# FENLAND COMMUNITY SAFETY PARTNERSHIP

# QUARTER 2 2018/19: CYBERCRIME

VERSION 1.0
OCTOBER 2018

| |
|---|
| 'Cambridgeshire Research Group' (CRG) is the brand name for Cambridgeshire County Council's Research & Performance Function. As well as supporting the County Council we take on a range of work commissioned by other public sector bodies both within Cambridgeshire and beyond.<br><br>All the output of the team and that of our partners is published on our dedicated website www.cambridgeshireinsight.org.uk<br><br>For more information about the team phone 01223 715300 |

| **Document Details** | |
|---|---|
| Title: | Fenland Community Safety Partnership Q1 Strategic Assessment 2018/2019 |
| Date Created: | October 2018 |
| Description: | The purpose of this document is to provide the Fenland Community Safety Partnership with an understanding of key community safety issues affecting the district. |
| Produced by: | Jamie Leeman<br>Senior Research Analyst, Cambridgeshire County Council |
| Additional Contributions: | Alan Boughen, Aarron Locks<br>Fenland District Council<br><br>Nigel Sutton<br>Fraud and Cyber Security Advisor<br>Specialist Crime Team (Serious & Organised, Fraud & Cyber)<br>Intelligence and Specialist Crime Department<br>Cambridgeshire Constabulary |
| On behalf of: | The document has been produced by the CRG, on behalf of Fenland Community Safety Partnership and is available to download from Cambridgeshire Insight<br><br>**Alan Boughen**<br>**Community Safety Partnership Support Officer** |
| Geographic Coverage: | Fenland district and Cambridgeshire County where relevant |
| Time Period: | 2018, plus historical data where relevant |
| Format: | word |
| Status: | Draft 0.1 |
| Usage Statement: | This product is the property of the Research Group, Cambridgeshire County Council. If you wish to reproduce this document either in whole, or in part, please acknowledge the source and the author(s). |
| Disclaimer: | Cambridgeshire County Council, while believing the information in this publication to be correct, does not guarantee its accuracy nor does the County Council accept any liability for any direct or indirect loss or damage or other consequences, however arising from the use of such information supplied. |

# Contents

## SECTION 1: EXECUTIVE SUMMARY

### KEY FINDINGS

There is a continued concern that cybercrime is massively underreported both locally and nationally and it is difficult to get a true picture of the problem in Fenland. The Action Fraud cyber profile for Cambridgeshire showed that there were 153 crimes reported to Action Fraud from Cambridgeshire between October 2017 and March 2018 with approximately £271,000 lost by victims across the force-wide area.[1]

Cybercrime is a broad umbrella term incorporating a number of crime types. It is important that the key distinction between **cyber-enabled** and **cyber-dependent is made.** This distinction will help the partnership to agree on the focus for future activity both in understanding cybercrime and also in working to tackle it.

Due to the complex, sophisticated and often international nature of **cyber-dependent** crimes (such as hacking or the spread of malicious software), it is difficult for the community safety partnership to tackle. Despite this, these attacks can be avoided through potential victims taking some basic precautions and the CSP can help raise awareness in this area. **Cyber-enabled crime** often crosses into other, more traditional, crime and community safety issues that the partnership already have sight on through previous assessments or existing work streams, such as Fraud and Child Exploitation. It is therefore important that the partnership has some focus on 'cyber' as an **enabler** for other priority areas.

There is often a wider international element to a lot of cyber offences. As a result, there are often restrictions and difficulties in tracing cyber criminals and so provide challenges to identifying and pursuing offenders. This is particularly the case for **cyber-dependent** crimes. This means the focus of any activity delivered by FCSP should be focussed on **preventing victimisation.**

National evidence suggests that there is less variation across demographic characteristics in victimisation of cybercrime than other key crime types and the key message for the partnership is that **anybody** can be a victim of cybercrime, should they not be aware of mechanisms they can put in place to mitigate their risk.[2] Experimental statistics based on Action Fraud data broken down by force area are consistent with the Crime Survey of England and Wales (CSEW) findings in showing less variation than other crime types in rates across forces (where the victim lived) for the year ending September 2017.[3] Anybody can be a victim of cybercrime but the partnership should be mindful of vulnerabilities (particularly those highlighted in the 2017/18 Scams assessment such as social isolation and mental health) amongst potential victims.

[1] Cambridgeshire Cyber Profile, Action Fraud, https://www.actionfraud.police.uk/sites/default/files/Cambridgeshire%20-%20Cyber.pdf

[2] Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

[3] Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

There is a close relationship between cybercrime and fraud, including scams. The partnership identified scams as a priority area through 2017/18 and awareness raising in this area should continue due to the high harm felt amongst victims. This report will help the partnership understand cyber-related scams specifically and future opportunities to further develop the targeted scams programme of work that was delivered in 2017/18. The latest national figures for the year ending September 2017 indicate that the volume of fraud recorded by Action Fraud nationally is the highest it has ever been (272,980 offences).[4]

A significant proportion of cyber offences can be avoided if victims have the correct level of protection on their devices as well as the knowledge in how to protect themselves. High level crime prevention campaigns that convey this advice to the wider community would help to stop some of this criminality. Targeted campaigns aimed at sections of society vulnerable to these offences – such as the elderly, young people and small businesses also need to be released via avenues of communication that ensure they reach their target audiences. There are a range of resources that can promote and help deliver these messages. Even with protection, scammers change methodology so there will always be a need to update messaging to the public

## RECOMMENDATIONS

This section aims to summarise possible activity for the partnership to explore in order to improve local understanding of the threat of cybercrime and support county wide and existing work. This can be summarised into 4 key action streams.

- Due to the close relationship between cyber-related crime and scams, the partnership should look to develop scams related work that took place in 2017/18 with a cyber focus e.g disseminate Little Book of Cyber Scams to support Small and Medium Enterprises (SMEs) on staying safe in the cyber world and explore Silver Mondays (or similar opportunities) to disseminate messages to wider community
- Develop relationship with force-wide Fraud and Cyber Security Advisor to help identify opportunities for local delivery of key messages to partner staff and the community
- Support the Cyber Ambassadors scheme by raising awareness and using partners to help 'recruit' potential ambassadors in the district
- Use broad range of available campaigns and resources to disseminating appropriate messages across different partner networks such as Fenland for Business, Parish Councils

By placing a focus on cybercrime, the partnership have the opportunity to build on existing work around scams awareness and broaden the focus to the wider impact of cyber activity. It is recommended that the partnership look to build on the successful work in this area and place a 'cyber-enabled' focus.  For example, the Little Book of Cyber Scams offers the partnership to disseminate key messages around cyber-crime, in a similar way to that done around fraud and scams more broadly with the Little Book of Big Scams. Similarly, Silver Monday event delivered through the partnership in 2017/18 aimed at delivering fraud/scams awareness amongst elderly members of the community could be tailored to focus on cyber awareness too.

