Devon & Cornwall Police

Produced in Partnership with:

Safer Devon, Safer Cornwall, Safer Plymouth and Safer Communities Torbay

Serious and Organised Crime Local Profile

- Cyber Crime, Fraud and Counterfeit Goods -

2017 Update

Authorising Officer:	**T/ACC Jim Colwell**
Lead Author:	**Ruth Bailey, Strategic Analyst**
	Performance & Analysis Department
	With additional input from key stakeholders across the Peninsula

This profile has been written to inform and educate the Police and Partner Agencies only. Information within these profiles can be shared with individuals and organisations sitting as part of OCLP panels, co-ordinated by the Community Safety Partnership, or as part of CSEA groups or Safeguarding Boards. It is **not** to be shared externally with members of the general public or the press/ media. Please contact the authors at **strategicanalysisteam@devonandcornwall.pnn.police.uk** if you have any queries.

Contents

Section 1: National Updates and Reports

Section 2: Peninsula Overview of the Data

Section 3: Local Updates

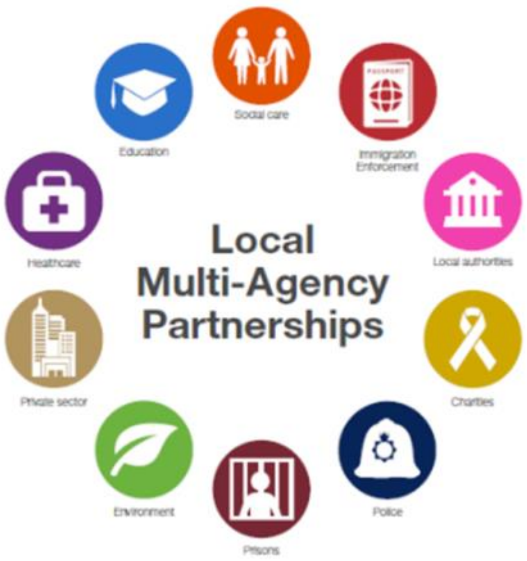
Section 4: Summary and Recommendations

Introduction

In November 2014, the Home Office published guidance on their expectation that every Police force in England and Wales would lead the production of an annual **Serious and Organised Crime Local Profile** in collaboration with **local multi-agency partnerships**. The aims of the local profile are to:

- Develop a common understanding among local partners of the threats, vulnerabilities and risks relating to serious and organised crime;
- Provide information on which to base local programmes and action plans;
- Support the mainstreaming of serious and organised crime activity into day-to-day policing, local government and partnership work; and
- Allow a targeted and proportionate use of resources.

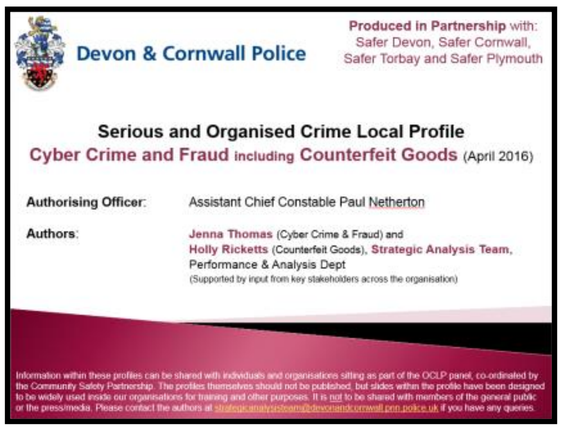
The profile was expected to address the Serious and Organised Crime topics of: Modern Slavery, Human Trafficking, Child Sexual Abuse and Exploitation, Cyber Crime, Serious Fraud, Counterfeit Goods, Organised Acquisitive Crime, Trafficking of Drugs, Trafficking of Firearms and Organised Immigration Crime.



Devon and Cornwall Police took this request seriously and decided, in consultation with partners, to produce a series of **thematic** local profiles, that would provide sufficient information and detail to achieve the above aims. The first profile to cover **Cyber Crime, Fraud and Counterfeit Goods** was written in 2015/16 and published in April 2016.

This first profile provided detailed **definitions** and **explanations** of the different types of cyber crime and fraud. If readers of the 2017 Update are unfamiliar with any of the terms used, then they should refer back to the 2016 document for further explanation.

The first profile covered **cyber enabled crime** as well as cyber dependent crime. It identified that while most crime types can be cyber-enabled, the most serious impact of this is seen in the facilitation of **sexual offences**, and that this is of greatest concern when this impacts on **children** and **young people**. As this is a topic explored in some depth in the **Child Sexual Exploitation and Abuse SOCLP**, the decision was made to focus the 2017 Update on **cyber dependent** crime alone.



Devon & Cornwall Police

Produced in Partnership with:
Safer Devon, Safer Cornwall,
Safer Torbay and Safer Plymouth

Serious and Organised Crime Local Profile
Cyber Crime and Fraud including **Counterfeit Goods** (April 2016)

Authorising Officer: Assistant Chief Constable Paul Netherton

Authors: **Jenna Thomas** (Cyber Crime & Fraud) and **Holly Ricketts** (Counterfeit Goods), **Strategic Analysis Team,** Performance & Analysis Dept
(Supported by input from key stakeholders across the organisation)

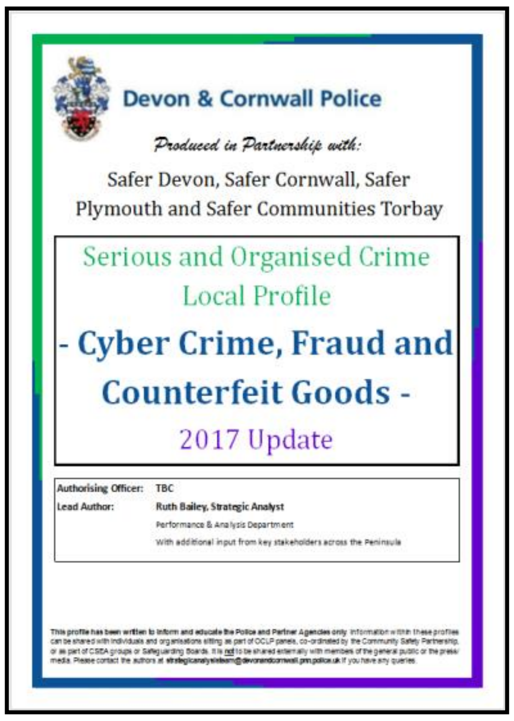
Information within these profiles can be shared with individuals and organisations sitting as part of the OCLP panel, co-ordinated by the Community Safety Partnership. The profiles themselves should not be published, but slides within the profile have been designed to be widely used inside our organisations for training and other purposes. It is not to be shared with members of the general public or the press/media. Please contact the authors at strategicanalysisteam@devonandcornwall.pnn.police.uk if you have any queries.

The first profile also contained many **case studies** demonstrating the impact of cyber crime and fraud on businesses and **vulnerable people**, particularly the **elderly**.

The 2017 Update provides a fresh analysis of Action Fraud data to examine whether there has been any change in the **key demographics** being affected by the different types of cyber crime and fraud in Devon and Cornwall. It also provides a greater focus on the impact of these crime types on **businesses** by breaking down the data down into crimes affecting individuals versus crimes affecting businesses.

The **key messages** are very similar to the first profile: there are different crime types that affect three different audiences (younger people, older people and businesses), therefore **awareness-raising** needs to be **targeted** accordingly. **Large sums of money** are being lost across the two counties, which can have a devastating impact on the business or individual concerned.

However, these crimes are **preventable**. Throughout the document, relevant **resources** are highlighted where appropriate **advice**, **guidance** and **support** can be accessed. **All of our partners** can help the Police to **prevent** cyber crimes and frauds from occurring, by finding **new** and **innovative ways** of ensuring that these resources are accessed and used by the relevant audiences.



Devon & Cornwall Police

Produced in Partnership with:

Safer Devon, Safer Cornwall, Safer
Plymouth and Safer Communities Torbay

Serious and Organised Crime
Local Profile
- Cyber Crime, Fraud and
Counterfeit Goods -
2017 Update

Authorising Officer: TBC
Lead Author: **Ruth Bailey, Strategic Analyst**
Performance & Analysis Department
With additional input from key stakeholders across the Peninsula

This profile has been written to inform and educate the Police and Partner Agencies only. Information within these profiles can be shared with individuals and organisations sitting as part of OCLP panels, co-ordinated by the Community Safety Partnership, or as part of CSEA groups or Safeguarding Boards. It is not to be shared externally with members of the general public or the press/media. Please contact the authors at **strategicanalysisteam@devonandcornwall.pnn.police.uk** if you have any queries.

As a starting point, **Devon and Cornwall Police's own website** has a page with resources and advice on online safety and fraud for individuals and businesses, with links to further resources: **https://www.devon-cornwall.police.uk/advice/your-internet-safety/**

Finally, there are a number of other ways in which **partner agencies** can support Devon and Cornwall Police in tackling cyber crime and fraud:

- Have an **identified cyber/fraud lead** who can represent the agency at a **strategic** level;
- Participate in an agreed single process for the **collection** and **sharing** of **intelligence**;
- Work together to **safeguard potential victims** and to give them the **information** and **skills** they need to better **protect** themselves;
- Frontline staff who regularly engage with vulnerable people can **raise awareness** with them about how frauds work, how they draw people in and the risks of engaging in this, as well as what they should do if they are approached in this way, i.e. **who** to **report** to and **how**.

NATIONAL UPDATE: CYBER

Headlines from the National Cyber Security Strategy 2016-21 and the NCA's Cyber Crime Assessment 2016

Since the last National Cyber Security Strategy was published in 2011, the scale and impact of technological change has accelerated. New technologies and applications have come to the fore, and there has been greater uptake of internet-based technologies worldwide, particularly in developing countries. These developments have significant advantages but as our reliance on networks grows, so do the opportunities for those who seek to compromise our systems and data. Malicious cyber activity knows no international boundaries. State actors are experimenting with offensive cyber capabilities, with a principal focus on the government, defence, finance, energy and telecommunications sectors. Cyber criminals are broadening their efforts and expanding their strategic modus operandi to achieve higher value pay-outs. Terrorists, and their sympathisers, are conducting low-level attacks and aspire to carry out more significant acts (HM Government).

> Our vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world. The National Cyber Security Strategy highlights the Government's drive to ensure that businesses, government and citizens are protected from cyber based threats, with £1.9bn investment being made.

The accelerating pace of technology and criminal cyber capability currently outpaces the UK's collective response to cyber crime. Technological advances, including the widespread use of anonymisation tools, and constantly improving criminal operating methods have made many corporate cyber security tools and basic procedures insufficient to protect corporate networks. The growing online criminal marketplace provides easy access to sophisticated and bespoke tools and expertise, allowing less skilled cyber criminals to exploit a wide range of vulnerabilities. This 'cyber arms race' is likely to be an enduring challenge, and an effective response requires collaborative action from government, law enforcement, industry regulators and, critically, business leaders (NCA, 2016).

> The NCA estimates that the cost of cyber crime to the UK economy is billions of pounds per annum – and growing.

Cyber criminals targeting the UK include international serious organised crime groups as well as smaller-scale, mostly domestic, criminals and hacktivists. The NCA assesses that the most advanced and serious cybercrime threat to the UK is the result of activity by a few hundred international cyber criminals, typically operating in organised groups, who target UK businesses to commit highly profitable malware-facilitated fraud (NCA, 2016). Much of the most serious cyber crime (mainly fraud, theft and extortion) against the UK continues to be perpetrated predominantly by financially motivated, Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, with emerging threats from South Asia and West Africa of increasing concern, and from inside the UK itself. These OCGs are principally responsible for developing and deploying the malware that infects the computers and networks of UK citizens, industry and government. These attacks are becoming increasingly advanced, aggressive and confrontational, as illustrated by the increasing use of ransomware and threats of distributed denial of service (DDoS) for extortion. It is often difficult for the UK and international law enforcement agencies to prosecute key individuals when they are located in jurisdictions with limited, or no, extradition arrangements (HM Government, 2016).

UK businesses, particularly in the financial sector, are also increasingly exploited and used as a vehicle to cash-out the proceeds of cyber crime committed in the UK and internationally (NCA, 2016).

Assessing the future threat: Cyber Terrorism

The current technical capability of terrorists is judged to be low, nonetheless, the impact against the UK to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are 'leaked' online) enable terrorist groups and their supporters to attract media attention and intimidate their victims.

As an increasingly computer-literate generation engages in extremism, we envisage a greater volume of low-sophistication disruptive activity. The potential will increase for a number of skilled extremist lone actors to emerge, as will the risk that a terrorist group will seek to enlist an established insider. Even a moderate increase in capability may constitute a significant threat to the UK.

Also of concern is the continuing threat from acts of less sophisticated but more widespread cyber crimes carried out against individuals or smaller organisations.

'Script kiddies' are less skilled individuals who use scripts or programmes developed by others to conduct cyber attacks. They have access to hacking guides, resources and tools on the Internet and their actions can have a disproportionately damaging impact on an affected organisation, due to the vulnerabilities found in commonly used systems.

https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Examples of Major Cyber Dependent Attacks

TalkTalk Compromise

In October 2015, UK telecommunications provider TalkTalk reported a successful cyber attack and a possible breach of customer data.

Subsequent investigation determined that a database containing customer details had been accessed via public-facing internet servers, with the records of approximately 157,000 customers at risk, including names, addresses and bank account details.

On the same day, several TalkTalk employees received an email with a ransom demand for payment in Bitcoins. The attackers detailed the structure of the database as apparent proof that it had been accessed.

TalkTalk's report of the breach helped the police, supported by specialists at the National Crime Agency, to arrest the main suspects, all based in the UK, in October and November 2015.

Lessons Learned:

This attack demonstrated that, even within large cyber-aware organisations, vulnerabilities can persist. Their exploitation can have a disproportionate effect in terms of reputational damage and operational disruption, and this incident generated substantial media attention.

The incident cost TalkTalk an estimated £60m and the loss of 95,000 customers, as well as a sharp drop in their share price.

However, TalkTalk's rapid reporting of the breach enabled law enforcement to respond in a timely manner, and both the public and government to mitigate the potential loss of sensitive data.

(HM Government, 2016).

Ukraine Power Grid Attack

A cyber attack on western Ukrainian electricity distribution companies Prykarpattya Oblenergo and Kyiv Oblenergo in December 2015 caused a major power outage, with disruption to over 50 substations on the distribution networks. The region reportedly experienced a blackout for several hours and many other customers and areas sustained lesser disruptions to their power supplies, affecting more than 220,000 consumers.

Use of the BlackEnergy3 malware has been blamed by some for the attack, after samples were identified on the network. At least six months before the attack, attackers had sent phishing emails to the offices of power utility companies in the Ukraine containing malicious Microsoft Office documents. However, the malware was not likely to have been responsible for opening the circuit breakers which resulted in the outage. It is probable that the malware enabled the attackers to gather credentials that allowed them to gain direct remote control of aspects of the network, which would subsequently enable them to trigger the outage.

Lessons Learned:

This Ukraine incident is the first confirmed instance of a disruptive cyber attack on an electricity network. Instances such as this further demonstrate the need for good cyber security practices across all of our Critical National Infrastructure (CNI) to prevent similar incidents occurring in the UK.

(HM Government, 2016).

WannaCry and the Impact on the NHS

On Friday 12 May 2017 a global ransomware attack, known as WannaCry, affected more than 200,000 computers in at least 100 countries. In the UK the attack particularly affected the NHS, although it was not the specific target. At 4pm on 12 May, NHS England declared the cyber attack a major incident and implemented its emergency arrangements to maintain health and patient care. On the evening of 12 May, a cyber-security researcher activated a kill-switch so that WannaCry stopped locking devices.

According to NHS England, the WannaCry ransomware affected at least 81 of the 236 trusts across England, because they were either affected by the ransomware or turned off their devices or systems as a precaution. A further 603 primary care and other NHS organisations were also infected, including 595 GP practices. As a result, 6,912 appointments were cancelled.

Operation Cunan was the national response to the attack. The South West Regional Cyber Crime Unit were then responsible for obtaining evidence from Plymouth NHS Hospitals Trust (Derriford Hospital) who were infected in the attack.

Lessons Learned:

The NHS had been warned it was vulnerable to this type of attack a year earlier. They had a plan in place but had not tested the plan at a local level. As a result, it was not immediately clear who should lead the response and there were problems with communication.

All organisations infected by WannaCry shared the same vulnerability and could have taken relatively simple action to protect themselves.

All organisations, boards and their staff should be taking the cyber threat seriously, understanding the direct risks to front-line services and should be working proactively to maximise their resilience and minimise the impacts on the public/customers.

