Cyber Crime: Findings from the 2019/20 Northern Ireland Safe

Community Survey

K Ross

September 2022









Männystrie O tha Laa

www.justice-ni.gov.uk

CONTENTS

	1. Summary Findings	3	Produced by Analytical Services Group, Department of Justice
	2. Introduction	4	For further information write to: Analytical Services Group, Financial Services Division,
	3. Worry about Cyber Crime	5	Department of Justice,
	4. Experience of Cyber Crime	7	Level 3, Block B,
	5. Perceptions of Cyber Crime	10	Castle Buildings, Stormont Estate,
_			Belfast BT4 3SG.
	Appendix 1 - Tabular Annex	14	Telephone: 028 9052 0185
	Appendix 2 - Technical Annex	27	Email: statistics.research@justice-ni.gov.uk

This bulletin is available on the <u>Department of Justice website (opens in a</u> <u>new window)</u>, in the Statistics and Research - Northern Ireland Safe Community Survey section.

Feedback on this publication can be provided directly to Analytical Services Group at the email address listed above.

1 Summary Findings

This bulletin presents findings from the cyber crime module included within the 2019/20 Northern Ireland Safe Community Survey.

- When asked about the cyber crime types most worried about, ranked first, second and third, findings suggest respondents were most likely to worry about identity theft and online banking misuse. Almost half (49%) selected identity theft as their first choice while a further 14% and 8% respectively selected it as their second and third crime types most worried about. Online banking misuse was the first option for just over a quarter (26%) of respondents and the second and third option for 37% and 10% respectively.
- The majority of respondents, two-in-three (66%), had not experienced cyber crime, while 15% indicated that they had been a victim. The remaining respondents, just under a fifth (19%), reported that someone had attempted to commit a cyber crime against them personally.
- Respondents who indicated that they had a cyber crime committed against them were most likely to have been a victim of online banking misuse (54%).
- Three quarters (75%) of those who had been a victim of cyber crime reported the incident(s) to someone. Respondents were most likely to have reported these to their bank, building society or credit card company (74%). For respondents who had not reported the incident(s), the most common reason given for not doing so was 'dealt with the matter myself/ourselves' (50%).
- Less than half (44%) of respondents knew where or how to seek advice about cyber security and staying safe online.
- Of the respondents who indicated they had children, around two-in three (67%) claimed they were very or fairly worried about them while online or using the internet and almost three-quarters (73%) would know how to apply security measures on a child's computer or device to protect them while online.
- Half (50%) of respondents were confident (either 'very' (4%) or 'fairly' (46%)) that the criminal justice system, government and police deal effectively with cyber crime. The same proportion had little or no confidence, with 40% and 10% respectively being 'not very' or 'not at all' confident.

2 Introduction

2.1 The focus of this publication

This bulletin draws on findings from the 2019/20 Northern Ireland Safe Community Survey (NISCS). The survey was formerly known as the Northern Ireland Crime Survey (NICS) but was renamed following a review in 2017/18. NISCS is a representative, continuous, personal interview survey of the experiences and perceptions of crime of 3,710 adults living in private households throughout Northern Ireland. Previously conducted on an ad hoc basis in 1994/95, 1998, 2001 and 2003/04, the survey began operating on a continuous basis in January 2005.

The focus of this publication is on a module contained within the NISCS relating to cyber crime. As part of the aforementioned review of the survey, this module was developed and asked for the first time in 2019/20 and will be included biennially thereafter. While the module asks about both experience and perceptions of cyber crime, respondents' experiences were not collected in the same way as, and are therefore not comparable with, the main victimisation estimates derived from the NISCS or those from the <u>Crime Survey for England and Wales (opens in a new window)</u>.

While some questions contained within the module were asked of all respondents, others were asked only of those who responded, via a separate question at the start of the module, that they used a computer, smartphone or other device to access the internet (83% of participants in 2019/20, Table 1, Appendix 1). The questions asked respondents about 'online/cyber crime' which will hereafter be referred to collectively as 'cyber crime'.

Throughout this report key findings are commented on in the text, with numerical details on each section available in the relevant tables comprising the Tabular Annex (Appendix 1). Figures can also be found in the accompanying Microsoft Excel and Open Data Source documents.

Further background information on this bulletin is available in the Technical Annex (Appendix 2). Additional NISCS 2019/20 reports on Experience of Crime (opens in a new window) (Campbell, Rice and Ross, February 2021), Perceptions of Crime (opens in a new window) (Ross and Campbell, March 2021) and Perceptions of Policing and Justice (opens in a new window) (Campbell, Ross and Rice, June 2021) have been published separately.