[4] Overview of fraud and  computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

The partnership should look to support improved local reporting of cyber-crime and cyber-related crimes such as fraud. This can be done by making the appropriate channels of reporting clear. The partnership should also work to raise general awareness of cyber-crime through promoting responsible use of the internet and raise awareness of available support e.g. the 'Get Safe Online' website and 'Take Five' campaigns.

The partnership should explore opportunities to work in partnership with Cambridgeshire Constabulary's Fraud and Cyber Security Advisor. This relationship could be used to help facilitate opportunities for the advisor to deliver key messages at local events or to identify suitable audience groups. Partner agencies should work to ensure that their staff are aware of the scams within the Little Book of Big Scams (LBoBS) and cyber scams within the Little Book of Cyber Scams especially those working directly with residents. In doing this the partnership will be able to establish strong, effective partnerships with specialist organisations, in order to educate staff in terms of the current cyber trends in line with the changing methods used by criminals.

Cambridgeshire Constabulary, led by the force's Fraud and Cyber Security Advisor, do have a cyber ambassador programme which aims to work with representatives from community groups and institutions to raise awareness within the community group or institution around the different types of cybercrime and assist in promoting prevention advice local areas. The partnership can play a key role in helping to recruit potential ambassadors to the scheme and disseminate key messages surrounding cybercrime.

The partnership should look to work those with internet access and those who are more at risk due to identified vulnerabilities including age, social isolation, loneliness, poor mental health or those that may be exploited due to age-related vulnerabilities. This may assist in preventing further or repeat crimes. Promoting the 'Tea and Tablet' sessions would be one way of doing this.

## SECTION 2: INTRODUCTION

The 2017/18 annual strategic assessment to the Fenland Community Safety Partnership (FCSP) highlighted that *'Cybercrime provides an environment for offending in a broad range of areas including Child Sexual Exploitation, exploitation of vulnerable adults and those with mental impairments. There is a concern that cybercrime is massively underreported locally.'*[5] The purpose of this report is to ensure that the partnership have an improved understanding of cybercrime in general whilst providing recommendations to increase wider awareness and support increased reporting locally.

As more and more of our lives are being administered, published and shared online, the risk of individuals across the district and county becoming a victim of online related crime continues to increase. Concerns around the threat of cybercrime and cyber-related fraud were reflected in the introduction of fraud and computer misuse into the Crime Survey of England and Wales (CSEW) in 2015.[6]

Cybercrime is a broad, over-arching term and the recommendations of this report will also be driven by understanding the types of interventions that the CSP can deliver to tackle cybercrime. It is believed that a large proportion of all cybercrimes would be avoidable with relevant simple steps and the CSP can play a role in raising awareness and driving interventions that can enable potential victims to put these steps in place.[7]

By focussing on cybercrime, FCSP are presented with the opportunity to deliver local activity to help tackle a force-wide priority. There has been work across the force-wide area to improve awareness of cybercrime and it is important that the CSP understands the nature of this work so that they can understand opportunities to support this locally. Through 2017/18, the FCSP placed focus and targeted activities around Scams prevention. It is important that this report recognises the close relationship between scams and online crime to ensure that any targeted work by the partnership on cybercrime is an extension of the scams related work.

## SECTION 3: CYBER CRIME

Cybercrime is an 'umbrella' term for lots of different types of crimes which either take place online or where technology is a means and/or target for the attack.[8] From this, it can be broken down into two broad categories- **cyber-dependent crimes** and **cyber enabled crimes.**

**Cyber-enabled crimes** are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. Example of cyber-enabled crimes include:

- Fraud (including mass-marketing frauds, 'phishing' e-mails and other scams, online banking and e-commerce frauds);
- Theft (including theft of personal information and identification-related data);

[5] Cambridgeshire Research Group, Fenland Q1 Strategic Assessment 2017/18, Scams, https://cambridgeshireinsight.org.uk/wp-content/uploads/2017/08/Q1Assessment_Victims_Scams1.2.pdf

[6] Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

[7] Get Safe Online, Protect Yourself, https://www.getsafeonline.org/protecting-yourself/

[8] Bedfordshire Police, What is cybercrime?

• Harassment;

• Sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery).

**Cyber-dependent** crimes are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DdoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud. Cyber-dependent crimes are sometimes referred to as 'pure' cyber-crime.

The Cambridgeshire constabulary cybercrime profile highlighted that the vast majority of recorded cybercrime in Cambridgeshire is **cyber-enabled.** It is important that the partnership understand this distinction as any focussed activity around cybercrime will be centred on this and the partnership should consider where they feel they could have the biggest impact.

The relationship between scams/fraud and cybercrime is very close. Fraud is the most commonly experienced crime in the UK. The Crime Survey of England and Wales 2017 indicated that there were 3.4 million incidents of fraud in the financial year ending March 2017. [9] Understanding of fraud in the UK is hampered by under-reporting; less than 20% of incidents are reported to the police. Cyber criminals targeting the UK include international serious organised crime groups as well as smaller-scale, mostly domestic, criminals and hacktivists. Whilst under-reporting of this offence type means that official figures are difficult to obtain, research into personal victims by the Crime Survey in England and Wales (CSEW) estimates that "around one in ten adults in the UK have been a victim of fraud or computer misuse" in the year to September 2017. They state that there were 3.2 million incidents of 'Fraud and Computer Misuse' in the survey year ending September 2017. In fact, 45% of all criminal incidents identified by the CSEW were either Fraud or Computer misuse, making it "the most prevalent crime" covered by the survey.[10]

### *Cybercrime: The scale*

Action Fraud is the UK's national reporting centre for fraud and cybercrime and is where individuals should report fraud if they have been scammed, defrauded or experienced cybercrime. Between October 2017 and March 2018 there were[11]:

