Hampshire Police and Crime Panel
'Cybercrime – Cyber-enabled Fraud' Proactive Scrutiny - Evidence

Contents:

Boldre Parish Council

To be honest this isn't something I've really seen any action from the police on or experienced myself. I've never seen anything from the Hampshire PCC on this subject, but a quick google gives a link to https://www.actionfraud.police.uk which seems pretty accessible.

I guess possible improvements could be on the Hants PCC site which doesn't have any quick links etc. to report issues. I've not seen any communication as a private individual on this subject from the PCC so I can't say that engagement with residents is good. I guess priorities should be education around our older residents who may be particularly susceptible to this sort of fraud if you believe what you see in the news. I don't know that there would be many criminals in Hampshire to pursue, so I guess that the request is to ensure that any issues found locally are past back to a central authority.

My views are that while the PCC is a very important part of our society locally it is the Neighbourhood Watch that is read and listened to by a lot of locals on matters of safety. I have a large email list of participants.

I do get a lot about scams through the Hampshire Alert system and where appropriate I pass on. Also note my last NW email in which I added my own warnings to help the elderly in particular.

I would go so far as to say that the Hampshire Alert system concentrates on this subject to the detriment of others. We have, as you know had two substantial break ins in our area recently and I was sent nothing by the Police authorities on either. Similarly when our village shop was broken into I was sent nothing. Probably because of the disastrous mess the Police made of apprehending the culprits. Embarrassed police? If the NW co-ordinator is sent nothing about the local shop being broken into then.....

If it was not for the very positive feedback I get from members of our NW I would either close it down or hand over running it to someone else. Gone are the days where we had a local policeman or at least one who would contact me with pertinent matters. I do realise manpower is short in the Police Force but it is a pity they cannot at least use the system they have set up to a good advantage

East Cowes Town Council

- *How well has the PCC, through holding the Chief Constable to account, ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud?*

REPONSE: East Cowes Town Council has had no information or correspondence regarding this question/subject from any source.

- *How effective have the PCC and his office been in engaging with appropriate partners to ensure a joined-up approach to identifying and tackling cyber enabled fraud?*

REPONSE: East Cowes Town Council has had no information or correspondence regarding this question/subject from any source.

- *What efforts have been made by the PCC to educate and inform the residents of Hampshire and the Isle of Wight to recognise and protect themselves from cyber-enabled fraud?*

REPONSE: East Cowes Town Council has had no information or correspondence regarding this question/subject, the closest answer would be some stickers regarding being careful of answering the door or phone but nothing regarding cyber-crime.

- *What are the key priorities which need to be considered by the PCC to reduce the threat posed to the residents of Hampshire and the Isle of Wight through cyber-enabled fraud?*

REPONSE: East Cowes Town Council cannot answer this question due to lack of information and/or correspondence on the subject.

- *What best practice exists which could also be considered by the PCC in his approach to preventing and tackling cyber-enabled fraud?*

REPONSE: City of London Police have a cyber-crime email site to send spam/suspicious emails; PCC could research this model and see if it could be replicated to help the situation in the Hants/IW area (and/or joining with other areas of South Coast). Also issuing public information to APPROPRIATE sources (social media, local radio & press) where the population will see it. Better responsibility by those institutions which are causing the rise in cyber-crime to combat it and invest in the public information.

Ecchinswell Sydmonton and Bishops Green Parish Council

3) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

I looked at all the newsletters and information from Hampshire and BDBC over 2016. I found nothing relating to cyber-fraud in any of the things that have been distributed via the clerk ('Safer North Hampshire' and 'Basingstoke and Deane Today').

A number of years ago I signed up for Hampshire Alerts because of information that ES&BG PC had passed on via the local neighbourhood watch coordinator. In the publication Rural Times (linked to the neighbourhood watch scheme there is always a column from the PCC and in the Summer 2017 and Autumn 2017 issues there were articlaes about cybercrime and some useful links to other websites. The autumn issue mentions a Cyber Protect Team – whose **"mission is to stop cybercrime from happening through education and engagement"**. There is no reference to this team on the HCC or Hampshire Constabulary websites. The Hampshire Constabulary website home page shows no links to cybercrime. Cybercrime is, however, mentioned within other sections of the website. Using the search facility does provide some useful information about cybercrime but does not mention the special team at all. After this research I would conclude that the PCC has not engaged well with residents via local government channels.

Possible improvements could include:
Making cybercrime a focus on the home page of the constabulary website
Giving the Cyber Project Team (if it really exists) a higher profile in the county
Including information on cybercrime issues in the publications sent to PC's – 'Safer North Hampshire' and 'Basingstoke and Deane Today'
Encouraging PCs to spread information within parishes using websites and newsletters. The first thing we have heard about this focus is when asked for feedback.

2) *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

Get the message into homes using as many media types as possible, TV, radio, police websites and publications, local government websites and publications.

Greyshott Parish Council

1) *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

   Speaking on behalf of an IT business serving many homes and businesses located within Hampshire I do think that more resource and time needs to be allocated to enable the PCC to be able to communicate and educate individuals, families and business owners as to the threats posed by cyber-attacks. I have sat in on two Hampshire based school sessions designed to educate parents and their older siblings as to the threats that are out there. These sessions outlined the risks but no enough was explained about prevention and steps to take to keep individuals safe.