(National Audit Office, 2017)

Emerging Threat

Spectre Vulnerability

This affects modern microprocessors that perform branch prediction. On most processors, the speculative execution resulting from a branch misprediction may leave observable side effects that may reveal private data to attackers. For example, if the pattern of memory accesses performed by such speculative execution depends on private data, the resulting state of the data cache constitutes a side channel through which an attacker may be able to extract information about the private data using a timing attack.

What does this mean?

This lets attackers access protected information in your device's memory, potentially revealing sensitive details like passwords, cryptographic keys, personal photos and emails etc. Fortunately, CPU and operating system vendors have responded quickly and pushed out patches to protect user's devices. Unfortunately these patches are in some cases causing system errors, and in other cases are significantly slowing down processing speed. People are recommended to update software as recommended by their provider, to update their browser to protect against Spectre and to keep their antivirus active.

FOCUS ON BUSINESS

Businesses and organisations, both public and private sector, hold personal data, provide services, and operate systems in the digital domain. With this technological transformation comes the responsibility to safeguard the assets they hold, maintain the services they provide, and incorporate the appropriate level of security into the products they sell. Consumers expect businesses and organisations to take all reasonable steps to protect their personal data and build resilience into the systems and structures on which they depend (HM Government, 2016).

The long-term impact of a cyber attack could include substantial loss of revenue, valuable data and other company assets. The impact of litigation costs and potential fines, the loss of confidence from reputational damage and possible executive-level dismissals could also result in immediate loss of shareholder value. Data breaches are among the most common cyber crimes committed against businesses. Almost all large companies and a substantial majority of smaller companies have experienced a data breach (NCA, 2016).

Cyber attacks are often the result of exploited, but preventable, vulnerabilities.

Many organisations continue to use vulnerable systems. Software on these systems will often rely on older, unpatched versions. These older versions often suffer from vulnerabilities that attackers look for and have the tools to exploit. An additional issue is the use by some organisations of unsupported software, for which patching regimes do not exist. Only by sufficient investment in people, technology and governance, will businesses reduce their exposure to potential cyber harm. Businesses and organisations must also understand that, if they are the victim of a cyber attack, they are liable for the consequences (HM Government, 2016).

Meanwhile, cyber-enabled fraud (most commonly targeting retail customers) is a rising cost for banks, retailers and other businesses (NCA, 2016).

We lack the skills and knowledge to meet our cyber security needs across both the public and private sector (HM Government, 2016). Although general cyber awareness is improving in the UK, as a result of significant investment in education and training by government, policing, retail financial institutions and others, private individuals are typically even less aware of malware infections on their home computers and other devices than corporate victims. Private individuals who are infected can be a major source of infection and vulnerability for many businesses – for example, when their infected computers are used by cyber criminals as part of a botnet to deliver further malware to businesses and other individuals.

Many businesses and most of the public are unsure about how best to protect against it and how to report it when it happens. In many instances, victims may not even be aware that it has taken place. This is a long-term education and training challenge that government and some businesses have recognised, and sustained efforts will be required to deliver the required change. (NCA, 2016).

The Threat from Insiders

In businesses, many staff are not cyber security aware and do not understand their responsibilities in this regard. Of concern are those insiders who **accidentally** cause harm through inadvertently clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data means their actions can cause just as much damage as a malicious insider.

23% of people who receive phishing emails will open them (NFIB, 2017).

Malicious insiders are trusted employees of an organisation, who have access to critical systems and data, and pose the greatest threat. They can cause financial and reputational damage through theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their access to facilitate or launch an attack to disrupt or degrade critical services on their organisation's network, or wipe data from the network.

A robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workforce and industrial and other forms of espionage, is key in a comprehensive approach to security (HM Government, 2016).

Directors of businesses should challenge their business management teams to go beyond compliance with minimum cyber security standards to ensure that rapidly evolving cyber security and resilience challenges are addressed and the threat to the UK is reduced (NCA, 2016).

Under-reporting continues to obscure the full impact of cyber crime on the UK. New estimates from the CSEW (next page) highlight the shortfall in established reporting, with only 16,349 cyber-dependent incidents reported to Action Fraud in a year. This limits the ability to develop effective responses.

Directors of businesses have an important role in addressing this under-reporting. The NCA has urged businesses to report when they are victims of cyber crime and to share more intelligence, both with law enforcement and each other (NCA, 2016).

'*Last year, the average cost of breaches to large businesses was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme*' *(2016 Government Cyber Health Check and Cyber Security Breaches Survey, HM Government, 2016).*

Resource

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The **Guide to the General Data Protection Regulation (GDPR)** explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection. Alongside the guide there are also a number of other tools to help organisations to prepare for the GDPR.

The GDPR introduces an obligation for companies to report any **breaches** of **personal data** held. This could result in an **increase** in cyber crimes reported.

CRIME SURVEY FOR ENGLAND AND WALES

(ONS, 2017)

In order to incorporate fraud and computer misuse and cybercrime figures into the CSEW, new questions were added to the survey from October 2015 for inclusion in the second half of the survey year. Sufficient data was gathered to produce first estimates which can be found in the Experimental Statistics July 2016 (2017 statistics have not yet been published). NB. The CSEW is a household survey and therefore results do not capture fraud against businesses.

Annual Estimates:

5.6m → **2 in 3 Fraud**

Fraud + Computer Misuse incidents

Majority = bank and credit account fraud

1 in 2 Cyber

1 in 5 Victims Said they had reported the crime

Estimated Losses from Fraud:

62% → **43%** Received a full reimbursement (typically from financial provider)

Lost money or goods

Bank and credit account fraud were most likely to result in an initial loss to the victim (70%), but were also most likely to result in a full reimbursement (84%).

Victim Characteristics (Most Common):

Age group:	45-54
No. of times victimised:	Once
Household income:	£50,000+
Area:	Rural + Affluent
Occupation:	Managerial / Professional

Estimated Losses from Computer Misuse:

22% → **100%** Computer viruses

Lost money or goods

Research by the City of London Corporation found that cyber-enabled frauds typically involved a greater financial loss than cyber-dependent frauds (CoLC, 2015).

Offence Types

- **Bank and credit industry fraud** made up **over 40%** of total incidents in the CSEW experimental data, compared with around 10% of total Action Fraud offences, indicating that this is an **underreported** area.
- **18%** of incidents identified by the CSEW were **non-investment** frauds, compared with **42%** of Action Fraud data, indicating that this is an offence which people are more comfortable reporting and vice-versa that **investment frauds** are **underreported**.
- Similarly 15% of Action Fraud offences were **Advance Fee** frauds, compared with just 2% of CSEW incidents.

The Total Cost of Fraud: Annual Estimates

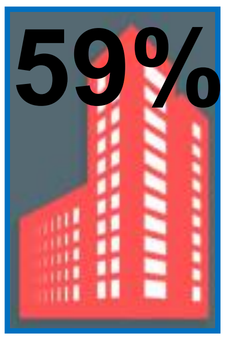
(Experian et al., 2017)

Annual UK fraud losses	£190 billion
Private sector fraud losses	£140 billion
Public sector fraud losses	£40.4 billion
Charities & charitable trusts	£2.3 billion
Losses to individuals	£6.8 billion

NATIONAL UPDATE: FRAUD

(NFIB, 2017)

From April 2016 - March 2017, there were **674,144 frauds** reported to the National Fraud Intelligence Bureau via Action fraud, Financial Fraud Action UK (FFA) and Cifas, including **20,562** (3%) **cyber-dependent** offences. There has been an increase in the reporting of fraud offences to Action Fraud nationally. The growth has been particularly noticeable in the reporting of cyber-dependent offences: the latter six months of this period saw a 61% increase compared with the first six months.



59%

Crimes against **businesses** including **8.5%** of **cyber-dependent** crimes.

Despite this, offences against businesses are still thought to be largely **underreported**.

Losses

Total losses reported to Action Fraud: **£2.2bn**

Mean average loss per report: **£7,400**

(Excluding reports where there was no reported financial loss)

Judicial Outcomes

66,191 Reports were disseminated from Action Fraud to forces across the country **for enforcement**.

11% Were reported back to NFIB with **judicial outcomes**.

79% Were **Charged/Summonsed**.

Top fraud categories:

- Cheque, Plastic Card and Online Bank Accounts
- Application Fraud (excluding Mortgages)
- None of the Above
- Telecom Industry Fraud
- Online Shopping and Auctions

Top cyber-dependent crime:

- Malware Infection Reports (37%)

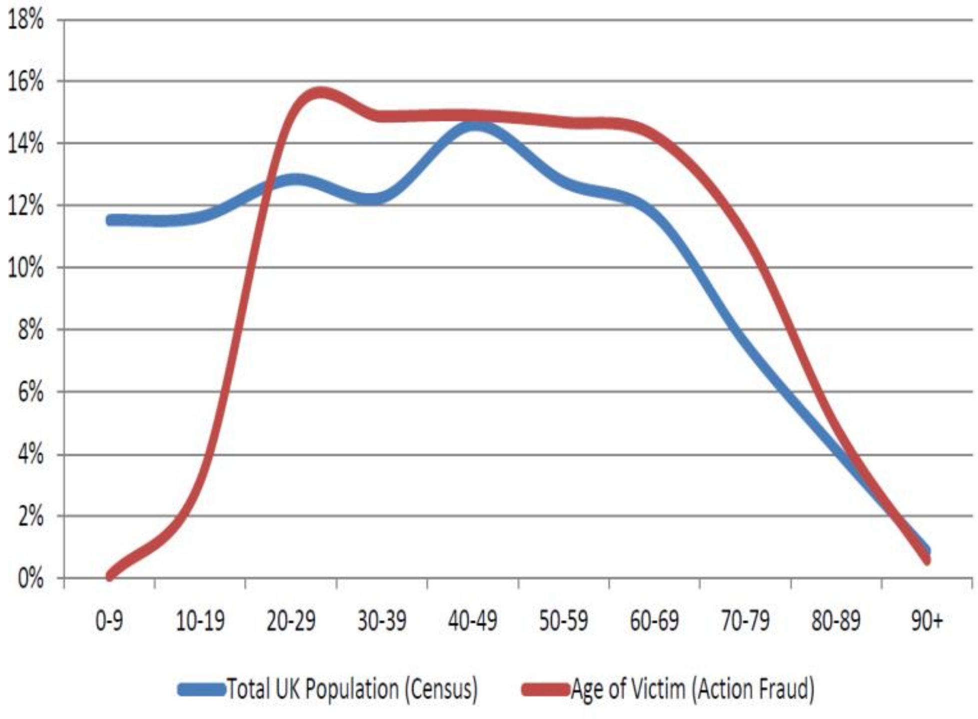
Devon and Cornwall Police show a similar pattern to the national picture of top fraud types, with the exception of **Computer Software Service Frauds** which account for a greater proportion than the national average.

Age

When seen as a percentage compared to the total population, the number of people reporting fraud tends to correspond to the distribution of age ranges of the population of the UK for all age groups 20 years old or over.

There is however a noticeable spike for Action Fraud victims aged between **20-29** when compared with the UK population; this could be due to this age group reporting higher than average Online **Shopping & Auction** frauds.

The over-representation for the **50-69** age groups is due to higher than average **Computer Software Service** fraud reporting.



IBANs

IBANs give an indication of where the victims of fraud are sending their money. *Not all countries have an IBAN code and it relates to only one method of payment exploited by fraudsters and so is only an indicator of money movement.*

These are the top 3 countries where a valid IBAN has been recorded and the percentage change when compared to the previous reporting period:

United Kingdom
= **37%** (↓ 5%)

Spain
= **12%** (↑ 4.8%)

Italy
= **6%** (↑ 2.6%)

As the National Lead Force for Fraud, City of London Police are able to offer advice and guidance to local forces investigating complex fraud.

OFFENCES AGAINST BUSINESSES

In this section, crimes which appear to have been committed against a business rather than an individual person have been separated out of the Action Fraud data, to examine which crime types are most commonly reported and which lead to the greatest financial harm.

Cyber Dependent Crimes

In 2016-17 there were 574 **cyber-dependent crimes** reported to Action Fraud, an **increase** of 17% compared to the previous financial year. Of these, 500 (88%) affected individual persons and **74** (**12%**) affected **businesses**.

Hacking: PBX/ Dial Through

16 (18%)

Hacking: Social Media and Email

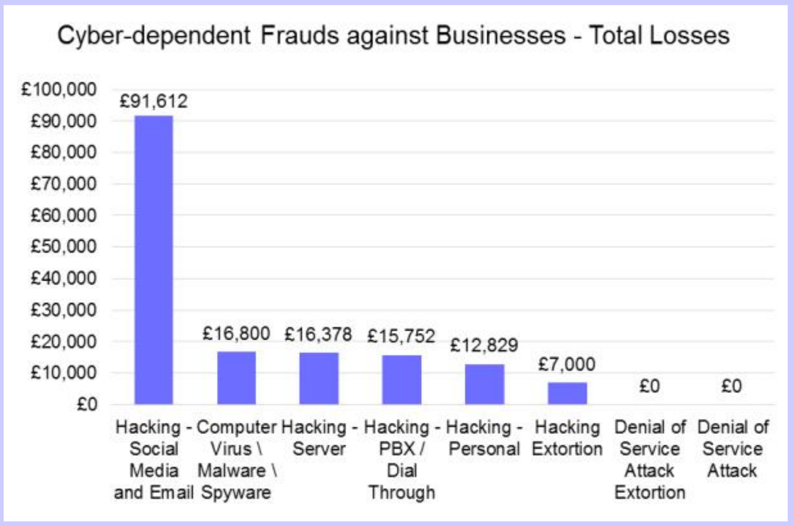
12 (16%)

Denial of Service Attack: Extortion

12 (16%)

Hacking: Server

11 (15%)



Cyber Enabled Frauds

In 2016-17 there were 5,244 **cyber-enabled frauds** reported to Action Fraud, an **increase** of 52% compared to the previous financial year. Of these, 4817 (92%) affected individual persons and **427** (**8%**) affected **businesses**.

Reported Losses:

£41,991,472

One victim reported a loss of **£40,000,000** under the category of '**Other Regulatory Fraud'** - the victim claimed that lands had been fraudulently signed over to another company.

The rest of the frauds amount to almost **£2,000,000**. Unhelpfully, the most common category was 'None of the Above' (28%), where losses amounted to over £870,000. It is likely that many of these offences were misclassified by the person reporting to Action Fraud. The next largest loss came from **'Mandate Frauds'** which were 16% of reported offences and accounted for over **£570,000** of loss, followed by **'Business Trading Fraud'** which was only 1.2% of reports but led to over **£357,000** of loss.

Traditional Frauds

In 2016-17 there were 478 **non-cyber frauds** reported to Action Fraud, a **decrease** of 12% compared to the previous financial year. Of these, 291 (61%) affected individual persons and **187** (**39%**) affected **businesses**.

Most Commonly Reported:

Retail Fraud (61%)

Reported Losses:

£113,868

(Commonly theft of petrol from fuel stations)

Most Financial Loss:

Corporate Employee Fraud (12%)

Reported Losses:

£5,207,754

Other High Loss:

Fraud by Abuse of Position of Trust (7%)

Reported Losses:

£247,780

Bitcoin

Cyber offences often involve a **ransom** demanded in Bitcoin with victims directed to addresses within the **dark web** to pay the ransom. The value of one bitcoin can vary massively. For example, in December 2016 it was valued at approximately

1 BC = £566

but by December 2017 it reached a peak of

1 BC = £15,000

before then taking a downturn and starting to decrease in value again. **Note**: Bitcoin is just one type of digital coin. Other popular cryptocurrencies include Litecoin, Ethereum, Zcash, Dash, Ripple and Monero.

Under-reporting

It is believed that many businesses take the approach that if they're able to recover their information or money, then they won't report the offence to the police or Action Fraud.

The problem with this is that law enforcement then lacks the **information** it needs to be able to effectively develop a **response** to the problem.

Engagement is needed with local businesses to determine what the extent of the problem is locally, and to encourage more consistent **reporting**.

Resources

Advice on how to deal with **Ransomware** attacks.

NO MORE RANSOM!

https://www.nomoreransom.org/en/index.html

Action Fraud is the main way for businesses to report cyber dependent crime and frauds.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

A Government-backed and industry supported scheme to guide businesses in **protecting themselves** against cyber threats.

CYBER ESSENTIALS

Properly implementing the Cyber Essentials scheme will **protect** against the vast majority of common internet threats. Documents are **free to download** from the website.

Also available is a **self-assessment questionnaire** to assess how cyber-secure a business actually is. The **Cyber Essentials badge** allows your organisation to advertise that it meets a Government-endorsed standard.

www.cyberessentials.ncsc.gov.uk

OFFENCES AGAINST INDIVIDUALS

In this section, crimes which appear to have been committed against an individual person rather than a business have been separated out of the Action Fraud data, to examine which crime types are most commonly reported and which lead to the greatest financial harm.