- **332,570 total crimes** reported to Action Fraud across the UK
- **£706 million** lost by victims nationally
- **62%** of reports were from businesses and **39%** from individuals.[12]

Further, analysis of the Crime Survey of England and Wales, which introduced fraud and online crime in 2015 shows that:

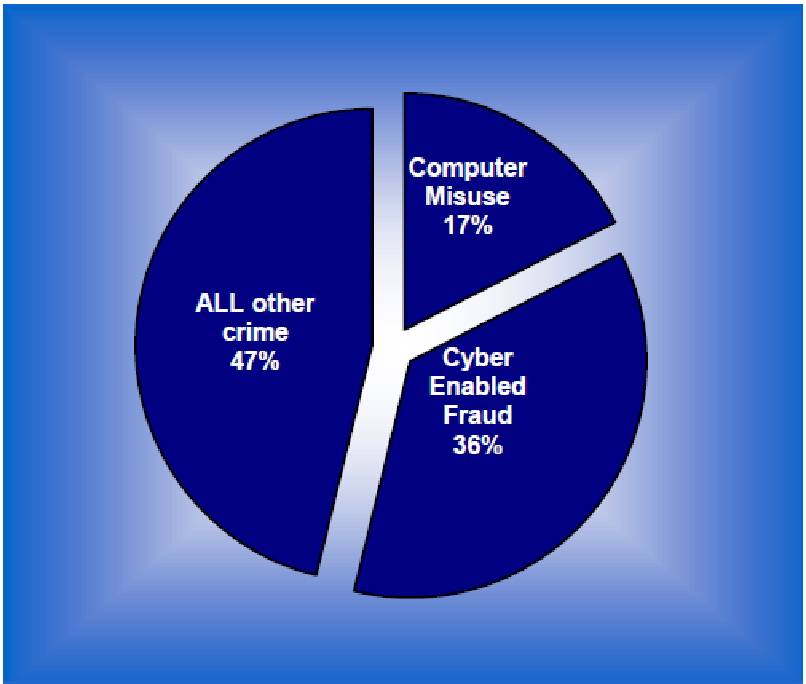
- the large majority of victims of fraud and computer misuse had been a victim only once (81%), with the remaining 19% having experienced more than one offence (within the same 12-month crime reference period)

[9] ONS, Crime in England and Wales, 2017
[10] ONS, Crime in England and Wales, 2017
[11] Action Fraud, What is Fraud and Cybercrime, https://www.actionfraud.police.uk/what-is-fraud
[12] Action Fraud, What is Fraud and Cybercrime, https://www.actionfraud.police.uk/what-is-fraud

- by offence type, repeat victimisation was more common among victims of bank and credit account fraud (15%) than other types of fraud (for example, consumer and retail fraud, 5%)
- with regard to computer misuse, 23% of incidents involved loss of money or goods, all relating to computer viruses (410,000 incidents)

Analysis of the CSEW surrounding fraud and computer misuse highlights that fraud and computer misuse crime is more prevalent than many traditional crimes, with data for the year ending September 2017 showing individuals to be 10 times more likely to be a victim of fraud and computer misuse than a victim of theft from the person and 35 times more likely than robbery.[13] Figure 1, below demonstrates the scale of both cyber enabled fraud and computer misuse crimes against all crimes in the UK.

Figure 1: Breakdown of all crimes including cybercrime, taken from NCA Cyber Crime assessment 2016[14]