3.1 Worry about cyber crime

Respondents to the 2019/20 NISCS were presented with a list of some of the more common types of cyber crime and were asked to rank in order, first, second and third, those that they worried about most. Figures are presented in Table 2. The options included were:

- Identity theft
- Online blackmail
- Online banking misuse
- Online romance fraud or extortion
- Cyber bulling or harassment
- Receiving calls or messages claiming an issue with their device or service asking for remote access or fees to fix it
- Being tricked into sending money or personal details or clicking on a fraudulent link/email/text
- Purchasing goods online that are counterfeit, not as advertised or not delivered
- Receiving unwanted, inappropriate material from an unknown source online
- Having their computer or device infected or interfered with by a virus
- Damage and loss to their business due to online fraud
- Don't really worry about any of these
- Findings show respondents were most likely to worry about identity theft and online banking misuse, with 49% and 26% respectively selecting them as their first option.
 For identity theft, a further 14% and 8% of respondents selected it as their second or third option, while the equivalent figures for online banking misuse were 37% and 10% respectively.

3 Worry about Cyber Crime

Respondents were least likely to worry about online romance fraud or extortion and damage and loss to their business due to online fraud with less than 0.5% of respondents selecting each of these as their first choice.

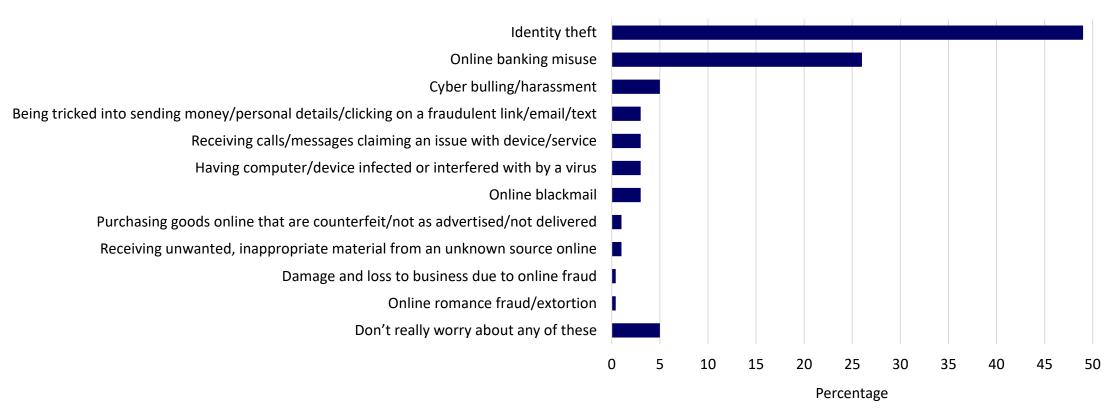


Figure 3.1: Worry about cyber crime: crime types ranked first by respondents (%), 2019/20

4 Experience of Cyber Crime

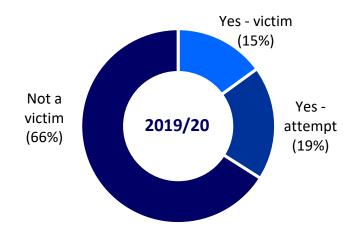
4.1 Experience of cyber crime

Questions were also included in the module to gauge respondents' experiences of cyber crime. Initially, participants were asked whether anyone had committed or attempted to commit cyber crime against them personally, either on their own personal or a workplace computer or device. The alternative response options were:

- Yes, I have been the victim of an online/cyber crime
- Yes, someone attempted to commit a crime online against me
- No

NISCS participants who had been a victim, that is those selecting the first option above, were then subsequently asked about the type(s) of cyber crime that they had experienced. The same crime types, as listed in section 3.1 (Worry about Cyber Crime), were presented to respondents. Results for these questions are given in Tables 3 and 4. The proportion of respondents who were a victim and subsequent sample size should be taken into consideration when reviewing results for the types of crime experienced and the follow-up questions asked of victims only. Findings presented in Table 3 suggest that the majority of respondents, two-inthree (66%), had not experienced cyber crime with 15% indicating that they had been a victim. The remaining respondents, just under a fifth (19%), reported that someone had attempted to commit a cyber crime against them personally.





1. Results exclude don't knows and refusals.

Of the respondents who had experienced cyber crime (not including attempts), over half (54%) had been a victim of online banking misuse, followed by over a fifth (22%) who had received calls or messages claiming an issue with their device or service and requesting access or a fee to repair it.

