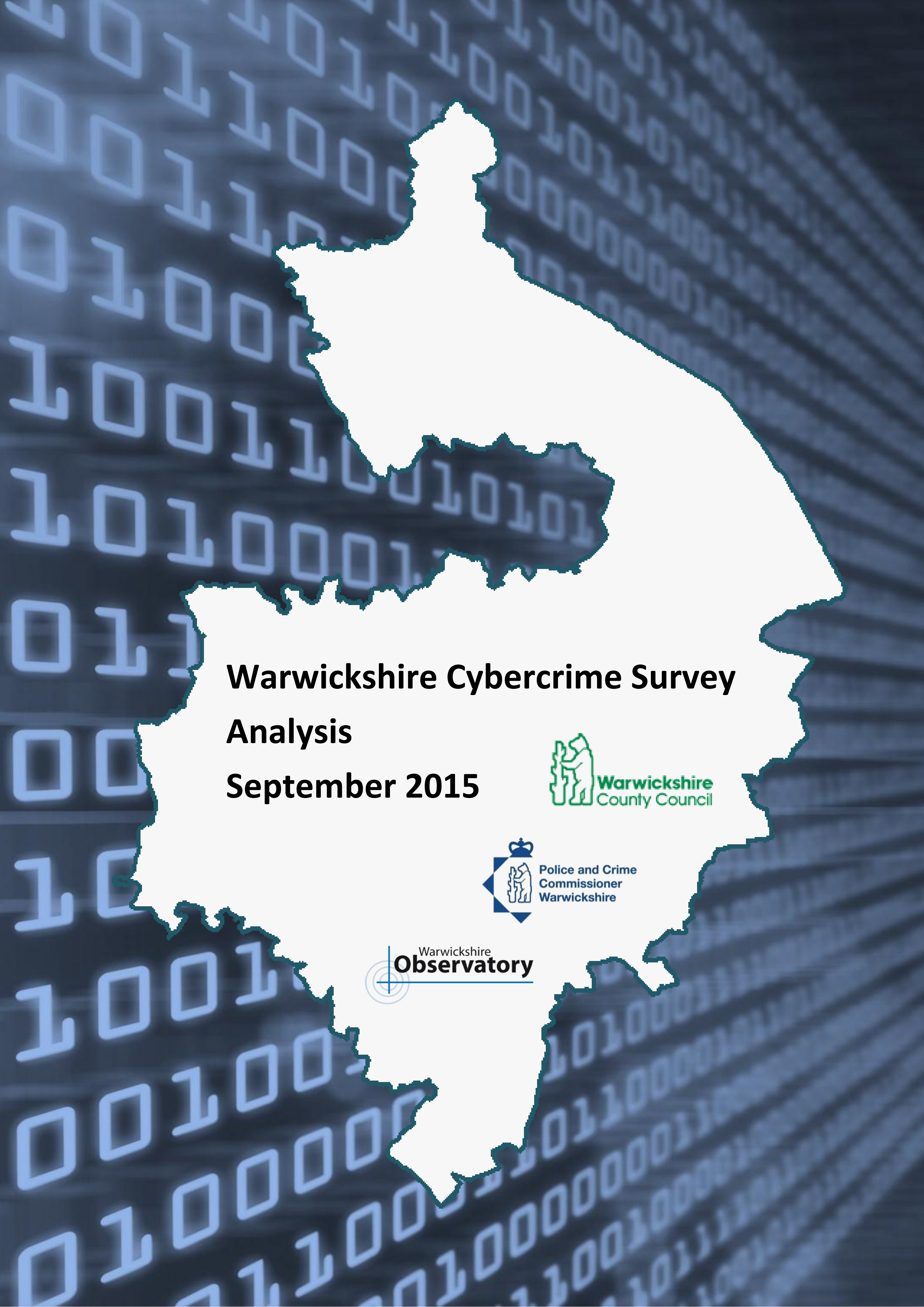


Warwickshire Cybercrime Survey Analysis

September 2015

Warwickshire County Council

Police and Crime Commissioner Warwickshire

Warwickshire Observatory

Introduction

The Warwickshire Cybercrime Survey ran from the 10th of February through to the 4th of May during which time a total of 766 responses were received. Participants were directed to the SurveyMonkey website and taken through a series of 36 questions.

Background

While there is no single definition of Cybercrime, it can be summed up as a term used to define any crime that takes place online or where a digital system is targeted by means of a criminal attack. On a national scale, Britain's 'National Security Strategy' rates Cybercrime as a Tier 1 threat on a par with international terrorism.

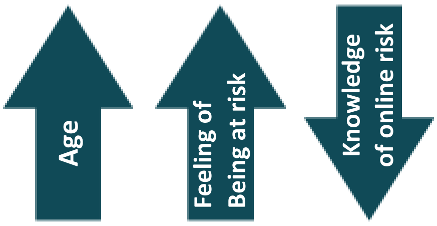
While Cybercrime is a major focus on a national scale, it is acknowledged that there is a fundamental lack of information about Cybercrime on a local level. Agencies such as Action Fraud and Trading Standards collect vital information on Cybercrime and the police have introduced a Cybercrime marker which can be applied to relevant offences. However, there is no single body which brings together all of the reported Cybercrime offences to give a true picture of the scale of the problem. Added to this is the knowledge that there is a significant volume of Cybercrime which is not reported or goes undetected.

Objective

The aim therefore of the survey is to start to build a picture of how Cybercrime affects people on a day-to-day basis giving a snap-shot of the types of Cybercrime that residents are falling victim to and to gauge how at risk people feel of being subjected to Cybercrime.

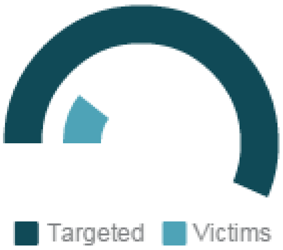
Note: The population of Warwickshire makes up 1% of the population of England. This makes Warwickshire an ideal sample area from which to gauge what is happening nationally.

Key Findings



As age increases, knowledge of online risks reduces slightly while the feeling of being at risk increases significantly

Over half of the respondents were targeted by phishing scams with 1 in 10 becoming victims



2.4%

Of respondents have no idea how to protect themselves online

Equivalent of

13,238

Residents in Warwickshire

Under 18s are the age group most targeted for online harassment or bullying with females targeted twice as much as males

#1

"Did not think anyone could help" was the number one reason for not reporting Cybercrime followed by "Did not know who to report it to"

One in five that spend over 7 hours a day online will become a victim of Cybercrime

Nearly one third of parents have neither applied online restrictions nor spoken to their children about internet safety

14.9%

Of respondents had been a victim of online crime in the last 12 months

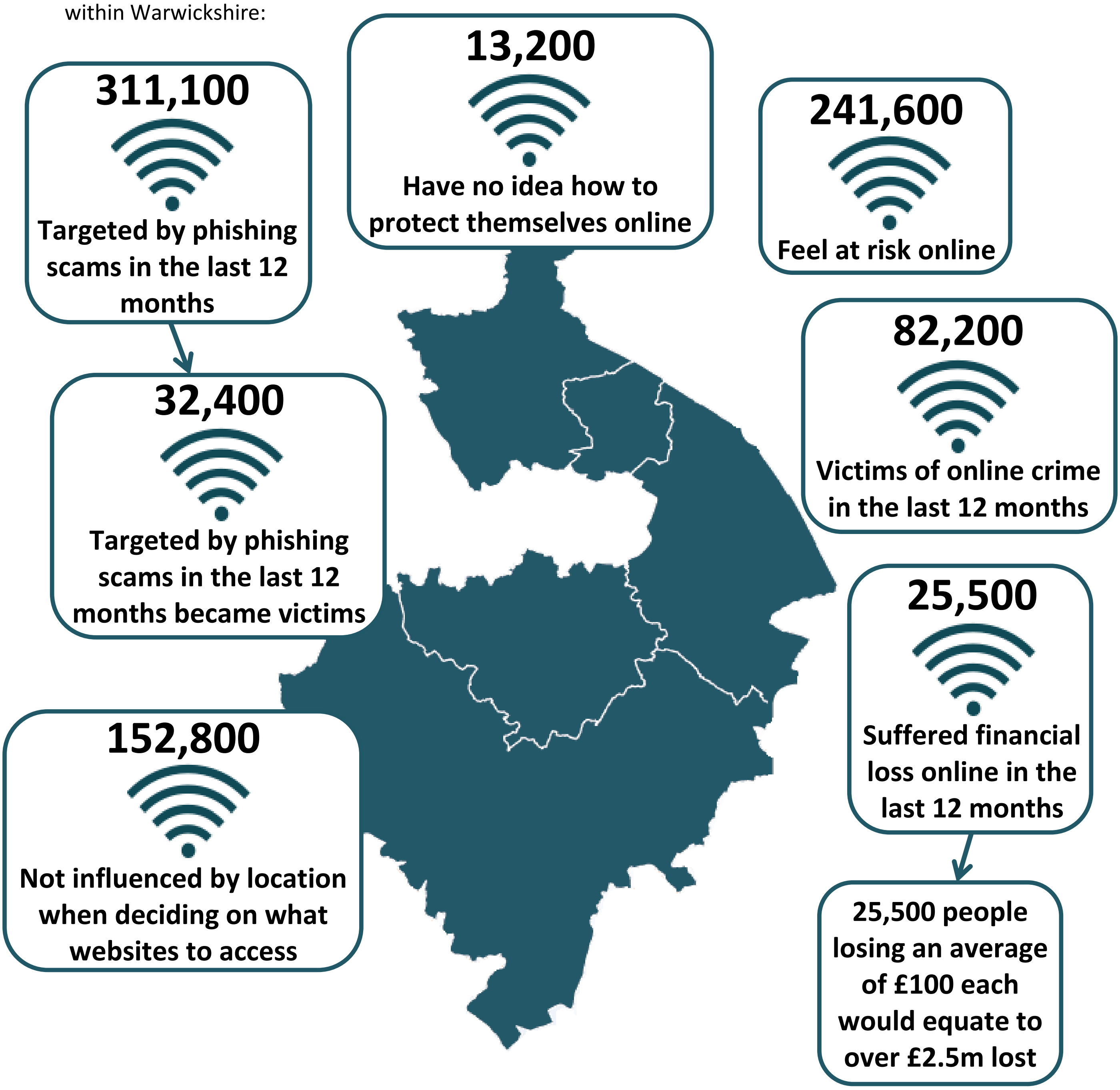
Equivalent of

82,187

Residents in Warwickshire

Key Findings - Potential Warwickshire Implications

The following visualisation has been created by scaling up the responses to questions within the survey. The percentage of respondents for the selected questions has been applied to the Warwickshire population of 551,594 (ONS Census, 2014 mid-term population estimate). This gives an idea of the potential numbers of people who may be affected by different aspects of Cybercrime within Warwickshire:



311,100 Targeted by phishing scams in the last 12 months

32,400 Targeted by phishing scams in the last 12 months became victims

13,200 Have no idea how to protect themselves online

241,600 Feel at risk online

82,200 Victims of online crime in the last 12 months

25,500 Suffered financial loss online in the last 12 months

25,500 people losing an average of £100 each would equate to over £2.5m lost

152,800 Not influenced by location when deciding on what websites to access

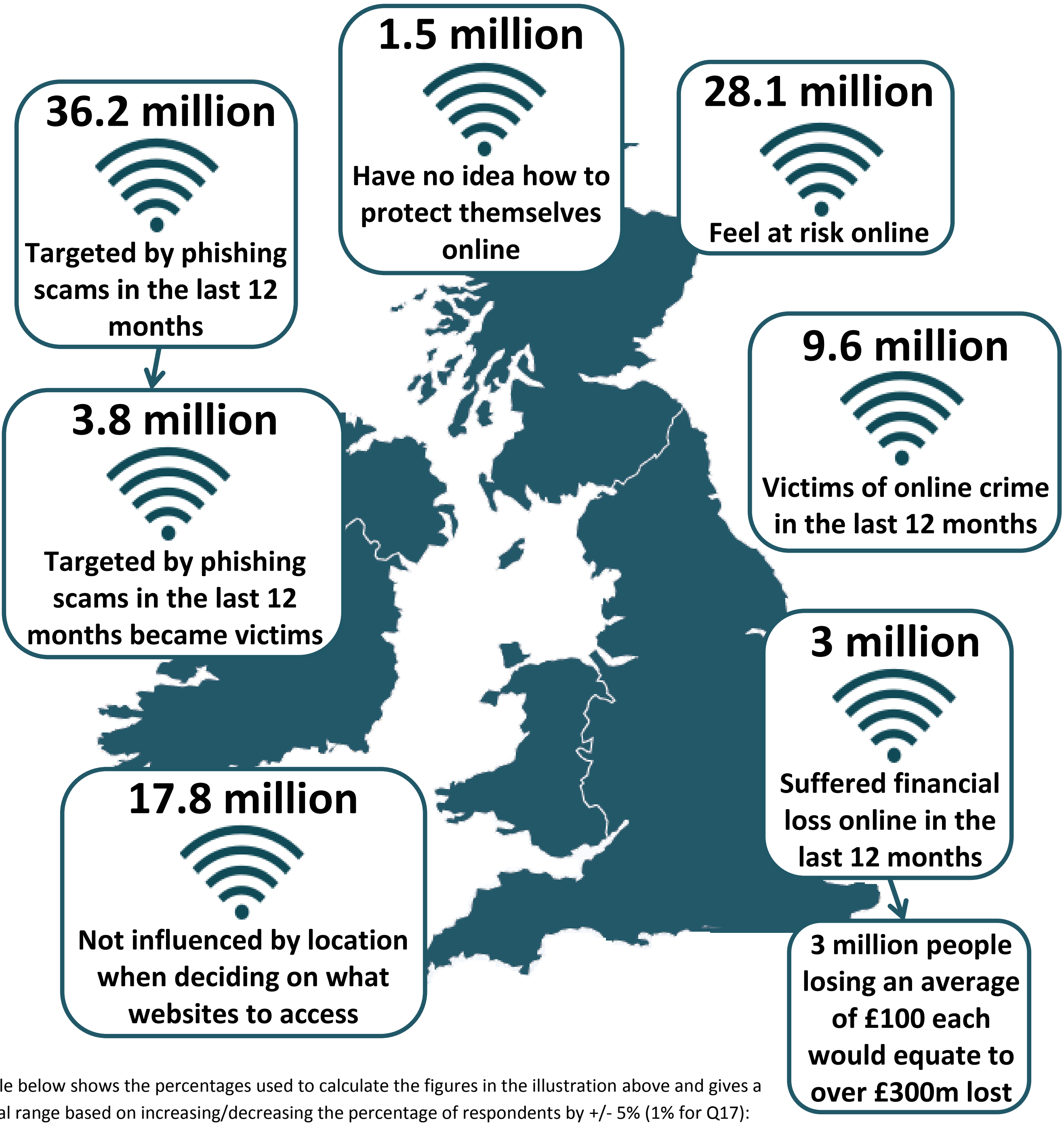
The table below shows the percentages used to calculate the figures in the illustration above and gives a potential range based on increasing/decreasing the percentage of respondents by +/- 5% (1% for Q17):

Question no.	Question & Respondent percentage	Equal to	-5%	+5%	Range
Q4	27.7% not influenced by location when deciding on which websites to access	152,792	125,212	180,371	125,000 to 180,000
Q8	43.8% feel at risk online	241,598	214,018	269,178	214,000 to 269,000
Q9	56.4% targeted for phishing scam	311,099	283,519	338,679	284,000 to 339,000
Q10	10.4% targeted became victims in the last 12 months	32,354	16,799	47,909	17,000 to 48,000
Q10	14.9% had been a victim of online crime in the last 12 months	82,188	54,608	109,767	55,000 to 110,000
Q13	31% suffered a financial loss, (based on 82,187 victims of online crime)	25,478	21,369	29,587	21,000 to 30,000
Question no.	**Question & Respondent percentage**	**Equal to**	**-1%**	**+1%**	**Range**
Q17	2.4% have no idea how to protect themselves online	13,238	7,722	18,754	8,000 to 19,000

Police and Crime Commissioner Warwickshire

Key Findings - Potential UK Implications

When making inferences about the potential levels of Cybercrime in Warwickshire we can be reasonably confident that the survey provided a representative population sample. However, to make inferences for the UK requires much more of a leap. For the purposes of this section the survey percentages have been applied to the 2014 UK population of 64.1 million people. The aim being to give a rough idea of the potential impact of Cybercrime in the UK:



36.2 million — Targeted by phishing scams in the last 12 months

3.8 million — Targeted by phishing scams in the last 12 months became victims

1.5 million — Have no idea how to protect themselves online

28.1 million — Feel at risk online

9.6 million — Victims of online crime in the last 12 months

3 million — Suffered financial loss online in the last 12 months

3 million people losing an average of £100 each would equate to over £300m lost

17.8 million — Not influenced by location when deciding on what websites to access

The table below shows the percentages used to calculate the figures in the illustration above and gives a potential range based on increasing/decreasing the percentage of respondents by +/- 5% (1% for Q17):

Question no.	Question & Respondent percentage	Equal to	-5%	+5%	Range
Q4	27.7% not influenced by location when deciding on which websites to access	17,755,699	14,550,700	20,960,700	14.6 to 21 million
Q8	43.8% feel at risk online	28,075,799	24,870,800	31,280,800	24.9 to 31.3 million
Q9	56.4% targeted for phishing scam	36,152,400	32,947,400	39,357,400	33 to 39.4 million
Q10	10.4% targeted became victims in the last 12 months	3,759,849	1,952,230	5,567,470	2 to 5.6 million
Q10	14.9% had been a victim of online crime in the last 12 months	9,550,900	6,345,900	12,755,900	6.3 to 12.8 million
Q13	31% suffered a financial loss, (based on 9,550,900 victims of online crime)	2,960,779	2,483,234	3,438,324	2.5 to 3.4 million
Question no.	**Question & Respondent percentage**	**Equal to**	**-1%**	**+1%**	**Range**
Q17	2.4% have no idea how to protect themselves online	1,538,400	897,400	2,179,400	897,000 to 2.2 million

Section One: Respondent Profiles

Section Summary

- **Just under half of respondents live in Warwick or Stratford District**
- **The 60-74 age group is the best represented**
- **The sample demographics are a fair representation of the Warwickshire population**

Who replied?

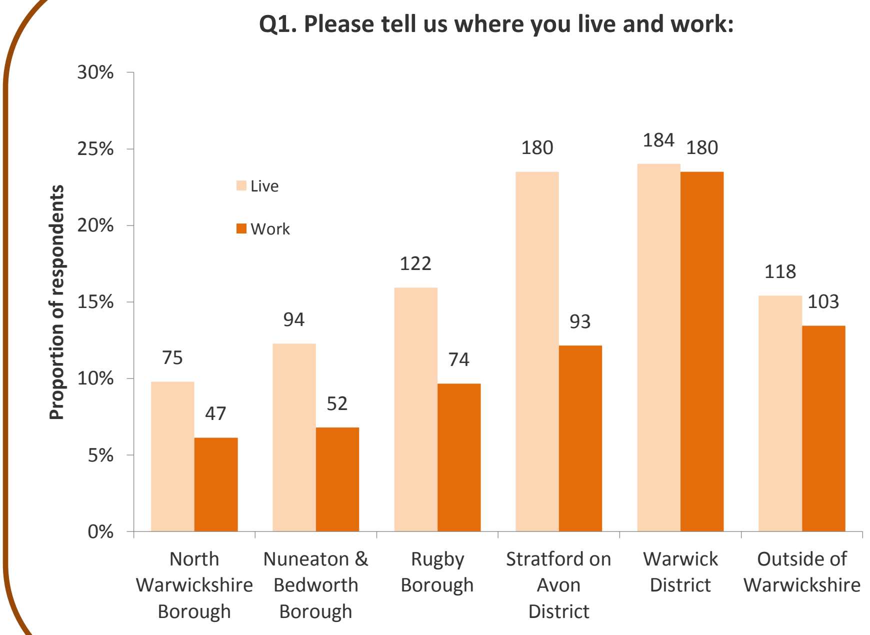
Sample

▪ The survey was open to people of all ages and from any location. Promotion of the survey was mainly carried out within Warwickshire through a number of channels.

Number of respondents

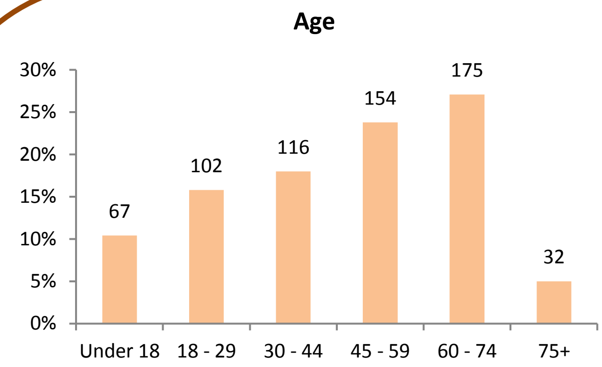
▪ There were 766 respondents which represents 0.14% of the population of Warwickshire

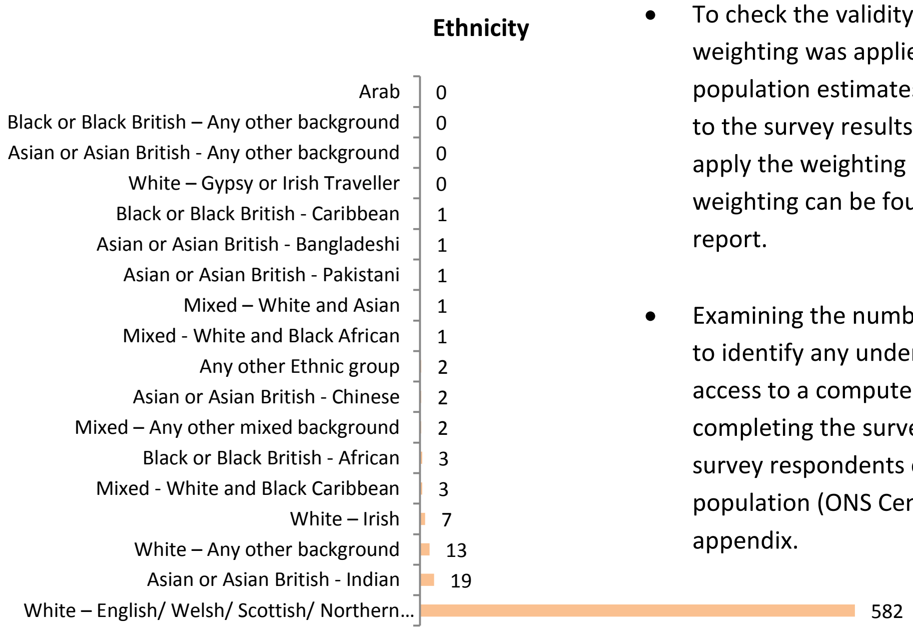
Note: The full demographic breakdown of respondents can be found in the appendix at the end of the report.



- The highest number of respondents live in Warwick District and Stratford District with a combined total of 364 (47.5%)
- In terms of where respondents work, Warwick District tops the list with 23.5% followed by those who work outside of Warwickshire which make up 13.4% of the total. It may be that around half of the respondents living in Stratford District are either in retirement, unemployed or work outside of the District.
- Warwickshire County Council has a number of offices and staff based in Warwick which may be part of the reason for the high levels of respondents to the survey living and working in Warwick District.

Note: The 'live' columns total more than the number of respondents, this is due to respondents being able to select multiple answers to this question.





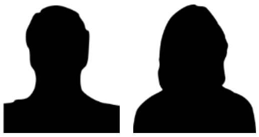
- Examining the number of respondents by age group it is apparent that certain age groups are much better represented than others. While 60-74 year olds are strongly represented with 175 respondents, under 18s make up just over 10%. This may be a reflection on the demographic groups that have the time and motivation to complete a survey of this type and is a factor to consider when interpreting the responses to each question.

- To check the validity of the sample by age and gender, weighting was applied based on the mid-year 2014 Census population estimates. The weighted results were so close to the survey results that it was not deemed necessary to apply the weighting in the report. The breakdown of the weighting can be found in the appendix at the end of the report.

- Examining the number of respondents by ethnicity helps to identify any underrepresented groups. Language and access to a computer were potential barriers to completing the survey. The comparison in ethnicity of the survey respondents compared to the Warwickshire population (ONS Census 2011) can be found in the appendix.