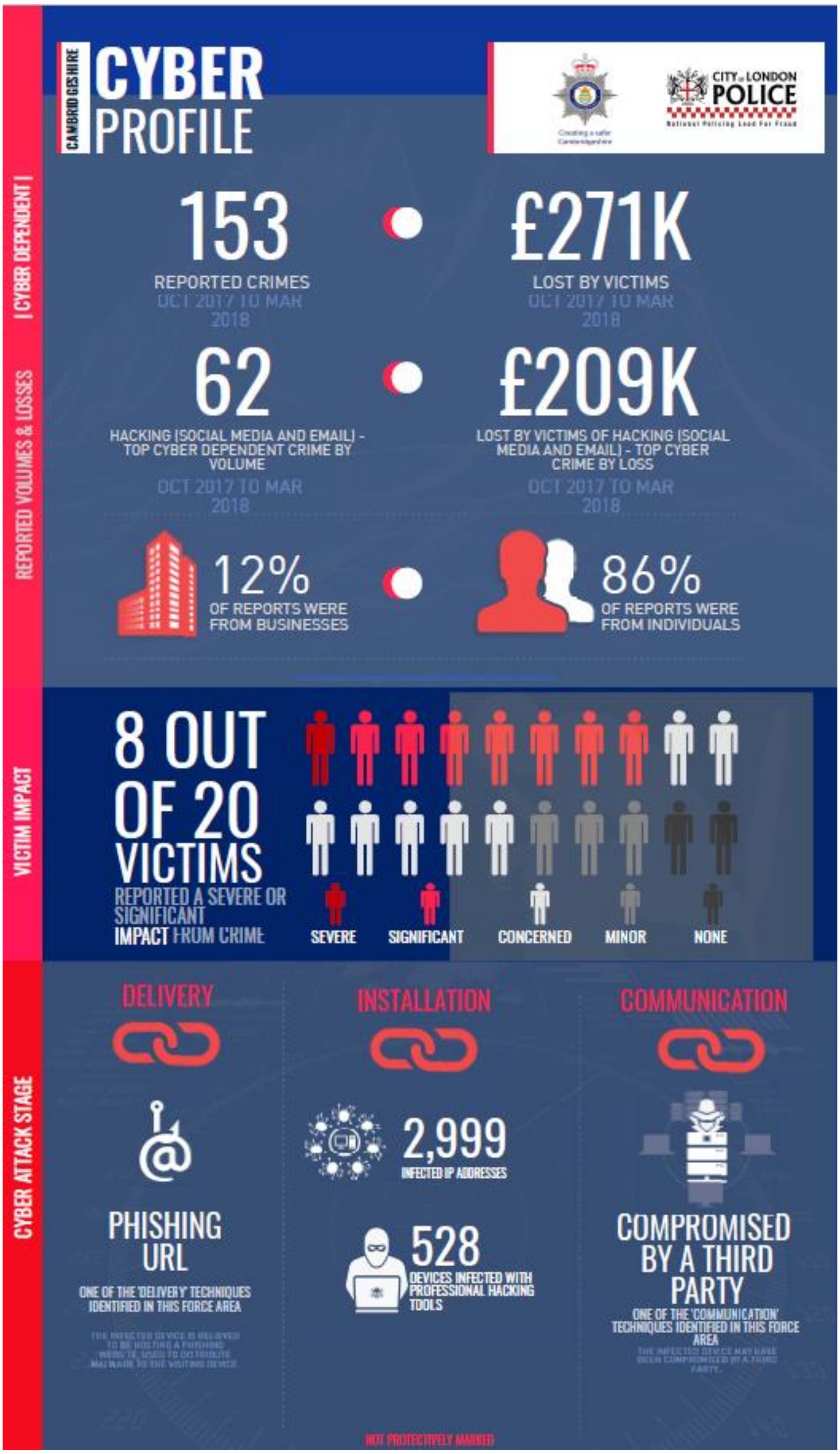

Cyber Crime as a proportion of total UK crime in 2015 (Source: ONS)[15]

The Action Fraud **cyber profile** for Cambridgeshire showed that there were 153 crimes reported in Cambridgeshire between October 2017 and March 2018 with approximately £271,000 lost by victims across the force-wide area. Of those reports, 12% were reported from businesses and 86% of reports were from individuals. The infographic (Figure 2) produced by action fraud for

13 https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25
14 http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
15 Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

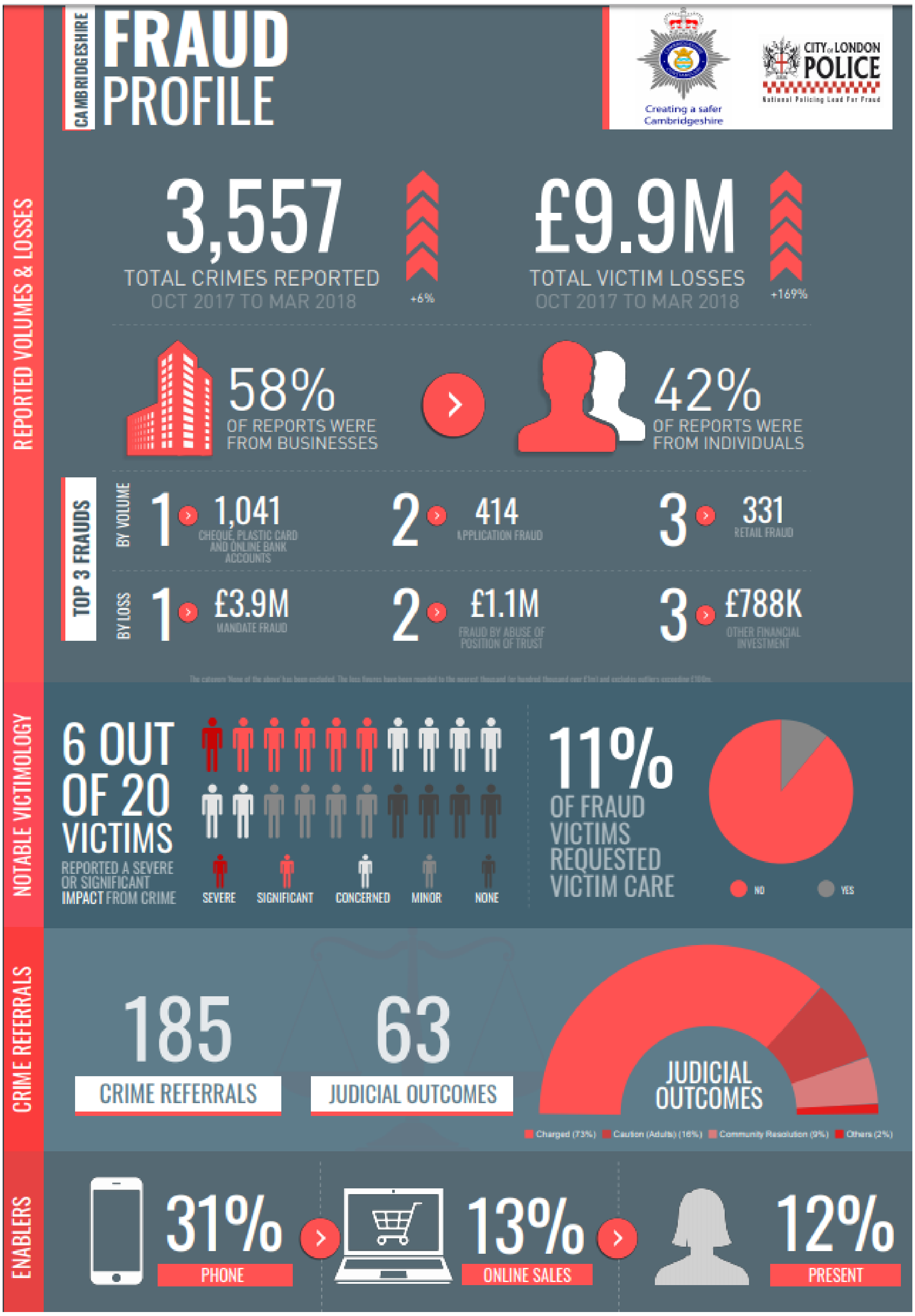
Cambridgeshire shows the level of impact, both financial and emotional, that cybercrime can have on individuals.

Figure 2: Cambridgeshire Cyber Profile, Action Fraud- October 2017 to March 2018



As shown in the Action Fraud infographic above (Figure 2) for Cambridgeshire, 86% of reported offences to Action Fraud were from individuals and 12% were from Business. This difference between individual and business reports may in fact be down to a lower reporting rate of cybercrime amongst businesses. The **Cambridgeshire Fraud profile,** provided by Action Fraud below, paints a different picture to total cybercrime with 58% of frauds reported by business.

Figure 3: Cambridgeshire Fraud Profile, Action Fraud- October 2017 to March 2018



### *Which groups in society are most likely to be victim of fraud and computer misuse?*

In order to understand cybercrime and how the partnership can support those most vulnerable to becoming a victim of a cybercrime, it is important that understand those most at risk. The reality though is that anybody across the district is at risk of becoming a cyber victim and actually, the partnership would be best focussing on targeting prevention activities at the enabler of cybercrime, i.e the device, rather than purely focussing on the individual.

