BE		4	73	17	24	14	7	11	14	2
BG		7	61	12	12	13	8	11	5	7
CZ		5	63	5	28	14	2	3	6	3
DK		2	59	9	33	19	6	11	11	3
DE		4	78	24	25	27	14	13	5	4
EE		7	68	9	14	20	2	3	3	0
IE		0	52	17	16	19	16	15	3	12
EL		3	79	17	18	20	8	10	5	1
ES		2	83	14	21	14	9	7	4	2
FR		3	67	8	17	15	1	6	14	3
HR		1	84	11	16	18	4	5	1	2
IT		3	72	19	42	31	8	12	4	3
CY		3	77	18	23	24	3	4	4	4
LV		7	64	19	26	16	2	2	6	3
LT		4	74	13	14	17	5	4	4	5
LU		1	71	17	19	23	5	11	1	0
HU		9	56	8	17	16	1	4	10	6
MT		2	56	11	10	12	7	3	12	7
NL		5	69	9	19	19	2	7	11	3
AT		2	69	15	10	33	6	7	8	4
PL		6	84	5	12	9	4	3	5	3
PT		3	74	11	15	14	7	6	3	7
RO		6	74	29	35	28	28	23	4	7
SI		4	78	10	20	21	7	10	7	2
SK		7	57	10	24	22	2	2	7	4
FI		4	74	8	26	15	0	3	7	1
SE		3	77	6	18	16	1	8	17	4


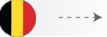
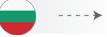
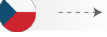
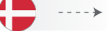
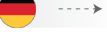
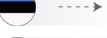
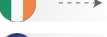
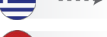
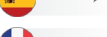
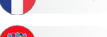
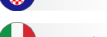
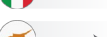
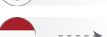
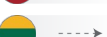
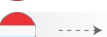
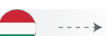

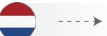
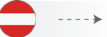
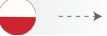

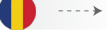

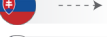
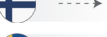
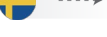

Q10b_5 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Ransomware

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		6	69	12	20	19	6	8	5	5
BE		10	63	13	21	19	5	10	13	2
BG		7	58	12	11	13	7	11	4	15
CZ		14	44	2	17	19	2	2	8	10
DK		1	62	7	31	17	7	10	10	4
DE		4	80	26	22	26	14	13	4	4
EE		9	73	7	11	18	1	4	4	1
IE		1	54	11	19	20	9	12	3	13
EL		4	81	17	18	21	7	10	2	1
ES		2	78	14	19	18	7	7	2	3
FR		6	67	6	18	12	2	6	9	6
HR		5	77	11	14	15	2	3	2	4
IT		5	62	12	39	26	6	9	2	4
CY		4	80	11	23	24	4	5	3	4
LV		12	51	17	16	21	2	3	8	6
LT		4	78	12	13	13	5	5	7	7
LU		3	55	11	24	17	4	9	0	7
HU		8	69	6	9	12	2	4	6	7
MT		3	51	7	12	10	6	3	17	8
NL		6	57	6	20	16	1	7	12	6
AT		0	68	16	6	29	5	7	8	5
PL		6	87	6	8	8	2	3	4	2
PT		4	60	14	11	10	7	6	6	17
RO		16	58	26	30	27	24	19	2	10
SI		3	80	11	19	24	7	12	6	1
SK		16	30	8	24	26	3	2	6	10
FI		2	76	8	18	15	0	2	6	2
SE		4	80	4	16	17	1	8	8	3


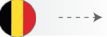
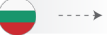
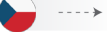
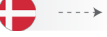
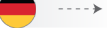
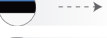
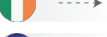
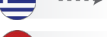
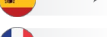
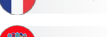
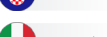
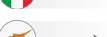
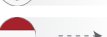
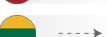
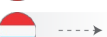
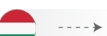

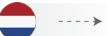
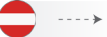
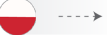

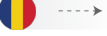

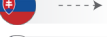
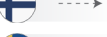
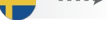

Q10b_6 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Unauthorised accessing of files or networks

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		6	62	12	25	21	7	9	6	5
BE		8	62	13	24	18	7	12	15	2
BG		7	60	16	12	16	8	12	5	9
CZ		10	45	4	24	25	2	2	7	6
DK		2	58	7	31	17	6	11	11	3
DE		5	68	23	21	25	13	15	5	7
EE		6	64	8	14	28	1	3	4	1
IE		1	46	12	23	22	10	15	2	10
EL		5	65	17	20	26	8	12	3	2
ES		4	70	13	25	17	7	5	4	4
FR		7	54	8	24	16	1	7	10	5
HR		5	69	11	18	26	4	5	2	3
IT		1	64	14	48	27	10	12	2	2
CY		2	62	10	32	28	4	7	3	4
LV		11	51	14	20	24	3	2	8	2
LT		6	59	14	14	25	3	4	7	5
LU		3	58	19	23	18	6	13	1	4
HU		9	52	7	16	15	2	5	12	7
MT		4	51	7	11	7	7	2	18	8
NL		6	50	8	23	21	1	10	10	5
AT		4	52	13	7	33	8	9	5	7
PL		8	71	6	13	13	4	3	6	7
PT		1	77	13	13	19	7	7	3	5
RO		10	65	25	32	29	24	17	1	5
SI		5	70	12	18	32	6	13	6	2
SK		10	39	9	28	32	4	2	6	4
FI		7	57	7	30	21	0	3	6	3
SE		12	55	6	19	22	1	8	12	6





