Notes:

Question 12 in the survey asked respondents to give details about incidences where they have been victims of Cybercrime. A selection of these responses are shown throughout the document in speech bubbles accompanied by the following symbol:



What people said:

Based on the percentages of answers to certain questions, scaling up of the results has been carried out to give an indication of the potential impact for Warwickshire. The scaling up has been based on the Office for National Statistics 2014 Mid-year population estimate of 551,594 people living in Warwickshire. In the section summary sections Warwickshire scaling up is indicated by the following symbol:

Section Two:

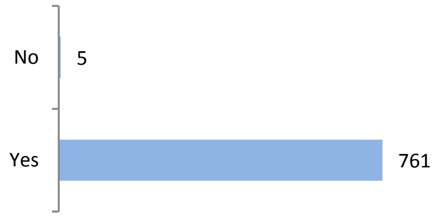
Internet Usage

Section Summary

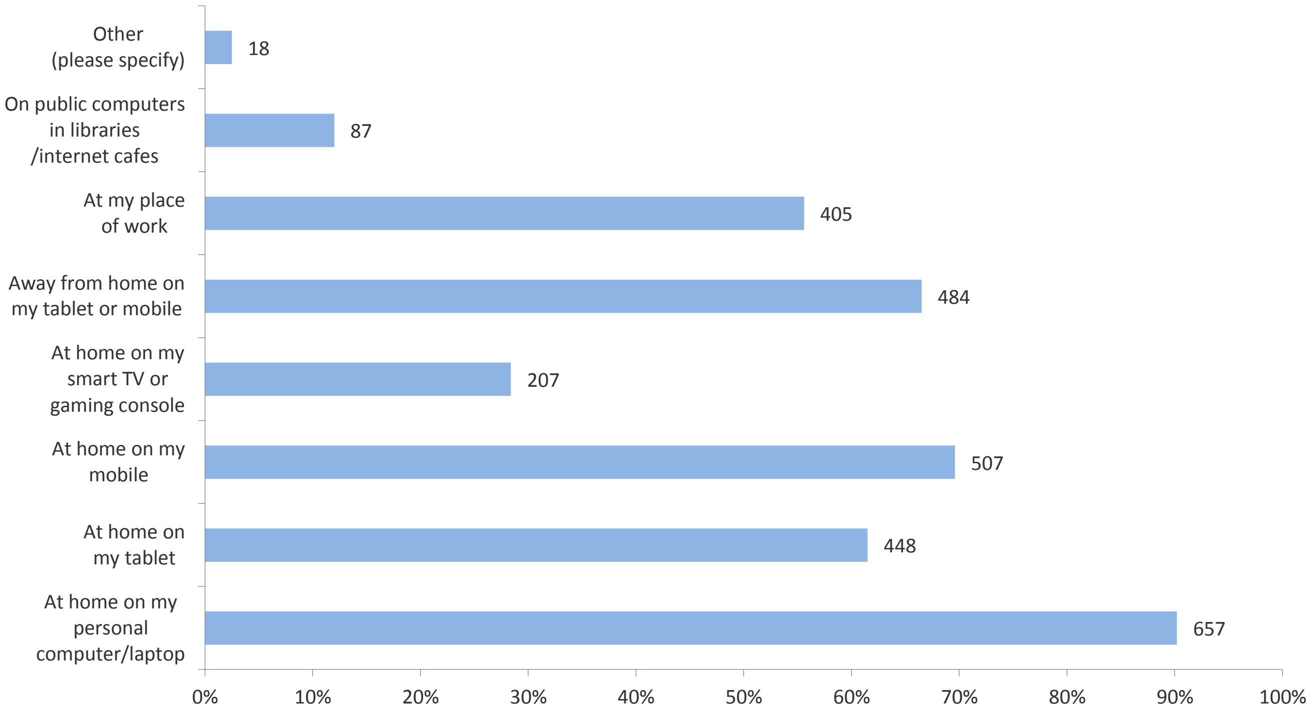
- **The majority of respondents use multiple devices to connect to the internet at home**
- **Almost a quarter of under 18s use the internet for between 5 and 7 hours per day**
- **Under 30s are the biggest users of social media**
- **The feeling of being at risk online increases with age**

"An estimated 241,598 residents in Warwickshire feel at risk online"

Q2. Do you use the internet?

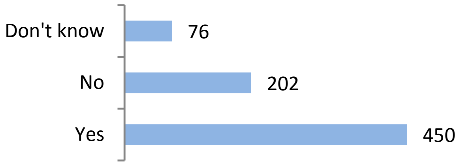


Q3. In what ways do you use the internet? (tick all that apply)



- Of the 728 respondents to answer this question, 657 (90.2%) use the internet at home on a personal computer or laptop.
- Of the 657, 406 also used a tablet to access the internet at home while 457 used a mobile. This demonstrates the range of options now available to access the internet and highlights the need to secure multiple devices.
- Within 'Other', six respondents advised they use the internet at school or college.

Q4. If you access the internet both at home and outside, does your location influence which websites you are willing to access? e.g. accessing online banking whilst using free Wi-Fi at a coffee shop.



- Taking into account that 27.7% of respondents are not influenced by location when deciding on which websites to access, this would translate into 152,791 residents in Warwickshire.

Public Wi-Fi Risks

Access to free public Wi-Fi has become commonplace in locations such as coffee shops, restaurants and hotels which has in particular benefited working professionals. There are however a number of risks attached to using public Wi-Fi:

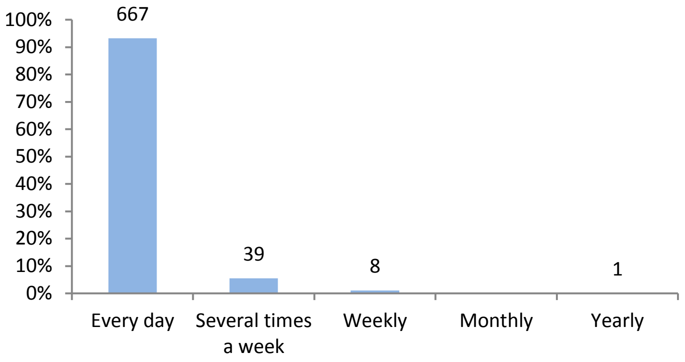
- Often no authentication is required to access the network, the connection is not encrypted and not secure and the sites you visit and what you type is visible to those in range
- Wi-Fi connections may be compromised or even set up by an attacker to trick users into connecting and sharing sensitive information

Public Wi-Fi Safety Tips

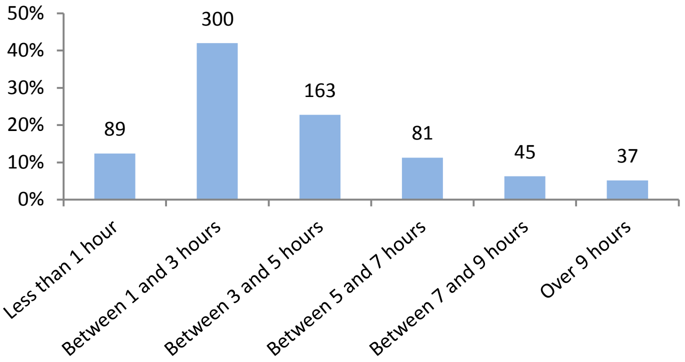
- Turn your Wi-Fi OFF when you don't need it to avoid connecting unnecessarily
- For business use, a 'Virtual Private Network' (VPN) will encrypt data and make you a far less appealing target
- Avoid using websites where you share personal information such as social media or online banking*

*Experts advise that using a banking app is the safest method to access your bank details online. The app manages the connection and ensures that all the traffic between you and the bank is secure.

Q5. How often do you access the internet?



Q6. How much time do you spend online on an average day?

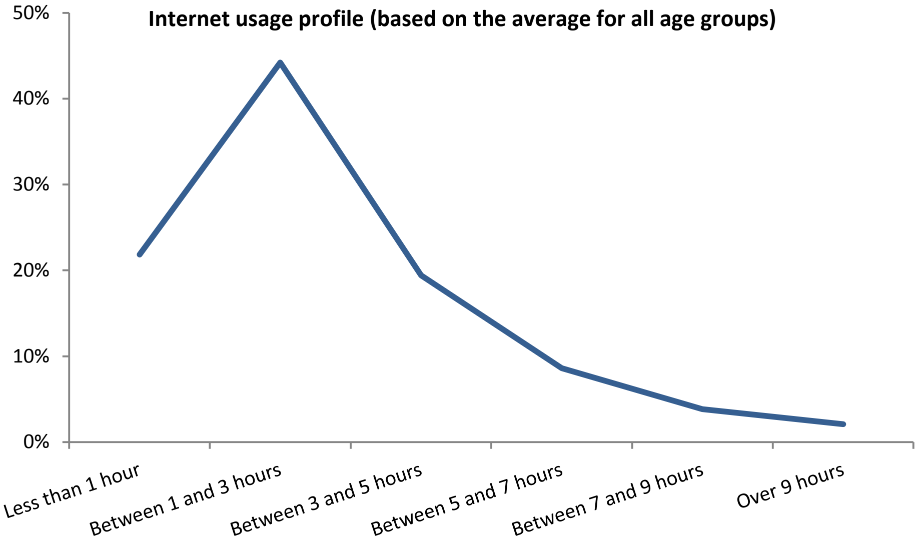


The results of Q5 and Q6 give an indication as to just how much technology and the internet has become integral to our daily lives. 93.3% of respondents use the internet every day with 87.6% spending over an hour a day online. Examining the responses of the 37 that responded 'over 9 hours' reveals that the majority used the internet for work as well as at home, there were also individuals who listed gaming and social media under what they use the internet for (see Q7).

Q6. Analysis

The following table and graph examine the breakdown of the Q6 responses by age of the respondent. Highlighted in dark blue in the table are the three highest percentages for each age group:

	Age Group					
Time Band	under 18	18-29	30-44	45-59	60-74	75+
Less than 1 hour	7.5%	5.9%	2.6%	**13.7%**	**18.9%**	**40.0%**
Between 1 and 3 hours	**32.8%**	**28.4%**	**41.4%**	**40.5%**	**53.1%**	**43.3%**
Between 3 and 5 hours	**17.9%**	**25.5%**	**25.9%**	**26.1%**	**20.6%**	**10.0%**
Between 5 and 7 hours	**23.9%**	**19.6%**	**14.7%**	10.5%	4.0%	6.7%
Between 7 and 9 hours	7.5%	9.8%	8.6%	7.2%	2.3%	0.0%
Over 9 hours	10.4%	10.8%	6.9%	2.0%	1.1%	0.0%

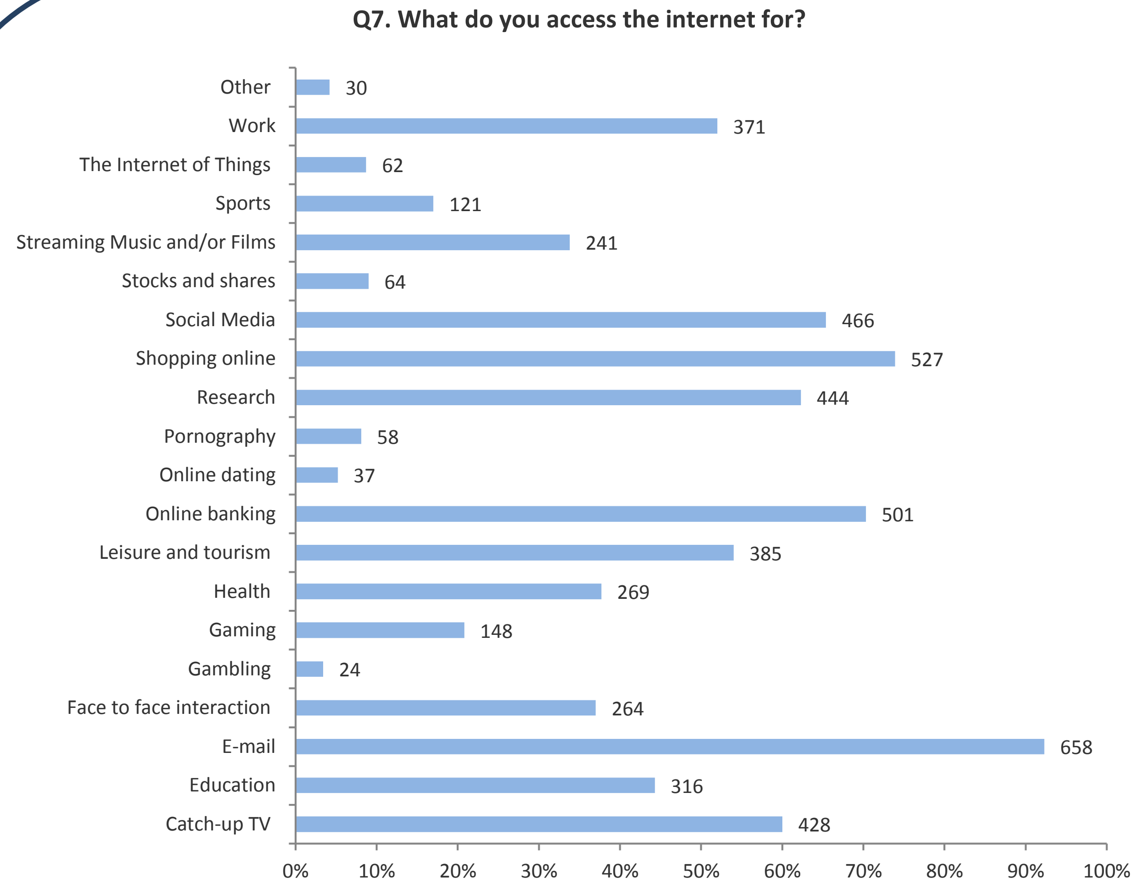

Internet usage profile (based on the average for all age groups)

For all age groups the highest percentage of respondents spend between 1 and 3 hours online per day. Examining the highlighted time bands for each age group we see that for the 45 and overs there is a far higher proportion of respondents that use the internet for 5 hours or less a day compared to those that use the internet for over 5 hours a day. In comparison, the under 45s are more likely to spend over 9 hours a day online than they are to spend less than 1 hour.