As mentioned previously, analysis of the CSEW surrounding fraud and computer misuse highlights that fraud and online crime is more prevalent than many traditional crimes but analysis also shows that there was typically less variation than seen in other types of crime in the rate of fraud victimisation across different groups in society. However, some personal and household characteristics were associated with being a victim of fraud and those with the higher risk of victimisation often differed from other crime types and it is important that the partnership understands this.

Within the Crime Survey of England and Wales, fraud victimisation was identified as being higher in the middle of the age distribution, where adults aged 35 to 44 were more likely to be a victim of fraud (7.4%) than 16 to 24 year olds (4.9%) or those aged 65 or over (65 to 74, 5.4%; 75 and over, 2.8%).[16] Ultimately though, there is less variation across demographic characteristics in victimisation than other key crime types and they key message for the partnership is that anybody can be a victim of cybercrime, should they not put the correct mechanisms in place to avoid it.

## UNDERSTANDING CYBER ENABLED SCAMS

As mentioned, there is a close relationship between cybercrime and scams, a priority area of the partnership in 2017/18. Example of cyber-related scams include[17]:

- Online shopping and auction fraud: Scammers often look to establish fake shopping sites to take payment for goods that they will not supply.
- Online ticketing scams: Scammers set up websites offering tickets that they do not have access to and cannot provide but are happy to take payment for.
- Internet scams: Scammers attempt to place programs onto victims' computers in order to steal data. These are cyber dependent crimes that can be avoided through taking appropriate precautions.
- Mass market fraud (scam email): Email can be used to help facilitate mass mail scams where victims are targeted in order to give away personal details with the lure of a prize of financial gain. Often the most vulnerable are targeted.
- Holiday fraud: Scammers target online holiday booking and accommodation sites to scam unsuspecting customers into paying for accommodation that is unavailable or does not existing.

[16] Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

[17] Little Book of Big Scams, Cambridgeshire County Council, https://ccc-live.storage.googleapis.com/upload/www.cambridgeshire.gov.uk/residents/consumer-protection/CCC_LBOBS_Third%20Edition_ONLINE.pdf?inline=true

## EMERGING THREAT IN ONLINE DATING

A study by the National Crime Agency identified a significant increase in serious sexual assaults carried out by a stranger that have been initiated through online dating. The 2016 report found that there had been a six-fold increase in these offences from 2009 – 2014, from 33 offences in 2009 to 184 in 2014.[18] The report showed that:

- 85% of victims were female
- 42% of victims were aged 20-29
- In 43% of cases the first meeting took place within one week of the initial online contact
- More than half of victims had engaged in communications of a sexual nature with the offender prior to the offence taking place

The report[19] identifies that the very nature of these offences may lead to barriers in reporting. The victim may feel their willingness to engage in sexual conversations with the offender online, or agreeing to meet at their residence on the first date, somehow makes the sexual assault that follows their fault.[20] It is important to highlight here that the 'cyber' element to online dating crimes is the enabler the specific crime can be varied and not always financially motivated.

*Recommendation: the partnership should recognise the vulnerabilities around online dating and look for opportunities to raise awareness of the risks*

## CYBERCRIME RELATING TO CHILDREN AND YOUNG PEOPLE

### *Emerging Threat in Online Grooming*

Online grooming relates to the use of digital technologies to build an emotional connection to a person to gain their trust for the purposes or abuse or exploitation. Many victims do not recognise that they are being groomed or that what has happened to them is abuse. Groomers may use social media sites, instant messaging app or online gaming platforms to connect with young people. They spend time learning about the person's interests from their online profiles to build a relationship. Groomers will look for information that suggests that the person has low self-esteem or is vulnerable. This area of Cyber Enable crimes has strong overlaps in two key areas of risk;

- Child Sexual Exploitation
- Radicalisation

[18] National Crime Agency (NCA), Emerging Threat in Online Dating, http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file
[19] National Crime Agency (NCA), Emerging Threat in Online Dating, http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file
[20] National Crime Agency (NCA), Emerging Threat in Online Dating, http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file

Again, here are two crime types where online activity can act as an enabler of other crime types.

The 2016 Health Related Behaviour Survey found that 92% of year 8 and year 9 pupils in Fenland and East Cambridgeshire responded that they have access to the internet outside of school lessons with 60% responding that they spent at least 3 hours using the internet on the day before the survey. Clearly, there is a large proportion of young people in Fenland regularly using the internet and exposed to possible scams. Within the survey, 93% of pupils responded that they have been told how to stay safe while online while 59% said they always follow the advice they have been given. In order to prevent online scam victimisation it is important that young people understand the principles of staying safe online. Within Fenland and East Cambridgeshire, 28% of pupils responded that they have found school lessons about personal safety 'quite' or 'very' useful. This was lower than the proportion of pupils that gave this response in 2014 (36%) while 17% (12% in 2014) have found them 'not at all' useful and 23% (17% in 2014) couldn't remember any.[21]

## CYBERCRIME RELATING TO THE ELDERLY

National evidence suggests that the elderly may be particularly vulnerable to fraud, which can be cyber related, particularly where the motivation is for financial gain.[22]Age UK's report[23] – Only the tip of the iceberg, suggest that 'Older people may be especially at risk due to social isolation, cognitive impairment or bereavement'. The same report raises concerns about the recent changes to private pensions allowing the over 55s to access all their pensions saving as cash which could encourage scammers to target the age group even more. The survey undertaken by Age UK found that 53% of older people (65+) believe that they have been targeted by fraudsters and of those that gave further details; 70% had lost money. Research included in the report suggested that the financial loss to elderly victims (55+) was likely to be twice as much per scam as for younger age groups.[24]

Financial scamming is a problem that can affect everyone but certain groups within our communities are more vulnerable to becoming a victim of a scam. There are

- Older people who are targeted more often by certain scams such as doorstep, mail, telephone and investment scams. Older people who have no other form of social support are more likely to listen to a sales pitch. This type of contact is more likely to expose older people to scammers.