Q10b_7 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Unauthorised listening in to video conferences or instant messages

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representati ve body or trade body	Someone else	Don't know
EU27		9	62	11	20	18	6	7	5	8
BE		16	61	13	18	12	5	10	14	3
BG		8	60	13	12	12	7	13	5	11
CZ		16	51	4	18	15	3	2	7	7
DK		3	57	7	30	16	6	11	11	4
DE		11	58	17	19	25	11	11	5	13
EE		16	58	5	12	19	2	2	3	4
IE		2	44	13	20	19	9	15	3	13
EL		4	73	14	17	21	8	11	2	3
ES		7	71	9	19	14	5	3	2	6
FR		9	57	7	17	13	1	6	9	10
HR		5	74	11	11	17	3	3	1	5
IT		7	67	16	37	25	8	12	1	3
CY		4	65	9	25	29	6	5	3	6
LV		15	48	14	16	17	2	2	7	8
LT		9	53	15	13	21	6	4	5	10
LU		6	61	14	23	14	4	8	0	4
HU		19	45	5	12	13	1	3	5	16
MT		3	51	7	7	8	4	3	11	15
NL		10	58	5	15	16	2	8	10	7
AT		6	50	14	6	26	3	9	5	12
PL		11	71	6	12	13	3	3	5	5
PT		4	74	14	12	11	6	8	2	7
RO		15	65	25	31	27	25	19	2	8
SI		4	78	10	15	23	7	10	6	4
SK		17	43	7	22	21	3	3	6	6
FI		12	51	7	28	17	1	2	6	4
SE		11	55	3	18	15	2	6	11	9

Q10b_8 If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to? Any other breaches or attacks

		Would not report to anyone	The police	Another official authority	Seller or service provider	Your Internet service provider	A consumer protection organisation	A business representative body or trade body	Someone else	Don't know
EU27		7	66	11	21	18	6	7	6	7
BE		8	65	11	23	12	5	9	13	2
BG		9	60	12	12	12	7	14	6	9
CZ		10	67	4	13	14	1	1	5	6
DK		3	57	7	31	16	6	10	12	4
DE		11	66	18	18	23	13	13	4	7
EE		11	60	8	11	24	1	3	6	4
IE		0	53	13	19	25	6	15	4	12
EL		2	77	18	19	22	10	12	3	1
ES		4	75	13	24	14	5	4	2	7
FR		6	63	7	20	12	1	5	11	8
HR		3	71	11	16	19	3	4	1	5
IT		7	66	13	39	28	7	9	1	4
CY		4	69	13	22	20	3	4	4	10
LV		9	54	17	18	14	2	2	6	10
LT		7	59	12	11	21	3	4	6	7
LU		3	73	17	21	12	4	7	1	3
HU		12	62	5	10	9	2	5	7	9
MT		3	54	10	13	17	3	3	17	7
NL		14	49	5	16	12	1	7	11	12
AT		3	63	13	7	28	3	5	5	8
PL		7	78	5	11	11	3	3	6	4
PT		3	74	11	14	14	4	5	4	8
RO		13	65	28	29	24	23	18	2	10
SI		6	72	11	14	19	7	11	8	4
SK		16	36	8	27	21	2	2	6	10
FI		6	69	6	20	16	0	3	6	2
SE		6	52	3	12	17	1	5	11	20

Q11 Why did you not report the incident (or incidents) to the police?

		Expected it would be reported by another authority (e.g. Internet provider/bank)	The police couldn't have done anything	Tried to report it but police were not interested	Dealt with the incident internally	Did not know the police dealt with this type of incident	Inconvenient/too much trouble	Too trivial/not worth reporting	Other	Don't know
EU27		11	23	2	52	16	18	44	7	4
BE		19	28	0	63	9	27	52	14	1
BG		5	29	0	48	14	8	27	13	4
CZ		16	35	0	68	22	29	60	7	1
DK		8	23	4	50	6	12	46	6	3
DE		16	37	0	47	22	24	52	14	10
EE		10	10	2	57	12	8	46	12	3
IE		2	25	7	38	17	9	23	5	8
EL		13	27	2	58	21	13	56	0	0
ES		18	14	0	57	9	12	33	19	0
FR		5	13	4	66	13	1	31	5	5
HR		7	28	2	32	17	4	56	7	0
IT		5	18	3	42	18	16	33	4	4
CY		5	7	0	59	4	5	21	16	0
LV		19	37	3	62	15	20	53	7	2
LT		14	25	2	70	16	18	48	6	3
LU		5	44	10	39	19	6	33	13	6
HU		13	15	0	37	10	9	52	3	3
MT		12	35	0	59	11	20	35	10	6
NL		12	31	3	41	13	19	49	10	7
AT		8	27	1	29	4	15	25	4	6
PL		10	24	2	61	7	31	56	9	4
PT		10	13	8	20	20	12	27	2	16
RO		22	45	3	76	28	38	53	8	5
SI		1	21	0	48	8	9	35	10	4
SK		18	24	1	70	22	42	58	7	4
FI		12	28	1	44	11	24	57	5	2
SE		16	39	0	48	19	21	50	9	8

Flash Eurobarometer 496 - SMEs and cybercrime / Fieldwork: 26/11 - 17/12/2021

(%) Base: n=3 183 - Companies that have experienced at least one type of cybercrime in the last 12 months and did not report the incident to the police