2) *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

   We haven't to date received communication directly from the PCC.

3) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

   None of our residential customers have ever been contacted by the PCC to our knowledge.

4) *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

   National TV and radio advertisements could be run to raise initial awareness and to direct the population to helpful resources. Also billboard advertising is affective along with using social media tactics such as Facebook / Twitter.

5) *Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?*

   End user education is the first thing to address as most often Cyber Crime is made possible due to a human action such as clicking on an email link. Good

strong antivirus / internet security is the next item to implement. We've learned that Cyber Crime seldom occurs unless the victim makes a mistake such as leaving a digital door open. Strong password policies are critical in this day and age as well as ensuring that common passwords are not used repeatedly on multiple platforms.

6) *Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?*

Using the NHS security breach as an example. I am aware of two hospitals of which the ground staff never received a briefing before, after or during the Cyber Attack which encrypted much of the NHS data and rendered some of its services useless. Increased budgets must be allocated to IT systems and in particular IT security. Old unpatched systems, poor security software, unreliable backups and uneducated computer users make it an easier job for digital intruders / hackers to gain access to valuable data.

Hampshire and Isle of Wight Neighbourhood Watch (HINWA)

[Name] has asked me to send you our HINWA response to the PCC's survey concerning cyber crime and cyber related fraud. Please find this attached together with a collaborative project which has enabled me to work alongside Hampshire Constabulary colleagues over the past two years,

There is much to achieve to inform and safeguard our communities to become much more resilient to the recent change in the crime landscape because of cyber crime. We wish our county to be proactive and I hope very much that the two documents attached will evidence the concern and focus which NW has brought to this agenda.

We hope very much to work also with the PCC and his team to address the issues raised.

Thankyou for the opportunity to share our concerns and hopes.

I remain available should there be a need to clarify the two attachments. I also met with [Officer Name] at a Netley related meeting last week and she and I have already arranged to meet at the OPCC on 4th January. I hope this heralds an effective collaboration with you all on all things related to cyber crime.

HINWA Response to the Hampshire Police and Crime Panel's scrutiny of Cybercrime – Cyber-Enabled fraud.

December 2017

Context and response to the change in the crime landscape:

For the last 3 years Hampshire and Isle of Wight Neighbourhood Watch Association (HINWA) has prioritised raising concern about the growing frequency of all types of related crime. With the encouragement and support of available personnel and resources Hampshire Constabulary has recognised the rapid increase and complexity of cyber related crimes and encouraged a collaborative approach.

Achievements to date include:

1. Participation in the CyberCrime Prevent and Protect Working Group;
2. Submission and acceptance by the DCC and ACC Ben Snuggs of a collaborative proposal; (copy attached)
3. Establishment of a small but expert group of NW members to focus on relevant issues; This group proposed the recent recommendation to the PCC regarding development of a joint initiative to provide RFI covers for smart cards.
4. Close collaboration with a named cyber crime prevention member of the Constabulary to ensure effective participation from initial stages of planning of cyber related projects;
5. Liaison with the Special Constabulary cyber crime related expertise;

6. Promotion of ‘Get Safe on Line’ and ‘Friends Against Scams’ materials to all NW schemes and their residents;
7. Working with Safer Neighbourhood Teams where cyber related fraud becomes an issue.
8. Successful request to develop a specific RFI cover for smart cards with the PCC to include PCC, Constabulary and NW logo’s to demonstrate a shared commitment by all to tackle cyber related crime. This to act as a face to face ‘talking point’ to raise public awareness.

Specific response to the proactive scrutiny:

1. NW respects the huge disadvantage Hampshire Constabulary has because of unreasonable budget cuts both current and intended. We have offered support at every level because the lack of expertise at local level, poor quality and outdated computer equipment and availability of police colleagues to work with us. At best the constabulary is reactive rather than proactive.
Our involvement with police colleagues is at a strategic and developmental level. We would wish also to be strategic partners with the PCC in the near future.
However a local, robust constabulary response is very necessary given the frequency, variety and complexity of frauds and cyber related crime so that within budget constraints the local level of constabulary expertise should match the level of threat posed.

2. Unfortunately HINWA feel they have neither been informed nor valued as a partner/collaborator thus far in developing strategy and projects to combat cyber related crime with the OPCC despite NW representing a huge proportion of residents across our two counties. This is a missed opportunity and we trust that both the recent development of the smart card protector project and this scrutiny will address this short-coming.

3. We unfortunately feel there has been a lack of available crime prevention material on the PCC website and are pleased that recently this is being addressed. We applaud the recent promotion of raising awareness of children and students using the Youth Commission.

4. HINWA emphasises the need for collaborative partnership working to ensure effective and smart use of all possible expertise. Cyber crime is developing so rapidly and our response should not be ‘delivered’ to residents by the PCC nor the Constabulary but rather a collaboration of all to raise awareness and make our communities more resilient. We
recommend a **‘togetherness’** approach for increased success of outcomes.