---

21 Cambridgeshire HRBS Survey, 2016

22 Only the tip of the iceberg, Age UK, https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

23 Only the tip of the iceberg, Age UK, https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

23 Only the tip of the iceberg, Age UK, https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

24 Only the tip of the iceberg, Age UK, https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

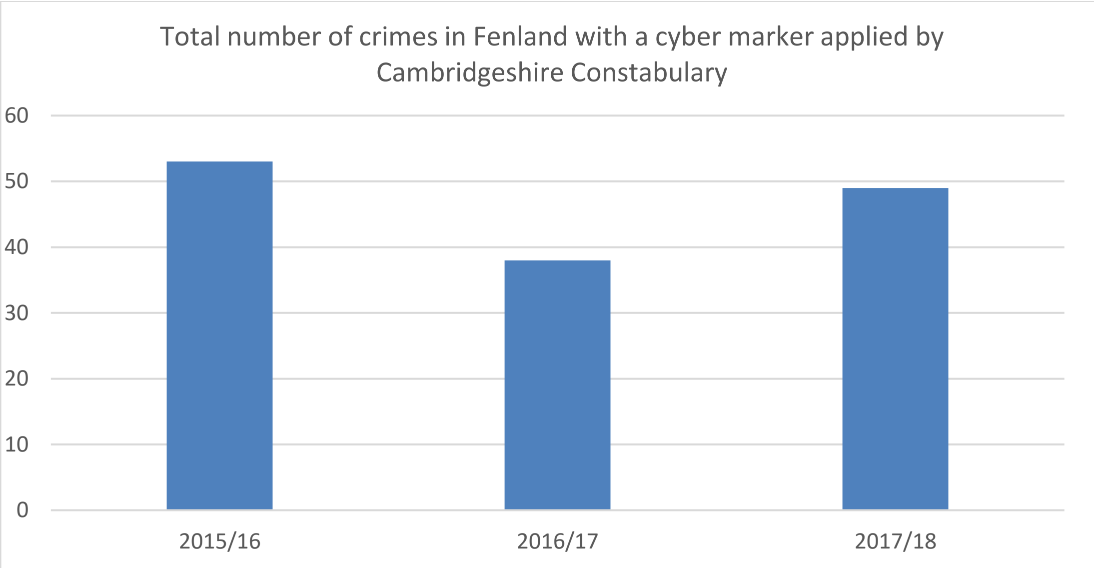
• Socially isolated individuals as they are often invisible to local services and their involvement in scams may remain hidden. Loneliness amongst those that are socially isolated may encourage someone to respond favourably to an approach from a scammer.

• Those with Dementia and cognitive impairment may lack financial literacy skills and judgement meaning that they may be targeted by scammers. Dementia causes a fluctuation of mental capacity, which can make it difficult for people to understand risk and apply caution to decision making. This makes people with dementia at increased risk of responding to a scam.

## SECTION 4: CYBERCRIME IN FENLAND

Between March 2017 and April 2018, there were 490 police recorded crimes with a cyber-marker applied across the Cambridgeshire and Peterborough force-wide area including 49 crimes in Fenland specifically.  The 2017/18 total in Fenland was a 28.9% increase on 2016/17 (38). It should be noted though that not all cyber related crimes are recorded by Cambridgeshire Constabulary with many reports doing directly to Action Fraud.  This means that police recorded crime with an online marker applied does not give a full picture of cybercrime in Fenland alone.

Figure 4: Police recorded crimes in Fenland with a cyber marker applied, by year




Data released by Action Fraud show that 583 Fraud and Cyber-related crimes were referred to Cambridgeshire police between April 2016 and March 2017.   This made up around 0.89% of all reported fraud and cybercrime nationally.  Of these 583 referred crimes, there were 444 total outcomes with 78 judicial outcomes and 366 non-judicial outcomes.

Figure 5 below outlines all those crimes recorded by Cambridgeshire Constabulary with a cyber marker applied in Fenland. This does not paint a full picture of cybercrime as a whole, as most cyber-related crime (particularly fraud) are reported directly to Action Fraud. It does though, give some indication into the variety of cyber-enabled crimes across the district over the past three years and highlights the links between individual's online presence and traditional crime types.

Figure 5: A breakdown of all crimes with an on-line crime marker in Fenland, 2015-2018

| Crime Type | Count |
|---|---|
| HARASSMENT | 82 |
| OBSCENE PUBLICATIONS, ETC. AND PROTECTED SEXUAL MATERIAL | 45 |
| SEXUAL GROOMING | 30 |
| MALICIOUS COMMUNICATIONS | 27 |
| BLACKMAIL | 23 |
| SEXUAL ACTIVITY INVOLVING A CHILD UNDER 13 | 20 |
| SEXUAL ACTIVITY INVOLVING A CHILD UNDER 16 | 15 |
| OTHER OFFENCES AGAINST THE STATE & PUBLIC ORDER | 12 |
| OTHER THEFT | 5 |
| ABUSE OF CHILDREN THROUGH PROSTITUTION & PORNOGRAPHY | <5 |
| COMMON ASSAULT | <5 |
| EXPOSURE AND VOYEURISM | <5 |
| OTHER CRIMINAL DAMAGE | <5 |
| OTHER NOTIFIABLE OFFENCES | <5 |
| PUBLIC FEAR, ALARM OR DISTRESS | <5 |
| RACIALLY OR RELIGIOUSLY AGGRAVATED HARASSMENT | <5 |
| RACIALLY OR RELIGIOUSLY AGGRAVATED PUBLIC FEAR, ALARM OR DISTRESS | <5 |
| THEFT FROM A SHOP | <5 |
| THEFT IN A DWELLING OTHER THAN FROM AN AUTOMATIC MACHINE OR METER | <5 |
| THREAT OR POSSESSION WITH INTENT TO COMMIT CRIMINAL DAMAGE | <5 |

Unfortunately, data from action fraud at a district level, to best understand levels in Fenland was not received for the purposes of this report.  As cybercrime knows through geographical barriers though it is expected that the scale and level of harm within the district will be in line with national and county wide statistics.