By comparing the answers from Q6 to Q10 (Over the last 12 months, are you aware of being a victim of online crime?) it is possible to get an idea of whether or not the length of time someone is online affects their level of risk:

- 89 respondents spent less than an hour a day on average online, 85 of the 89 answered Q10 and 14 had been a victim of online crime (16.5%).
- 544 respondents spent between 1 and 7 hours per day online, 526 of the 544 answered Q10 and 73 had been a victim of online crime (13.9%).
- 82 respondents spent over 7 hours per day online, 78 of the 82 answered Q10 and 16 had been a victim of online crime (20.5%).

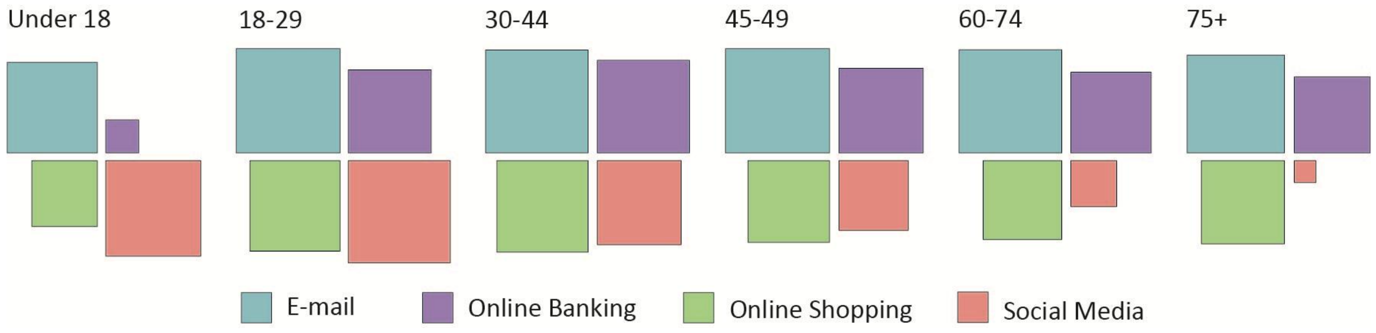
This would suggest that spending less time online does not necessarily make you less likely to be targeted for online crime; however it also suggests that 1 in 5 of those that spend over 7 hours online per day will become a victim of online crime.



- E-mail was the most common use of the internet with 92.3% of respondents selecting this option.
- Both shopping online and online banking are significantly popular uses of the internet. As these are both major platforms for financial transactions it is important to note that both are used by between 70 and 74% of respondents.
- The use of the internet for catch-up TV was significant with 60%, social media scored highly with 65.4%.
- A high number of respondents use the internet for research, although only 15.8% of these have taken the time to conduct research into protecting themselves online (based on Q16 Responses).

Q7. Analysis

The visualisation below illustrates the top four internet uses based on the Q7 responses. Each square has been scaled to show the proportion each category is used by the different age groups:

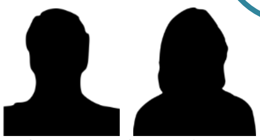


- Social media is used most by the under 30s
- All age groups over 18 are frequent users of online banking and shopping online
- E-mail is used by all age groups in fairly equal measure

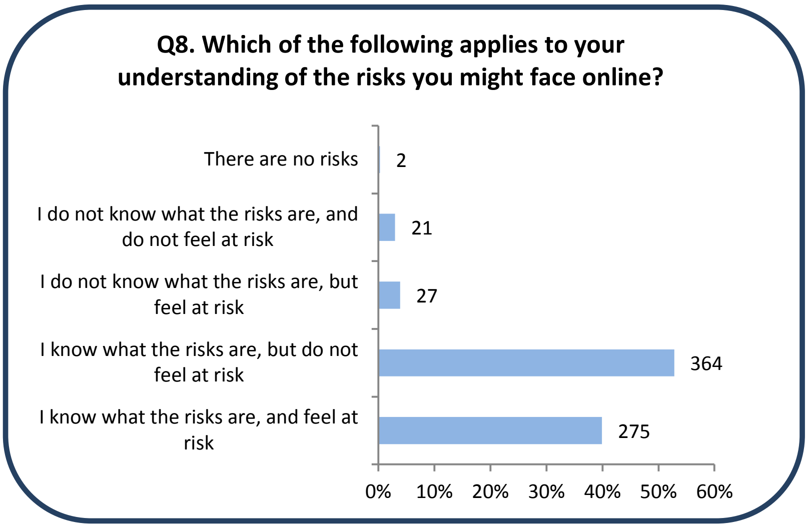
Shopping online was the second most popular activity behind using e-mail. Shopping via the internet offers the customer a wide range of choice while saving the time and effort of visiting the high street. There are however a number of risks associated with purchasing goods over the internet including:

- Receiving goods which don't match the description
- Making payments to bogus or fake online shops and never receiving the purchased goods
- Security risks when purchasing using an unsecured Wi-Fi connection
- Entering your personal and banking details onto a fraudulent website

"In January my wife bought me a pair of shoes off a web site after we had seen a particular style in a shop. The website had perfect photos of the exact shoes, so they were ordered. We became suspicious after they didn't arrive promptly. After two (weeks/months?) some shoes arrived – from China – but they were made of cheap imitation leather and nothing like the proper style. We contacted our bank who were excellent – they requested photos to be sent to the manufacturer to confirm they were fakes and then refunded the debit card payment. We supplied all of the website information to the bank. It was annoying as I was left with no proper shoes and the inconvenience, but at least we were not out of pocket."



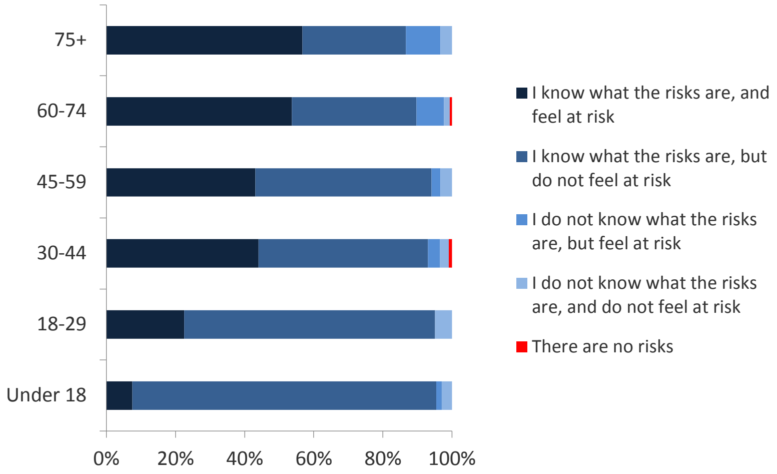
What people said:

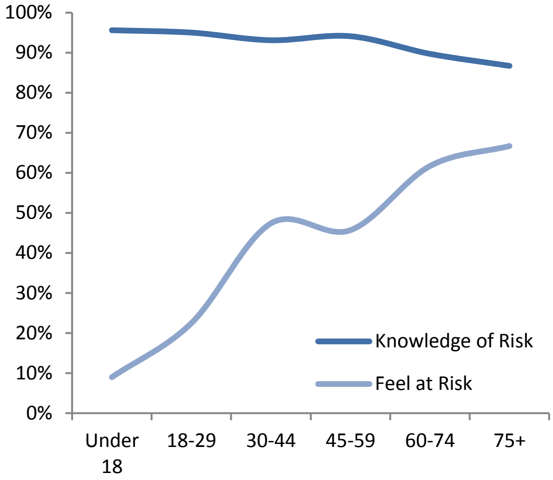


Q8. Which of the following applies to your understanding of the risks you might face online?

Q8. Analysis

Illustrated in the chart and graph below is the proportional breakdown by age group for the responses to Q8:





It is evident from the chart that there is a big difference in the perception of online risk depending on the age of the respondent. Illustrated by the graph, the overall trend is that as age increases, knowledge of the online risks reduces slightly while the feeling of being at risk increases significantly. In total just 9% of under 18s feel at risk compared to 66.7% of 75 and overs.

Of the 689 respondents who answered Q8, 302 felt at risk (combining both those that did and did not know what the risks are) which is 43.8%. This would equate to an estimated 241,598 residents in Warwickshire that feel at risk online.

Elderly Focussed Reporting and Information

Age UK

The Age UK website includes the "Staying safe online" section located under the technology & internet heading within the work & learning tab. The site advises that an estimated £670m is lost annually by victims of the most common online scams and provides a wealth of information including protecting your computer, identifying scams and safe online shopping and banking. The site provides a contact number for the Age UK Advice service and also signposts users to the Action Fraud website.

☎ **0800 169 65 65**

www.ageuk.org.uk

With the over 60s feeling most at risk online and having least knowledge of the risks, this raises a question around the effectiveness of support for this age group. While online self-help is widely available this may not be the preferred learning method for all internet users. This disparity in feeling of being at risk online between different age groups is an area which could be considered for further study.

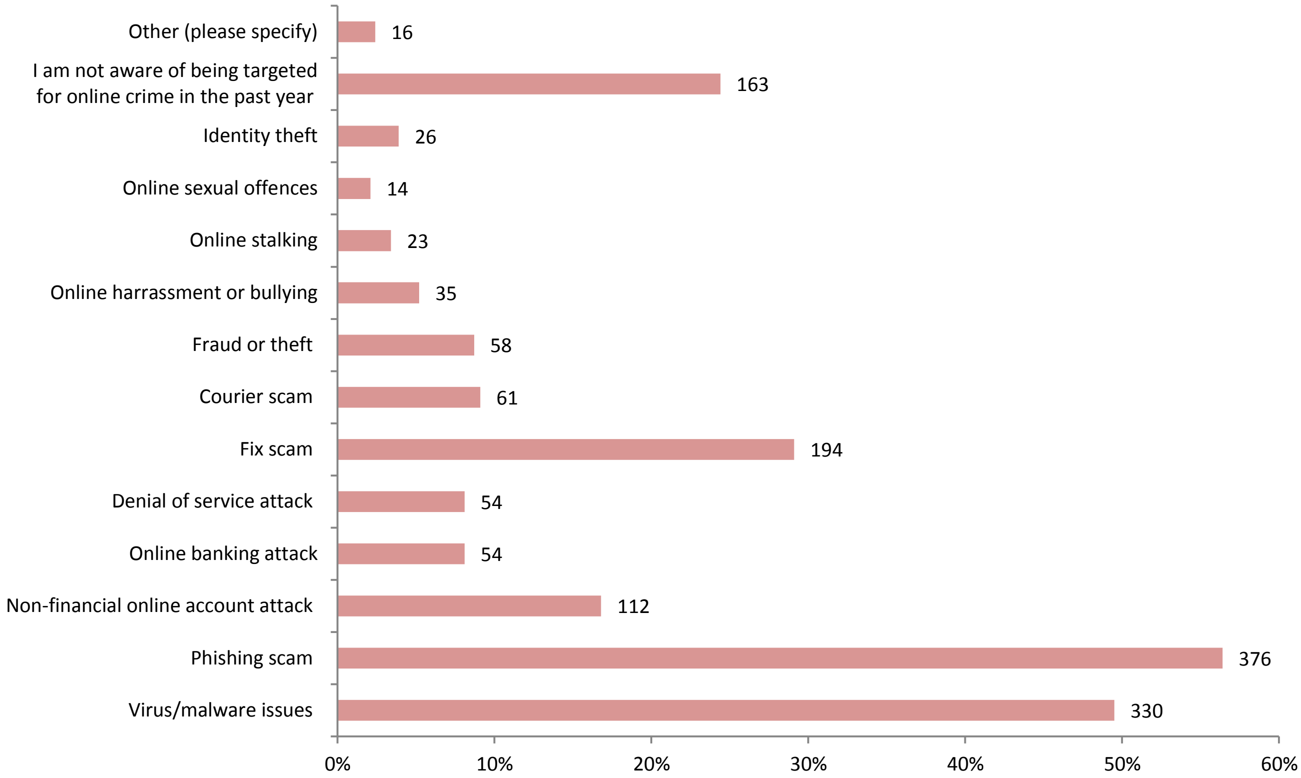
Section Three: Cybercrime Types and Reporting

Section Summary

- 14.9% of respondents have been a victim of online crime in the last 12 months
- For almost half of the victims the crime had a psychological/emotional impact
- Under 18s are the most likely to be affected by online harassment/bullying while the over 75s are the main target for fix scams and courier scams
- The top reason for not reporting Cybercrime was "did not think anyone could help"

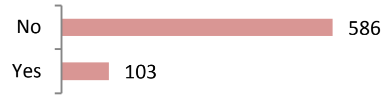
"An estimated 82,188 victims of online crime in the last 12 months"

Q9. Over the past 12 months are you aware of being targeted by any of the following types of online crime?