4 Experience of Cyber Crime

In contrast, at 1% each, online romance fraud or extortion and damage and loss to their business due to online fraud were among the crime types least likely to be experienced by participants.

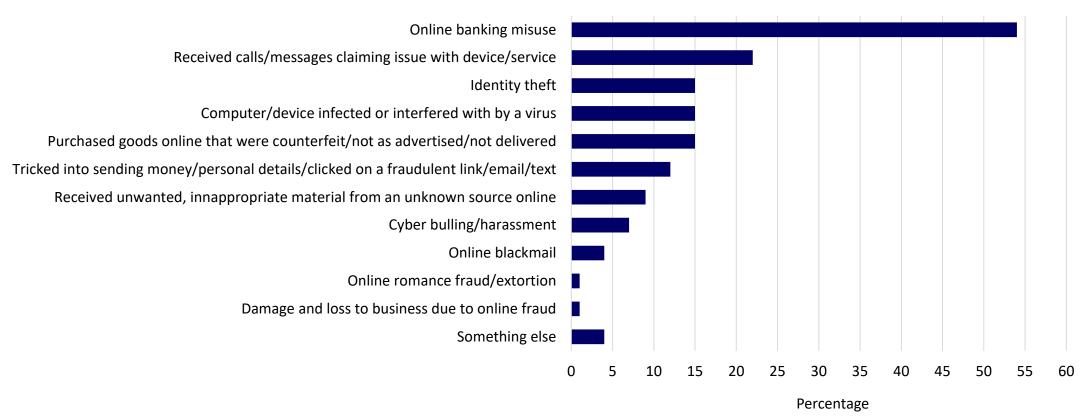


Figure 4.2: Experience of cyber crime by crime type (%), 2019/20

4 Experience of Cyber Crime

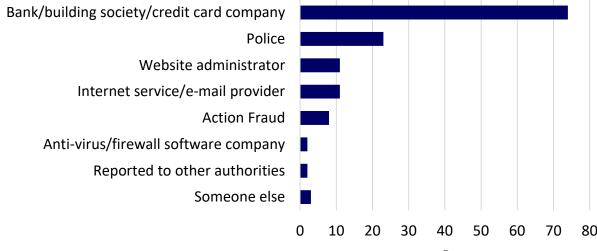
4.2 Reporting of cyber crime incidents

Tables 5 and 6 present findings on whether those who had experienced cyber crime reported the incident(s) to anyone and, if so, to whom it was reported. Respondents were presented with a list of organisations; more than one option could be selected. Participants were also asked if they felt their report(s) was dealt with satisfactorily (Table 7). For those who had not reported their experience of cyber crime, the reasons for not doing so are given in Table 8.

- Of the respondents who had experienced cyber crime, the vast majority, three quarters (75%), had reported the incident(s). When asked to whom it was reported, respondents were by far most likely to have reported it to their bank, building society or credit card company (74%). Just under a quarter (23%) of NISCS participants had reported the incident to the police. Almost nine-in-ten (87%) respondents felt their report was dealt with satisfactorily.
- At 50%, 'dealt with the matter myself/ourselves' was the most common reason given by respondents for not reporting an incident, while 'dislike/fear of police' (1%) was among the least likely reasons to be given.

Figure 4.3: Reporting of cyber crime incidents: to whom

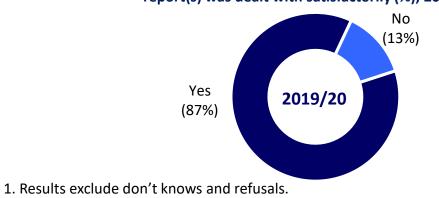
the incident(s) was reported (%), 2019/20



1. Results exclude don't knows and refusals.

Percentage

Figure 4.4: Reporting of cyber crime incidents: whether the report(s) was dealt with satisfactorily (%), 2019/20





5.1 Protection or steps taken to safeguard against cyber crime

Respondents who used a computer, smartphone or other device to access the internet were then asked about any protection or steps they take to safeguard themselves against cyber crime. Respondents were again offered a range of response options such as 'use strong passwords' and 'update software regularly'. Participants were able to select more than one response; a 'None' option was also included for respondents who do not take any steps. Results are given in Table 9.

At 81%, respondents were most likely to use strong passwords to protect themselves against cyber crime. Other common steps taken by respondents included ignoring popup requests or fraudulent e-mails asking for personal information (68%), installing anti-virus or firewall software on their device (64%) and limiting personal detail shared on social media (61%). A small proportion of respondents, 2%, reported that they do not take any steps to safeguard themselves against becoming a victim of cyber crime.