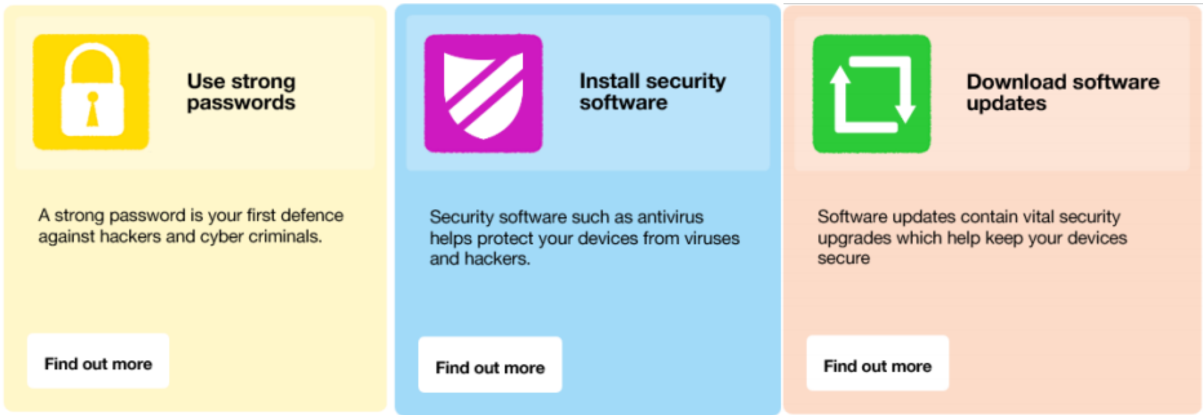
## SECTION 5: TACKLING CYBERCRIME

As this report has identified, the partnership should look to enable everybody to protect themselves against cybercrime. The key message that Cambridgeshire Constabulary give to individuals and business is that we should:

- **Engage in cultural change- modify the way that we behave and interact online and put cyber security at the heart of all activity.**
- **Accept that it is 'when' not 'if'**
- **Cyber and Information Security- not always about technology**
- **Most offences are preventable with very simple steps**
- **Use work practice at home**

### EDUCATION AND AWARENESS

With the suggestion that up to most cybercrimes could be avoidable if appropriate steps were taken to avoid them, the Partnership should look to actively promote exactly what the types of steps that people should be taking are. For a start, three simple steps suggested by cyber aware are use strong passwords, install appropriate security software and always download software updates.




Courtesy of www.cyberaware.com

There are a number of national organisations set up to offer information, advice and guidance on how to stay safe online. It is important that the partnership look to promote these key messages locally.

**Get Safe Online-** Get Safe Online is a website set up to provide advice and guidance to individual in an easy to understand way. It provides practical advice across a range of topics under the cybercrime umbrella and it is recommended that the Partnership promote these messages through appropriate channels, including social media and amongst staff members.

**Take 5 Campaign-** Campaign to raise fraud awareness: https://takefive-stopfraud.org.uk/

**Cyber Aware-** Cyber Aware (formerly Cyber Streetwise) aims to drive behaviour change amongst small businesses and individuals, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals: install the latest software and app updates and use a strong, separate password for your email. This is based on expert advice from the National Cyber Security Centre, a part of GCHQ. The Partnership should ensure that local business are receiving this advice and guidance: https://www.cyberaware.gov.uk/

**Cyber Essentials-** Cyber Essentials is a Government backed scheme that will help individuals protect their organisation, whatever its size, against a whole range of the most common cyber-attacks. It offers advice and guidance but also the opportunity to gain certification in cyber awareness: https://www.cyberessentials.ncsc.gov.uk/

**Age UK-** Age UK provide tailored advice and guidance on staying safe online for the elderly: https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/

**NSPCC-** NSPCC provide tailored advice and guidance to children and young people for staying safe online: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

As mentioned, around 62% of reports to Action Fraud between October 2017 and March 2018 were from businesses and 39% from individuals. In order to tackle cybercrime against businesses, Fenland for Business, the economic arm of Fenland District Council, organised an event in Chatteris in December 2017 designed to help local businesses understand cybercrime and internet security

## PARTNERSHIP WORKING AND BUILDING ON EXISTING NETWORKS

Alongside national campaigns and guidance, the partnership can also draw of locally tailored information, guidance and expertise to deliver key messages around cyber safety locally.

### LITTLE BOOK OF CYBER SCAMS

Similar to the Little Book of Big Scams, the Eastern Region Special Operations Unit- covering Bedfordshire, Cambridgeshire, Essex, Hertfordshire, Kent, Norfolk and Suffolk have released the Little Book of Cyber Scams. The aim of this booklet is to increase awareness of different types of cyber scams and whilst the document is largely targeted at Small to Medium Size business, much of advice is relevant to all. Similarly, the guide includes advice and guidance to individuals and businesses on how to report should they be a victim of a cybercrime. It is key that the partnership promote these messages in order to address concern that cybercrime in underreported locally.

### SILVER MONDAYS

In 2017/18, the Partnership commissioned the County Council Community Protection team to deliver initiatives to build community resilience and protect the vulnerable against the financial and emotional harm caused by scams and rogue trading. This work is very closely linked to cyber-crime, particularly online fraud and emerging crimes such as online dating scams

### TEA AND TABLET SESSIONS

Cambridgeshire Libraries Service run monthly ‘Tea and Tablets’ sessions which is digital learning programme run in lots of libraries across the county and by Library staff. These sessions are generally aimed at older people in the community who are just learning to use their iPads or tablets, or want to get the best out of them, or just want a social group to network with. These are informal sessions where those attending learn with and from each other and covers the basics like how to google, how to search, how to keep yourself safe online. For example, there were 23 recorded sessions in Wisbech library between 2016 and 2017, with 213 people attending. The lead officer for these sessions has always included information about cybercrime and staying safe online. It is recommended that the partnership look to promote awareness and support the delivery of these messages.

## CYBER AMBASSADORS

Cambridgeshire Constabulary are seeking representatives from community groups and institutions from Cambridgeshire and Peterborough to become Community Cyber Ambassadors. Ambassadors will raise awareness within a community group or institution around the different types of cybercrime and assist in promoting prevention advice to your local area. Ambassadors are not expected to have an in depth knowledge of technology but an interest in learning more about cybercrime and an enthusiasm to promote the latest cyber prevention advice within your community group is essential. Cyber Ambassadors are asked to commit to delivering a minimum of two awareness events a year to their community group to help Cambridgeshire Constabulary to increase awareness around the county. This could be something as small as a coffee morning or arranging an awareness day within the community.

It is recommended that the partnership support this scheme by trying to identify potential groups across Fenland that may be interested in supporting this scheme.

## RAISING AWARENESS AMONGST PARTNERSHIP

As mentioned, there is national concern around general awareness of cybercrime. Whilst there are a number of information channels that can help the partnership to deliver messages to different audiences, it is also important that the partnership explores local resource to disseminate the latest information. For example, Cambridgeshire Constabulary has a Fraud and Cyber Security Advisor within the Specialist Crime Unit that can help to promote these messages.

