Warwickshire Cyber Crime Survey 2017

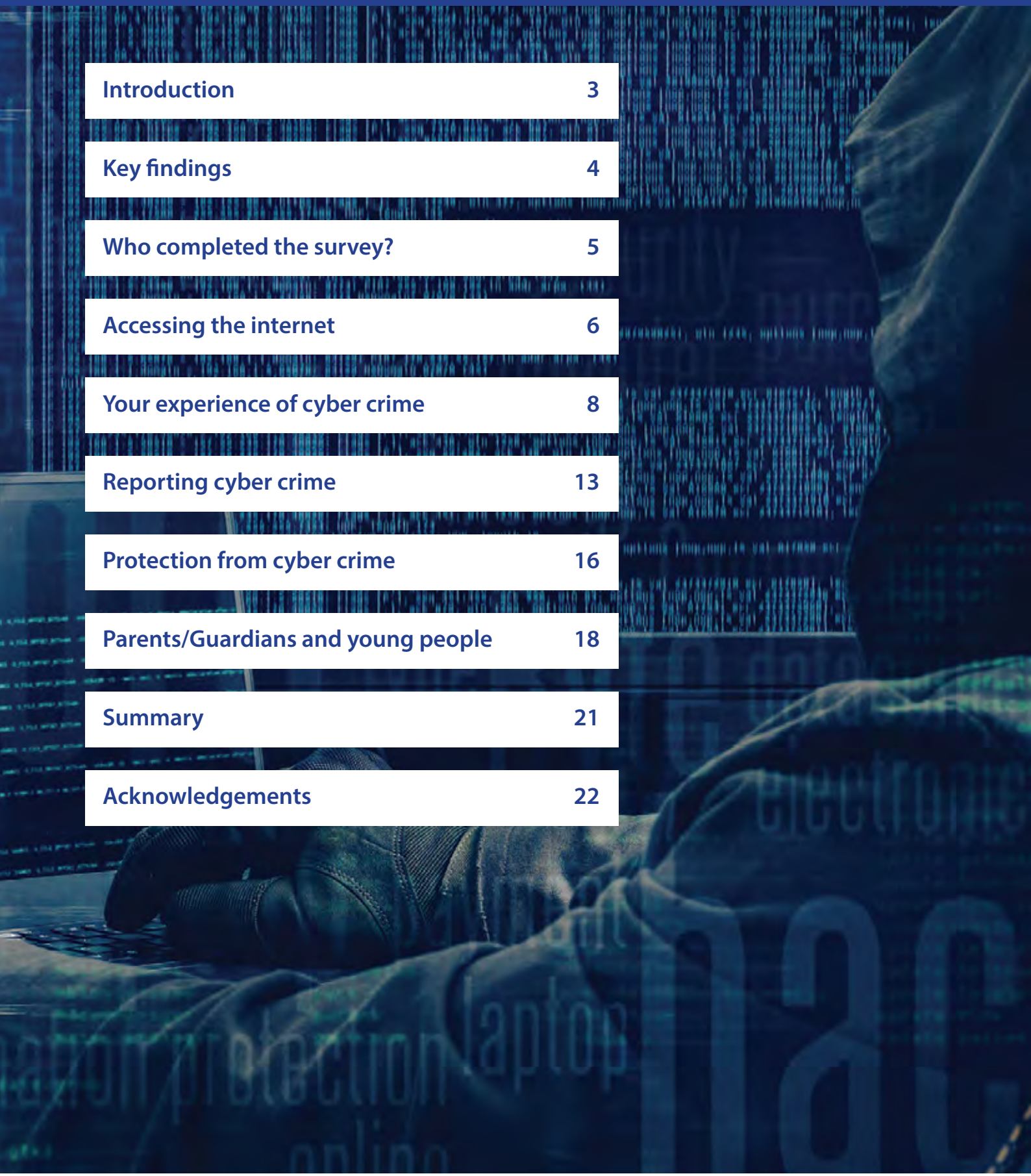
Headline Analysis

CYBER SAFE WARWICKSHIRE

Warwickshire County Council

Philip Seccombe Police and Crime Commissioner for Warwickshire

Contents



Introduction

Context of Survey

This is the second cyber crime survey completed in Warwickshire, carried out by Warwickshire County Council in conjunction with the Office of the Police and Crime Commissioner. Launched in November 2016, the survey ran for 3 months, addressing a number of key issues through 36 questions related to internet safety, asking respondents to identify their engagement with the internet, their perception of risks and their relationship with law enforcement in this area.

Offering insight into the experience of Warwickshire citizens in relation to cyber crime, the survey results will complement official crime statistics and other data sets collected by partner agencies such as Trading Standards and Victim Support. Cyber crime is currently under-reported and as such no one single data set can be relied upon by itself.