We wish to raise an immediate need to **redefine the notion of ‘vulnerability’**. Our Constabulary, Fire and Rescue Service and the PCC focus – as does

Neighbourhood Watch at county level – on our most vulnerable residents. However, as raised at the recent CyberCrime Prevent and Protect Working Group, there is a VERY different range of residents across our county who are vulnerable and are unaware and exposed to this new area of intrusive and often costly crime type.

5. As best practice we recommend using the focus group members who have volunteered their interest and professional expertise and working collaboratively at all levels of strategy and project development with members of HINWA who are so representative of both communities and those being targeted. **Crime Prevention and raising awareness in clear un-embedded messages is key.**

   We also wish to expand on the recent smart card cover project as a demonstration that **together** the PCC, Hampshire Constabulary and Neighbourhood Watch are determined to raise awareness and reduce opportunities of cyber related crime and fraud.

Research proposal to support the Digital Investigation and Intelligence

(cyber crime) initiative of Hampshire Constabulary: July 2016

The context:

It is my privilege as 'critical friend' and supporter of Hampshire Constabulary to maximise the strategic benefits of effective collaboration. The crime landscape has drastically changed. Cyber crime of all types is a serious matter of concern to residents and although we as Neighbourhood Watch can look for guidance and support from Trading Standards and Action Fraud there is currently little available from our constabulary at a local force level to help prevent and protect our communities.

'Think Digital' the NPCC College of Policing document (April 2015) encouraged local constabularies to urgently ensure strategic development of DII resources and response. It recommended 'sustainable innovation' by inviting collaboration to create an 'innovative ecosystem' to better respond to the current cyber challenges of risk, relevance and austerity.

The Home Office 'Modern Crime Prevention Strategy (March 2016) in recommendations to design out opportunities for offending off-line and on-line, emphasised the importance of a strong evidence based approach to crime prevention. Neighbourhood Watch provides a unique way of approaching, informing and therefore strengthening communities – making them more resilient to crime – through its extensive network across Hampshire and the Isle of Wight. The HO document recognises the value of crime prevention and has placed great emphasis on it. Together we can exploit Neighbourhood Policing as best practice!

As President of Hampshire and Isle of Wight Neighbourhood Watch Association I am

being made aware of real concerns over the unavailability of a local police response to the growing intrusion and extent of cyber crime. These include doubt that the majority of cyber crime incidents are reported. At a local level NW receives excellent incident reports about current local crimes but cyber crime does not figure in these updates. Is it being recorded? Police officers have also shared concern with me privately that there is no evidence trail of cyber crime. A strong evidence base can support appropriateness of strategic development, direction and resources but this would appear to be completely unavailable currently. If it were in place it would provide strong support for the need for extra resources, both human, digital and to develop crime prevention materials to ensure communities are kept safe from this change in the criminal landscape.

The 'tip of the iceberg' – the traditional accepted crime types of burglary, car crime, anti-social behaviour etc – are completely overshadowed by the growth in cyber crime which daily affects many more Hampshire and Isle of Wight residents. Members of NW have commented that this lack of ability to respond by Hampshire Constabulary is its current 'Achilles heel'!

How to support an 'outstanding' response for Hampshire Constabulary:

To support the current DII initiative by Hampshire Constabulary using the Prevent,

1.Protect, Pursue and Prepare (4P approach) this proposal aims to focus on collaboration with
residents of Hampshire communities and police officers to exploit the 'innovative ecosystem' mentioned above. It aims to address the following current weaknesses in availability of an appropriate police response to cyber crime at a local force level and evidence Hampshire Constabulary as a 'flagship' of excellent practice:

- To explore the model 'Appreciative Enquiry' to engage and maximise the benefits of collaboration to ensure a dynamic, appropriate innovative collective response to cyber crime within the 4P model.

- To urgently develop a reporting system, to include a variety of platforms, to enable a reliable evidence based audit of the amount, type and extent of cyber crime;

- To identify those residents most vulnerable to various types of cyber crime and intrusion into their private lives to help focus the production of appropriate crime prevention materials emphasising clear advice set within limited, appropriate text...not text embedded so that the messages are 'buried'

How?

Through consultation with officer leads within the force to develop with urgency a reporting platform for cyber crimes to enable an evidence based response to future development and also to inform and support future consideration for increased government and local funding to support increased expertise, digital resources, training and the development of crime prevention materials.

It will be important for collaboration at every stage of the current DII project to provide views and suggestions from a wide base of members of our communities and of the constabulary. This will undoubtedly not only affect the dimensions and direction of a local police response to cyber crime but evidence the ‘innovation’ invited through consultation and collaboration. Trust and Confidence in the constabulary will be enhanced within the force and those it seeks to serve.

A survey will be produced to capture opinions and suggestions, Interviews will take place to elicit further views. Where appropriate victims of cyber crimes will be asked confidentially to share their experiences to help build a landscape of actual examples across the two counties.

It will be important to discuss ‘vulnerability’ and to establish those ‘most vulnerable’ to various types of cyber crime to help develop and target appropriate crime prevention advice, materials and support the current constabulary and NW focus on this vital factor.