Cyber Dependent Crimes

In 2016-17 there were **500 cyber-dependent crimes** reported to Action Fraud which affected individual persons.

Computer Virus / Malware / Spyware

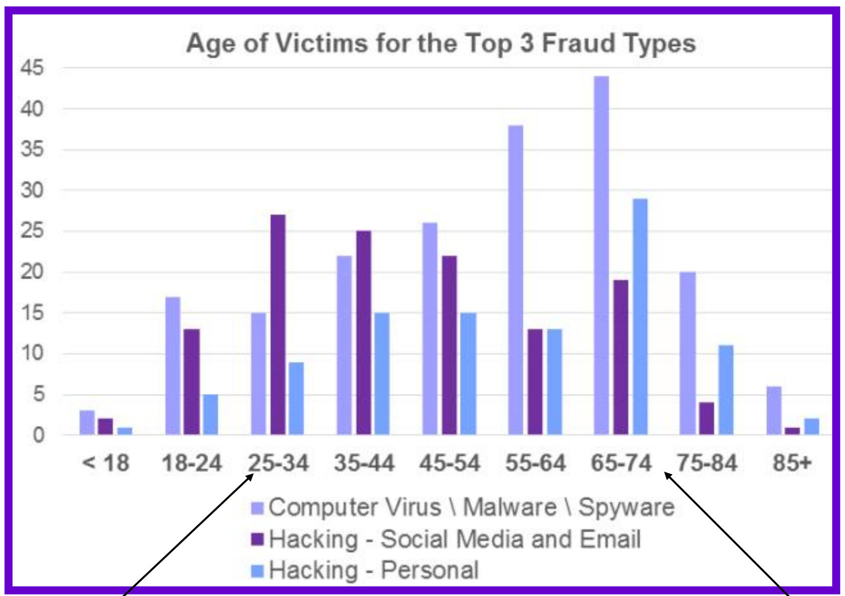
208 (42%)

Hacking: Social Media and Email

140 (28%)

Hacking: Personal

118 (23%)



Both genders report cyber-dependent offences in equal measures.

Younger people are more likely to report **Hacking of Social Media and Email.**

Older people are more likely to report **Computer Viruses/Malware/Spyware**.

Cyber Enabled Frauds

In 2016-17 there were **4,817 cyber-enabled frauds** reported to Action Fraud which affected individual persons.

Total Reported Losses:

£17,450,239

£6,418,462 of the losses were recorded under the category of '**None of the Above**'. A dip-sample suggests many of these offences should have been recorded under 'Computer Software Service Fraud' or 'Online Shopping and Auctions'. Inaccurate recording means there is a real lost opportunity to understand the true impact of these offences.

Most Commonly Reported 1:

Computer Software Service Fraud (25%)

Reported Losses:

£551,587

Most Commonly Reported 2:

Other Advance Fee Frauds (20%)

Reported Losses:

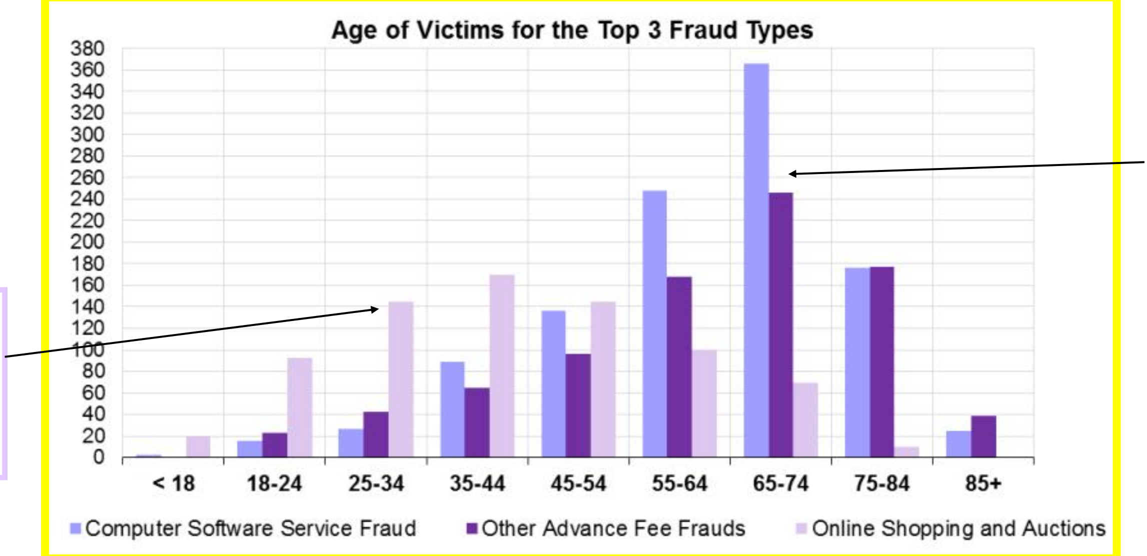
£1,199,299

Most Commonly Reported 3:

Online Shopping and Auctions (18%)

Reported Losses:

£1,457,292



Younger people are more likely to report **Online Shopping and Auctions frauds.**

Older people are more likely to report **Computer Software Service Fraud** or **Other Advance Fee Frauds**.

These findings are consistent with previous findings presented in the April 2016 SOCLP.

Younger People

The data also showed that, while less commonly reported, 'Cheque, Plastic Card and Online Bank Accounts (not PSP)' fraud, 'Other Consumer Non Investment Fraud' and 'Application Fraud (excluding mortgages)' were more common among younger adults than the elderly. 'Rental Fraud' and 'Lender Loan' fraud were also more commonly reported by younger adults.

Older People

'Lottery Scams' were more likely to be reported later in life, as were 'Other Financial Investment' frauds and 'Fraud Recovery' offences. 'Dating Scams', 'Mandate Fraud' and 'Consumer Phone Fraud' appear to more commonly affect those in mid-life to retirement age.

Gender Differences

Overall, females reported slightly more cyber-enabled frauds than males. There was little gender difference in most fraud categories, but **females** were more likely to report **Computer Software Service Fraud** and **Other Advance Fee Fraud** (possibly because these affect the elderly more where there is a population bias towards females) whereas **males** were more likely to report **Online Shopping and Auctions** fraud and **Other Financial Investment Fraud**.

Traditional Frauds

In 2016-17 there were **291 non-cyber frauds** reported to Action Fraud which affected individual persons.

Ticket Fraud

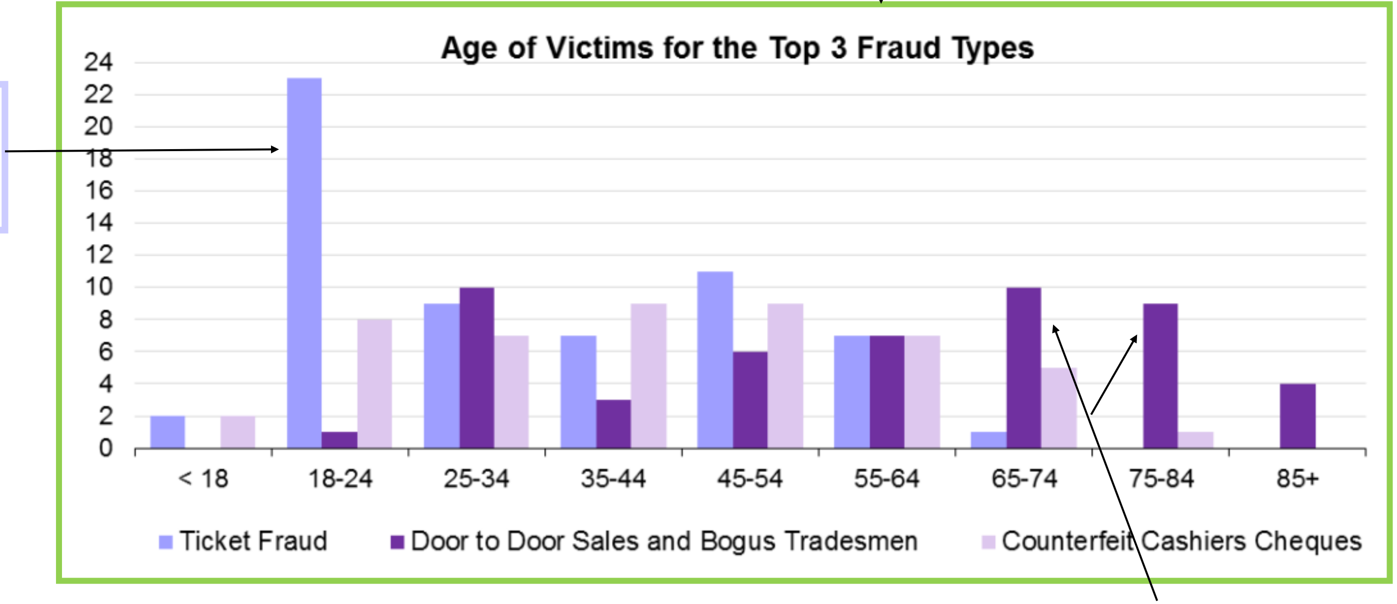
69 (24%)

Door to Door Sales and Bogus Tradesmen

64 (22%)

Counterfeit Cashiers Cheques

55 (19%)



Younger people are more likely to report being a victim of **Ticket** Fraud.

Older people reported being a victim of **Door to Door Sales and Bogus Tradesmen** more often than any other traditional fraud type.

Summary

In summary, people's **age** seems to be a key factor in which types of fraud they are likely to become victim of, and this applies to all types of fraud: cyber dependent, cyber enabled and traditional fraud. Therefore interventions to prevent people from becoming victims of fraud should ensure that age-appropriate messages are being delivered. The boxes below summarise the key types of fraud that appear to affect younger and older people, according to the Action Fraud data.

It should also be noted that people of **middle-age** are often affected by both ends of the spectrum, frauds which affect younger people and the frauds which affect older people. Targeting messages at this age group could therefore also be helpful as while they may be prevented from becoming victims themselves, they may also be able to share what they learn with older parents and younger children.

Younger People are more likely to be victims of:

Cyber Dependent

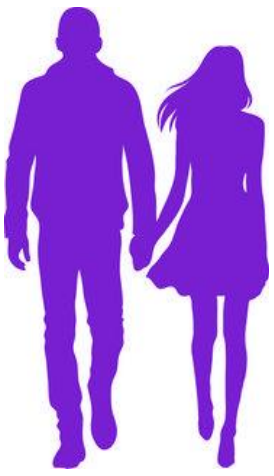
- Hacking of Social Media and Emails

Cyber Enabled

- Online Shopping and Auctions frauds
- Cheque, Plastic Card and Online Bank Accounts (not PSP) fraud
- Other Consumer Non Investment fraud
- Application fraud (excluding mortgages)
- Rental fraud
- Lender loan fraud

Traditional Fraud

- Ticket fraud



Older People are more likely to be victims of:

Cyber Dependent

- Computer Viruses/ Malware / Spyware

Cyber Enabled

- Computer Software Service fraud
- Other Advance Fees fraud
- Lottery scams
- Other Financial Investment fraud
- Fraud Recovery frauds

Traditional Fraud

- Door to Door Sales and Bogus Tradesmen

Resource

www.cyberaware.gov.uk

The **Cyber Aware campaign**, formerly Cyber Streetwise, gives the public the **advice** they need to **protect** themselves from cyber criminals. Targeted messaging delivered through social media and advertising and in partnership with businesses promotes two main goals:

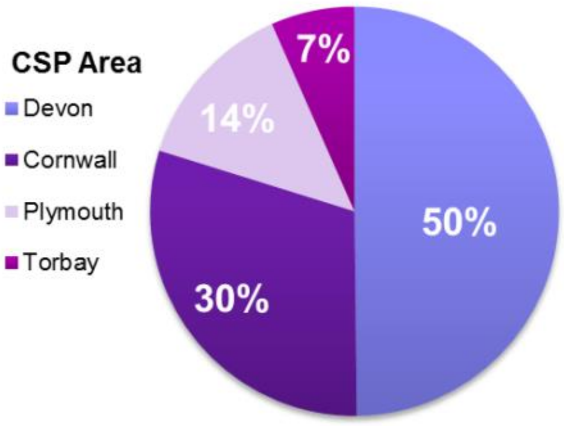
- using three random words to create a **strong password**;
- always downloading the latest **software updates**.

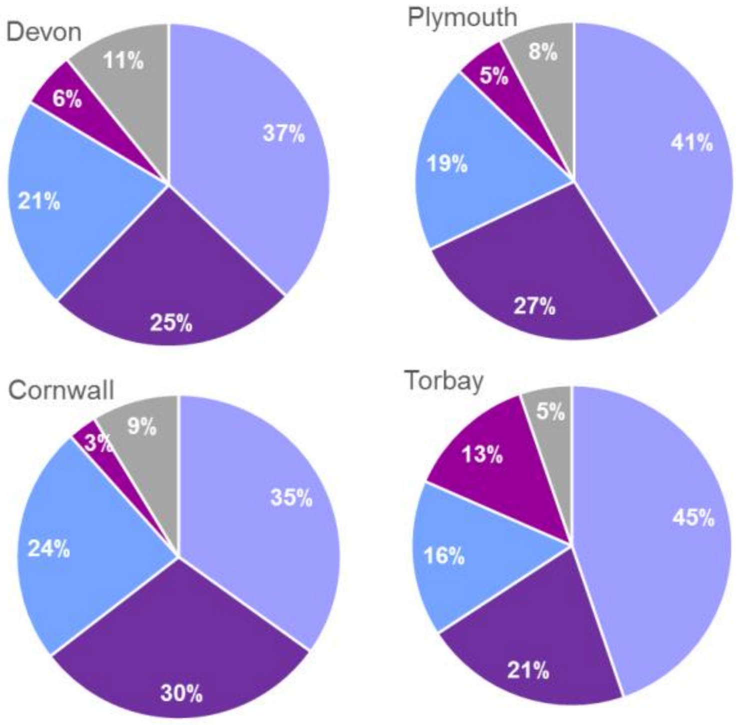
CYBER AWARE

COMPARISON OF CSP AREAS

This page looks at how the four **community safety partnership (CSP) areas** are similar or different in the proportions of the different types of offences being reported to Action Fraud.

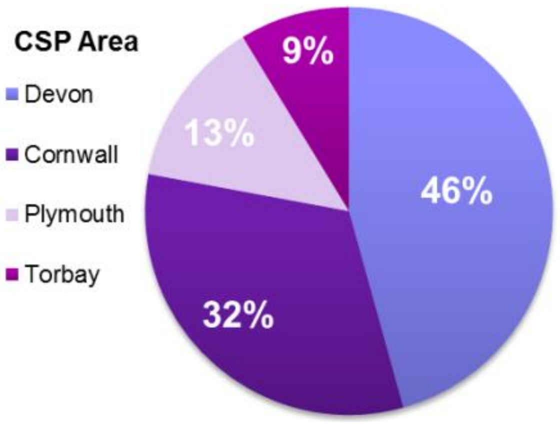
Cyber Dependent Crimes

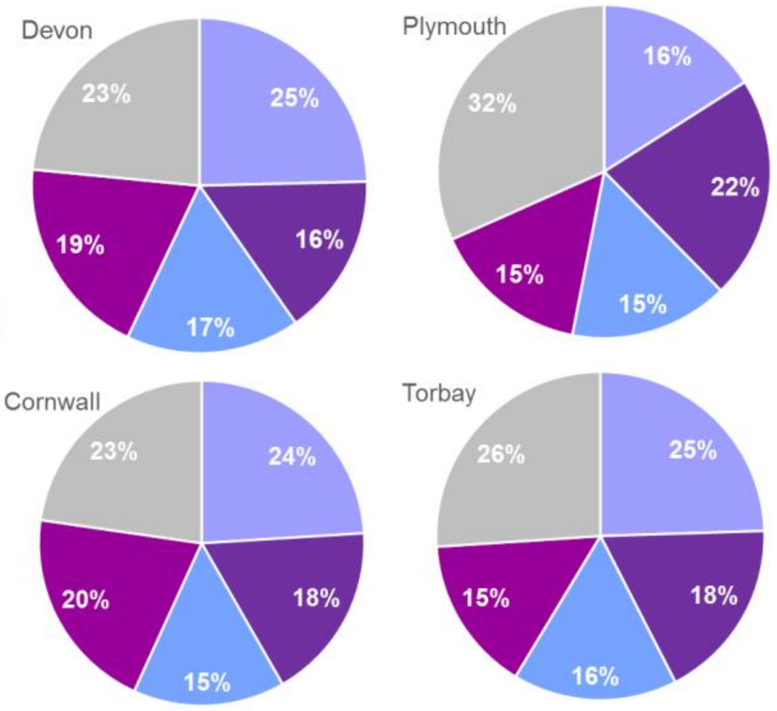




Computer Viruses/Malware are consistently the most highly reported cyber-dependent crimes across all areas, with it forming the highest proportion in **Torbay**. As previously established, this crime type tends to affect **older residents** more than younger, so this is likely to reflect Torbay's older demographic.