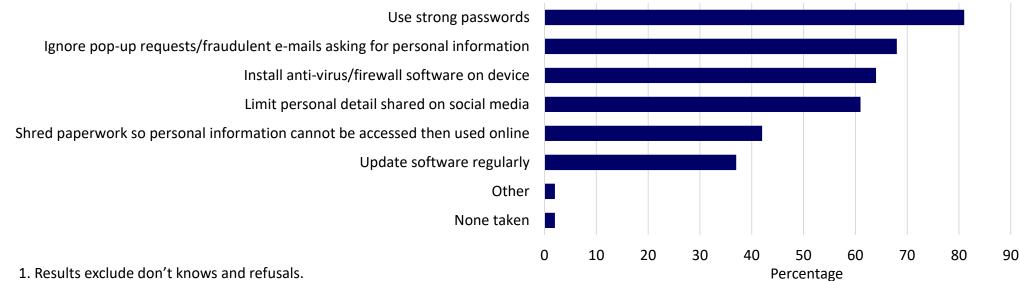


Figure 5.1: Protection or steps taken to protect against cyber crime (%), 2019/20

5 P

Perceptions of Cyber Crime

5.2 Awareness of help available and communication to the public

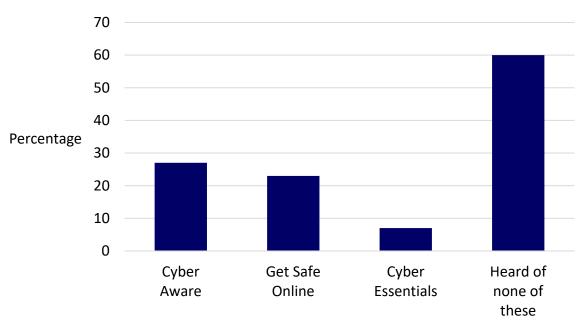
Questions were also included in the module to ascertain respondents' awareness of the help available for staying safe while online and to gauge their views of the best way to communicate information regarding cyber crime to the public. All respondents were asked:

- whether they knew where or how to seek advice about cyber security and staying safe online if they required it.
- whether they had heard of any of the following websites that provide advice about keeping safe online.
 - \circ GetSafeOnline
 - CyberAware
 - \circ CyberEssentials
- what they felt was the best way for the police, government and other agencies to get any messages about cyber crime across to the public in general.

Results can be found in Tables 10 to 12 respectively.

 Findings suggest that a higher proportion of respondents, 56%, did not know where or how to seek advice about staying safe online while 44% were aware of where to seek guidance regarding cyber security if required. In terms of awareness of the specific websites that provide advice about staying safe online, the majority of respondents, three-in-five (60%), had not heard of any of the three websites covered. Over a quarter of participants (27%) had heard of Cyber Aware, 23% had heard of Get Safe Online, while 7% were aware of the Cyber Essentials website.

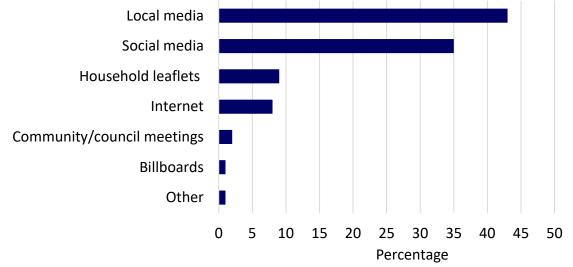
Figure 5.2: Awareness of cyber security advice websites (%), 2019/20



5 Perceptions of Cyber Crime

 Local media, selected by 43% of respondents, was considered as the best way for the police, government and other agencies to get any messages about cyber crime across to the public in general. This was followed by over a third (35%) who felt social media was the best method to convey information. In contrast, billboards (1%) and community/council meetings (2%) were least likely to be considered as the most effective way to communicate messages to the public.

Figure 5.3: Best way to communicate messages to the public about staying safe online (%), 2019/20



1. Results exclude don't knows and refusals.

5.3 Worry about children's safety while online

Respondents were then asked about the extent to which they worried about their children when they are online or using the internet, for example, being bullied, encountering unwanted inappropriate material, being groomed, being forced or encouraged to do something they shouldn't. A four point scale was used ranging from 'very worried' to 'not at all worried'. A 'not applicable/don't have children aged under 18' option was also included.