Hampshire Constabulary

1) *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

The engagement Digital Intelligence and Investigation Strategy that has been created within the Force provided a framework and a series of key milestones for the Force to move forward, whilst this encompasses more than just cyber-enabled fraud it provides a core element. The PCC has been supportive of tackling cyber enabled offences. The creation of the Digital Investigation Team (DIT) is taking place presently. This will consist in a team of a Detective Sergeant and four police officer investigators dedicated to dealing with digital / cyber crime. Whilst this will not be exclusively cyber related fraud it will include certain offences such as ransomware and will be able to provide technical advice to other officers and staff investigative cyber enabled fraud. The DIT will be operational in the first quarter of 2018. The PCC has been very supportive around the DIT.

The speed at which the landscape changes within the digital world creates a challenge for Constabularies and how to equip officers and staff with the knowledge, skills and abilities together with adapting procedures to respond or alter the public to the dangers remains a test. Given that traditional forms of training are unlikely to be able to keep place considerations as to how officers and staff can access trusted information when required.

The final quarter of 2017 has raise in the public perception around the issue of cryptocurrency; specialist understanding regarding intelligence and investigative response is an area for improvement. This is an unpredictable and unconventional, data rich environment that together with the block chain will become embedded in future investigation requirements and achieving a mature level of understanding. This is an area moving into 2018 that will require improvement.

3) *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

I am unable to answer this question.

4) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

Engagement via the PCC with the residents of Hampshire has been through the Cyber Protect team and also through Corporate Communications.

The Cyber Protect team consisting of a detective Sergeant and a staff member have engaged at 50 presentations during 2017. These include traditionally harder to reach groups including older people's groups, Small Medium Enterprises, education staff, charities, legal sector, farming community, neighbourhood watch groups, National Air Traffic Services (NATS), events with Chambers of Commerce and Parish Councils. Cyber enabled fraud has formed part of these events.

Fraud by email

Our Economic Crime Unit, cyber protect team and Corporate Communications Department worked closely with partner agencies and individual professionals from the private and education sectors in responding to a priority problem identified by local businesses. This issue was how to prevent the most frequent types of fraud committed by email against small to medium-sized businesses. Our creative hub team within the Corporate Communications Department produced a wide range of artistic concepts for consultation and consideration with representatives from our Safer Hampshire Business Partnership and Cyber Crime Prevent & Protect partnership group. Experiences and opinions from the business community guided the focus and style of our advice to help strengthen the precautions taken by businesses to protect themselves and their employees from fraud by email. A selection of fraud by email prevention messages presented in a range of formats was delivered to leading members of our Safer Hampshire Business Partnership in time for World Safer Internet Day in February 2017.

Sextortion (online blackmail)

Lead by DCI Gelman the Force have created and implemented a communications campaign aimed at increasing general public awareness of sextortion, specifically among young men aged between 17 and 23, a vulnerable victim group identified by police analysis in 2016. The design and delivery of this campaign was conducted in consultation with professional colleagues belonging to the Cyber Crime Prevent & Protect partnership group, and students from a local college in Eastleigh. Internal communications were produced first to ensure colleagues in Contact Management had received updated briefings about the level of service being provided to victims and potential victims of sextortion. Methods include targeted advertising of our prevention, protection & reporting advice through social media, namely

YouTube, Facebook and Twitter. In November 2016, police campaign messages with the hashtag #sextortion made 238,000 impressions on Twitter, and a media release generated positive national and local news coverage in partnership with the National Crime Agency (NCA). Victim call back surveys in 2017 by Contact Management identified 11 victims who gave positive feedback. Five (5) victims gave suggestions on how we could improve the service. Further evaluation is planned. A Digital Audio Exchange (DAX) advert with the Global Radio group was listened to 214,526 times by 27,737 unique users with a Listen Through Rate (LTR) of 96.6%. A visual banner ad received 6,653 impressions with 85 clicks making a Click Through Rate (CTR) of 1.28% to a page on the force website where advice for victims is available to read and download.

Ransomware

The Force supported Operation Cunan, the co-ordinated response to the WannaCry Ransomware attack in May 2017 with advice produced for our strategic stakeholders within the Safer Hampshire Business Partnership.

Support for national initiatives

The Forces Cyber Protect team and Corporate Communications Department have shown regular and consistent support for national initiatives from partner agencies including the City of London Police, Action Fraud, the Take Five campaign, and Get Safe Online. Messages with fraud prevention advice were shared via our social media channels, and distributed directly to key stakeholders and partner agencies that form our Safer Hampshire Business Partnership.

5) What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?

Raising awareness as to the dangers and pitfalls that business and the public can fall victim to represents the opportunity of having the greatest impact. Action Fraud is the recognised gateway for reporting offences and Internet Crime. A National relaunch with a reconstructed dashboard is being due to commence in March 2018, which should improve the experience of reporting fraud and allow victims to see how their reports are being dealt with. The changing of the recording process might lead to an increase to cyber related offences. Presently Cyber-related fraud and internet crime are not prioritised within the current Force Control Strategy

Protect message

6) Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?

Hampshire were the first Force in South East region to have a 24/7 Digital Medium Investigators (DMIs) response. This has meant that there is a call out capability for senior investigating officers (SIOs) to have the availability of a tactical advisor about retrieval of digital / cyber information to assist with major investigations.