It is recommended that the partnership explores opportunities to work with this advisor and draw on their knowledge of cybercrime to deliver targeted messages, in the most efficient and appropriate way. One possible way of doing this could be to arrange an event where partners and staff are invited to an event where the advisor delivers messages to raise awareness within partner organisations.

## WORKING WITH SCHOOLS

As mentioned, there is a growing threat of cyber-related crime amongst children and young people and key awareness and messaging is available through channels such as the NSPCC which could be promoted in partnership with schools.

## FENLAND COMMUNITY SURVEY

Each quarterly strategic assessment will contain a short summary of the key findings of the Fenland Community Safety survey. Surveys have been completed as part of the community engagement process and they are also available to complete through the internet via http://www.fenland.gov.uk/CSPsurvey . As is common for a community survey, responses mostly reflect low level but visible issues for community members, rather than the highest risk or harm issues. It is the role of the detailed strategic assessments to identify those crimes that can be hidden from the community or highest risk.

***Figures in brackets are from the previous survey April to June 2018.***

Over the period July to September 2018, 528 (490) responses were recorded. Responses can be broken down by geographical areas as: Chatteris 183 (126), March 122 (113), Whittlesey 105 (128) and Wisbech 118 (123). The majority of those surveyed were between the ages of 36 and 65. The volume of responses is low in terms of statistical reliance for the whole of the Fenland district but it can be used as an indicator for emerging issues.

When asked if they had been directly affected by ASB/Crime in the past three months, speeding/anti-social driving was again the highest profile issue across the district. Dog fouling and parking were highlighted issues in Chatteris, March and Whittlesey. Wisbech identified fly tipping as their 2nd issue with dog fouling, parking and street drinking all highlighted issues. March returned the highest 'no issues' at 32%(22%). Chatteris 18%(24%) and Whittlesey 15%(21%) saw fewer responses indicating no issues than the previous 2 surveys. Wisbech saw a positive increase with 15% (10%) indicating no issues.

When asked if their family had been adversely affected by ASB/crime the highest issues are broken down in table 1 below.

**Table 1: Has your family been adversely affected by ASB/crime? Fenland Community Survey (July to September)**

| Has your family been adversely affected by ASB/crime | | | |
|---|---|---|---|
| | 1st | 2nd | 3rd |
| Chatteris | Speed/ASB Drive | Parking | Dog Fouling |
| March | Speed/ASB Drive | Parking | Fly Tipping/Litter |
| Whittlesey | Parking | Speed/ASB Drive | Dog Fouling |
| Wisbech | Speed/ASB Drive | Street Drinking | Fly Tipping/Litter |

The following two tables provide a snap shot of how safe people feel and their perception of crime/ASB in their locality.

**Table 2: How safe do you feel where you live? Fenland Community Survey (July to September)**

| How safe do you feel where you live? | | | | |
|---|---|---|---|---|
| | Very Safe | Safe | Unsafe | Very Unsafe |
| Chatteris | 12%(12) | 71%(62) | 15%(26) | 2%(0) |
| March | 14%(23) | 71%(73) | 12%(5) | 3%(0) |
| Whittlesey | 5%(10) | 66%(74) | 28%(15) | 1%(2) |
| Wisbech | 8%(9) | 62%(67) | 27%(19) | 2%(5) |

**Table 3: Is there a problem with Crime and ASB where you live?,Fenland Community Survey (July to September 2018)**

| Is there a problem with Crime & ASB where you live? | | | | |
|---|---|---|---|---|
| | Not at all | Not much | Quite a problem | Big problem |
| Chatteris | 23%(36) | 51%(38) | 23%(24) | 4%(2) |
| March | 22%(40) | 56%(52) | 20%(8) | 2%(0) |
| Whittlesey | 22%(37) | 37%(48) | 30%(13) | 10%(2) |
| Wisbech | 14%(18) | 55%(54) | 19%(21) | 12%(7) |

*Please note: Figures do not add to 100% as some respondents skipped the questions*

***What should the CSP focus on?***

Across the district the issue the community felt the partnership should focus on was speeding/anti-social driving. This was the highest return for each area with an average of 36% (39%) across the four geographical areas. The partnership received a detailed strategic assessment on anti-social driving during 2017/18 and took specific recommendations to forward into the partnership's action plan.

Chatteris, March and Whittlesey indicated burglary/theft as their second priority with Wisbech selecting this as their third. Street Drinking was the second priority for Wisbech. The partnership are due to receive a strategic assessment in quarter 3 this year on alcohol and substance misuse, based on the findings of the 2017/18 end of year assessment and this will also offer a review of street drinking in the district, including within Wisbech. Drugs and substance abuse was the third priority for Chatteris and March.

## APPENDIX A


Action Fraud, What is Fraud and Cybercrime, https://www.actionfraud.police.uk/what-is-fraud

Action Fraud, Cambridgeshire Cyber Profile, https://www.actionfraud.police.uk/sites/default/files/Cambridgeshire%20-%20Cyber.pdf

Age UK, Only the tip of the iceberg, https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf

Age UK, Information and Advice, https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/

Cambridgeshire County Council, Little Book of Big Scams , https://ccc-live.storage.googleapis.com/upload/www.cambridgeshire.gov.uk/residents/consumer-protection/CCC_LBOBS_Third%20Edition_ONLINE.pdf?inline=true

Cambridgeshire Health Related Behaviour Survey Survey, 2016

Cambridgeshire Research Group, Fenland Q1 Strategic Assessment 2017/18, Scams, https://cambridgeshireinsight.org.uk/wp-

Cyber Essentials, https://www.cyberessentials.ncsc.gov.uk/

National Crime Agency (NCA), Emerging Threat in Online Dating, http://www.nationalcrimeagency.gov.uk/publications/670-emerging-new-threat-in-online-dating-initial-trends-in-internet-dating-initiated-serious-sexual-assaults/file

NSPCC, Online Safety, https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Take Five Campaign, https://takefive-stopfraud.org.uk/

ONS, Overview of fraud and computer misuse statistics for England and Wales, ONS, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25

Get Safe Online, Protect Yourself, https://www.getsafeonline.org/protecting-yourself/

Bedfordshire Police, What is cybercrime?

,