This time the survey was conducted across the West Midlands region as a whole, with colleagues from the policing areas of West Midlands, West Mercia and Staffordshire all wishing to assess the impact of online crime locally, to inform future strategies and preventative work. The survey and results focus on cyber crime at an individual level, though there is clear acknowledgement that businesses are also vulnerable to these crimes.

Definitions

'Cyber crime' can broadly be defined as crime that takes place online or where a digital system is targeted by means of a criminal attack. Discussions predominantly differentiate between 'cyber-enabled' crimes (traditional crimes conducted through the internet such as fraud and theft) and 'cyber-dependent' crimes (those that would not be possible without the internet such as a hacking, malware, viruses and bot-nets). The risk to individuals from either form of cyber crime continues to increase as daily activities continue to move online at a rapid rate'

Key findings

By extrapolating our findings to the Warwickshire population, the survey suggests:

Targeted by cyber

There have been nearly **15,000** successful phishing scams in Warwickshire in the last 12 months.

Over **5,500** residents have been a victim of an online romance scam.

9,900 have been victim of identity fraud.

30,000 fell victim to viruses and malware.

Over **6,000** online hate crimes.

Other online fraud and theft equates to **21,500** victims.

Impact of the crime

The biggest impact felt by victims of cyber crime was psychological and emotional.

At least **£8,848,300** has been lost by Warwickshire adults as a result of cyber crime.

This equates to each adult in Warwickshire losing just over **£20**.

Implementing cyber safety

Survey respondents suggest that the majority of residents in Warwickshire are implementing cyber safety measures.

Feeling of risk

59% of those surveyed feel at risk online

41% do not feel at risk online

Less than **1%** of respondents have no idea how to protect themselves online.

12% are not confident that they know how to protect themselves online.

67% are reasonably confident; **20%** are very confident.

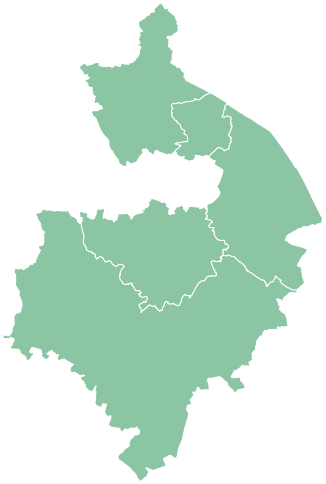
More people feel at risk, but only a small percentage of these do not know what to do at all to reduce this risk.

Compared to our previous survey, while a higher proportion of the public feel at risk online (**44%** in 2015, compared to **59%** now), fewer people have no idea how they can protect themselves online (**2.4%** in 2015, compared to **<1%** now).

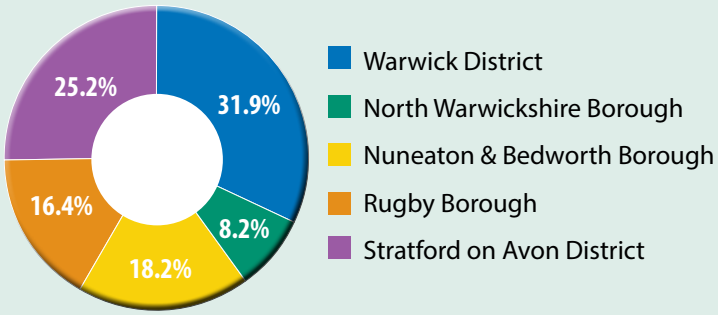
Who completed the survey?

Total respondents

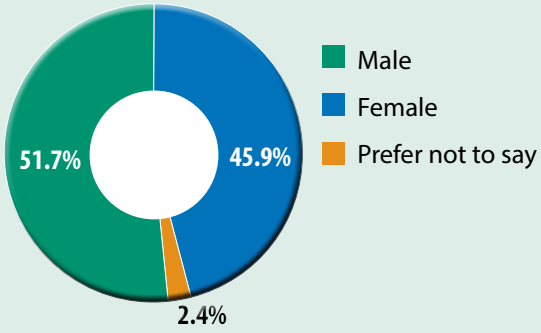
1,001 (30% of total regional respondents)