Romance fraud

The work to strengthen the service provided for victims of romance fraud received recognition from policing peers nationally in 2017. DCI Gelman, DS Dring, Sarah Cohen and Duncan Smith were nominated for an 'Innovation Award' at the Excellence in Fraud Policing Awards, which took place during the Serious and Organised Crime Exchange (SOCEX) Financial Crime Conference in Nottingham on Tuesday 21 November 2017. The runner-up award, sponsored by the City of London Police was devised to reflect the achievements of individuals and teams who have made outstanding, innovative contributions to fraud policing. We submitted an entry to highlight the work and dedication of our Economic Crime Unit officers, Cyber Protect colleagues, Crime Prevention Advisor Sarah Cohen, and the Force's Corporate Communications Department in supporting a woman who bravely shared her personal experience of a prolonged romance fraud. The victim, who is known as 'Jenny', out of respect of her wish to remain anonymous, took part in a film reconstruction of the fraud events that led her to losing a substantial sum of money. She was also drawn into laundering other people's money for a 'man' she thought loved her throughout the online relationship. The film was released as part of a communications campaign, along with advice on how to identify and avoid romance fraud for Valentine's Day this year. BBC South Today's website featured the video and was seen by over 36,000 people, and the story featured second on their evening news programme. The film can be viewed on the Force's YouTube channel which features Jenny's experience. The focus on helping victims after a reported fraud also formed a crucial part of the entry.

In March 2018 the PCC office is backing a campaign to further push Op Signature to the public, and this will feature crimes which are regularly committed against the vulnerable and elderly, these being doorstep crime, telephone and mail enabled fraud, and cyber enabled fraud.

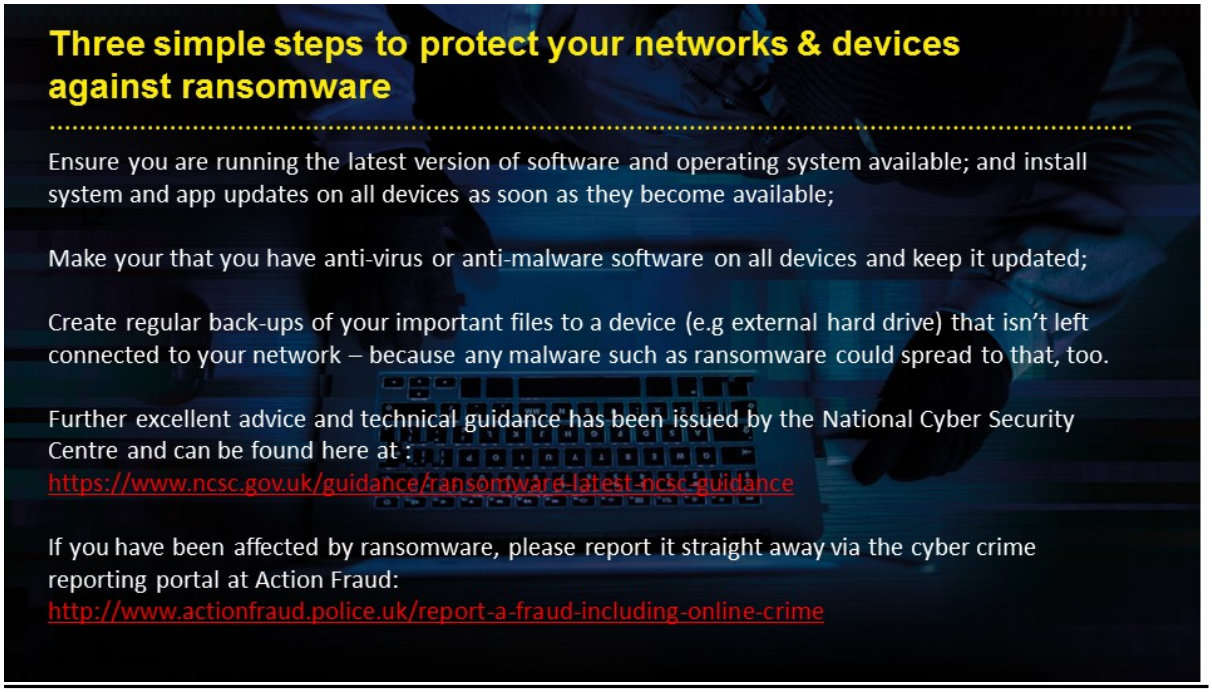
Cyber Specials Cyber Volunteers (CSCV)

Hampshire together with Gloucestershire have been nationally pioneering the concept of Cyber Specials Cyber Volunteers (CSCV). Working together with

academia and commercial business identifying people with digital / cyber skills to assist the Force. Initially created by Chief Specials Officer Tom Haye, CSCVs provide technical support and problem solving for the Investigation Command, Digital Media Investigations, Economic Crime, Internet Child Abuse, Force Intelligence and Digital Forensics. There have been a number of successful deployments with the CSCV in 2017 and they have been able to assist with the progression of investigations.