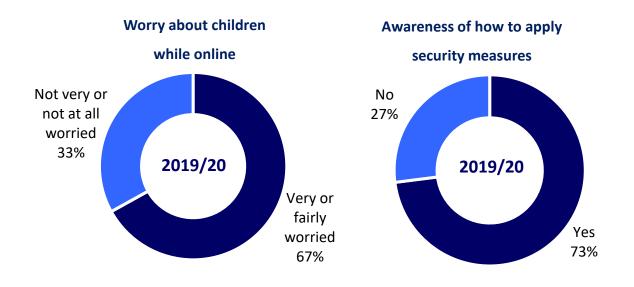
Findings showed that a substantial proportion of respondents, 61%, selected the not applicable option for this question. These responses were subsequently excluded and levels of worry recalculated to cover only those to whom the question did apply i.e. those who selected a level of worry as their response, thereby indicating they had children. While the figures presented in this section are based on the latter (i.e. excluding not applicable responses), both sets of results can be viewed in Table 13.

This subset of respondents was also asked a follow-up question on whether they would know how to apply security measures, for example parental controls and passwords, on their child(rens) computer or device to help protect them while online, figures for which are given in Table 14.

5 Perceptions of Cyber Crime

 Two-in-three (67%) respondents reported being very or fairly worried about their child(ren) while they are online or using the internet, while almost threein-four (73%) would know how to apply security measures on their child(rens) computer or device to help protect them while online.

Figure 5.4: Worry about children while online or using the internet and awareness of how to apply security measures on a computer or device (%), 2019/20



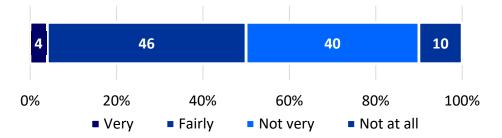
1. Results exclude don't knows and refusals.

5.4 Confidence in the criminal justice system, government and police

Finally, confidence levels were sought from respondents who were asked whether they were confident that the criminal justice system (CJS), government and police deal effectively with cyber crime. Again, a four point scale was used ranging from 'very confident' to 'not at all confident', figures for which are given in Table 15.

 Results show an equal split in the proportion expressing at least some confidence and those showing little or no confidence that the CJS, government and police deal with cyber crime effectively. Half of participants were either very or fairly confident (4% and 46% respectively) it is dealt with effectively, while an equivalent proportion were either not very (40%) or not at all (10%) confident.

Figure 5.5: Confidence that cyber crime is dealt with effectively (%), 2019/20



Appendix 1: Tabular Annex

 Table 1: Use of a computer, smartphone or other device that enables access to the internet (%)

% saying whether they use a computer, smartphone or other device		
Yes	83	
No	17	
Unweighted base	3,700	

Source: Northern Ireland Safe Community Survey 2019/20

Table 2: Types of cyber crime most worried about, ranked first, second and third (%)

% saying they are worried about	First	Second	Third
Identity theft	49	14	8
Online banking misuse	26	37	10
Cyber bullying or harassment	5	8	10
Being tricked into sending money or personal details or clicking on a fraudulent link/email/text	3	9	15
Receiving calls or messages claiming an issue with their device or service asking for remote access or fees to fix it	3	8	14
Having their computer or device infected or interfered with by a virus	3	8	19
Online blackmail	3	5	3
Purchasing goods online that are counterfeit, not as advertised or not delivered	1	6	12
Receiving unwanted, inappropriate material from an unknown source online	1	3	5
Damage and loss to their business due to online fraud	<0.5	1	2
Online romance fraud or extortion	<0.5	1	2
Don't really worry about any of these	5	-	-
Unweighted base	2,892	2,654	2,431

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who said they use a computer, smartphone or other device that enables access to the internet.

Table 3: Experience of cyber crime (%)

% saying	
Yes – I have been the victim of an online/cyber crime	15
Yes – someone attempted to commit a crime online against me	
No	66
Unweighted base	2,889

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who said they use a computer, smartphone or other device that enables access to the internet.
- 3. Respondents were asked whether anyone has committed, or attempted to commit, cyber crime against them personally, either on their own personal computer/device or a workplace computer/device.

Table 4: Experience of cyber crime by type of crime (%)

% saying they have experienced the following	
Online banking misuse	54
Received calls or messages claiming an issue with their device or service asking for remote access or fees to fix it	22
Identity theft	15
Had their computer or device infected or interfered with by a virus	15
Purchased goods online that are counterfeit, not as advertised or not delivered	15
Tricked into sending money or personal details or clicking on a fraudulent link/email/text	
Received unwanted, inappropriate material from an unknown source online	9
Cyber bullying or harassment	7
Online blackmail	4
Online romance fraud or extortion	1
Damage and loss to their business due to online fraud	1
Something else	4
Unweighted base	439

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who had been a victim of cyber crime.
- 3. Respondents could select more than one type of crime.