There are numerous variations of the different types of online crime, within this survey the two most prevalent types of online attack were phishing scams (56.4%) and viruses/malware (49.5%). A total of 58 respondents had been targeted in the form of online harassment/bullying or online stalking while 14 had been the target of sexual offences.

Q10. Over the last 12 months, are you aware of being a victim of online crime?



- Of the 689 responses to Q10, 14.9% had been a victim. Applying this percentage for Warwickshire would give an estimated 82,188 victims of online crime in the last 12 months.
- Cross referencing the responses of those who answered 'yes' to Q10 with Q14 shows that 70% of respondents who were the victims of online crime in the last 12 months reported the offence.

Q9. & Q10. Analysis

Listed in the table below are the responses to Q9 broken down by respondent age group. The percentages highlighted in dark red represent the five categories with the most responses for each age group:

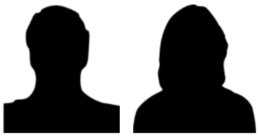
	Age Group					
Cybercrime Category	**Under 18**	**18-29**	**30-44**	**45-59**	**60-74**	**75+**
Virus/malware issues	**37.7%**	**37.6%**	**54.1%**	**56.8%**	**52.9%**	**37.9%**
Phishing scam	**21.3%**	**35.6%**	**64.0%**	**68.2%**	**64.9%**	**58.6%**
Non-financial online account attack	11.5%	11.9%	**19.8%**	**18.9%**	**14.9%**	**17.2%**
Online banking attack	4.9%	5.0%	9.9%	10.1%	7.5%	0.0%
Denial of service attack	**16.4%**	**12.9%**	14.4%	6.1%	1.7%	0.0%
Fix scam	8.2%	**14.9%**	**23.4%**	**35.1%**	**41.4%**	**48.3%**
Courier scam	8.2%	8.9%	5.4%	9.5%	9.2%	**17.2%**
Fraud or theft	3.3%	5.0%	11.7%	11.5%	6.3%	10.3%
Online harassment or bullying	**16.4%**	7.9%	1.8%	2.7%	1.7%	0.0%
Online stalking	6.6%	7.9%	3.6%	1.4%	0.6%	0.0%
Online sexual offences	4.9%	4.0%	0.9%	0.7%	0.0%	0.0%
Identity theft	4.9%	2.0%	3.6%	2.7%	3.4%	3.4%
I am not aware of being targeted	**45.9%**	**41.6%**	**15.3%**	**18.9%**	**20.7%**	13.8%
Other (please specify)	3.3%	1%	1.8%	4.7%	1.7%	0%

- It is clear that regardless of the age of the internet user there will be a significant level of contact with viruses, malware or phishing scams.
- Phishing scams almost double from the 18-29 to 30-44 age group and remain high through the older demographic age groups, this may suggest older internet users are being targeted for this type of online attack.

"I get so many phishing emails and cyber crime calls posing to buy something from my business using a fraudulent credit card – an average of two calls per week."

"I fell for a very believable attempt to obtain a new mobile phone via a false website in response to an email. My phone company detected the attempt and it was unsuccessful. I also had an attempt to add a new name/address to my credit card account – also blocked after a phone call."

"I usually get at least two phishing scams per day which go straight into the spam folder and are erased without opening them."



What people said:

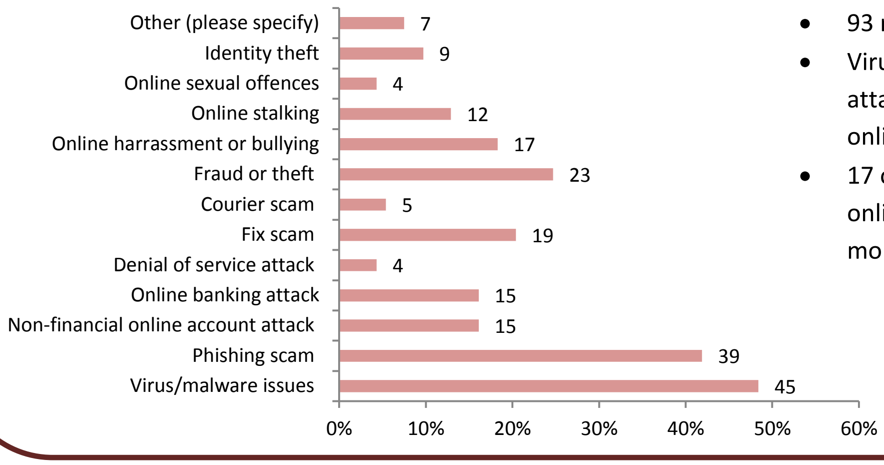
- Non-financial online attacks appear to be less of an issue for the under 30s compared to the over 30s with the highest proportion of respondents in the 30-44 age group for this category with 19.8%.
- Denial of service attacks are predominantly more of an issue for the under 45s, these attacks often relate to the intentional disruption of online gaming servers.
- Online harassment or bullying only featured in the top five for the under 18 age group, this would suggest that beyond the age of 18 internet users become less prone to this type of Cybercrime.
- The other category featuring in the top five for only one age group was courier scams for which the over 75s have been targeted almost twice as much as any other age group.
- In terms of proportion of respondents, the under 18s have the highest number unaware of being targeted with 45.9% while in contrast just 13.8% of the over 75s were unaware of being targeted.

The breakdown by age of the responses to question 10 provides the percentages of each age group that were victims of Cybercrime:

Age Group	No. of responses to Q10.	No. of victims	%
75+	30	4	13.3%
60-74	175	26	14.9%
45-59	153	26	17.0%
30-44	116	13	11.2%
18-29	102	9	8.8%
Under 18	67	12	17.9%

It is worth noting that while the under 18 age group feel least at risk online (Q8), they are also the age group with the highest proportion of victims.

Q11. Over the past 12 months, what type of online crime have you been a victim of?



- 93 respondents chose to answer this question.
- Virus/malware issues along with phishing attacks were the two most prevalent types of online crime.
- 17 of the 93 respondents had been victims of online harassment or bullying in the last 12 months.

Q11. Analysis

By listing the responses from Q11 against the responses to Q9 a picture can be built of the Cybercrime types which are most likely to result in the person targeted becoming a victim*:

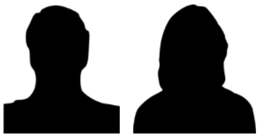
Cybercrime Category	No. of Respondents Targeted (Q9)	No. of Respondents that were Victims (Q11)	Percentage Targeted that became Victims
Online stalking	23	12	52.2%
Online harassment or bullying	35	17	48.6%
Fraud or theft	58	23	39.7%
Identity theft	26	9	34.6%
Online sexual offences	14	4	28.6%
Online banking attack	54	15	27.8%
Virus/malware issues	330	45	13.6%
Non-financial online account attack	112	15	13.4%
Phishing scam	376	39	10.4%
Fix scam	194	19	9.8%
Courier scam	61	5	8.2%
Denial of service attack	54	4	7.4%

*This is based on the assumption that all of those who answered Q9 also answered Q11 and is dependent on the respondents view on if they would consider themselves a ‘victim’.

- Around one in every two respondents targeted for online stalking/harassment or bullying considered themselves victims. Females were twice as likely to be a victim of online harassment or bullying as males.
- Over one in three of those targeted for fraud or identity theft become victims.

"My email address was cloned so that there were five of 'me' active! One was in Switzerland and interested in buying guns from an American company and another was in Newfoundland booking fishing trips. The other two were in England but they were detected before anything happened."

"Approximately six months ago, I had a message/email from my cousin saying he was abroad and was stranded and needed money. It turned out his Facebook account had been hacked and someone was trying to get money out of his contacts."

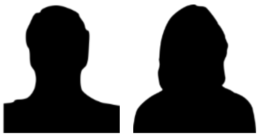


What people said:

- Fix scams in which those targeted receive a phone call from a bogus IT company are low on the list with 9.8% of those targeted becoming victims. However, given that 1 in 10 are falling victim this means that the attacker need only make 10 phone calls before they gain access to a victims computer.

"I had to change my phone number around November because of constant calls regarding my computer – this had been going on for about a year."

"I had a fix scam in February when I got a phone call supposedly from a representative of Windows wanting access to my computer."



What people said:

- Phishing scams are the most prolific category of attempted Cybercrime with 56.4% of respondents targeted. 10.4% of attempts resulted in a target becoming a victim. Applying these percentages to the Warwickshire population we can estimate that 311,099 residents in Warwickshire have been targeted by phishing scams in the last 12 months resulting in 32,354 becoming victims.

Phishing Scams Risks

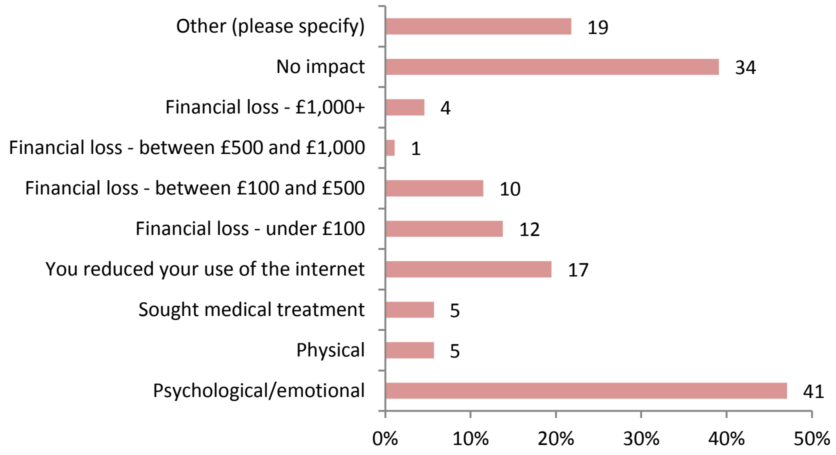
This is a scam where fraudsters send an email, instant message or text message prompting you to provide your personal details, such as passwords and user names. The fraudsters often try to make their messages look like they are from legitimate companies. Sometimes they direct you to a website which looks legitimate but is actually bogus to prompt you to input your details. The captured information is then used for crimes, such as identity theft and bank fraud. The message can also contain links or attachments which will infect your computer, or other device, with a virus.

- In serious cases personal details can be used to commit crimes such as identity theft and bank fraud
- Elaborate versions include phone phishing where an e-mail will direct the victim to call a number which connects to a person or an automated response ready to take the victims details
- Some links within phishing e-mails contain viruses and opening these could infect the device used to access the e-mail i.e. computer or smartphone

Phishing Scams Safety Tips

- Warning signs to look out for include spelling mistakes in the e-mail subject, you don’t know the sender, the content makes an offer that seems too good to be true (e.g. that you have won the lottery)
- Hovering the mouse cursor over links in suspicious e-mails (without clicking) will often reveal that the destination address is not the website of the organisation that supposedly sent the e-mail
- Remember that legitimate organisations will rarely if ever contact you in this way, if in any doubt contact the company directly to verify
- Stay Safe Online (www.staysafeonline.org) who provide information for individuals and business about how to use the internet safety use the concept of “When in doubt, throw it out” advising that “If it looks suspicious, even if you know the source, it’s best to delete or, if appropriate, mark it as junk e-mail”

Q13. What impact did the online crime(s) have on you?



- Of the 87 respondents to this question, almost half felt that being victim of an online crime had a psychological/emotional impact while just under a third suffered a financial loss.
- Examining the ‘other’ responses words including ‘annoyance’ ‘irritation’ and ‘hassle’ featured while other responses included ‘loss of data’ and ‘computer being quarantined’.

17.2% of the 87 respondents suffered a financial loss of £100 or more. Based on the estimation of 82,188 victims in Warwickshire this would mean 14,136 victims losing £100 or more (equivalent of over £1.4 million loss).

Q13. Analysis

The table below provides an estimated amount lost per person for the responses to Q13.