Operation Signature and the Banking Protocol

Traditional types of fraud are still being committed however there have been instances of initiation and identification of vulnerable people whilst it might not be considered in the Operation Signature which is the force campaign to identify and support vulnerable victims of fraud within Hampshire. Operation Signature was introduced in 2016 with the purpose of supporting people vulnerable to fraudsters in our communities. Increasingly fraud is becoming more complex and deceptive, much of which is targeted at vulnerable people, therefore raising awareness and education around cyber enabled to reduce the number of victims is paramount. DS Sarah Dring has been instrumental with the adoption of Op Signature from Sussex and adapting it so that it is bespoke for Hampshire. Additionally Hampshire has been an early adopter for the Banking Protocol, which links in with the banking industries Know Your Customer (KYC).



Regular fraud prevention comms

Please find below a recap of a summary of Corporate Comms in 2017 regarding Cyber enabled fraud:-

January 2017

Advice issued on PPI scam:

http://www.highfieldresidents.org.uk/new-scam-alert-issued-to-hampshire-residents-09117/

Internal communications published regarding two alerts from the NFIB & a feedback survey from the City of London Police:

http://intranet/Intranet/News/Cyber+fraud+alerts+affecting+Hampshire.htm

February 2017

Dating scam advice issued:

https://www.964eagle.co.uk/news/local-news/2214666/advice-given-after-hampshire-dating-website-scams/

Man sentenced for fraud offences:

https://www.facebook.com/HantsPolice/posts/10154879728626341

Rogue traders warning in Portsmouth (plus update including notification of arrest and charge):

http://www.portsmouth.co.uk/news/crime/update-bogus-builders-dupe-portsmouth-woman-79-out-of-1-000-1-7828220

Courier fraud scam in Bordon:

https://www.hampshirealert.co.uk/da/171490/Please_be_aware_of_latest_telephone_scam.html

Dating fraud prevention film and advice for Valentine's Day:

Hampshire Constabulary YouTube film:
https://www.youtube.com/watch?v=G3uDrNG_SAc

Coverage of accompanying media release:

BBC Online: http://www.bbc.co.uk/news/uk-england-hampshire-38959329

The Eagle radio station: https://www.964eagle.co.uk/news/local-news/2225828/warning-issued-for-people-in-hampshire-who-use-dating-websites/

The Eagle radio station: https://www.964eagle.co.uk/news/local-news/2222968/hampshire-online-dating-fraud-victim-loses-more-than-20000/

Southern Daily Echo:
http://www.dailyecho.co.uk/news/15090846.WATCH__Hampshire_woman_reveals_heartache_over___20_000_dating_site_scam/

On The Wight: https://onthewight.com/police-warning-about-online-dating-and-romance-fraud/

March 2017:

Southampton man jailed after defrauding women:

https://www.hampshire.police.uk/news/general/southampton-man-jailed-after-defrauding-two-vulnerable-elderly-women-out-hundreds-pf-thousands-pounds/

Internal communications published in support of our @HCCyberProtect Twitter account going live:

http://intranet/Intranet/News/Help+protect+our+local+businesses+from+cyber+criminals.htm

April 2017:

Rogue trader Mark Kempster ordered to pay back £16,692:

https://www.hampshire.police.uk/news/general/rogue-trader-ordered-pay-back-16692/

Rogue trader sentenced after causing damage to home:

https://www.hampshire.police.uk/news/general/rogue-trader-sentenced-after-marchwood-incident/

May 2017:

Courier fraud scam in Odiham:

https://www.hampshirealert.co.uk/da/179745/Appeal_for_information_after_couple_lose_cash_to_fraudsters.html

Hampshire Constabulary supports Op Liberal week of action:

https://www.hampshire.police.uk/news/general/hampshire-police-support-national-crackdown-rogue-traders/

June 2017:

Advice given following distraction burglaries in Southampton:

https://www.hampshire.police.uk/news/general/advice-issued-following-distraction-burglaries-southampton/

Warning to Hampshire residents following new telephone scam in Farnborough:

https://www.hampshire.police.uk/news/general/warning-hampshire-residents-following-new-telephone-scam/

Courier fraud warning following incidents in Southampton and Eastleigh:

https://www.hampshire.police.uk/news/general/warning-issued-after-elderly-people-targeted-fraudsters-southampton-and-eastleigh/

July 2017:

Rogue trader warning after Sandown incident:

https://onthewight.com/rogue-trader-warning-after-sandown-incident/

August 2017:

Advice issued following courier fraud scam in Alton:

https://www.hampshire.police.uk/news/general/members-public-urged-be-vigilant-following-fraud-alton/

Fraud prevention advice issued after Southampton couple loses £25,000:

https://www.hampshire.police.uk/news/witness-appeals/fraud-prevention-advice-issued-after-southampton-couple-loses-25000/

Elderly people targeted by fraudsters in the New Forest:

https://www.hampshire.police.uk/news/general/warning-issued-after-elderly-people-targeted-fraudsters-new-forest/

Advice issued via Hampshire Alert after Cifas warned of record rises in identity fraud: https://www.hampshirealert.co.uk/da/189374

Cyber protection advice issued after reports of banking Trojan attacks in Hampshire:

https://www.hampshirealert.co.uk/da/187494/Banking_Trojan_cyber_attacks_in_Hampshire_-_how_to_protect_your_devices.html

September 2017:

CCTV released following rogue trader incident:

https://www.hampshire.police.uk/news/witness-appeals/cctv-released-following-rogue-trader-incident/

Computer Software Service Fraud (CSSF) in August/September 2017 – social media screen grab examples attached to this email in a Microsoft Word document.