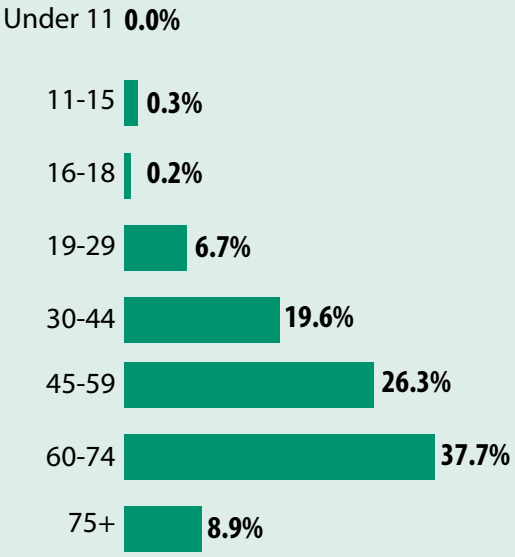
District/Borough breakdown



Respondents by gender



Respondents by age



Age UK

www.ageuk.org.uk/work-and-learning/technology-and-internet/internet-security/staying-safe-online/

The Age UK website include a 'Staying safe online' section. The site advices 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 of Age UK Advice services and also signposts users to the Action Fraud website where people can report cyber crime.

The 'Staying safe online' section can be found under

'Information and advice', 'Work and learning', 'Technology and internet'.

Accessing the internet

What devices do users use to access the internet?

98%

A computer or laptop was the most popular device used to access the internet

80%

Phone

69%

Tablet

42%

Smart Devices

Where do you access the internet?

	At Home	At Work	In Public
Computer/Laptop	31%	48%	15%
Phone	26%	37%	63%
Tablet	22%	12%	20%
Smart Devices (i.e. Smart TV)	14%	2%	2%
Gaming Console	7%	1%	-
Total	100%	100%	100%

If you access the internet both at home and 'outside', does your location influence which websites you are willing to access?

	Response Percent
Yes	65.8%
No	21.3%
Don't Know	5.1%
N/A (I do not access the internet outside of my home)	7.9%

65.8%

Positively, the majority of respondents stated that their location influenced their internet use

How often do you access the internet?

93.6%

of respondents access the internet every day.

How much time do you spend 'on' the internet?

- The majority of respondents spent an average of 1-3 hours online per day (47.7%)
- This is interesting as it appears to suggest that respondents did not consider the time they were at work as time 'spent on' the internet.

Answer options	Response Percent
Less than 1 hour	**16.1%**
Between 1 and 3 hours	**47.7%**
Between 3 and 5 hours	**18.0%**
Between 5 and 7 hours	**8.4%**
Between 7 and 9 hours	**5.2%**
Over 9 hours	**4.6%**

What do you access the internet for?

Activity	% of respondents
E-mail	**97.5%**
Online Banking	**80.5%**
General Browsing	**71.8%**
News and Current Affairs	**66.1%**
Education/Research	**61.1%**
Leisure and Tourism	**61.1%**
Buying and Selling Online	**60.1%**
Social Media	**56.3%**
Health (booking an appointment)	**48.9%**
Work	**46.6%**

NB. Respondents were asked to identify 'all that apply' to them in this question, presumably resulting in individuals selecting more than one response/activity where applicable. Therefore, each percentage shown is related to the total responses to the survey (X% of 1,001).

Your experience of cyber crime

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

93%

Overall, the majority of respondents in Warwickshire stated that they were aware of potential risks of online activity.

39%

stated that despite knowing about the risks, they did not feel at risk of becoming victim to online crime.

54%

stated that they did feel at risk of becoming victim to online crime.

Looking at respondents who stated that they felt at risk, the survey results reveal that British respondents, between the ages of 45-59 and 60-74 years of age feel most at risk, split evenly between male and female respondents.

Over the past 12 months, are you aware of having being targeted or becoming victim of any of the following types of online crime?

Reassuringly, most respondents stated they had been targeted, but not become victim of online crime. The top three issues individuals were targeted by were:

1. E-mail/Text Scam
2. Virus/ Malware issues
3. Fix Scam

Phishing Scam Risks

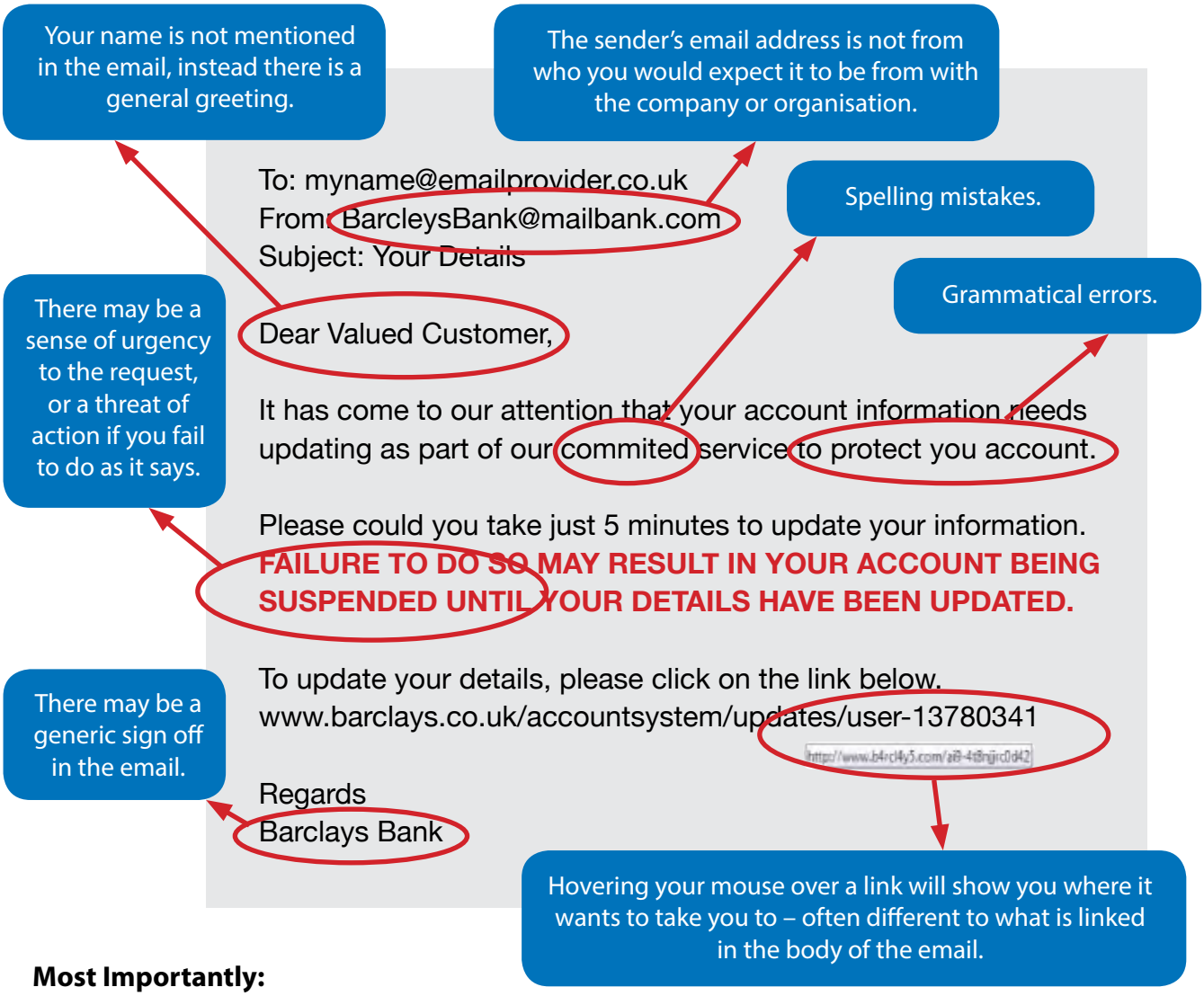
This is when fraudsters send out an email, instant message or text prompting you to provide your personal details, such as user names passwords or financial information.

Messages are often made to look like they are from legitimate companies, banks or organisations.

Sometimes they will direct you to a website where you are asked to input your personal information, for the criminals to capture, and use for crimes such as bank fraud and identity theft.

In some cases, an attachment is included in the email, which, when downloaded, installs a virus or malicious software to your device. This can then either steal your financial information, hold your device to ransom, or even spy on you via your webcam and microphone.

Phishing Scam Warning Signs



Most Importantly:

- Do not click on any link contained in an email – always go directly to the website the email is claiming to be from, and sign into your account from there.
- If in doubt, throw it out!

Analysing data related to what respondents had become victim of, the most frequently experienced 'cyber crimes' were:

The following table illustrates responses by crime type, echoing the above.

	Being targeted by	Become victim of
Virus/Malware issues (any software used to disrupt a computer operation or steal sensitive information from within the computer- often blocked by anti-virus software).	44%	6%
E-mail/Text Scam (an attempt to get sensitive information such as passwords or usernames by masquerading as a trustworthy source).	64%	3%
Non-financial online account attack (E.g: Facebook, E-mail).	22%	4%
Online banking attack.	10%	3%
Denial of Service Attack (E.g: X-Box live service down, network connection down due to deliberate attack).	7%	3%
Fix Scam (E.g: an offer to fix computer or device as a scam to gain access to it).	37%	3%
Courier Scam (E.g: a cold-caller claiming to be from your bank or the police convinces you to hand over sums of money or bank cards in the belief that they are protecting that account from fraud or theft).	10%	1%
Fraud or Theft (E.g: iTunes/PayPal account hacked, E-Bay non-receipt of goods following payment).	13%	1%
Online Harassment or bullying.	3%	2%
Online Stalking.	2%	2%
Online Sexual Offences (E.g: Revenge Porn, Sextortion, Online Sexual Abuse, Indecent imagery etc.).	2%	1%
Romance Fraud.	3%	1%
Hate Crime.	1%	1%
Identity Theft.	3%	2%
I am not aware or being targeted or being victim of online crime in the last year.	11%	4%

Dealing with, and reporting online hate crime

Screenshot any evidence of hate crime online, then:

Report It To The Site Itself

Most websites have rules known as 'acceptable use policies' that set out what cannot be put on their website. Most do not allow comments, videos and photos that offend or hurt people.