Amount lost	Number of respondents	Central estimate of amount lost	Number of respondents multiplied by central estimate	Possible loss range*
Under £100	12	£50	£600	£0 - £1,200
Between £100 and £500	10	£300	£3,000	£1,000 - £5,000
Between £500 and £1,000	1	£750	£750	£500 - £1,000
Over £1,000	4	£1,500	£6,000	£4,000 - £8,000

*Maximum loss for 'over £1,000' given a value of double the minimum loss due to the small cohort size

There were a total of 27 respondents that had suffered a financial loss as a result of Cybercrime in the last 12 months. Combining the totals for the number of respondents multiplied by the central estimate and dividing by the total number of respondents gives an average loss per person of £383.33.

Applying this average figure to Warwickshire and the UK would result in the following:
The estimated Warwickshire number of Cybercrime victims is 82,187, applying the 31% experiencing financial loss this would be 25,478.

- 25,478 victims losing £383.33 each would equate to a total loss of £9,766,481

The UK estimated number of Cybercrime victims is 9,550,900, applying the 31% experiencing financial loss this would be 2,960,779.

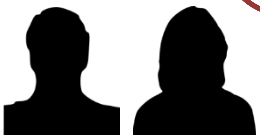
- 2,960,779 victims losing £383.33 each would equate to a total loss of £1,134,955,414

These estimates are however only based on the average of 27 victims. Over 80% of the 27 victims lost between £0-500 and so to avoid a disproportionate effect on the results the maximum loss figure was capped at £2,000 as there were only four respondents within this cohort. It is of course more than possible that the average amount lost by victims for Warwickshire and the UK are in reality higher than this and that the total loss estimates are at the conservative end of the scale.

The psychological/emotional impact of Cybercrime can be of huge significance to the victim and can take many different forms. Online bullying/harassment can have very direct implications, Childline advise that it can be upsetting and confusing for the victim and the 24 hour nature of social media can leave the victim feeling powerless to make it stop.

"Between the ages of 15 and 18 I was frequently harassed online, usually sexually, when I tried to report it I was then 'trolled' on the reporting page by people who believe that being bullied online and sent sexual documents was something everyone should just get used to. The social networks did nothing."

"I was harassed online on a daily basis between May and June2014. It is still ongoing, but in an occasional capacity, by the same individuals."



What people said:

Regarding fraud based offences, being fooled into handing over your personal details or money to an attacker can result in a feeling of guilt or embarrassment. Added to this are the financial implications of being scammed, in the most severe cases individuals have been duped out of their life savings.

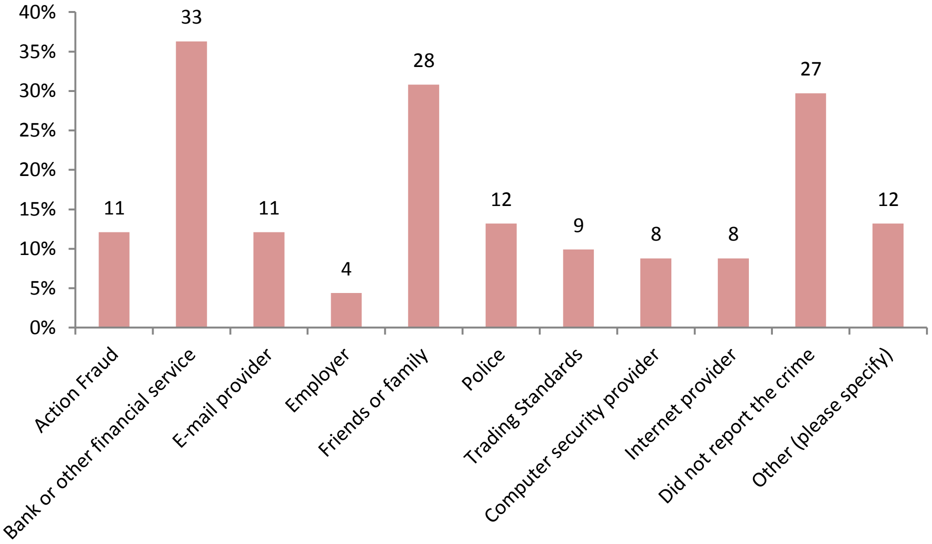
"My banking details were compromised from a third-party shopping website which had been hacked. Access was obtained by criminals to my account after they placed a divert on my landline. They proceeded to transfer money from my account to one of theirs and were able to do so by diverting my bank's verification call to their own number. The amount that the criminal transferred out of my account equated to approximately £270. My phone provider accepted blame for their lack of security, as did the online shopping company that was attacked. All the money was refunded by my bank."

"Every few months money was taken out of my account, originally via a fake driving licence site but who since have sold my details on. I am a pensioner and I did not realise the money was going out as they were fairly small payments for things such as online gaming and fortune telling, which I certainly did not ask for."

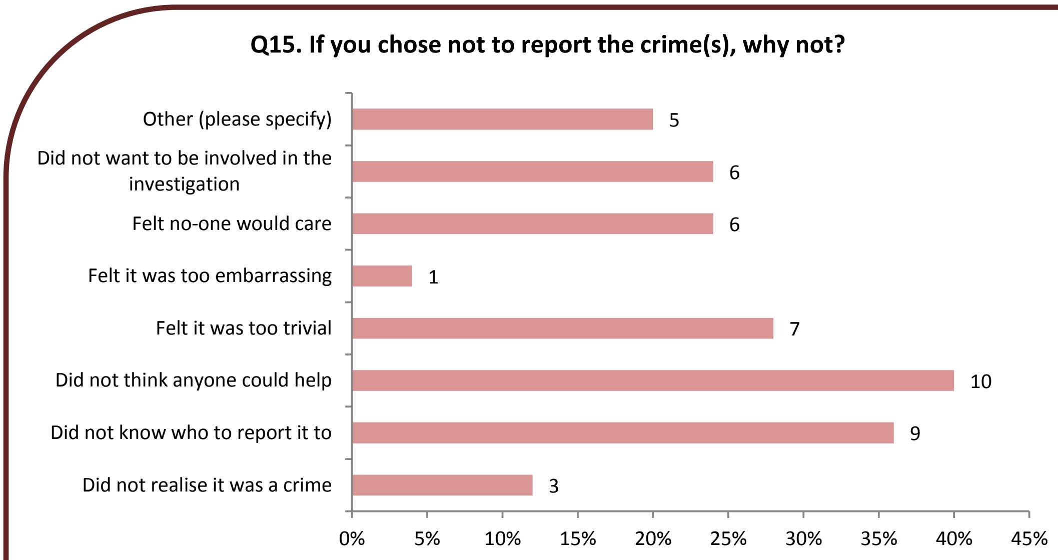
"In the last year I had experience of buying an item then having my bank account targeted by direct debits that were not set up or approved by me, an average of £120 on three occasions, all from buying an item that cost less than £10."

"I have had regular charges made against my debit card, after using it to make a payment on a site that purported to be a government site – I was renewing my driving license."

What people said:



- Based on the response to this question, the 91 respondents were more than twice as likely to report the crime to friends and family than to the police, trading standards or action fraud.
- Just under 30% did not report the crime to anyone.
- 16 of the 33 respondents that reported the crime to banks or financial services had suffered a financial loss based on the responses to Q13.
- Under 18s are the age group most likely to not report the crime.
- 30-44 year olds are the most likely to report to a bank or financial service.



- To be able to address the under-reporting of Cybercrime it is necessary to establish the reasons for not reporting, a total of 25 respondents answered question 15.
- The top reason given being 'Did not think anyone could help'.
- Of the respondents that 'Felt it was too trivial', cross referencing with Q11 shows us that three had been victim of phishing scams, two had been victim of virus/malware and one each for non-financial online attack, fix-scam and fraud/theft.
- Within those who 'Did not know who to report it to', seven had been victims of virus/malware, five victims of phishing scams and three victims of fix scams.
- For those who 'Did not think anyone could help', the most popular responses to Q11 were virus/malware (7) and phishing (3). Every offence category except courier scam had at least one victim suggesting that the feeling that 'nobody can help' is a common response to Cybercrime in general.

Listed below are the details for two of the main pathways for reporting different types of Cybercrime and two of the most widely recognised sources for Cybercrime information online.

Action Fraud

Action Fraud is the UK's national fraud and internet crime reporting centre where you should report fraud if you have been scammed, defrauded or experienced Cybercrime. Fraud and internet crime can be reported any time day or night using the online reporting service. Help and advice is available over the phone through the Action Fraud contact centre where customers can speak directly to fraud and internet crime specialists between 8am and 8pm Mon-Fri and 9am to 5pm Sat-Sun.

☎ **0300 123 2040**

www.actionfraud.police.uk

ActionFraud
Report Fraud & Internet Crime
0300 123 2040

Use for: Reporting if you have been scammed, defrauded or experienced Cybercrime

Trading Standards/Citizens Advice Consumer Service

National Trading Standards has a dedicated eCrime Team which was set up as part of a wider strategy to protect consumers and tackle rising online crime. The service is linked with the Citizens Advice Consumer Helpline (number below) through which online scams can be reported.

☎ **03454 04 05 06**

www.tradingstandardsecrime.org.uk

Use for: Reporting online scams & rip-offs

NATIONAL TRADING STANDARDS
eCrime Team
Protecting Consumers
Safeguarding Businesses

Get Safe Online

Get Safe Online describe themselves as “the UK’s leading source of unbiased, factual and easy-to-understand information on online safety.” The website is packed with information covering the whole spectrum of online crime and provides detailed information on a range of topics from how to create a secure password to advice on safeguarding children online.

www.getsafeonline.org

Use for: Cybercrime advice and information

Stay Safe Online

Stay Safe Online is powered by the National Cyber Security Alliance (NCSA). The NCSA’s mission is to “educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals use, the networks they connect to, and our shared digital assets.”

www.staysafeonline.org

StaySafeOnline.org
National Cyber Security Alliance

Use for: Cybercrime advice and information for home users, small and medium size businesses, primary and secondary education.

At a local level it is also important to note that the police non-emergency number (101) can be used to report certain online crime types such as online bullying/harassment. For cases of Cybercrime where the victim has been threatened with physical harm it is particularly important to report to the police.

CALL YOUR LOCAL POLICE
☎ 101
IN AN EMERGENCY ALWAYS CALL 999

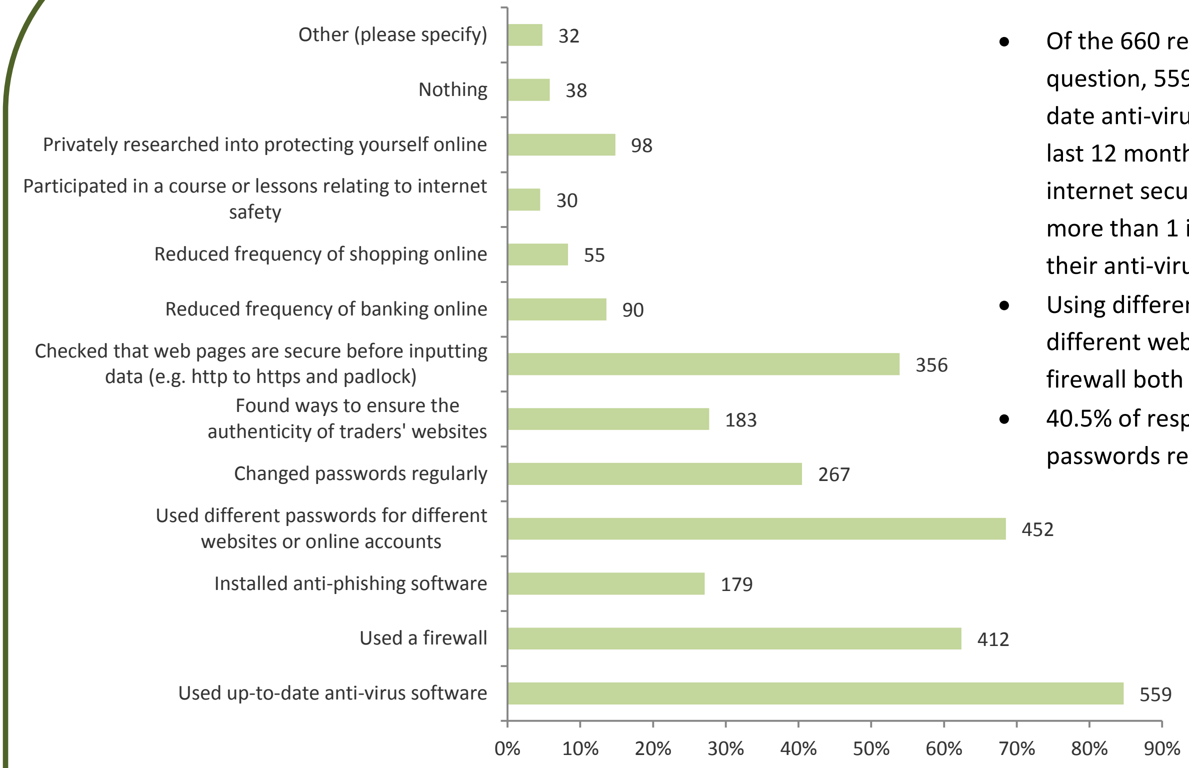
Section Four: Internet Security

Section Summary

- More than 1 in 10 respondents are not using up-to-date anti-virus software
- Less than half regularly change their passwords
- 2.4% have no idea how to protect themselves online