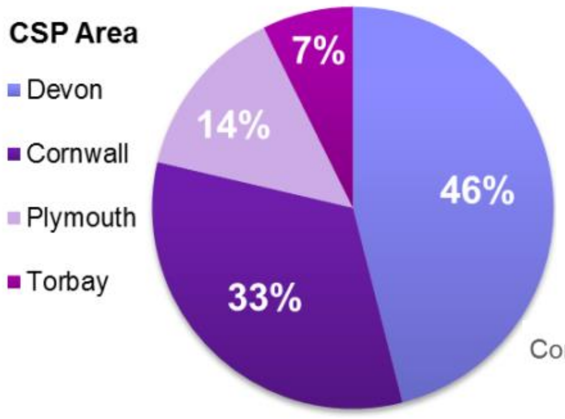
Cyber Enabled Frauds

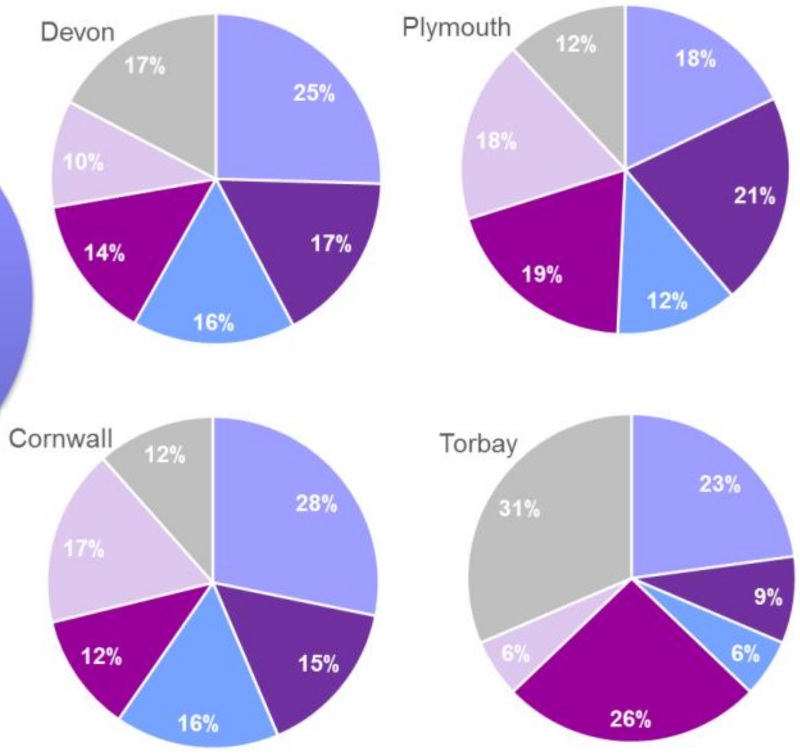




Computer Software Service Fraud is the most commonly reported cyber-enabled fraud in all CSP areas **except Plymouth**. This is a fraud that more commonly affects **older residents**, and Plymouth's demographic is slightly **younger** than the other areas, partly due to the population of **university students**. This may also explain the slightly higher proportion of **Online Shopping and Auction** frauds in Plymouth as this tends to affect **younger residents** more.

Traditional Frauds





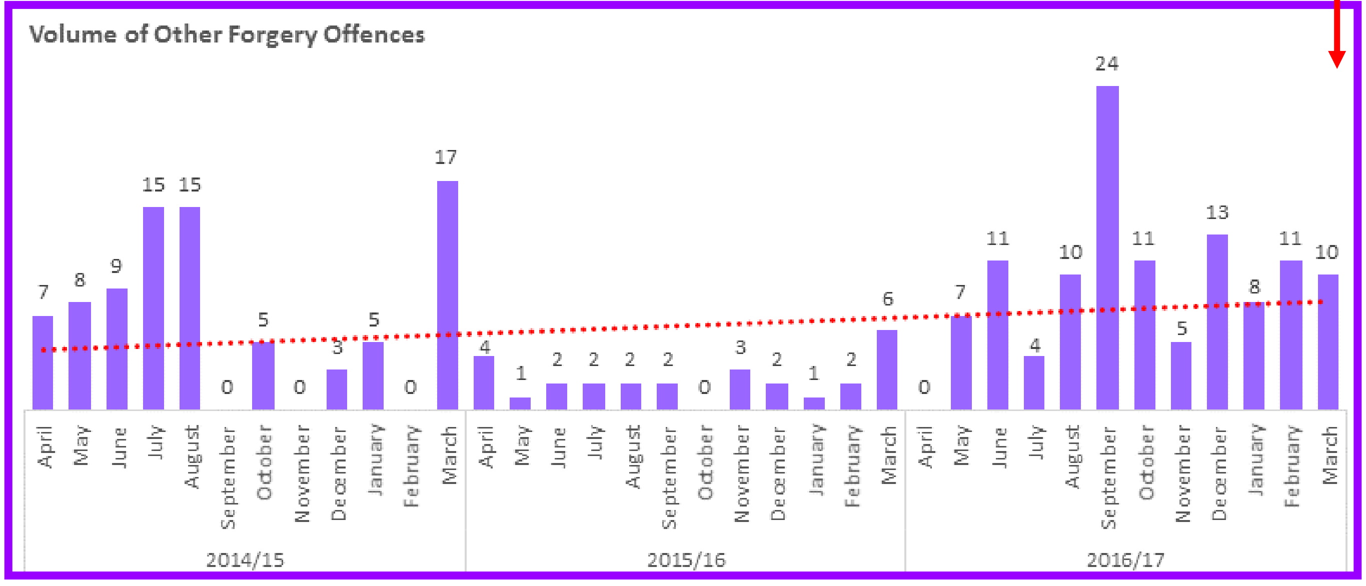
There is more variety across CSP areas with these fraud types as the overall numbers are much smaller. **Retail fraud** impacts most on **businesses** and forms the highest proportion in **Cornwall** and **Devon**. **Door to Door Sales** impacts most on **older** people and is proportionally highest in **Torbay** which has an older population.

COUNTERFEIT GOODS

Crime Data: On Devon and Cornwall Police's crime recording system, crimes relating to counterfeits and forgeries are recorded in the 'Other' crime category. 'Other' data was extracted for the period 1st April to 31st March for the years 2014/15, 2015/16 and 2016/17, so that any trends over time could be examined. The table below shows that only a low volume of these crimes have been recorded, with an apparent reduction in recording off all crime types in the year 2015/16 and a significant rise again in 2016/17.

Home Office Group Description	2014/15	2015/16	2016/17	Grand Total
Other Forgery	84	27	114	225
Forgery or Use of Drug Prescription	17	13	12	42
Making, Supplying or Possessing Articles for Use in Fraud	7	5	24	36
Fraud, Forgery etc associated with Vehicle or Driver Records	7	8	3	18
Possession of False Documents	2	3	4	9
Grand Total	**117**	**56**	**157**	**330**

The Home Office group '**Other Forgery**' covers a number of different offence descriptions. However, the most common of these within the current data set, accounting for **84%** of these offences is "**Pass as genuine a thing knowing it was a counterfeit of a currency note / protected coin** - Forgery and Counterfeiting Act 1981".



It is not known why there was such a great reduction in this offence type in 2015/16, but there was a **322% increase** in 2016/17 compared to the previous year. If you compare 2016/17 to 2014/15 there was still a **36% increase**.

Value of the counterfeit notes: The most common forgery seen in this data set was £50 notes (29 offences) followed by £20 notes (27 offences). Additionally, there were nine offences where fake **Irish** £20 notes were used, another nine where fake **Scottish** £20 notes were used and another four offences where fake **Scottish** £50 notes were used. There were four offences that stated **Scottish** counterfeits had been used, but not what their value was. There was only one offence where a fake £5 note had been used and one fake 50 **euro** note.

Method of Offending: One or more offenders enters a store, café, bar etc and purchases a very low value item, paying with a £20 or £50 note, so they leave with the change in genuine money. Whether they are successful or not in passing the forgery, it is common for the offender(s) to enter a number of different venues in the local area to make multiple attempts at using the counterfeit notes.

Resource

www.bankofengland.co.uk/banknotes/counterfeit-banknotes

The **Bank of England** provides detailed advice and guidance about counterfeit currency.

BANK OF ENGLAND

Police-held Intelligence

There are relatively low levels of intelligence mentioning 'counterfeit' goods: less than 100 items for the year ending March 2017. The intelligence recorded in the six months to March 2017 was examined in more detail to establish what type of goods are being counterfeited or sold within the Peninsula (although untested intelligence should not be taken as fact). Devon & Cornwall Police share relevant intelligence with Trading Standards and HMRC and vice versa.

Tobacco: This was the most commonly mentioned counterfeit item. Some was being sold from shops, some from individuals in pubs and on the street, some from private residential addresses and some online. There is one submission which raises concerns about an individual selling counterfeit tobacco and also exploiting vulnerable people by forcing them to repay money owed with sexual favours.

Aftershave and perfume: There were seven submissions regarding the selling of counterfeit aftershave and/or perfume, imitating major brand names. Some was being touted in venues such as bars and social clubs, while some was being advertised on 'buy and sell' pages on Facebook.

Clothes, shoes and handbags: There were six submissions mentioning either clothes, shoes or handbags, with a mix of sales in person and online.

DVDs: There were only two submissions regarding counterfeit DVDs, one in Cornwall and one in North Devon. Both are individuals selling them from their own homes.

Alcohol: One shop was suggested to be selling counterfeit Smirnoff vodka at £6 for a litre.

Money: In addition to actual goods there were 18 intelligence submissions relating to counterfeit money, although a number of these could be attributed to a single individual who was using Facebook, Twitter and WhatsApp to sell the counterfeit money using a variety of accounts under different names. The minimum order was £100 for £1,000 of fake notes.

NATIONAL BANKING PROTOCOL

The National Banking Protocol

The **Financial Fraud Action UK** are leading a nationwide initiative referred to as The Banking Protocol: a crime prevention initiative delivered in partnership with financial institutions, law enforcement and Trading Standards designed to identify victims in branch who are in the process of completing a face-to-face financial transaction; this may be a withdrawal, transfer or loan application, which is suspected to be linked to ‘rogue trader’ type offences or frauds involving an element of social engineering such as romance frauds, investment frauds or courier fraud.

The aim is to train every single front-facing employee of banks, building societies and Post Offices to spot scams before money is handed over. Cash payments to fraudsters are typically much harder to trace than online payments, with the vast majority of cases going unsolved.

The original London-wide pilot prevented **£1.3 million** in financial harm in just **three months**, from rogue trading, romance scams, investment scams, courier fraud and elder abuse.

By the end of June 2017, 18 police forces had launched the Protocol, and a further **£3.2 million saved**, with **34 arrests** made, directly attributed to the initiative.

In September 2017, The National Banking Protocol won a Government Counter-Fraud award for ‘outstanding collaboration’.

Devon and Cornwall

Devon and Cornwall Police and the Finance Industry are working together to tackle fraud by implementing the ‘Banking Protocol’. This has thwarted **£820,000** of financial fraud in Devon and Cornwall in just **four months** of operation.

The key element of the ground-breaking scheme is that local bank or building society branch staff can alert police to suspected scams by an agreed protocol allowing local police officers to arrive at the branch **before** any transfer of funds takes place and to provide **local support** for the victim.

Nationally the Protocol has stopped more than **£9 million** of potential fraud in first year of operation figures from UK Finance show.

Local Case study: “Rosemary”, aged 83, from Devon:

This is a genuine example of the Banking Protocol in action in the Devon and Cornwall Police force area. The victim’s name has been changed.

83-year-old Rosemary visited her local bank in Devon on a Thursday afternoon, one day in November 2017.

Unknown to the bank staff when she arrived, Rosemary had been subjected to days of constant phone calls and harassment from scammers. Days before she went to her bank the man at the end of the phone introduced himself as a **fraud investigator** working in the **head office** of her **bank**, explaining that someone in her branch was **stealing money** from her account. He told her she needed to act swiftly to ensure her money was safe and needed to transfer the money into a ‘safe’ bank account.

Rosemary received a number of similar subsequent calls from the scammers putting **pressure** on her to transfer money into this ‘safe’ account.

By the time Rosemary visited the bank she was in a state of some **distress**.

The bank staff had received **training** in the Banking Protocol and realised that any suspicious transfer or withdrawal of cash warrants a few probing questions to ensure that the customer isn’t falling victim to a fraud. Rosemary, of course, had been briefed by the scammers not to say anything to alert the bank staff to their fictitious fraud “sting” on the bank. She had been instructed to give a **plausible story** to explain where the money was going. However, the staff used their awareness and training and it became clear that Rosemary’s request to transfer **£4,500** to an account elsewhere in the country was a **scam**.

Rosemary agreed to await the arrival of the police. The bank called 999 and police arrived promptly to give Rosemary the reassurance that she was indeed the victim of a scam.

Thankfully the money stayed in Rosemary’s account and an enquiry was commenced to trace the owner of the so called ‘safe account’.

Rosemary was fortunate, thanks to the Banking Protocol, **not to lose any money**, even though the experience was very **stressful** and **worrying** for her.

Resources

Friends Against Scams is a National Trading Standards Scams Team initiative which aims to protect and prevent people from becoming victims of scams by empowering communities to... 'Take a Stand Against Scams.'

https://www.friendsagainstscams.org.uk/

Take Five is a national campaign led by UK Finance which `offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud.

https://www.takefive-stopfraud.org.uk

Provided by the NFIB which is run by the City of London Police as a national service. You can register to receive direct, verified, accurate information about scams and fraud in your area.

https://www.actionfraudalert.co.uk

CYBER NETWORK

FOR REPORTING, ADVICE AND GUIDANCE

National Level

THE NATIONAL CYBER SECURITY CENTRE (NCSC)

https://www.ncsc.gov.uk/

The NCSC was set up to help protect our critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK Internet through technological improvement and advice to citizens and organisations. Our vision is to help make the UK the safest place to live and do business online.

What they do: Support the most critical organisations in the UK, the wider public sector, industry and SMEs. When incidents do occur, we provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

ACTION FRAUD

www.actionfraud.org.uk

The UK's national centre for internet fraud and cybercrime reporting plus advice.

A central point of contact for reporting and for information about fraud and cybercrime.

GET SAFE ONLINE (GSOL)

https://www.getsafeonline.org/devonandcornwall/

Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety. Devon and Cornwall Police work with GSOL who provide a unique resource of practical advice on how to protect yourself, your computers and mobile devices and businesses against fraud, identity theft, viruses and many other problems that may be encountered.

Regional Level

REGIONAL CYBER CRIME UNIT (RCCU)

https://www.swrocu.org.uk/cyber.aspx

The RCCU is a small team of specialist cyber-crime investigators who will tackle the most serious of cyber-related attacks including Network Intrusion, Denial of Service (Dos) attacks and serious computer hacking offences. The unit will also work with industry to develop preventative strategies to enable them to protect themselves from cyber-attacks.

SOUTH WEST CYBER SECURITY CLUSTER (SWCSC)

https://southwestcsc.org/

A not-for-profit collaboration raising cyber security awareness and best practice in the South West. Supported by the police, leading universities, industry experts and business organisations, the Cluster exists to raise the profile of cyber security issues and help the region's businesses and organisations take steps to counter the threats.

Local Level

D&C Police DIGITAL CAPABILITIES UNIT

The Digital Capabilities Unit (DCU) within Devon and Cornwall Police forms part of the Serious and Organised Crime Branch. It comprises of two Detective Constables, a Police Staff Investigator, a **Cyber Protect Officer** and a Detective Sergeant. The DCU has responsibility for the investigation of complex and serious internet related crimes.

The Force **Cyber Protect Officer (CPO)** role was introduced into both Devon and Cornwall Police and Dorset Police forces in January 2017.

Their role includes: taking guidance, advice and alerts from the **National Cyber Security Centre** (NCSC), which are then filtered down and made more digestible for the public; helping to run events on cyber safety awareness, linking in with the **Get Safe Online team**; reactively visiting businesses and victims of more serious cyber crime incidents to give prevention advice to help stop them becoming repeat victims and to gather information; actively looking for different ways of getting messages out to the public; encouraging reporting to **Action Fraud** or **Police** as relevant.