Look out for the website's 'contact us' page, which should be clearly linked. Others will have a 'report this page', or 'report this post' button that you can click.

Report It To The Host Website

If a website itself is hateful or supports violence, then let the website's hosting company know. You can find out which company hosts a website by entering their web address on the 'Who is hosting this?' website.

You can also contact your own internet service provider to get more information.

Report Illegal Internet Material To The Police

If the website or material you have seen online matches the description of illegal content and you think it originates in the UK (e.g. you know who the user is; or the website has a .co.uk address) you should report it to the police – use the screenshots collected as evidence.

You can do this via the True Vision website.

True Vision's website also contains more information and support for those affected by hate crime, whether it is happening off or online.

Ransomware

Ransomware allows criminals to remotely lock your device, and hold your personal files stored on this to ransom. The files will only be unlocked once a payment to the criminal(s) has been processed. On some occasions, the ransomware will claim that the user has viewed illegal or pornographic material online. This further encourages the user to pay the ransom without seeking any help.

Ransomware can get onto your device via:

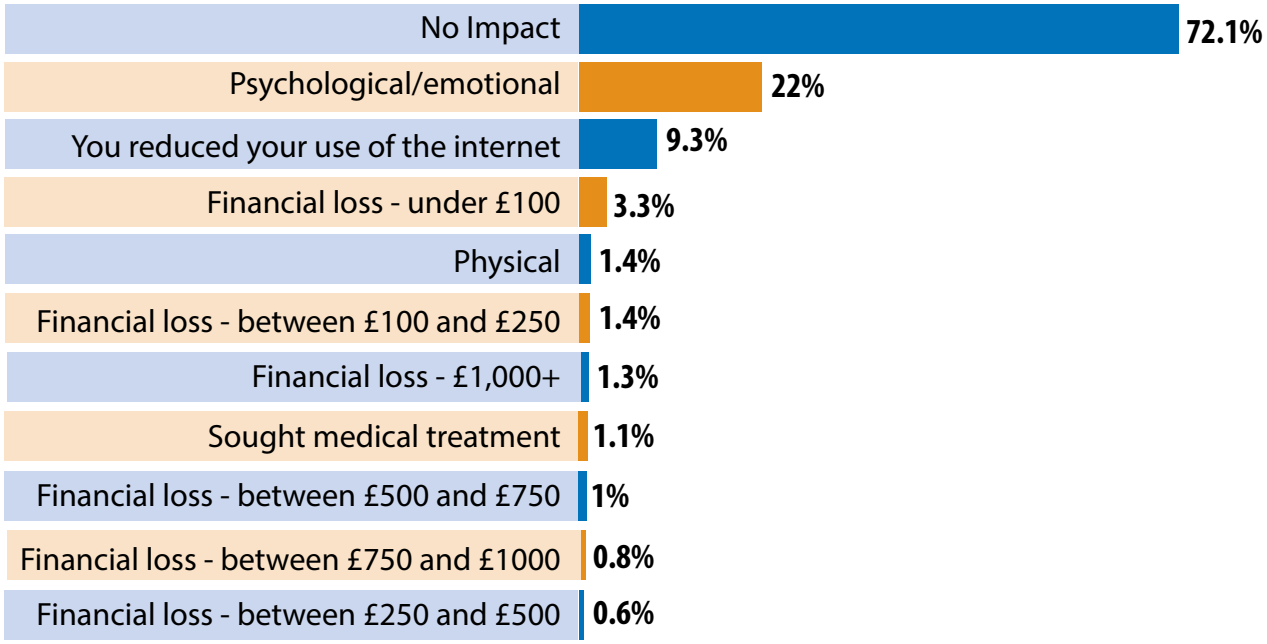
- clicking on a malicious link within an email
- opening a malicious attachment within an email
- visiting a corrupt website (sometimes you only have to open the page to have the malware install on your device)
- connecting corrupt USB sticks to the device
- connecting corrupt CDs or DVDs to the device

What to do if you have Ransomware on your device

- If your computer has been locked by ransomware, seek professional advice from a trustworthy source (e.g. an IT specialist)
- Restore your files from their latest back-up

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

The majority of respondents stated that becoming a victim of online crime did not have an impact on them (72%). Of those that did identify an impact, the most identified response/impact was psychological and emotional, followed by a reduced use of the internet. This is shown in the table here.