"An estimated 13,238 people in Warwickshire have no idea how to protect themselves online"

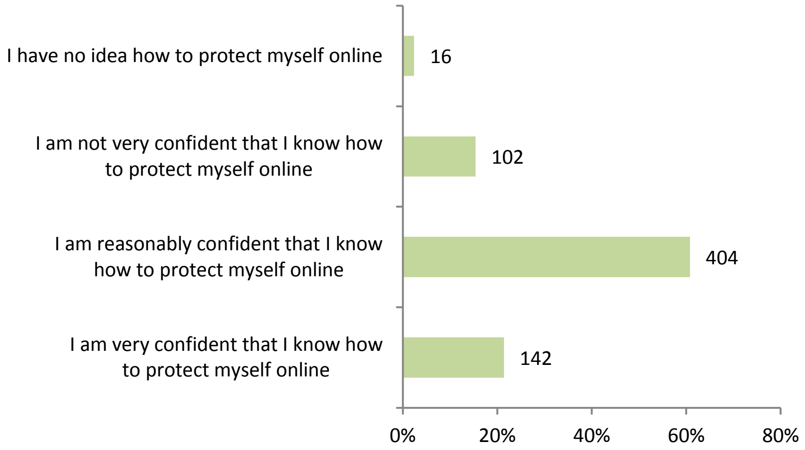
Q16. What have you done in the last 12 months to improve your internet security?



- Of the 660 respondents to this question, 559 have used up-to-date anti-virus software in the last 12 months to improve internet security. Therefore more than 1 in 10 fail to keep their anti-virus up-to-date.
- Using different passwords for different websites and using a firewall both scored highly.
- 40.5% of respondents change passwords regularly.

Cross referencing Q16 with Q17, 80 of the 142 respondents (57.1%) who felt they are confident that they know how to protect themselves online reported changing their passwords regularly. Given that changing passwords regularly is one of the more basic and necessary online security measures it is perhaps surprising that less than 2 in 3 that feel confident online are taking this precaution. This may suggest that changing of passwords is one of the less appealing security measures possibly because of the need to remember a large number of passwords for a range of accounts.

Q17. How confident do you feel in your knowledge of how to protect yourself from the range of threats online?



- 82.2% were either reasonably or very confident that they know how to protect themselves online. This was also the percentage for parents /guardians with children under 18 who felt reasonably or very confident.
- 2.4% of respondents have no idea how to protect themselves online.
- Applying the 2.4%, an estimated 13,238 people in Warwickshire have no idea how to protect themselves online.

The respondent comments below provide some real life examples of the sort of difficulties that can arise when account security is breached through hacking:

"About 12 months ago, my email account was hacked and an email sent to all my contacts. A teacher at my daughter's school alerted me to this as he had received an inappropriate email from 'me'. I immediately emailed all my contacts telling them not to open the email from 'me' and then changed my password. I now change my password on a regular basis and have a strong password."

"Someone hacked into my eBay account and listed an item for sale. A few days later they demanded money, threatening me with the police."

What people said:

A number of respondents also provided information relating to viruses/Trojans:

"I had my last laptop come up with a 'frozen' page, which looked genuine, saying I was illegally downloading porn and that I had to pay a fine to have it unblocked. As I knew I hadn't, I reported it to the police and my internet provider."

"My anti-virus software detected and blocked some stuff, not sure what it was."

"I had an email to my work account, clicked the link and it took my contacts list."

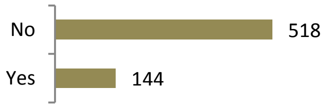
What people said:

Section Five: Children and the Internet

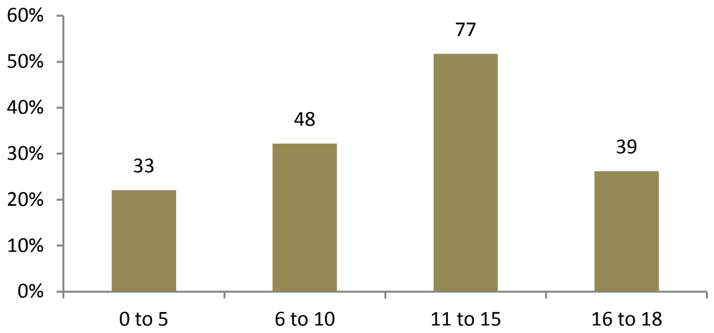
Section Summary

- **Almost a third of parents have neither applied online restrictions nor spoken to their children about internet safety**
- **Parents are less likely to monitor the internet use of older children**

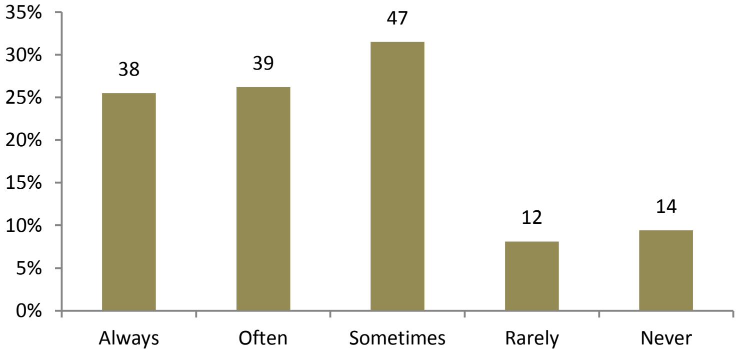
Q18. Are you the parent/guardian of any children (under 18) living in your household that use the internet?



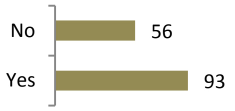
Q19. What are the ages of children in your household who use the internet?



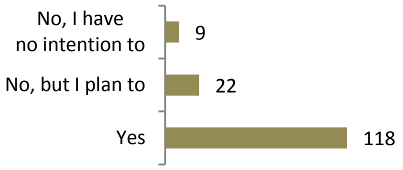
Q20. Do you monitor their internet use?



Q21. Have you applied online restrictions to the use of the internet for any children in your household?

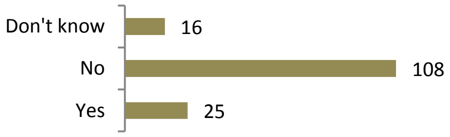


Q22. Have you spoken to your children about internet safety?



- Just under a third of parents have neither applied restrictions nor spoken to their children about internet safety

Q23. Have your children ever experienced internet/cyber bullying?



Q20. Analysis

While over 79% of parents have spoken to their children about internet safety, 37.6% do not apply any online restrictions when their children are using the internet at home. The table below illustrates the link between levels of monitoring and age of children. The highlighted figures represent the two highest totals for each column:

Age Group	Never	Rarely	Sometimes	Often	Always
0 to 5	3	1	5	3	22
6 to 10	1	1	11	17	18
11 to 15	6	5	30	28	8
16 to 18	9	6	17	4	4

Based on the table there is a correlation between age and level of monitoring with parents more likely to regularly monitor the internet use of those aged between 0 and 10. Clearly as children get older and more independent it becomes more difficult to keep track of their internet usage.

Children Focussed Reporting and Information

There are a number of agencies which provide advice and information relating to keeping children safe online. Two of the more widely known sites are listed below:

CEOP Command

The NCA's CEOP Command (formerly the Child Exploitation and Online Protection Centre) works with child protection partners across the UK and overseas to identify the main threats to children and coordinates activity against these threats to bring offenders to account. CEOP Command protects children from harm online and offline, directly through NCA led operations and in partnership with local and international agencies. (*source: https://www.ceop.police.uk*)

☎ **0870 000 3344**

www.ceop.police.uk

Use to report: Suspicious behaviour online toward a child & illegal content online.

CEOP

A National Crime Agency command

ChildLine

The ChildLine website includes specific advice sections for bullying (including cyber/online bullying) and online and mobile safety (including information on grooming & sexting). Those accessing the site are able to speak to counsellors about their experiences via the telephone number, e-mail or online chat. Users are signposted to the CEOP website if they need to report online activity.

☎ **0800 11 11**

www.childline.org.uk

ChildLine 0800 1111

Summary

This is the first survey of its kind in Warwickshire and will help to provide a baseline for future studies. The results have re-affirmed some of the presumptions about who is being targeted for certain types of Cybercrime and has revealed some interesting statistics about internet usage and how at risk people feel online.

Certain areas have been highlighted where further education is required especially around the use of public Wi-Fi and what people are doing to improve their internet security. While under 18s had the greatest knowledge of online risks, this age group also had the highest percentage of victims of Cybercrime.

Reporting of Cybercrime is an area which could be improved, the notion that ‘nobody can help’ is something that needs to be addressed if levels of reporting are to be improved and the true level of Cybercrime is to be established.

Survey Limitations

The survey was titled “Warwickshire Cyber Crime Survey” which could encourage a level of selection bias. There is a risk that the survey will have been completed by a disproportionately high number of victims whereby those who had been a victim of Cybercrime may have been more motivated to complete the survey than those who hadn’t.

646 of the 766 respondents answered Q25 (how old are you?), therefore where age breakdowns have been given for selected questions in the analysis it is based on those that answered this question.

Where estimates have been made for the Warwickshire and UK impact, an assumption has been made that Warwickshire is representative of the UK as a whole. Clearly these are very general estimates and provide only a rough indicator of potential Cybercrime levels for Warwickshire and the UK. It has also been assumed that all Warwickshire residents have access to the internet.

Future Actions

Explore ways to deliver the survey results in Warwickshire and encourage people to do more to protect themselves online.

Ask what more should/could we do to educate parents and better protect young people.

Further research into the most effective way to provide information to the over 60s to both inform about online risks and reduce the feeling of being at risk online.

Look at ways to get the message across to inform people about the risks of using open Wi-Fi networks for personal and financial transactions.

Appendix

Below is the full breakdown of respondent demographics:

Gender (634 responses)

54% (340) were females and 46% (294) were males.

Age (646 responses)

The highest number of respondents (175) were in the age group 60-74

There were 361 respondents aged over 45 and over (56%) and 285 aged under 45 (44%).

Long Standing Illness or Disability (637 responses)

124 answered yes, 513 answered no.

Ethnicity (638 responses)

91.2% (582) were White – British

3% (19) were Asian or Asian British - Indian

2% (13) were White – Any other background

First Language (633 responses)

English is the first language for 617 (97.5%)

The other first languages were made up of: Polish (3), Portuguese (2), Slovak (1), Hungarian (1), French (1), Urdu (1), Spanish (1), Russian & Latvian (1), Khachi (1), Gujerati (1), Tamil (1), Welsh (1)

Religion (643 responses)

51.9% (334) Christian

35.6% (229) No religion

5.6% (36) Preferred not to say

3.3% (21) selected 'Other'

1.6% (10) Muslim

0.8% (5) Sikh

0.6% (4) Buddhist

0.5% (3) Jewish

0.2% (1) Hindu

Sexuality (636 responses)

88.8% (565) were heterosexual or straight

5.7% (36) preferred not to say

2.4% (15) were bisexual

2.2% (14) were gay or lesbian

Ethnicity Profile

The table below has been created by comparing the ethnicity percentages from the 2011 Census to the ethnicity profile of the survey respondents:

Ethnic Group	Residents in Warwickshire	Census Percentages	Survey Percentages
All categories: Ethnic group	545,474	%	%
White: English/Welsh/Scottish/Northern Irish/British	482,607	88.5%	91.2%
White: Irish	5,216	1.0%	1.1%
White: Gypsy or Irish Traveller	494	0.1%	0.0%
White: Other White	17,371	3.2%	2.0%
Mixed/multiple ethnic group: White and Black Caribbean	3,090	0.6%	0.5%
Mixed/multiple ethnic group: White and Black African	698	0.1%	0.2%
Mixed/multiple ethnic group: White and Asian	2,606	0.5%	0.2%
Mixed/multiple ethnic group: Other Mixed	1,555	0.3%	0.3%
Asian/Asian British: Indian	16,435	3.0%	3.0%
Asian/Asian British: Pakistani	1,728	0.3%	0.2%
Asian/Asian British: Bangladeshi	284	0.1%	0.2%
Asian/Asian British: Chinese	2,349	0.4%	0.3%
Asian/Asian British: Other Asian	4,300	0.8%	0.0%
Black/African/Caribbean/Black British: African	2,173	0.4%	0.5%
Black/African/Caribbean/Black British: Caribbean	1,733	0.3%	0.2%
Black/African/Caribbean/Black British: Other Black	537	0.1%	0.0%
Other ethnic group: Arab	467	0.1%	0.0%
Other ethnic group: Any other ethnic group	1,831	0.3%	0.3%

Source: ONS Census Warwickshire population figures, 2011

Weighting of Responses

Highlighted in section one (Respondent Profiles) was the disparity in respondents age groups. To check how the survey sample compared to Warwickshire, weightings were applied for both gender and age groups based on the Census Mid-year Population Estimates, 2014. The results of this are illustrated in the tables below:

Age Group	11 and over Population	No. of returns	% of Population	% of returns	**Weighting**
11-17	43,234	67	8.96%	10.37%	**0.86**
18-29	77,035	102	15.96%	15.79%	**1.01**
30-44	103,265	116	21.40%	17.96%	**1.19**
45-59	116,004	154	24.04%	23.84%	**1.01**
60-74	93,463	175	19.37%	27.09%	**0.71**
75+	49,565	32	10.27%	4.95%	**2.07**
Total	482,566	646	100.00%	100.00%	**1.00**

11-29	120,269	169	24.92%	26.16%	**0.95**
30-44	103,265	116	21.40%	17.96%	**1.19**
45-59	116,004	154	24.04%	23.84%	**1.01**
60+	143,028	207	29.64%	32.04%	**0.92**
Total	482,566	646	100.00%	100.00%	**1.00**

Source: ONS Census Mid-year Population Estimates, 2014

The population group of 11 and over has been used based on the assumption that children aged 10 and under have not participated in the survey (exact ages of participants not known). The first table lists the age groups as they appeared in the survey, based on this the 75+ age group is the most under-represented and the 60-74 age group the most over-represented.