Table 5: Reporting of cyber crime: whether the incident(s) was reported to anyone (%)

% saying	
Yes	75
No	25
Unweighted base	439

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who had been a victim of cyber crime.

 Table 6: Reporting of cyber crime: who the incident(s) was reported to (%)

% saying they reported the incident(s) to	
Bank, building society or credit card company	74
Police	23
Website administrator	11
Internet service or e-mail provider	11
Action Fraud	8
Anti-virus or firewall software company	2
Reported to other authorities	2
Someone else	3
Unweighted base	328

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who had been a victim of cyber crime and had reported the incident(s) to someone.
- 3. Respondents could select more than one response.

Table 7: Reporting of cyber crime: whether the report was dealt with satisfactorily (%)

% saying	
Yes	87
No	13
Unweighted base	323

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who had been a victim of cyber crime and had reported the incident(s) to someone.

Table 8: Reporting of cyber crime: reasons given for not reporting the incident(s) (%)

% saying	
Dealt with matter myself/ourselves	50
No loss or damage/police would not have been interested	22
Inconvenient/too much trouble	12
Didn't know how to report it	8
Partly my/a relative's/a friend's fault or felt too ashamed or embarrassed to report it	7
Dislike/fear of police	1
Other	16
Unweighted base	111

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who had been a victim of cyber crime and had not reported the incident(s) to anyone.
- 3. Respondents could select more than one response.

Table 9: Protection or steps taken to safeguard against cyber crime (%)

% saying they	
Use strong passwords	81
Ignore pop-up requests or fraudulent e-mails asking for personal information	68
Install anti-virus/firewall software on device	64
Limit personal detail shared on social media	61
Shred paperwork so personal information cannot be accessed then used online	42
Update software regularly	37
Other	2
None taken	2
Unweighted base	2,907

- 1. Results exclude don't knows and refusals.
- 2. Asked of respondents who said they use a computer, smartphone or other device that enables access to the internet.
- 3. Respondents could select more than one response.

Table 10: Awareness of where or how to seek advice about cyber security and staying safe online (%)

% saying whether or not they know where or how to seek advice		
Yes	44	
No	56	
Unweighted base	3,683	

Source: Northern Ireland Safe Community Survey 2019/20

1. Results exclude don't knows and refusals.

Table 11: Awareness of websites that provide advice about keeping safe online (%)

% saying they had heard of	
Cyber Aware	27
Get Safe Online	23
Cyber Essentials	7
Haven't heard of any of these	60
Unweighted base	3,707

Source: Northern Ireland Safe Community Survey 2019/20

Table 12: Best way for the police, government and other agencies to convey messages about cyber crime to the public in general (%)

% saying	
Local media (for example TV, newspapers, radio)	43
Social media (for example Facebook, Twitter, Instagram, YouTube)	35
Household leaflets	9
Internet	8
Community/council meetings	2
Billboards	1
Other	1
Unweighted base	3,609

Source: Northern Ireland Safe Community Survey 2019/20

Table 13: Worry about children when online or using the internet (%)

% saying	All respondents	Excluding 'Not applicable/don't have children under 18'
Very worried	13	33
Fairly worried	13	33
Not very worried	7	19
Not at all worried	5	14
Not applicable/don't have children under 18	61	-
Unweighted base	3,679	1,359

- 1. Results exclude don't knows and refusals.
- 2. Percentages may not sum to 100 due to rounding. Similarly, the combined proportion who were very/fairly worried, referenced in section 5.3, is 67%. The individual figures given in the above table do not sum to this due to rounding.
- 3. The 'Excluding Not applicable/don't have children under 18' figures are based on respondents who selected a level of worry as their response, thereby indicating they had children.

Table 14: Awareness of how to apply security measures on a child(rens) computer or device to help protect them while online (%)

% saying whether or not they know how to apply security measures		
Yes	73	
No	27	
Unweighted base	1,358	

Source: Northern Ireland Safe Community Survey 2019/20

- 1. Results exclude don't knows and refusals.
- 2. This was not asked of those who responded 'Not applicable/don't have children under 18' to the question covered in Table 13.