The role-holder is linked into the **Regional Cyber Crime Unit** who are still not seeing a high volume of cyber-dependent crimes reported, most likely due to the risk to their reputation. The Cyber Protect Officer attends events where offences are informally disclosed and can therefore help get an understanding of the true volume of victimisation.

The Cyber Protect Officer proactively engages with businesses, particularly councils, by delivering awareness raising presentations. She also takes requests to deliver Protect talks and events to businesses and groups across the peninsula. Visiting different community groups allows targeted awareness raising, for example, the Women's Institute provides a platform to provide specific messages about crimes which affect an older demographic. Sometimes people disclose that they have been victims of cyber crime following these talks because they didn't realise that it was a criminal offence. If money is lost, often it is assumed that their bank would deal with it or was the only party who needed to know, and so getting the message out there that these offences do have a criminal element is key to encouraging reporting.

The role-holder is able to refer victims to the **South West Cyber Security Cluster** (SWCSC) who are a group of local cyber security professionals who provide free advice and support to victims.

The Cyber Protect Officer does not deal with cyber crime affecting children because schools will have in place their own arrangements with various supporting agencies and charities such as the South West Grid for Learning, or the NSPCC. From a policing point of view, protect messages are dealt with by the Youth Services team and CEOP (Child Exploitation and Online Protection Command).

As of January 2018, the role of the Cyber Protect Officer in Devon and Cornwall Police is held by Laura Cowie:

Email: CyberProtect@devonandcornwall.pnn.police.uk Phone: 01626 326426

@DC_CyberProtect

DEVON AND TORBAY

THE LOCAL PARTNERSHIP PERSPECTIVE

Devon, Somerset & Torbay Trading Standards

Devon, Somerset & Torbay Trading Standards (DSTTS) took the lead in responding to the first iteration of the Cyber Crime, Fraud and Counterfeit Goods SOCLP on behalf of Safer Devon Partnership (SDP).

Current Areas of Focus:

- Mass-Marketing Scams
- Shadow Economy / Intellectual Property / e-crime
- Doorstep Crime

Training for Staff:

- Training to partners on spotting scams and helping victims – also available online.
- In-house training for our officers.
- Specific training for scams officers from Social Services on mental capacity and safeguarding.
- National College of Policing training (*Researching, Identifying and Tracing the Electronic Suspect* course).

Local Action Plan:

- Day-to-day work ongoing;
- Currently working on our Strategic Assessment to aid service planning for 2018/19;
- Plan to continue awareness work with community partners;
- Will support national campaigns highlighting cyber safety, doorstep crime and fraud;
- Work with Safeguarding Boards on helping those with Care Needs to avoid fraud.

Gaps:

- Assessing the real scale of the problem.
- Limitations of statistics and interpretation: do more complaints reflect an increased problem, or success at raising awareness and reporting? Do fewer complaints reflect success of awareness raising or a shift in consumer behaviour to redress elsewhere (e.g. Facebook, Resolver, etc.)?

Achievements:

- Cybercrime Conference for businesses, held in October 2016.
- Regular events for consumers and community groups highlighting cybercrime as a means of fraud.
- Use of social media for advice and warnings– officer appointed.
- Scams awareness month was supported with events and talks with partners, including banks and the police.
- Scams information was given out at the Devon County Show.
- Better partnership working - joined Adult Safeguarding Boards in Devon, Somerset and Torbay to help them support those with care needs to avoid financial abuse.
- We are developing a website resource for carers and have obtained access to Carefirst and Connexus to enhance victim support and prioritisation.

Challenges:

- Changing nature of scams;
- Equipment/technical knowledge;
- Identifying/prosecuting perpetrators as often based outside of our jurisdiction;
- Hard to reach the most affected - elderly and young;
- Double reporting - via Action Fraud and Citizens Advice;
- Victim denial;
- Consumers not always clear on who to contact.

Prosecutions

We have achieved notable successes across our key work areas over the past year with 13 prosecutions occurring in this strategic assessment period resulting in:

- Exeter man who sold counterfeit tobacco being sentenced to a 15-week prison sentence suspended for a year, ordered to complete 150 hours unpaid work and pay £5000;
- Rogue trader who conned the elderly being sentenced to 38 months in prison with his accomplice jailed for 12 weeks for money laundering;
- Fraudulent builder being required to pay significant Confiscation Order of more than £100,000;
- Online trader who sold counterfeit goods being ordered to pay £20,000 within 3 months or face 8 month prison sentence;
- Carpet cleaner found guilty of fraud being sentenced to 32 weeks imprisonment suspended 2 years, 180 hours community service, and ordered to pay compensation to victims.

Intelligence Submissions Relating to Cyber-enabled Activity

Intellectual Property Crime: 91 reports, accounting for 7% of all intelligence submitted in the given period. A decrease of 47 (34%) reports compared with the previous period.

Scams: 57 reports, accounting for 5% of all intelligence submitted in the given period. Scams reported were Bogus Services, Lotteries & Cash Rewards and Internet Scams. A third of Bogus Services scams were indicated to have involved use of the internet or mobile phones. Scams intelligence submissions decreased for the third year, this year by 72 (56%) reports. The downward trend is due to changes to protocol, now only entries containing new information are submitted.

Devon, Somerset and Torbay Trading Standards (cont…)

Intelligence submissions relating to **e-Crime activity:** The key e-Crime categories were **Intellectual Property** and **Scams**. There were 207 complaint reports identified as e-Crime, of which, sales on **eBay** and **Facebook** accounted for 30%. The top trader practices were **bogus selling** and **counterfeiting**.

There is a continuing issue with online selling platforms enabling individuals to import goods from overseas and sell them through the internet direct to the consumer so the seller may never see the goods. Enforcement and inspection methods will need to change, as the UK sellers do not have traditional shops: DSTTS have recommended that proactive monitoring of selling websites should be considered.

Looking Forward: We continue to take cases from the **National Scams Team** and provide help, advice and support where possible to those referred.

DSTTS Strategic Assessment will recommend that we should continue to participate in National **Operation Jasper** (online sales), as well as ensuring online **local monitoring** takes place on a more regular, planned programme. Given the proportion of sales on **Facebook**, we are proposing that some Operation Jasper work should focus on this platform by:

- Carrying out market surveillance to identify illegal goods being sold;
- Sending cease and desist advice to sellers if we believe goods may be counterfeit, unsafe or age restricted;
- Raising awareness of the dangers of counterfeit, unsafe and age restricted goods on Facebook.

We must continue to share information with local communities about scams and so empower them to avoid being victims, by:

- Using Social Media and taking part in talks and partner events to spread information;
- Providing consumers with information about scams and clarifying how to report them

We have applied to the LGA for grant funding for scams work and will undertake a project depending on the outcome of this application.

Some Success Stories:

May 2017:
A **rogue trader** who preyed on the vulnerable and defrauded 21 elderly victims out of £108,000 over two years, has been jailed. He was sentenced to 38 months in prison.

He had touted for business by cold calling victims and advertising in local papers. He would give an initial quote then claim he had identified ‘extra’ problems. Victims found themselves handing over thousands of pounds more than was originally agreed. In one instance an elderly man in South Devon paid £7,500 for work worth just £170.

September 2017:
Victims of a jailed **rogue plumber** from North Devon will receive more than £16,000 under the Proceeds of Crime Act.

DSTTSS investigated him after complaints that his work was shoddy and vastly over-priced. One elderly couple had been charged almost £4,000 for a boiler that cost £1,700 and £870 for a pipe costing £87.

A woman who gave up work to assist with looking after her parents, discovered that approximately £500 per month was being spent on **scam mail** and an additional £100 per month on **health supplements**.

After Trading Standards got involved, the couple have signed up to the **Mailing Preference Service** (MPS) and the **Telephone Preference Service** (TPS) to reduce the amount of scam mail and phone calls being received.

A couple in their 70s living in East Devon were living in a small flat on a limited income. The husband enjoyed participating in **lotteries** and the wife liked to buy **health supplements** and **gourmet treats**. The couple also made regular donations to a **charity** by Direct Debit and did not know how to stop these payments. In total the couple believed they were spending approximately £220 per month.

Trading Standards visited and helped to get the Direct Debit cancelled and also signed them up to the TPS and MPS which reduced the amount of scam mail and calls received. The husband agreed to spend his money on his wife instead of the lotteries and the wife agreed to speak to her doctor about only buying supplements from local stores and chemists.

Update from Torbay CSP

Priorities are:

- Information security (linked to the GDPR).
- PREVENT work linked to anti-radicalisation.
- Promotion of online positive messages to our workforce to ensure they keep engaging safely with the online world.
- Reporting concerns around children and school staff. Consideration is being given to having cyber mentors in schools to help encourage children to report. We are also promoting use of the Professionals Online Safety Helpline.

Update from North Devon and Torridge CSPs

North Devon and Torridge CSPs arrange a Junior Lifeskills input each year. Various agencies deliver various 10 minute bitesize inputs to Year 6 children. This year the CSP devised a cyber-bullying input, recognising the effect of it on young people. This was delivered to around 1,300 Year 6 children over a two week period.

Update from Mid Devon CSP

- The ICT team in Mid Devon attended the LRF Cyber Threat Seminar in October 2017.
- Laura Cowie, the Cyber Protect Officer for Devon and Cornwall Police, will be presenting to partner agencies and Mid Devon District Council Staff in December 2017. She is also delivering a presentation to the Town and Parish Clerks and a Tenants Group, as well as now being linked into many business forums in the area.

PLYMOUTH

THE LOCAL PARTNERSHIP PERSPECTIVE

Plymouth Trading Standards: Overview

The findings of the previous OCLP have been incorporated into the Plymouth Trading Standard's Action Plan.

Current Action Plan/Areas of Focus:

- Mass-Marketing Scams
- Shadow Economy / Intellectual Property / e-crime
- Doorstep Crime

Training for Staff:

- Scams Conference
- Specialist vulnerable witness evidence course
- Specialist Investigation course
- Legal update course including money laundering and POCA
- The team now has an accredited Financial Investigator and two accredited Counter Fraud specialists.

Achievements:

Awareness raising through the Scam Conference and the media.

A number of e-crimes were identified and referred to Action Fraud and 66 intelligence reports investigated over the last year.

No evaluations have been carried out to date, but we have had successes with those who are no longer victims of fraud and are no longer losing money. We estimate that for those we visit twice, the success rate is around 30% and for those we have engaged in extensive support, the success rate is around 90%.

Gaps:

No gaps have been identified to date apart from the capacity to visit 650+ victims of scams but assistance now been offered by the Police.

Trading Standards: Scams/Fraud:

- Developing a scams Action Plan.
- Participating in the National Scams Team project. 800+ Plymouth residents were identified as being scam victims; 250 have been visited with £500,000 detriment detected. Plymouth TS are working with police to visit victims.
- Educating consumers and victims, particularly the vulnerable as well as potential victims in sheltered accommodation and care homes, about scams by engaging the media, using press releases and our website.
- Hosted the Scams Conference in September at Plymouth Guildhall to raise awareness among partner agencies to highlight how the vulnerable are scammed.
- Have also given talks to a wide range of agencies including Plymouth Community Homes, sheltered housing wardens and PCC staff so that they can identify and refer potential victims.
- We have a current Crown Court case against a car dealer for offences under the Fraud Act.
- We have been working in partnership with the Citizens Advice Bureau to highlight Scams Awareness Month in July.
  - ⇒ Several events took place including visiting the main Library to give out literature and speak to residents.
  - ⇒ We also spent the morning at Barclays Bank asking their customers whether they are Scam Aware. Several people told us they had been victims and we were able to help them by offering further advice.
  - ⇒ We also visited 'The Foyer' which helps 16-25 year olds towards independent living. CAB and our officers spoke with the residents about the scams which affect people of their age group. Most of these scams originate from social media and younger adults are increasingly being caught out.

Trading Standards: Doorstep Crime

- Improve community safety in Plymouth and support older and/or vulnerable people to lead independent and safe lives by addressing rogue doorstep trading and the fear of it.
- Inspection of suspected "Rogue Traders" when working on site, including testing of the work they have carried out to check the standard.
- Education and support of potential victims, including education of those who make regular contact with them, such as mobile hairdressers.
- Working on intelligence – leaflet drop areas where there has been rogue trader activity.
- Maintaining links with banks, building societies and post offices to help protect victims. Awareness raising conducted led to one bank informing police when a large sum of money was requested by a customer in payment for rogue work.
- Participate in multi-agency working in neighbourhoods such as crime prevention focus weeks.
- Helping victims of Doorstep Crime by developing links with Victim Support, Silverline and the Victim Care Unit, and 'target hardening' in areas of rogue activity.
- Work with Adult Social Care to develop strategies to best deal with Doorstep Crime.
- Work with Public Health to develop victim profiles.
- Ensure unit compliance with the Regional Doorstep Crime Matrix.

Trading Standards: Shadow Economy / Intellectual Property / E-crime

- Regular monitoring of Plymouth traders selling illegal goods on Facebook. Several warning letters were sent to those selling counterfeits. In the last year, six warrants were executed and counterfeit goods were seized; there are several investigations ongoing into large-scale supply of counterfeit clothing and tobacco.
- The team took part in some joint work with HMRC called Operation Ebbtide. This was a large-scale regional operation targeting illicit tobacco. Two HMRC teams visited Plymouth checking retail outlets and storage units. Tobacco detection dogs were also used. HMRC made some seizures of non-duty paid products and useful intelligence was gained from the exercise.
- Plymouth has participated in Op Jasper which was a National Trading Standards investigation into Facebook sellers. Several sellers were identified and action taken.
- Operation Locknife was an investigation into the large scale supply of smuggled and counterfeit tobacco. Four warrants were executed on the same day at private addresses across the city. As a result we seized 1,974 packets of cigarettes and 1,349 pouches of hand rolling tobacco, amounting to a street value of £25,000. We also seized £7,430 in cash.
- Regular checks are undertaken at car boot sales and markets.
- A number of e-crime scams were detected and referred to Action Fraud; consumers were advised.

Trading Standards: Prosecutions

- A major investigation into counterfeit clothing sold over e-bay has taken several years to conclude. It involved executing 7 warrants, seizure of vast amounts of counterfeit clothing and sophisticated printing equipment, and complex POCA investigations into 4 defendants and a Company. All the defendants were given suspended prison sentences and community orders. £66,000 was confiscated under Proceeds of Crime and the gang were ordered to pay £8,000 in costs.
- Prosecution of an e-Bay seller of counterfeit and unsafe cosmetics. A man who sold fake Mac lipstick which had over 300 times the legal amount of lead in it has been prosecuted for counterfeiting and safety offences. The seller pleaded guilty to seven offences after a warrant was executed on his home address and fake cosmetics and watches were seized. He was sentenced to a total of six weeks in prison suspended for 12 months. He was also ordered to pay £400 costs and £115 victim surcharge. Among the haul were lipsticks and mascaras branded as MAC. The products were sent for testing and the fake cosmetic was found to contain dangerously high levels of lead. The worst was a fake MAC lipstick called 'Lady Danger' that contained 3702mg/kg of lead – the permitted limit is 10mg/kg.
- A trader from Wales was prosecuted for illegally importing a puppy and mis-describing it on Gumtree to the Plymouth purchaser. The puppy was imported at too young an age, which meant it breached legislation aimed at preventing rabies. We had to seize the puppy and quarantine it until properly vaccinated. The seller pleaded guilty and was fined £3,421, costs of £1,748, and compensation of £823.
- 66 intelligence reports have been investigated over the last year, the vast majority of which, relate to Facebook….

The breakdown on work area for these figures is:

Subject	No. of Reports	Percentage
Illegal Tobacco	33	50.0%
Counterfeit Goods	27	40.1%
Product Safety	3	4.5%
Fair Trading	3	4.5%
Total	**66**	**100%**

Enforcement Action	Number
Investigation	9
Investigation leading to warrant / inspection	6
Prosecution	1
Caution	2
Cease & Desist Letter	11
Recorded for intelligence / future development	15
Referral to NTS eCrime Team for development	2
Referral to Home Authority	3
Facebook Content Removal - approved	1
Referred to Other Agency	4

Safer Plymouth Update - Cyber Crime and Fraud

- We are working with police in sharing the messages about cyber crime and fraud.
- Cyber-enabled crime is a rising issue in Plymouth as we are seeing a spike in this type of crime.
- We have made cyber-enabled crime a priority theme for the partnership. From this we will work to create an action plan to include things such as awareness raising around this type of crime.
- We have a Healthy Relationships programme that will be rolled out in schools in the New Year which will tackle some cyber-enabled issues with young people.

CORNWALL

THE LOCAL PARTNERSHIP PERSPECTIVE

Cornwall Trading Standards

Cornwall Trading Standards felt that the previous SOCLP reflected their existing priorities and plans and so business has continued in these areas.