Victim Support

www.victimsupport.org.uk

There are trained Cyber Champions at Warwickshire Victim Support who can assist with some practical advice, as well as emotional support following a cyber crime.

If you've been affected, call your local victim care team in Warwickshire on **01926 682 693**.

Lines are open 8am-8pm Monday to Friday, and 9am-5pm on Saturdays.

If you need support outside of their open hours, call the **Supportline** for free on **08 08 16 89 111** or request support via the website.

Reporting cyber crime

Who did you report the crime(s) to?

- Half of respondents who became a victim of online crime did not report the crime, suggesting that more needs to be done to increase the reporting of online criminality.
- In instances where the crime was reported, most reported to their bank/financial service, followed by their friends or family and Action Fraud. This is helpful as it indicates that people report to a range of places and we need to rely on many datasets to give us the full picture of cyber crime.

Reporting Fraud, Viruses and Scams

www.actionfraud.police.uk

In the first instance, Action Fraud is where you should report. If you have been scammed, defrauded or experienced cyber crime. 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 Action Fraud contact centre where customers can speak directly to fraud and internet crime speacialists between 8am and 8pm Mon-Fri and 9am to 5pm Sat-Sun on **0300 123 2040**.

For cases where a crime is in progress, or the victim has been threatened, dial **101**.
In an emergency, dial **999**.

Crimes where messages or images of harassment or of intent to harm are sent, it is particularly important to 'screenshot' the material, and report the crime to the Police.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Source of reporting	Response Percent
Action Fraud	**10.9%**
Bank or other financial service	**22.2%**
E-mail provider	**12.7%**
Employer	**3.0%**
Friends or family	**14.5%**
Police	**3.7%**
Victim Support	**0.3%**
CrimeStoppers	**0.3%**
Citizens Advice Bureau	**0.4%**
Website where offence occurred (I.e: Instagram, ASKfm, Tumblr)	**9.7%**
Trading Standards	**1.9%**
Your computer security provider	**5.2%**
Your internet provider	**7.6%**
You did not report the crime	**50.2%**

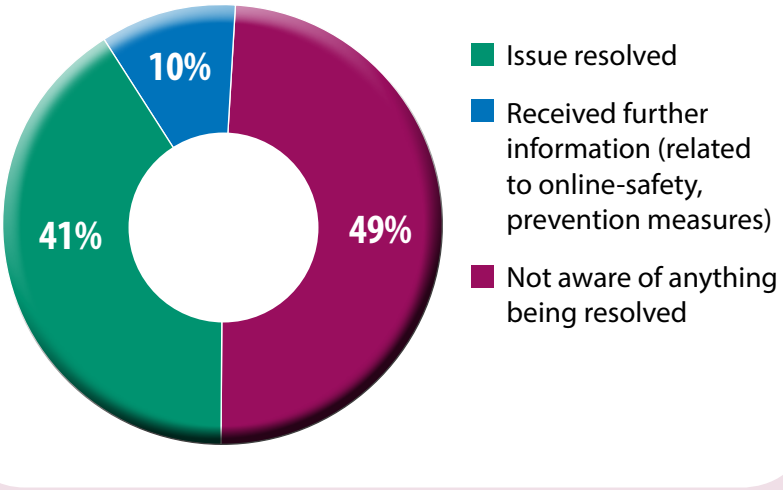
Trading Standards/Citizens Advice Consumer Service

www.tradingstandardsecrime.org.uk

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 Service, through which online scams can be reported (see number below). You can also report a scam or rogue trader to your local Trading Standards team via this number.
03454 04 05 06

If you did report the crime, what was the outcome?

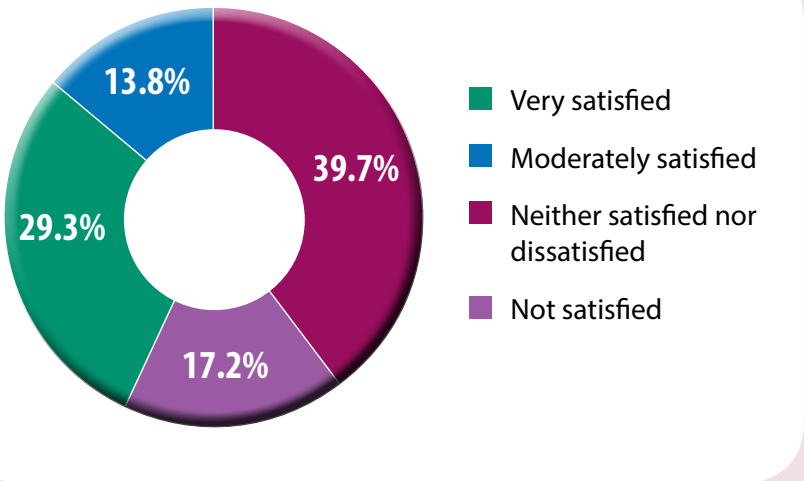
Almost half of respondents who reported a cyber crime were not aware of any outcome. This is significant as it may be a contributory factor towards the low reporting rates of online criminality.