Table 15: Confidence that the criminal justice system, government and police deal effectively with cyber crime (%)

% saying they are	
Very confident	4
Fairly confident	46
Not very confident	40
Not at all confident	10
Unweighted base	3,370

Source: Northern Ireland Safe Community Survey 2019/20

Appendix 2: Technical Annex

About the NISCS

Closely mirroring the format and core questions of the CSEW, the NISCS is an important source of information about community safety issues such as levels of, and public attitudes to, crime and anti-social behaviour. Its results play an important role in informing and monitoring government policies and targets. Within the <u>2016-21 Draft Programme for</u> <u>Government (opens in a new window)</u> (PfG) and the <u>Northern Ireland Civil Service Outcomes Delivery Plan (opens in a new window)</u>, the Department of Justice lead on Indicator 1 related to reducing crime. Survey findings also informed the <u>Northern Ireland Policing Board's Strategic Outcomes for Policing in Northern Ireland 2016-2020 (opens in a new window)</u> (NIPB, 2016) and the <u>Annual Policing Plan 2019-20 (opens in a new window)</u> (NIPB, 2019).

An alternative, but complementary, measure of crime to offences recorded by the police, the main aims of the NISCS are to:

- measure crime victimisation rates experienced by people living in private households regardless of whether or not these crimes were reported to, or recorded by, the police;
- monitor trends in the level of crime, independent of changes in reporting levels or police recording practices;
- measure people's perceptions of and reactions to crime (for example, the level and causes of crime, the extent to which they are concerned about crime and the effect of crime on their quality of life);
- measure public confidence in policing and the wider criminal justice system; and
- collect sensitive information, using self-completion modules, on people's experiences regarding crime-related issues, such as domestic violence.

Recorded crime figures cannot, by their nature, provide an impression of the extent of concern about crime (often described as 'fear of crime') among different sections of the community. Hence, it is necessary to complement the police figures with information drawn from the NISCS, which, for the crime types it covers, provides a more complete measure of the extent and impact of crime against private households and their adult occupants. Further information on recorded crime statistics can be found in the <u>Police Service of</u> <u>Northern Ireland (PSNI) User Guide to Police Recorded Crime Statistics (opens in a new window) (PDF, 1MB)</u> (PSNI, 2018). While some of the core interviewer-administered modules for NISCS 2019/20 were (generally) based on CSEW 2019/20, some modification has been necessary to reflect local issues and the fact that the smaller NISCS sample size would not have generated robust results for follow-up questions asked of small sub-sections of the sample.

Frequency and sample size of the NICS/NISCS

Initially, the then NICS was conducted on an ad hoc basis, before becoming a biennial survey in 2001. At that time, the Community Attitudes Survey (CAS) was also being conducted on a continuous basis, facilitating annual reports on topics linked to crime, policing and the criminal justice system. Increasingly, however, the CSEW was becoming a key vehicle to track progress against Public Service Agreement (PSA) and other targets related to the criminal justice and health sectors in England and Wales. Hence, interest increased among officials and Ministers in what the NICS had to offer in terms of direct comparison, while, in light of the improved security situation, many of the issues originally covered by CAS were becoming less relevant.

Accordingly, it was decided that a more effective use of resources would be to discontinue CAS at the end of 2003 and to move fieldwork for the NICS to a continuous basis with effect from January 2005. This would facilitate the monitoring of annual trends and more regular direct comparison with England and Wales. It was also decided to increase the target achieved sample size for the NICS from 3,000 to 4,000. This would contribute to increased accuracy of headline results and generate more robust analyses for various socio-demographic characteristics. However, unavoidable budgetary pressures resulted in the need to reduce the target achieved sample size; a moderate decrease was first made in-year 2013/14, from 4,000 to 3,500, with a full sample reduction to 2,000 first being implemented in 2014/15. Following a review of the survey during 2017/18 (details of which can be found in the <u>Safe Community Survey (opens in a new window)</u> section of the Department of Justice website), the target sample size has been increased with effect from April 2018 onwards. It is anticipated that around 3,500 interviews will now be achieved annually. Additional information, covering issues such as sampling design and methodology is available within the survey <u>User Guide (opens in a new window)</u> (DoJ, 2022) and associated <u>Quality Report (opens in a new window)</u> (DoJ, 2019).

Sampling and fieldwork

The initial NISCS 2019/20 sample consisted of 7,500 addresses, randomly selected from the NISRA Address Register (NAR). The NAR is developed within NISRA and is primarily based on the Land and Property Services (LPS) POINTER database. Visits to each address by an interviewer from the NISRA Central Survey Unit resulted in an eligible sample of 6,576 occupied addresses, from which attempts were made to interview one randomly selected adult respondent at each address.