Current Priority Areas/Areas of Focus:

- Mass-marketing scams: postal, telephone, email and online scams;
- Doorstep fraud: 'traditional' artifice crime at victims' homes;
- Illegal sales of tobacco and alcohol, including via social media sites;
- Sales of illegal products online: counterfeit goods and unsafe consumer goods.

Positive Interventions and Activities:

As part of the response to tackle mass-marketing scams, 'Trading Standards Volunteers' have been appointed to conduct at home interventions with suspected victims of mass marketing scams. These interventions aim to educate, advise and support victims and public warnings are also issued via press releases. Cornwall Trading Standards aims to intervene with at least 120 suspected victims of mass-marketing frauds (scam mail) each year. Each intervention is conducted at the home of the suspected victim, where a gentle review of the letters to which they have been responding is undertaken, alongside education and demonstration of others who have fallen victim to the same or similar scams. An assessment is made as to the sort of sums of money sent in response to the scam mail. Such interventions may require multiple return visits, to earn the trust of the victim and to wean them off what can become an addiction. Where possible, further, on-going support is sought from family members, friends or charity/community groups to prevent a return to sending payment to scam mailings. Call blocker devices may be provided where appropriate. In one example alone, 120kg of scam mail was retrieved from the home of one victim.

Cornwall Trading Standards conducted a successful joint response with Police to reports of itinerant sellers of counterfeit goods at a tourist hot-spot. Complaints from local shopkeepers prompted Trading Standards to attend Perranporth beach on 10th August 2017 amid reports that fake clothing and handbags were openly being sold by street traders. Trading Standards Officers were joined by a Police Officer from Devon & Cornwall Police and together seized dozens of branded items, including fashion hand bags, clothing, boots, perfume, sun glasses, speakers, headphones and sportswear.

Difficulties/Gaps:

Difficulties encountered are predominantly around investigations that require covert surveillance on social media sites (i.e. sale of counterfeits on Facebook pages and closed groups, etc.).

Referrals from Police Call Centres suggest a need for further training in Doorstep Fraud (bogus tradesmen), Mass Marketing Scams (bogus prize notifications, bogus computer support services, on-line dating scams, etc.). Incidents of Doorstep Fraud are often referred by 101/police officers to Action Fraud, rather than to the local Trading Standards department. Action Fraud will compile details of similar incidents and may produce assessments and referrals in due course. A referral from Action Fraud may take place many weeks after a crime has been committed, long after the perpetrators have fled the scene. Local Trading Standards teams are able to provide an immediate response to the incident, but call handlers and officers are not trained in what Trading Standards teams cover and will often only refer doorstep fraud incidents to Action Fraud or will dismiss incidents as being a "civil dispute". Training for call handlers is vital as they are the first point of contact for (predominantly) vulnerable/elderly victims of doorstep crime. Training needs to be a rolling programme as the call centres have a high turnover of staff.

It is suggested that a half-hour's briefing/explanation from an *operational* level Trading Standards officer be included in all Police call-centre training. This would provide handlers with a very basic knowledge of the triggers for when to also refer to Trading Standards – an A5 size poster, suitable for display within Police call-centres and that explains these triggers is available from Cornwall Trading Standards. Similarly, an opportunity to input into initial police training would have an enormous positive effect on officers knowing from day one how they should deal with doorstep crime and who they can call for assistance.

Update from Cornwall Council:

Cornwall Council's Corporate Fraud Team has engaged in partnership with **Cornwall Housing Ltd** to investigate instances of **Tenancy Fraud**. Since August 2014 we have recovered 70 properties, successfully prosecuting seven individuals for tenancy fraud related offences, including fraudulent "Right to Buy" applications. In 2017/18 to date there have been 21 recoveries, with a notional value of **£424,000** to the Council.

Cornwall Council's Corporate Fraud Team investigate instances of **Council Tax Support** and **Single Person Discount Fraud**. Since 1 April 2016, using the tools available to them, the team have recovered **£361,396** in overpayments, raised **£7,184** in administrative penalties and have prosecuted seven individuals for fraud.

In March 2014 Cornwall Council were chosen as a Pilot Authority for the creation of the **Single Fraud Investigation Service (SFIS)**. This change resulted in SFIS taking over responsibility for the investigation of **Housing Benefit fraud**. Cornwall Council played a significant role in the development of processes and procedures, which have been adopted nationally. Through this work, since 1 April 2016, **£2.2 million** in benefit overpayments have been recovered, **£118,423** in administrative penalties have been raised and there have been 81 prosecutions.

The Corporate Fraud Team is also responsible for investigating cases of **whistleblowing** and any potential **internal fraud** matters. These cases range from incorrect mileage and expense claims and individuals being paid twice their salary and making no effort to remedy the error to accusations of bribery, corruption and abuse of position. In such cases any loss the Council is exposed to is recovered in full in addition to the consideration of criminal proceedings.

The Corporate Fraud team has a good working relationship with local **Police** enabling us to investigate issues holistically. They also share information with the fraud teams at **NHS Kernow** and **RCHT**, as there are common issues affecting the same people.

The Council also has its **Forensic Services** team, who monitor and investigate **cyber crime**, focusing on **internet misuse** (both internal and on the public network), **computer misuse** and **investigation**. The team have a range of unique tools that allow them to analyse computer activity, identifying key words or unauthorised websites, the use of which can lead to dismissal for staff and criminal proceedings for staff, Members and the users of our public network.

Moving Forwards

The team aims to **raise awareness** of fraud, bribery and corruption across the Council and its partners, so that all officers and Members are aware of the risk of fraud and their **responsibility** towards managing it. They will continue to conduct **proactive counter fraud reviews**, focusing on local as well as national fraud indicators and will advise management on how to improve arrangements. They will actively **share data** with partners, particularly in relation to individuals in receipt of direct care payments, to ensure that the risk of duplication in effort and expenditure is minimised and will review the activities of common suppliers.

Within the Cornwall family of businesses they will take more action to **review** and **mitigate** against the **risk of white collar fraud**; the deliberate manipulation of data (financial or otherwise) for personal gain. Creation of local government companies, increasing commercialisation of activities and heavy budget pressures can lead to management deliberately **misrepresenting performance** either for **personal gain** (through a bonus payment) or to **avoid sanction**.

SUMMARY AND RECOMMENDATIONS

Since the production of the first Cyber Crime, Fraud and Counterfeit Goods profile in 2016, it has been identified by Community Safety Partnerships that these topics are **less of a priority** to local areas than other Serious and Organised Crime topics such as Child Sexual Exploitation and Abuse, and Modern Slavery, which have an easy to identify impact on **vulnerable people**. As such, much of the local activity that has taken place in relation to fraud has been conducted by **Trading Standards**, as part of their day-to-day work on frauds affecting the **elderly**. However, this leaves some **large gaps**, such as frauds affecting **younger people**, **businesses** and **cyber dependent** crimes. Tackling this problem cannot be Trading Standards alone, but it also does not require a large investment of extra resources. Fraud and cyber crimes are **extremely preventable** - it just requires people to be **educated** to recognise scams and to take appropriate steps to **protect** their computers and devices. The advice is already **freely available** as demonstrated by the **links to resources** provided throughout this document.

Recommendations for Community Safety Partnerships:

- Review your actions plans and communication strategies etc. for other areas and consider how **cyber dependent** and **fraud prevention messages** could be **incorporated** into those existing plans/strategies.
- Liaise with Devon and Cornwall's **Cyber Protect Officer** to understand what activity she is undertaking in your area and where the gaps are that you could assist in delivering.
- Build/develop working relationships with your local **Trading Standards Officers** to ensure you really understand which aspects of these problems they are tackling and which they are not, and to understand how you might support/build on some of their initiatives etc.
- Consider: Are you confident that **other than Trading Standards**, are the organisations working with older people in your area **sufficiently trained** in identifying the indicators of/vulnerability to scams?
- Consider: The **demographics** of people vulnerable to higher levels of economic fraud are likely to be more affluent middle- to late-middle aged people, living in more rural areas (very different to other traditional crime types) - can you use this information to **target** communications/awareness raising?
- Consider: How can you raise awareness with **young adults** about the types of cyber/fraud they are most vulnerable to?
- Consider: How could you encourage **practitioners** and **communities** to **register** for the **free** Devon and Cornwall Police **alert system**, which includes updates on frauds/scams at https://alerts.dc.police.uk/ ?

There is national guidance around cyber security, such as the National Cyber Crime Strategy 2016-21.

- Review the guidance and ensure recommendations are being implemented locally.

Cornwall Trading Standards have identified that there is an issue with police call centre staff and officers not always responding in the most appropriate way to calls regarding **doorstep trading fraud** or **mass marketing scams** etc. They sometimes refer to Action Fraud instead of **notifying Trading Standards** who can respond much more quickly. Doorstep Crime is often viewed (incorrectly) as a 'civil' matter, when in fact there are criminal offences under legislation enforced by Trading Standards, which they can investigate and take appropriate enforcement action (including prosecution).

Recommendations for the Police:

- It is suggested that a half-hour's briefing/explanation from an **operational level Trading Standards officer** should be incorporated into all Police **call-centre training**. This would provide call-handlers with a basic knowledge of the triggers for when to refer to Trading Standards – an A5 size poster, suitable for display within Police call-centres that explains these triggers is available from Cornwall Trading Standards.
- Similarly, an opportunity to input into **initial police training** would have a positive effect on officers knowing from day one how they should deal with doorstep crime and who they can call for assistance.

We would like partners to support us in the fight against cyber crime and fraud by encouraging their frontline staff who encounter vulnerable people to provide them with advice and guidance on how to protect themselves against these crimes. However, it may not be realistic for all frontline staff to receive full training in these areas and to have the knowledge necessary to provide this guidance.

Recommendations for the Police:

- Consideration should be given to how we can best support partners in being able to provide this guidance to potential victims. For example, **Corporate Communications** could consider whether it's viable to produce a short series of leaflets (one for older people, one for younger people and one for businesses) which partners could distribute, which gives clear advice and guidance on how to **recognise** fraud/cyber crime and **who** to **report** to under different circumstances.

REFERENCE LIST

City of London Corporation, 2015. *The Implications of Economic Cybercrime for Policing.* [pdf] Available at: <https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf> [Downloaded 16 October 2017].

Consumer Protection Partnership (CPP), 2017. *Consumer Protection Partnership: Update Report 2017.* [pdf] Available at: <https://www.gov.uk/government/publications/consumer-protection-partnership-update-report-2017> [Downloaded 30 October 2017].

Experian, Crowe Clark Whitehill, University of Portsmouth's Centre for Counter Fraud Studies, 2017. *Annual Fraud Indicator.* [pdf[Available at: <https://www.croweclarkwhitehill.co.uk/wp-content/uploads/sites/2/2017/11/Annual-fraud-indicator-2017.pdf> [Downloaded 13 November 2017].

Experian, PKF Littlejohn, University of Portsmouth's Centre for Counter Fraud Studies, 2016. *Annual Fraud Indicator.* [pdf] Available at: <http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf> [Downloaded 6 June 2017].

Get Safe Online, 2017. [online] Available at: <https://www.getsafeonline.org> [Accessed 05/09/17].

HM Government, 2016. *National Cyber Security Strategy 2016-21.* [pdf] Available at: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021> [Downloaded 28 June 2016].

Information Commissioners Office - https://ico.org.uk/

National Audit Officer, 2017. *Investigation: WannaCry Cyber Attack and the NHS*. [pdf] Available at <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf> [Downloaded 29 December 2017]

NCA, Strategic Cyber Crime Industry Group, 2016. *Cyber Crime Assessment 2016 Need for a stronger law enforcement and business partnership to fight cyber crime*. [pdf] Available at: <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file> [Downloaded 16 October 2017].

Office for National Statistics (ONS), 2017. *Crime in England and Wales: year ending Sept 2016.* [online] Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016> [Accessed 01 July 2017].

Public Health England, 2017. Cyberbullying: An analysis of data from the Health Behaviour in School-aged Children (HSBC) survey for England, 2014. [pdf] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/621070/Health_behaviour_in_school_age_children_cyberbullying.pdf> [Downloaded 5 September 2017].

APPENDIX 1: METHODOLOGY

The analysis within the data section is based on **Action Fraud** data for the financial year of **2016-17**.

Cyber-Dependent Fraud Categories:

- NFIB50A - Computer Virus / Malware / Spyware
- NFIB51A - Denial of Service Attack
- NFIB51B - Denial of Service Attack Extortion
- NFIB52E - Hacking Extortion
- NFIB52D - Hacking - PBX / Dial Through
- NFIB52B - Hacking - Personal
- NFIB52A - Hacking - Server
- NFIB52C - Hacking - Social Media and Email

Cyber-Enabled* Fraud Categories:

- NFIB3E - Computer Software Service Fraud
- NFIB1H - Other Advance Fee Frauds
- NFIB3A - Online Shopping and Auctions
- NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)
- NFIB3D - Other Consumer Non Investment Fraud
- NFIB5B - Application Fraud (excluding Mortgages)
- NFIB5D - Mandate Fraud
- NFIB1J - Lender Loan Fraud
- NFIB1B - Lottery Scams
- NFIB1D - Dating Scam
- NFIB2E - Other Financial Investment
- NFIB3B - Consumer Phone Fraud
- NFIB1G - Rental Fraud
- NFIB1E - Fraud Recovery
- NFIB2A - Share Sales or Boiler Room Fraud
- NFIB17 - Other Regulatory Fraud
- NFIB4A - Charity Fraud
- NFIB16B - Pension Fraud committed on Pensions
- NFIB1A - "419" Advance Fee Fraud
- NFIB9 - Business Trading Fraud
- NFIB6A - Insurance Related Fraud
- NFIB15 - HM Revenue & Customs Fraud (HMRC)
- NFIB5C - Mortgage Related Fraud
- NFIB90 - None of the Above*

Non-Cyber* Fraud Categories:

- NFIB10 False Accounting
- NFIB1C Counterfeit Cashiers Cheques
- NFIB14 Fraudulent Applications for Grants from Government Funded Organisations
- NFIB16C Pension Liberation Fraud
- NFIB19 Fraud by Abuse of Position of Trust
- NFIB18 Fraud by Failing to Disclose Information
- NFIB1F Inheritance Fraud
- NFIB2B Pyramid or Ponzi Schemes
- NFIB2D Time Shares and Holiday Club Fraud
- NFIB3C Door to Door Sales and Bogus Tradesmen
- NFIB3F Ticket Fraud
- NFIB3G Retail Fraud
- NFIB7 Telecom Industry Fraud (Misuse of Contracts)
- NFIB8A Corporate Employee Fraud
- NFIB8B Corporate Procurement Fraud

DATA LIMITATIONS

1. The data represents all offences that have been **reported** to Action Fraud and subsequently **recorded**. It does not reflect offences which have occurred but have not been reported.

2. Some duplicates incidents may still be present owing to the victim reporting the fraud twice (usually when they have remembered further detail), or due to a second person reporting the same offence on their behalf. If a second entry is made, a new reference number is given and therefore records must be read to identify duplicates. Where possible these have been identified and removed, but this is a manual process some may have been missed due to human error.

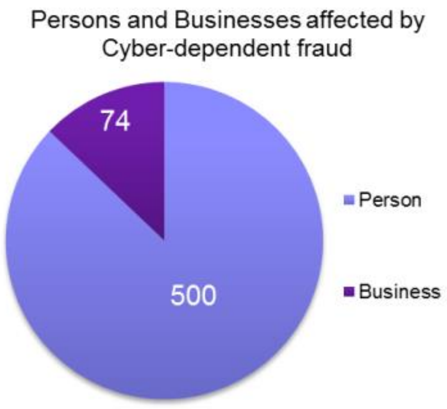
3. *There are no official 'cyber-enabled' or 'non-cyber' fraud categories, as such, 'cyber-enabled frauds' represent those which experts advise commonly include a cyber element and so figures quoted should be used as an indication only.

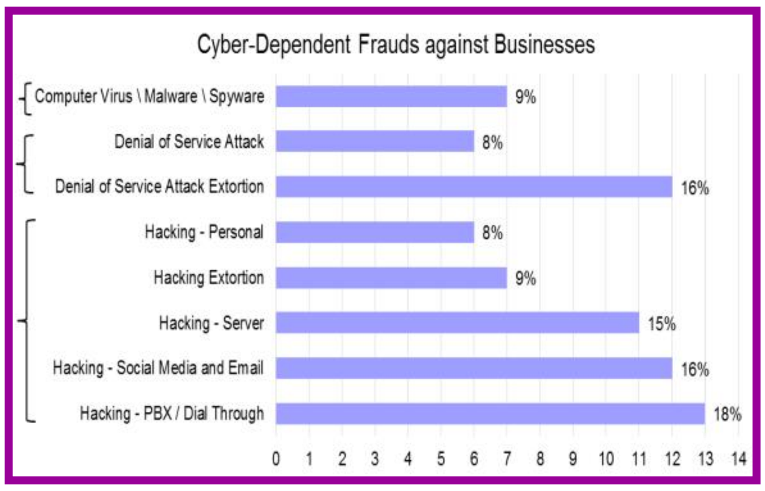
4. When analysing the cyber-dependent data, some inaccuracies in the recording of NFIB fraud categories were identified. A small number of random checks were subsequently carried out on some of the cyber-enabled and non-cyber NFIB types and the same was found that some were listed incorrectly. This therefore indicates that the data is only as good as the knowledge of the people logging the offences. Additionally, because the cyber status of the offence has been determined from the NFIB code, it is possible that the total number of offences quoted here may not be entirely accurate if said offences have been incorrectly listed as a fraud that would have been categorised in a different subset. As such the results shown here should be interpreted with caution.