Despite this, it should be recognised that 41% of respondents to this question stated that their issue had been resolved following reporting the crime, suggesting that alternative modes of reporting are partially efficient at resolving issues.

If you reported the crime, how satisfied were you with the outcome?

Similarly, responses indicate that a greater proportion of respondents were satisfied with the outcome, compared with those who were not satisfied (43% vs. 17%).



If you chose not to report the crime(s). Why not?

The most common reason for not reporting instances of cyber crime was perceptions of triviality, followed by not being aware that issues were crimes and not thinking anyone could help. This is important as it suggests that education initiatives may be needed to increase awareness of types of crime that may be conducted through the internet, in addition to agencies responsible for prosecuting/responding to such activity.

64%
'felt it was too trivial'

28%
'did not know who to report it to'

23%
'did not think anyone could help'

Protection from cyber crime

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

	Response Percent
I am very confident that I know how to protect myself online	**20.0%**
I am reasonably confident that I know how to protect myself online	**66.9%**
I am not very confident that I know how to protect myself online	**12.4%**
I have no idea how to protect myself online	**0.8%**

Though respondents were evenly split in their perception of risk, the majority were either 'reasonably' or 'very' confident in their knowledge of how to protect themselves online.

Positively, less than 1% of respondents stated they had no idea how to protect themselves from online threats.

Anti-Virus Software

Did you know that you can get anti-virus software for your tablets and smartphones, as well as laptops and computers?

For more information on viruses and malware, and how you can protect your devices from these, visit the Get Safe Online website.

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

Reassuringly, only 6% of respondents had done 'nothing' to improve their internet security in the last 12-months. The majority of respondents, however, stated that they had applied anti-virus/password protection etc. to at least one of their electronic devices. Security measures were most applied to laptop and computers rather than phones or tablets. This is important as it suggests that awareness could be in need of raising about the online risks to devices beyond the 'traditional' computer, particularly given the increasing prevalence of 'smart-devices' such as TVs and fridges.

Answer Options	On one device	On all devices
Used an up-to-date anti-virus software	**88%**	**35%**
Used a firewall	**75%**	**28%**
Installed anti-phishing software	**43%**	**19%**
Ensured software was up to date on all programs/applications	**78%**	**45%**
Used stronger, different passwords for different accounts	**75%**	**44%**
Used secure wifi networks	**69%**	**44%**
Used Virtual-Private-Networks (VPN)	**22%**	**12%**
Checked websites' authenticity before purchasing products or disclosing personal/private information	**67%**	**40%**
Checked that web pages are secure before inputting data (E.g: https:// and padlock)	**68%**	**42%**
Reduced frequency of online banking	**23%**	**10%**
Reduced frequency of buying and selling on-line	**15%**	**8%**
Participated in a course or lessons related to internet safety	**8%**	**4%**
Researched independently into protecting myself online	**23%**	**14%**
Nothing	**6%**	**3%**

Cyber Safe Warwickshire

www.cybersafewarwickshire.com

Cyber Safe Warwickshire is a dedicated local resource, full of the latest cyber crime news, alerts, and safety tips.

Get advice on how to protect yourself from the wide variety of cyber crime issues, as well as contact details for relevant support services, sources of further information, and where you can go to report the issue.

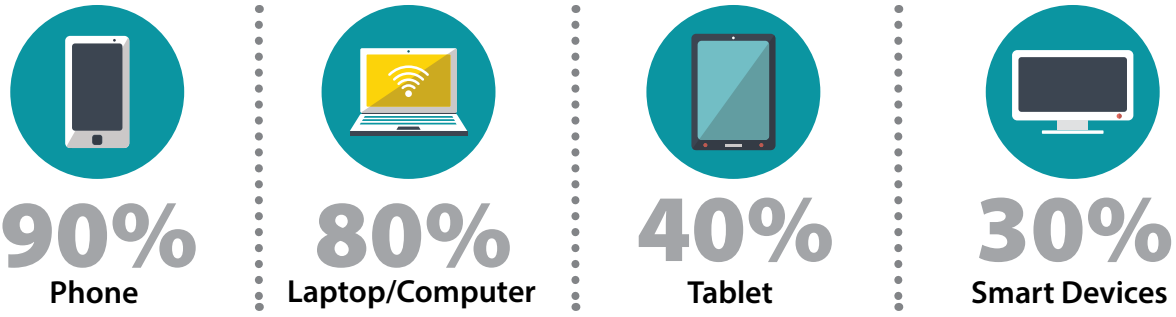
CYBER SAFE WARWICKSHIRE

Parents/Guardians and young people

Part of the survey was aimed at either parents/guardians or young people under the age of 18. This was done to assess any safety measures implemented by parents, as well as young people's perceptions of their threat from cyber crime.