For the second table the age groups of 11-17 & 18-29 and 60-74 & 75+ have been combined. Based on this table the comparison between the survey respondents and Warwickshire population is a much closer match. Applying these very slight changes in weighting did not change the results enough to require the weighting to be applied to the survey results.

Gender	11 and over Population	No. of returns	% of Population	% of returns	**Weighting**
Male	237,159	294	49.15%	46.45%	**1.06**
Female	245,407	339	50.85%	53.55%	**0.95**
Total	482,566	633	100.00%	100.00%	**1.00**

Source: ONS Census Mid-year Population Estimates, 2014

As with the age groups it is apparent that the breakdown of respondents by gender is a close match to the Warwickshire population. It was therefore not necessary to apply the gender weightings to the survey results.

Reporting & Information Summary

Within the body of the report a range of different contacts for information and reporting of different types of Cybercrime were provided. These contacts are listed again below:

National Contacts

Agency	Use for Reporting	Use to Report…	Use for Information	Description	Contact Number	Web Address
ActionFraud Report Fraud & Internet Crime 0300 123 2040	✓	If you have been scammed, defrauded or experienced Cybercrime	✓	Action Fraud is the UK's national fraud and internet crime reporting centre where you should report fraud if you have been scammed, defrauded or experienced Cybercrime.	0300 123 2040	www.actionfraud.police.uk
age UK	-	-	✓	Predominantly aimed at older internet users. Provides a wealth of information including protecting your computer, identifying scams and safe online shopping and banking.	0800 169 65 65	www.ageuk.org.uk
CEOP A National Crime Agency command	✓	Suspicious behaviour online toward a child & illegal content online	✓	CEOP Command (formerly the Child Exploitation and Online Protection Centre) works with child protection partners across the UK and overseas to identify the main threats to children.	0870 000 3344	www.ceop.police.uk
ChildLine 0800 1111	-	-	✓	The Childline website includes specific advice sections for bullying (including cyber/online bullying) and online and mobile safety (including information on grooming & sexting).	0800 11 11	www.childline.org.uk
NATIONAL TRADING STANDARDS eCrime Team Protecting Consumers Safeguarding Businesses	✓	Online scams & rip-offs	✓	National Trading Standards has a dedicated eCrime Team which was set up as part of a wider strategy to protect consumers and tackle rising online crime. The service is linked with the Citizens Advice Consumer Helpline through which online scams can be reported.	03454 04 05 06	www.tradingstandardsecrime.org.uk
GET SAFE ONLINE .org	-	-	✓	Get Safe Online describe themselves as "the UK's leading source of unbiased, factual and easy-to-understand information on online safety." The website is packed with information from how to create a secure password to advice on safeguarding children online.	-	www.getsafeonline.org
StaySafeOnline.org National Cyber Security Alliance	-	-	✓	The mission of the National Cyber Security Alliance is to educate and empower a digital society to use the internet safely at home, work and school.	-	www.staysafeonline.org

Local Contacts

Agency	Use for Reporting	Use to Report...	Use for Information	Description	Contact Number	Web Address
Warwickshire POLICE	✓	Incidents of Cybercrime, in particular if the victim has been threatened with physical harm	✓	The public are able to call 101 which is the national police non-emergency number. The Wawickshire Police website also signposts users to the 'Internet Watch Foundation' (IWF) website if they need to report child sexual abuse images.	**101**	**www.warwickshire.police.uk**
Police and Crime Commissioner Warwickshire			✓	The Warwickshire Office of the Police and Crime Commisioner website provides a wealth of information for local residents and is committed to tackling cybercrime.	**01926 412 322**	**www.warwickshire-pcc.gov.uk**
Warwickshire County Council Community Safety Team			✓	The Warwickshire County Council Community Safety Team remit is to reduce crime & disorder and anti-social behaviour through delivery of projects on a local level. The team can be contacted for local Cybercrime issues and advice on where to report.	**01926 412 338**	**www.warwickshire.gov.uk (navigate to Community Safety Team)**
safe in... warwickshire			✓	The Safe in Warwickshire website is a product of the multi-agency Safer Warwickshire Partnership Board providing regular updates on a range of crime and community safety topics including Cybercrime.	**Email: community safety@ warwickshire.gov.uk**	**www.safeinwarwickshire.com**

Glossary

Anti-spyware

Anti-spyware software helps stop malicious programs stealing confidential information from your computer.

Anti-virus

Security software that helps protect your computer from viruses spread online.

Attachment

A file which has been attached (sent with) an email. This could be an image, a video or any other document. You can usually attach a file to an email by clicking an icon in the shape of a paperclip.

Authentication

The process for verifying that someone or something is who or what it claims to be. In private and public computer networks (including the internet), authentication is generally done with passwords.

Courier scam

A courier scam is when fraudsters call and trick you into handing your cards and PIN numbers to a courier on your doorstep.

Denial of service attack

Deliberate overloading of a service by criminals to make it unavailable to legitimate users. For example, by arranging millions of simultaneous visits to a website – normally from a Bot Net.

Encryption

The process of converting data into cipher text (a type of code) to prevent it from being understood by an unauthorised party.

Firewall

A piece of hardware or software that controls what information passes from your computer to the internet, and who or what can access your computer while you're connected.

Fix Scam

Victims are cold called, usually by phone and told that there is a problem with their computer and for a nominal fee the suspect can fix it. The suspects often claim to be working with Microsoft who have identified that the computer has been infected with a virus and offer an update or fix.

Identity theft

The crime of impersonating someone – by using their private information – for financial gain.

Internet of Things
The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human interaction.

Malware
Software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Short for ‘malicious software’.

Phishing
An attempt at identity theft in which criminals lead users to a counterfeit website in the hope that they will disclose private information such as user names or passwords.

Smart TV
A television with more advanced computing ability and connectivity than a standard television.

Spam
Unsolicited commercial e-mail. Also known as junk e-mail.
Streaming
Streaming means listening to music or watching video in ‘real time’, instead of downloading a file to your computer and watching it later.

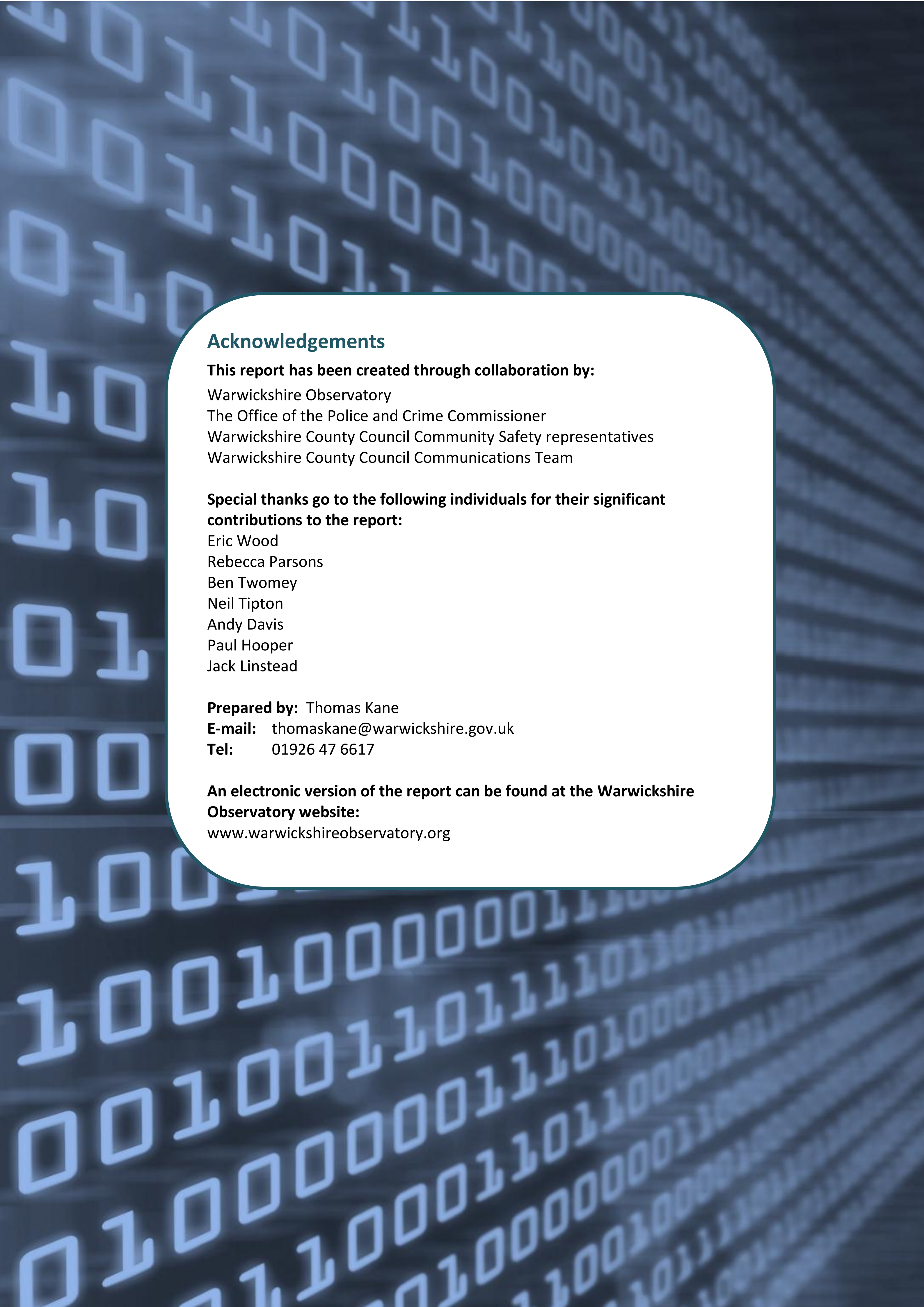
Tablet
An ultra-portable, touchscreen computer which shares much of the functionality and also the operating system of smartphones, but generally with more computing power.

Virtual Private Network (VPN)
Virtual Private Network: a method of creating a secure connection between two points over the internet. Normally used only for business-to-business communications.

Virus
A file written with the sole intention of doing harm, or for criminal activity.

Wi-Fi / Wireless network
A local area network which uses radio signals instead of a wire to transmit data.

Wireless hotspot
A publicly accessible wireless internet connection.



Acknowledgements

This report has been created through collaboration by:

Warwickshire Observatory
The Office of the Police and Crime Commissioner
Warwickshire County Council Community Safety representatives
Warwickshire County Council Communications Team

Special thanks go to the following individuals for their significant contributions to the report:

Eric Wood
Rebecca Parsons
Ben Twomey
Neil Tipton
Andy Davis
Paul Hooper
Jack Linstead

Prepared by: Thomas Kane
E-mail: thomaskane@warwickshire.gov.uk
Tel: 01926 47 6617

An electronic version of the report can be found at the Warwickshire Observatory website:
www.warwickshireobservatory.org