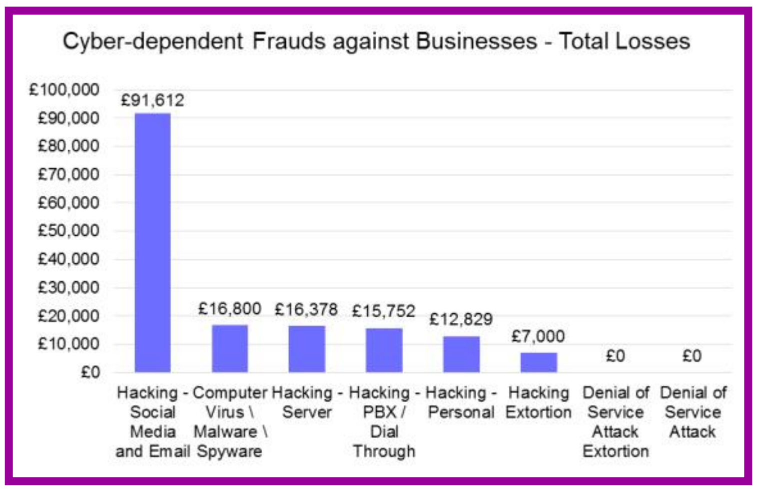
5. The data provided does not specify whether the victim was a business or an individual, so in order to provide this breakdown, where the victim name is in fact the name of a business, this has been captured. Additional key word searches have been conducted in an attempt to identify any businesses which could not be identified by the victim name, however, in lieu of reading every individual entry, some businesses may have been missed and so the figures presented should be used as an indication of businesses affected.

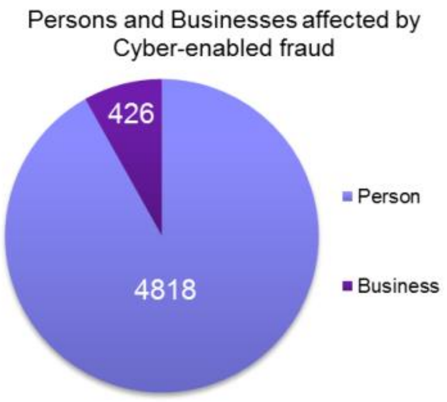
6. Total losses are calculated from the figures reported by the victim, however, in some cases these will be estimates. Occasionally losses have been entered even if the victim did not actually pay the requested amount to the suspect and so it may be advisable to read these as potential losses rather than actual losses.

Offences Against Businesses

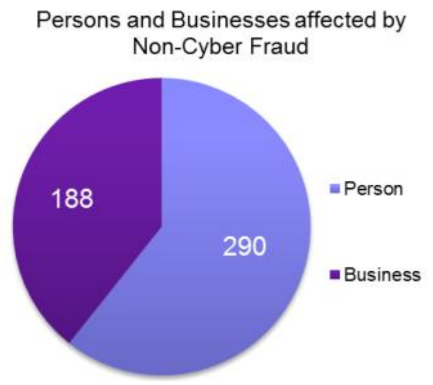






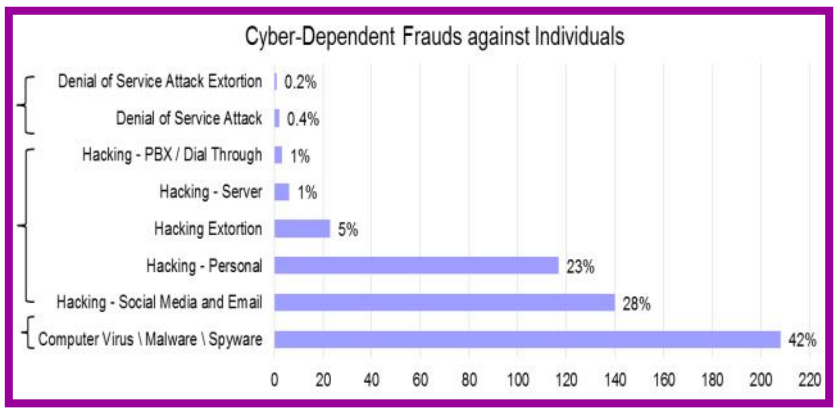


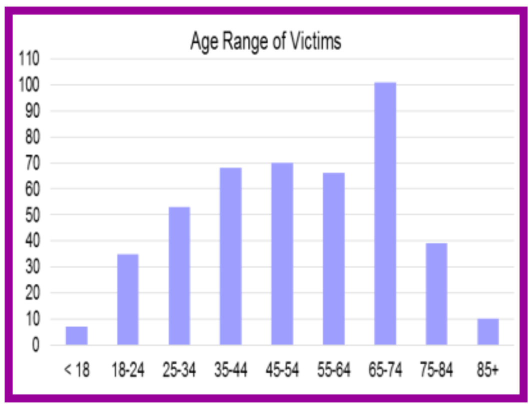
Fraud Category	Total	% of Total	No. of Businesses which Lost Money	% of Businesses who Lost Money	Total Losses
None of the Above	122	28.6%	73	59.8%	£870,206
Mandate Fraud	68	16.0%	34	50.0%	£570,472
Other Consumer Non Investment Fraud	60	14.1%	11	18.3%	£16,297
Other Advance Fee Frauds	50	11.7%	11	22.0%	£40,877
Cheque, Plastic Card and Online Bank Accounts (not PSP)	45	10.6%	12	26.7%	£77,498
Online Shopping and Auctions	37	8.7%	11	29.7%	£17,841
Computer Software Service Fraud	14	3.3%	0	0.0%	£0
Application Fraud (excluding Mortgages)	10	2.3%	5	50.0%	£35,310
Business Trading Fraud	5	1.2%	4	80.0%	£357,320
Charity Fraud	4	0.9%	2	50.0%	£38
Rental Fraud	3	0.7%	1	33.3%	£350
Other Regulatory Fraud	2	0.5%	1	50.0%	£40,000,000
Consumer Phone Fraud	2	0.5%	2	100.0%	£916
Insurance Related Fraud	2	0.5%	2	100.0%	£4,694
"419" Advance Fee Fraud	1	0.2%	1	100.0%	£6,733
Fraud Recovery	1	0.2%	1	100.0%	£745
Lender Loan Fraud	1	0.2%	1	100.0%	£345
Grand Total	**427**	**100.0%**	**171**	**40.0%**	**£41,991,472**

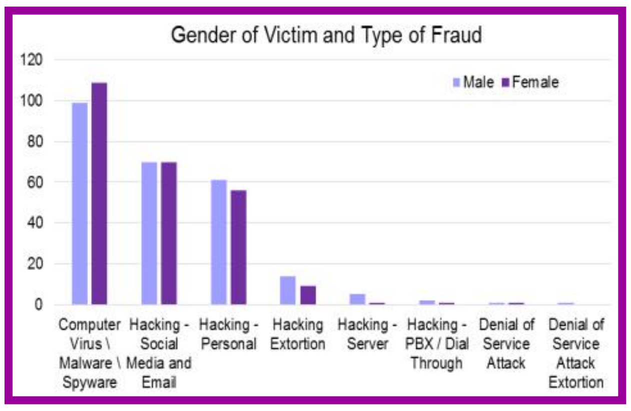


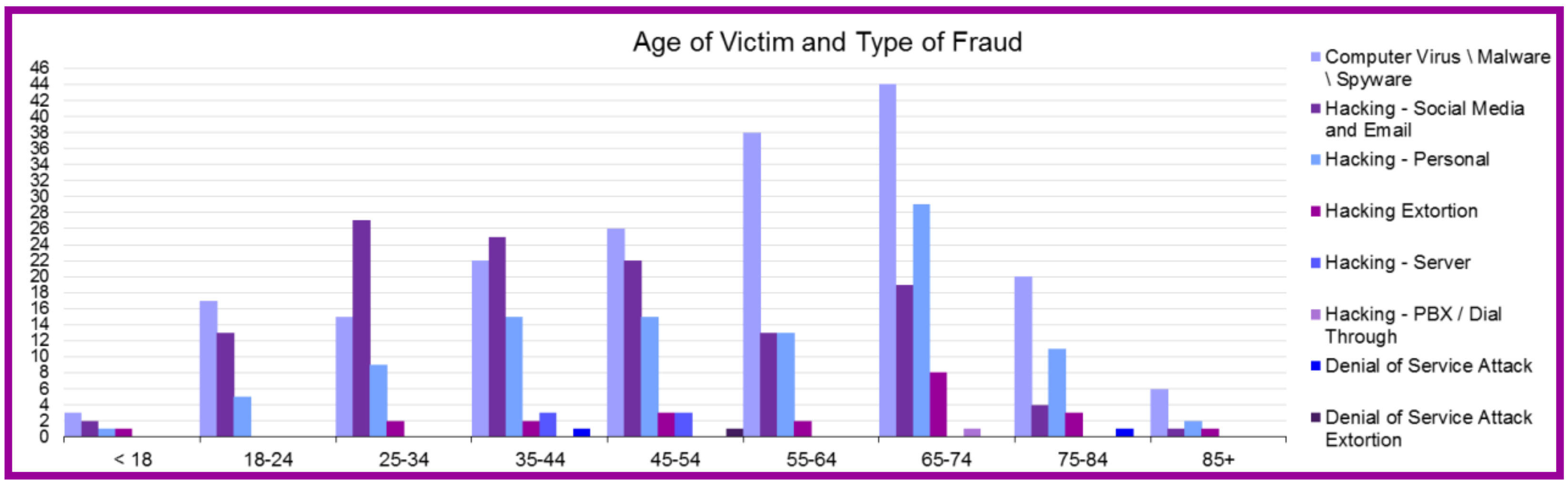
Fraud Category	Total	% of Total	No. of Victims Who Lost Money	% of Victims Who Lost Money	Total Losses
Retail Fraud	115	61%	101	87.8%	£113,868
Corporate Employee Fraud	23	12%	22	95.7%	£5,207,754
Counterfeit Cashiers Cheques	23	12%	0	0.0%	£0
Fraud by Abuse of Position of Trust	14	7%	8	57.1%	£247,780
Door to Door Sales and Bogus Tradesmen	7	4%	5	71.4%	£16,790
False Accounting	2	1%	2	100.0%	£136
Ticket Fraud	1	1%	1	100.0%	£125
Corporate Procurement Fraud	1	1%	1	100.0%	£55,000
Fraud by Failing to Disclose Information	1	1%	0	0.0%	£0
Fraudulent Applications for Grants from Government Funded Organisations	1	1%	1	100.0%	£5,000
Grand Total	**188**	**100%**	**141**	**75.0%**	**£5,646,453**

Offences Against Individuals - Cyber Dependent



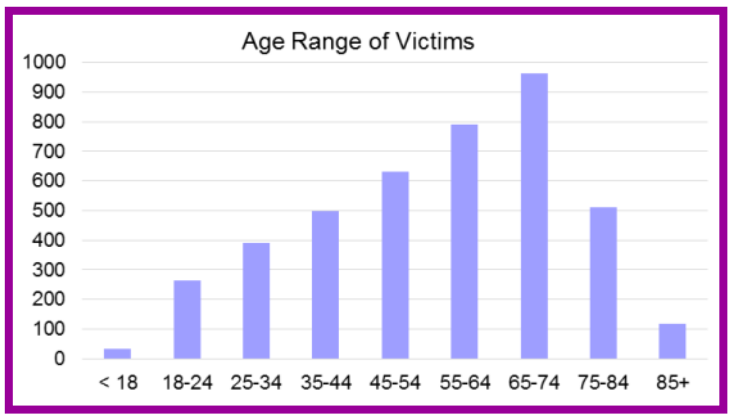


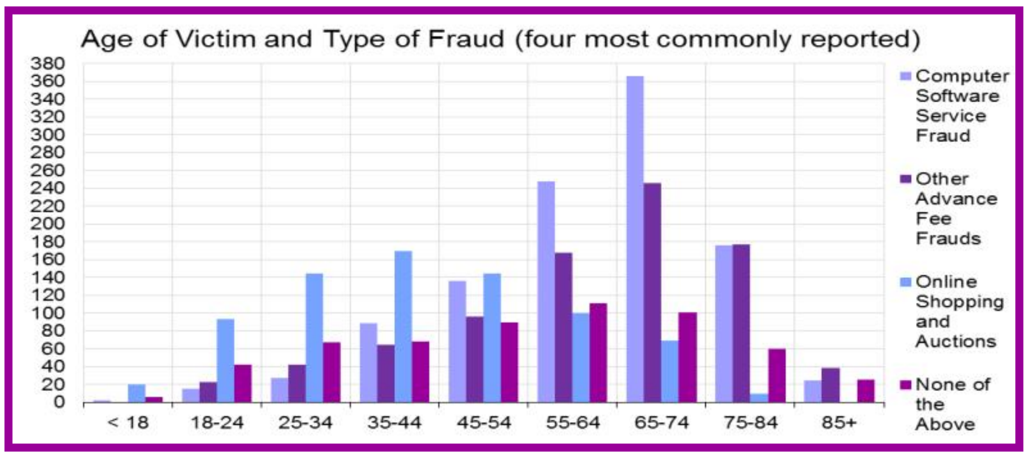


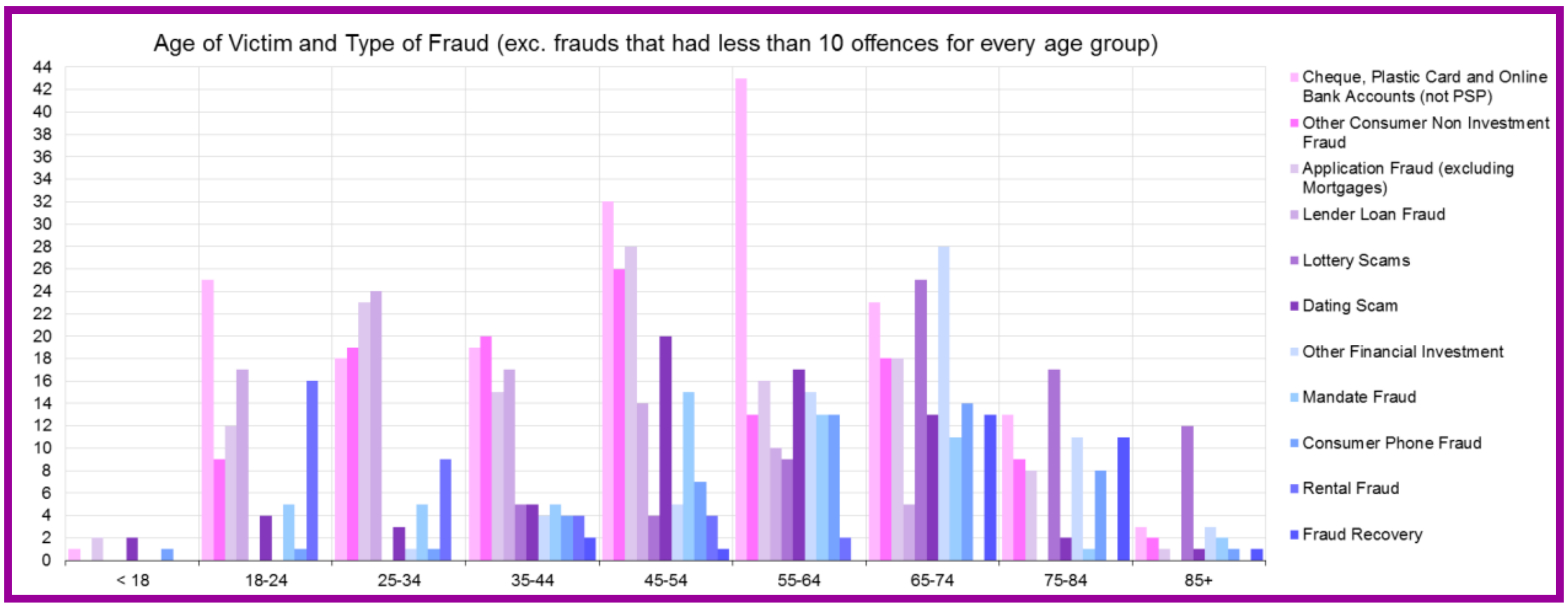


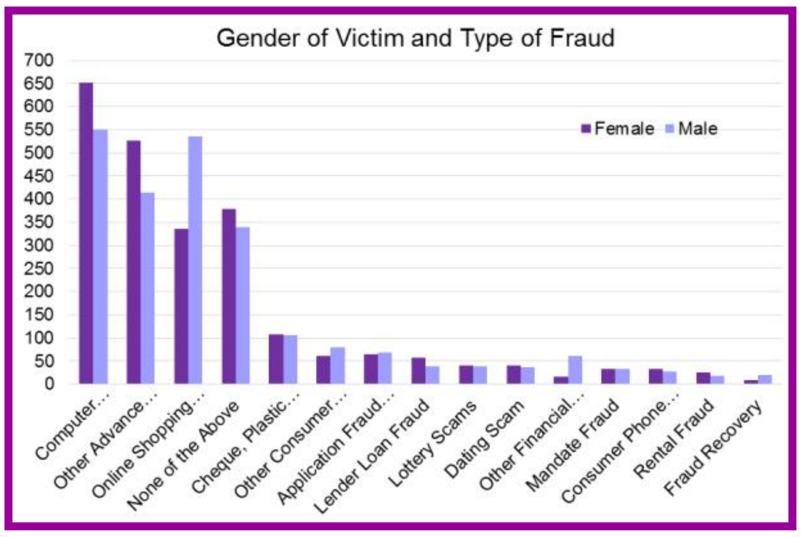
Offences Against Individuals - Cyber Enabled