Selecting only one person at each address means that individuals living in large households have a lower chance of being included in the sample than those living in small households. Accordingly, the data presented in this publication have been weighted by household size to prevent a bias towards small household sizes.

In January 2005, the then NICS began operating on a continuous basis. This bulletin refers primarily to fieldwork undertaken during the financial year 1 April 2019 to 31 March 2020, which involved complete interviews with 3,710 people aged 16 years and over. This represents an eligible response rate of 56%.

Respondents were assured in advance of the interviews that any information they provided would be treated as entirely confidential and that the level of detail produced in publications or in any subsequent analyses would not allow for identification of individuals. The interviews typically lasted under an hour for non-victims, although those involving respondents who disclosed several crimes could last much longer.

Rounding, error and statistical significance

Don't knows, refusals and non-valid responses have been excluded from the analyses. Percentages may not always sum to 100 or numbers may not sum to an overall total due to the effect of rounding. Full unrounded figures are available in the accompanying Microsoft Excel and Open Data Source versions of the Tabular Annex.

Due to a combination of both sampling and non-sampling error, any sample is unlikely to reflect precisely the characteristics of the population. Because NISCS estimates are subject to sampling error, differences between estimates from successive years of the survey or between population subgroups may occur by chance. For the purposes of the survey, where differences emerge as being statistically significant, these are reported at the 5% (p<0.05) level of probability (two-tailed tests). This means that, for any observed result that is found to be statistically significant, one can be 95% confident that this has not happened by chance.

As a result of the sample reduction in recent years, the respective confidence limits of any percentages from the survey were wider than was the case previously and the margin of difference between findings required to achieve 'statistical significance' was widened accordingly. This means that absolute differences in percentages which would previously have been 'statistically significant' with the larger numbers then sampled (and the much narrower range of error for any findings) may not necessarily be found to be statistically significant with the reduced sample size. This should be borne in mind when considering any long-term trends presented in survey tables.

Further information on the 2019/20 sweep of the NISCS is contained within the NISCS 2019/20 Technical Report (forthcoming, via the <u>Safe Community Survey (opens in a new</u> <u>window</u>) section of the Northern Ireland Department of Justice website).

Appendix 3: National Statistics Status



National Statistics status means that our statistics meet the highest standards of trustworthiness, quality and public value, and it is our responsibility to maintain compliance with these standards.

The designation of these statistics as National Statistics was confirmed in July 2020 following a <u>Compliance Check (opens in a</u> <u>new window)</u> by the <u>Office for Statistics Regulation (opens in a new window)</u>. NISCS statistics last underwent a <u>full assessment</u> (<u>opens in a new window</u>) against the <u>Code of Practice (opens in a new window</u>) in 2012/13.

As part of the recent compliance check, we have made the following improvements:

 published a <u>Future Programme of Work (opens in a new window)</u> that details the list of developments that the department plan to scope in terms of feasibility of implementation.

Appendix 4: References

Campbell, P, Rice A and Ross, K. (2021) Experience of Crime: Findings from the 2019/20 Northern Ireland Safe Community Survey (opens in a new window). DoJ Research and Statistical Bulletin. Belfast: DoJ

Campbell, P, Ross K and Rice, A. (2021) <u>Perceptions of Policing and Justice: Findings from the 2019/20 Northern Ireland Safe Community Survey (opens in a new window)</u>. DoJ Research and Statistical Bulletin. Belfast: DoJ

Department of Justice (2022) Northern Ireland Safe Community Survey User Guide (opens in a new window)

Department of Justice (2019) Northern Ireland Crime Survey Quality Report (opens in a new window)

Northern Ireland Executive (2016) Programme for Government 2016-21 and Outcomes Delivery Plan (opens in a new window)

Northern Ireland Policing Board (2019) Annual Policing Plan 2019-20 (opens in a new window)

Northern Ireland Policing Board (2016) Strategic Outcomes for Policing in Northern Ireland 2016-2020 (opens in a new window)

Office for National Statistics (ONS) (2020) Crime in England and Wales: year ending March 2020 (opens in a new window)

Police Service of Northern Ireland (2018) User Guide to Police Recorded Crime Statistics in Northern Ireland (opens in a new window) (PDF, 1MB) (Updated January 2018)

Ross, K. and Campbell, P. (2021) <u>Perceptions of Crime: Findings from the 2019/20 Northern Ireland Safe Community Survey (opens in a new window)</u>. DoJ Research and Statistical Bulletin. Belfast: DoJ