Results indicate:

- Reassuringly, the majority of parents/guardians monitor their internet use (92%). Despite this, only 42% always monitored their internet access, suggesting that this may need to be improved. (Q23);
- Reassuringly, 73% of parents had applied restrictions to the use of the internet for any children in their household (Q24);
- 100% of parents/guardians had either already spoken to or planned to speak to their children about internet safety. (Q25);
- The majority use a phone or laptop/computer to access the internet. (Q27);



- Most young people stated that their school had spoken to them about internet safety (86%), followed by their parents (29%). Over half of young people had also seen/read advice online relating to internet safety (57%). (Q29);

Cyber Bullying

Whilst this survey suggests that the majority of young people have not experience cyber bullying, it is fully recognised that this may not be a reflection of the true scale of this problem, largely due to the small proportion of responses from under 18's (0.5%).

The NSPCC have reported that in 2015/16, 25,700 Childline counselling sessions with children focussed on issues relating to bullying.

More information and support relating to cyber bullying is available via the NSPCC website.

www.nspcc.org.uk

NSPCC

Internet Matters

www.internetmatters.org

Internet Matters offers support for parents to give them the knowledge and resources needed to have conversations with their children about their online behaviours. They have created information that will help parents to learn about, to talk about and to deal with the main online safety issues that children face, including bullying, sexting, grooming and self-harm.

internet matters.org

CEOP Command

www.ceop.police.uk

0870 000 3344

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 National Crime Agency-led operations and in partnership with local and international agencies.

CEOP
A National Crime Agency command

Office of the Police and Crime Commissioner

www.warwickshire-pcc.gov.uk

01926 412 322

Warwickshire Police and Crime Commissioner Philip Seccombe has set a priority of ensuring cyber crime is tackled head on. He funds the Cyber Safe Warwickshire campaign in order to help everyone understand the best ways to enhance their cyber security and reduce their chances of becoming a victim.

Philip Seccombe
Police and Crime Commissioner
for Warwickshire

Warwickshire County Council Community Safety Team

01926 412 261

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 cyber crime issues and advice on where to report.

Warwickshire
County Council

Safe In Warwickshire

www.safeinwarwickshire.com
communitysafety@warwickshire.gov.uk

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 cyber crime.

safe in... warwickshire

Summary

Cyber crime is a real problem in Warwickshire, and many people feel at risk. However, the majority also know what measures they can take to reduce this risk. If we are to use this survey to inform our work, it would suggest that focus is given to the vulnerable groups and those who do not have any knowledge of how they can protect themselves.

Our definition of vulnerable groups is those whose confidence interferes with online behaviour. This is both those who are under and over-confident while online.

Cyber Safe Warwickshire Partnership

Representatives from the county, district and borough councils, Police, Trading Standards, Office for the Police and Crime Commissioner, Education, Federation of Small Businesses, Chamber of Commerce, Youth Justice, Victim Support and Neighbourhood Watch attend. They meet quarterly to update the countywide action plan in response to cyber crime across the 4 P's (Protect, Prepare, Prevent and Pursue).

Cyber Crime Advisors

Since April 2016, the Office of the Police and Crime Commissioner has funded two Cyber Crime Advisors, who are hosted by Warwickshire County Council. They are tasked with raising awareness of cyber crime, providing preventative advice and signposting the public to further support and information. Their Business Crime Advisor colleague provides this service for local small and medium businesses.

The Cyber Crime Advisors are contactable via either email below;

alexgloster@warwickshire.gov.uk

samslemensek@warwickshire.gov.uk

The Business Crime Advisor is contactable via **alexcharleswilliams@warwickshire.gov.uk**

Acknowledgements

This report has been created through collaboration by:

Warwickshire County Council Insight Service

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:

Louise Williams

Alex Gloster

Sam Slemensek

Rebecca Parsons

Neil Tipton

Sarah Mainwaring

Paul Coxon

Prepared by: Sarah Mainwaring

E-mail: sarahmainwaring@warwickshire.gov.uk

An electronic version of the report can be found at:

www.cybersafewarwickshire.com

CYBER SAFE WARWICKSHIRE

Warwickshire County Council

Philip Seccombe Police and Crime Commissioner for Warwickshire