Fraud Category	Total	% of Total	No. of people who lost money	% of people who lost money	Total Losses
Computer Software Service Fraud	1206	25.0%	259	21.5%	£551,587
Other Advance Fee Frauds	940	19.5%	183	19.5%	£1,199,299
Online Shopping and Auctions	871	18.1%	683	78.4%	£1,457,292
Cheque, Plastic Card and Online Bank Accounts (not PSP)	214	4.4%	143	66.8%	£347,946
Other Consumer Non Investment Fraud	139	2.9%	110	79.1%	£348,797
Application Fraud (excluding Mortgages)	135	2.8%	54	40.0%	£361,096
Lender Loan Fraud	95	2.0%	85	89.5%	£25,819
Lottery Scams	79	1.6%	22	27.8%	£841,579
Dating Scam	78	1.6%	57	73.1%	£488,108
Other Financial Investment	76	1.6%	63	82.9%	£1,562,859
Mandate Fraud	66	1.4%	46	69.7%	£233,929
Consumer Phone Fraud	62	1.3%	22	35.5%	£1,009
Rental Fraud	43	0.9%	27	62.8%	£22,106
Fraud Recovery	28	0.6%	12	42.9%	£36,532
Share sales or Boiler Room Fraud	16	0.3%	13	81.3%	£472,899
Other Regulatory Fraud	13	0.3%	6	46.2%	£2,562,191
Pension Fraud committed on Pensions	12	0.2%	6	50.0%	£517,143
"419" Advance Fee Fraud	10	0.2%	0	0.0%	£0
Charity Fraud	9	0.2%	6	66.7%	£1,586
HM Revenue & Customs Fraud (HMRC)	4	0.1%	0	0.0%	£0
Insurance Related Fraud	3	0.1%	0	0.0%	£0
Mortgage Related Fraud	1	0.0%	0	0.0%	£0

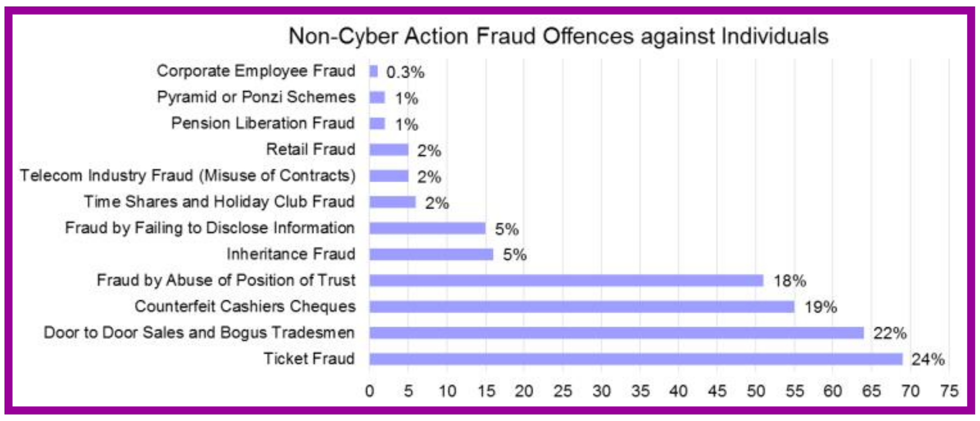


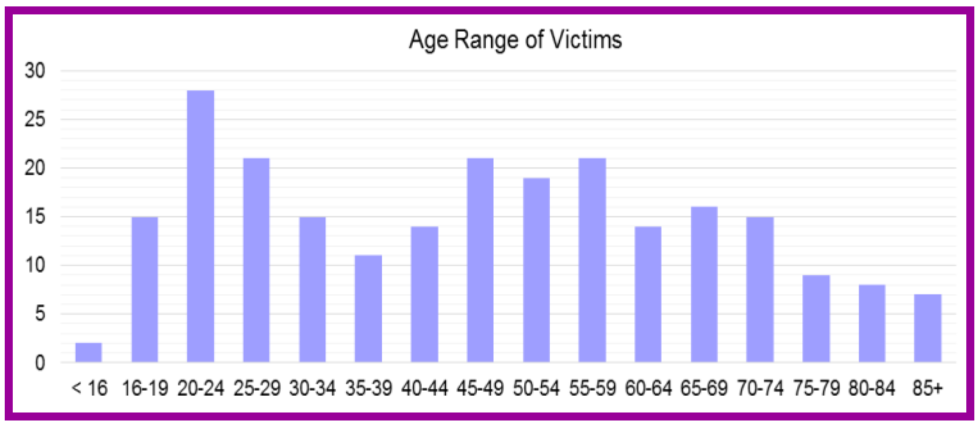


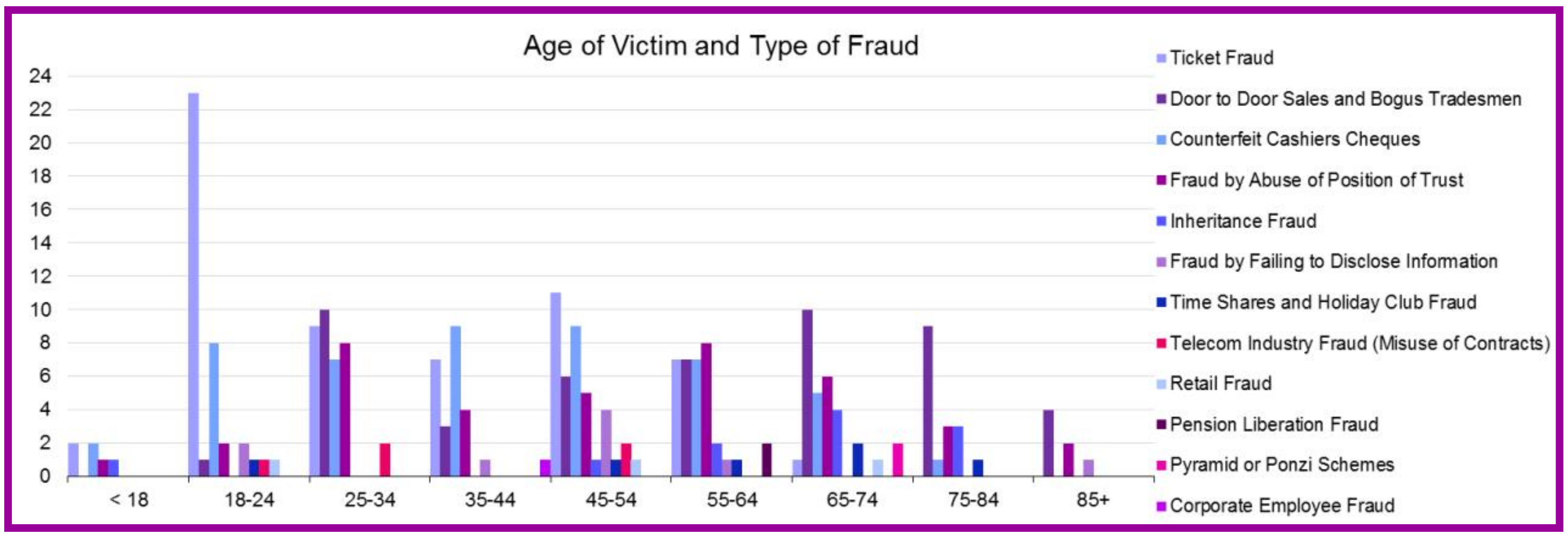


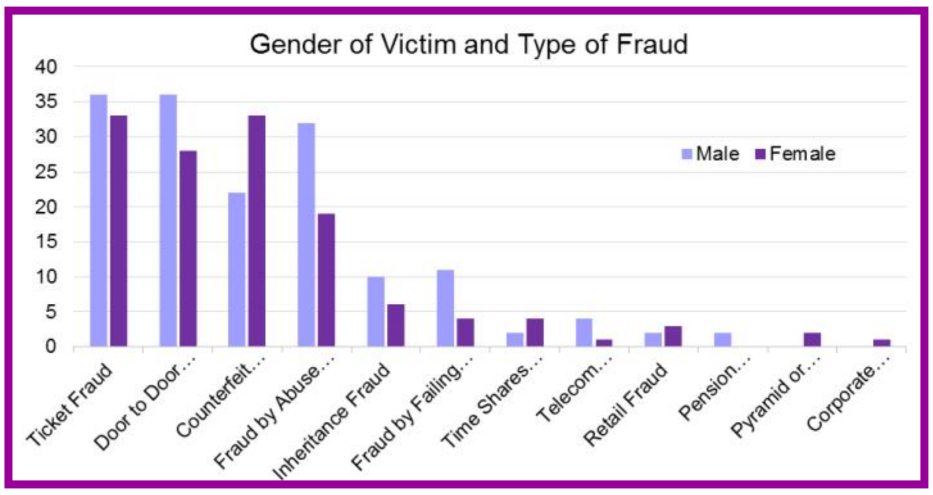


Offences Against Individuals - Other Fraud









APPENDIX 2

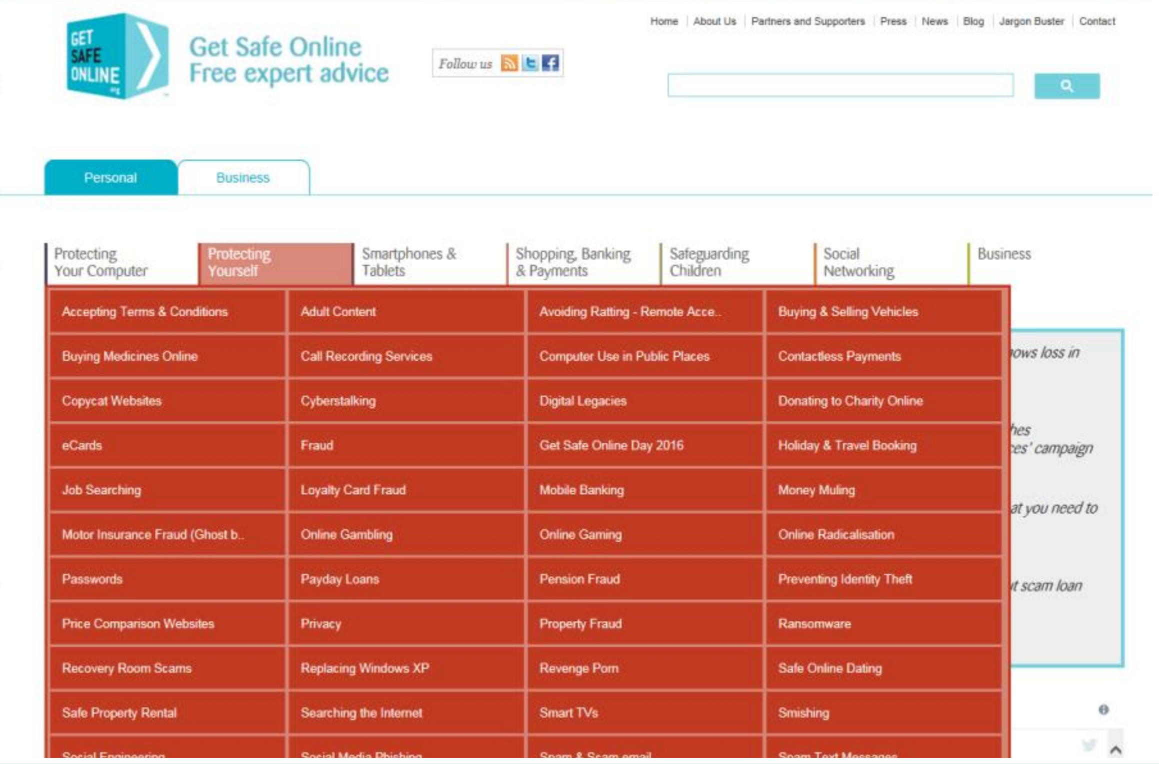
FURTHER DETAIL ON SOME OF THE RESOURCES IDENTIFIED

Get Safe Online

Get Safe Online (GSOL) is the UK's leading source of unbiased, factual and easy-to-understand information about online safety. The website is a unique resource providing free, practical, expert advice and downloadable resources and campaign material on a vast range of topics - from ransomware to identity fraud to online gaming to radicalisation - to protect yourself, your children, your technology and your business against from many problems encountered online. The site also offers up to date news, tips and stories from around the world.

GSOL is Cyber Essentials and IASME certified.

www.getsafeonline.org



Accepting Terms & Conditions	Adult Content	Avoiding Ratting - Remote Acce..	Buying & Selling Vehicles
Buying Medicines Online	Call Recording Services	Computer Use in Public Places	Contactless Payments
Copycat Websites	Cyberstalking	Digital Legacies	Donating to Charity Online
eCards	Fraud	Get Safe Online Day 2016	Holiday & Travel Booking
Job Searching	Loyalty Card Fraud	Mobile Banking	Money Muling
Motor Insurance Fraud (Ghost b..	Online Gambling	Online Gaming	Online Radicalisation
Passwords	Payday Loans	Pension Fraud	Preventing Identity Theft
Price Comparison Websites	Privacy	Property Fraud	Ransomware
Recovery Room Scams	Replacing Windows XP	Revenge Porn	Safe Online Dating
Safe Property Rental	Searching the Internet	Smart TVs	Smishing
Social Engineering	Social Media Phishing	Spam & Scam email	Spam Text Messages

Cyber Essentials

Cyber Essentials is a Government -backed and industry supported scheme to guide businesses in protecting themselves against cyber threats. The scheme was developed to show organisations how to protect themselves against low-level "commodity threat". It lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organisations should have in place. The vast majority of cyber attacks use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the Internet which enable even low-skill actors to exploit these vulnerabilities. Properly implementing the Cyber Essentials scheme will protect against the vast majority of common internet threats.

'*Last year, the average cost of breaches to large businesses was £36,500. For small firms the average cost of breaches was £3,100. 65% of large organisations reported they had suffered an information security breach in the past year, and 25% of these experienced a breach at least once a month. Nearly seven out of ten attacks involved viruses, spyware or malware that might have been prevented using the Government's Cyber Essentials scheme*' *(2016 Government Cyber Health Check and Cyber Security Breaches Survey, HM Government, 2016).*

Cyber essential documents are free to download from the website. Any organisation can use the guidance to implement essential security controls. Also available is a self-assessment questionnaire to assess how cyber-secure a business actually is.

The Cyber Essentials badge allows your organisation to advertise that it meets a Government-endorsed standard.

www.cyberessentials.ncsc.gov.uk

South West Cyber Security Cluster

The SWCSC is a not for profit collaboration raising cyber security awareness and best practice in the South West.

The Cluster is a formal group of cyber secure businesses who help victims. Representatives of businesses give their time and learn from each other to create awareness and offer support in regard to cyber related issues.

The Cluster is led by a steering group to which Devon and Cornwall Police (DCP) have a position.

Details of events, conferences and training days can be found at the websites.

The Digital Capabilities Unit within DCP can refer victims to the Cluster for free advice and support to help following an incident and to protect them in future. Continuous support services can are also available for businesses at a charge.

https://southwestcsc.org