October 2017:

Get Safe Online 'Scammer Nanas' initiative in October 2017 - https://www.getsafeonline.org/scammernanas/

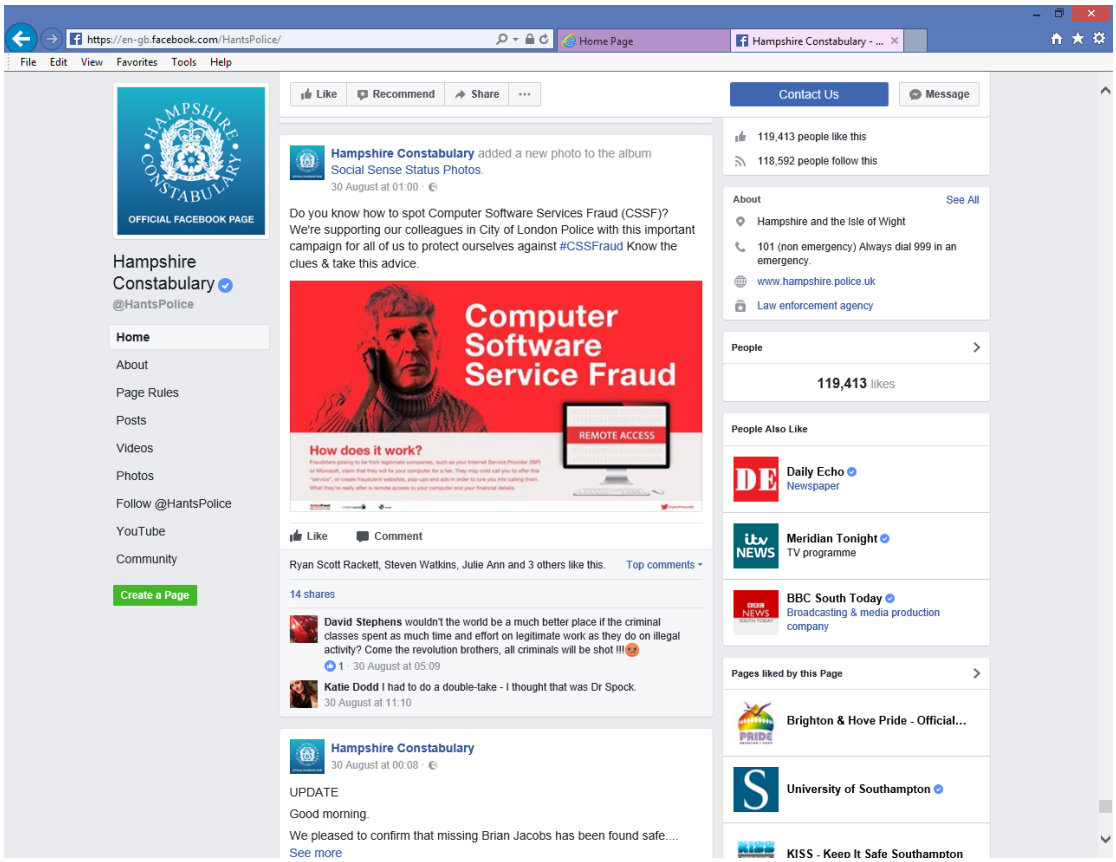
City of London Police's identity theft prevention campaign in summer 2017 - customised graphics provided for Hampshire Constabulary. Click on the Google Drive link below to download the graphics:

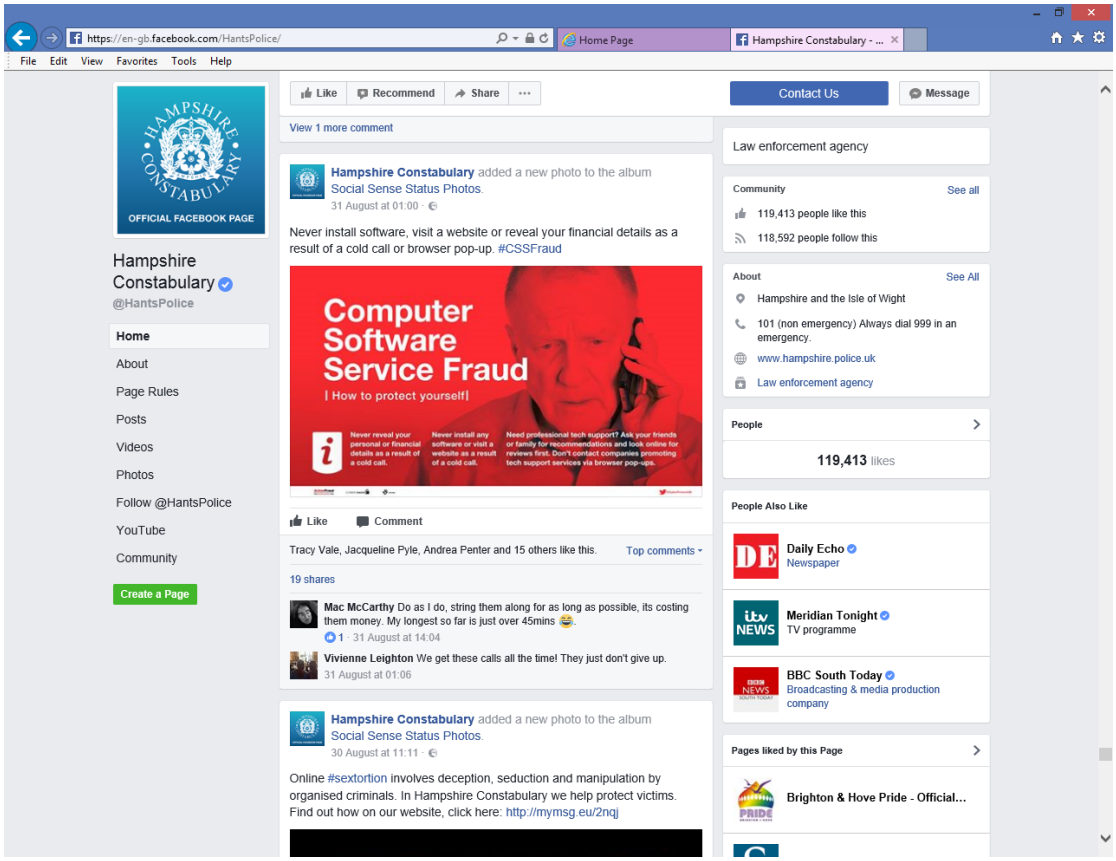
https://drive.google.com/drive/folders/0B-oiXugDzyxmeWFxVzFKcDB1OGM

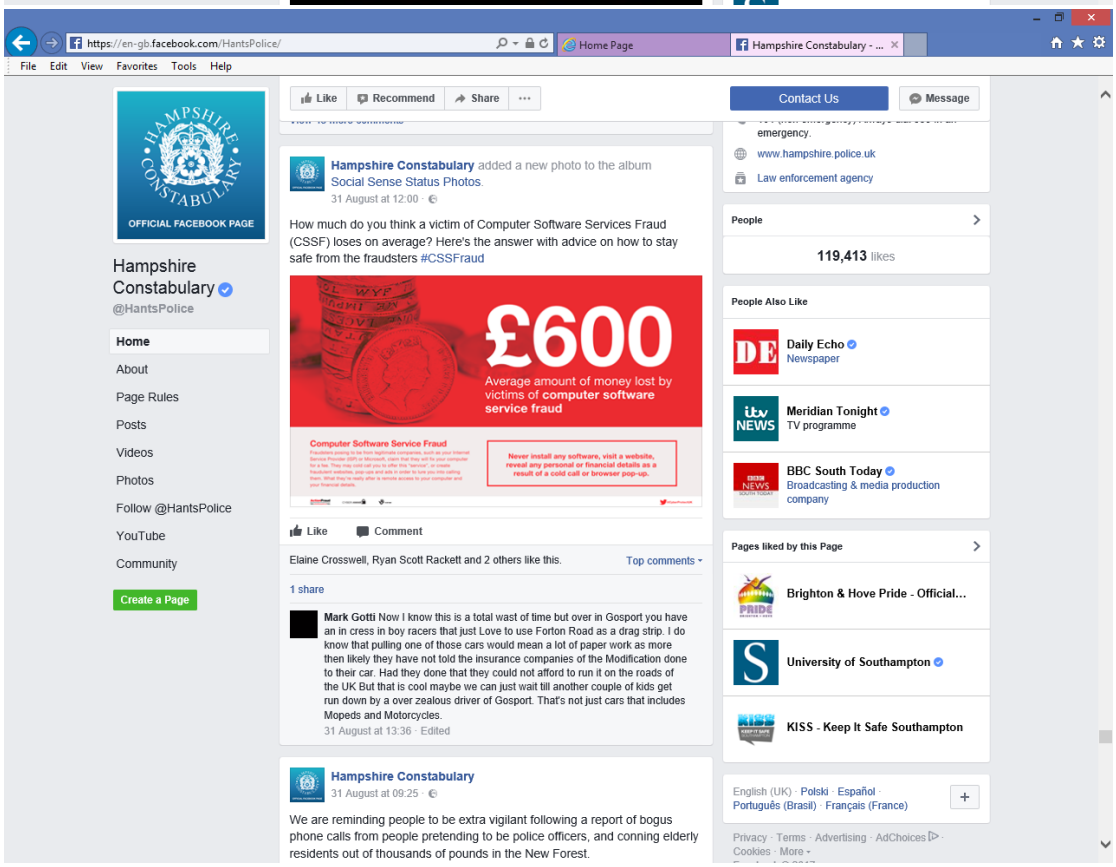
Ransomware in October & July 2017 – an example of City of London Police content attached to this email in a PNG file 'PROTECT advice for small business and home users.'

Hampshire Constabulary Facebook page screen grabs

30 August 2017 – 31 August 2017




https://en-gb.facebook.com/HantsPolice/
Home Page
Hampshire Constabulary - ...
File Edit View Favorites Tools Help
OFFICIAL FACEBOOK PAGE
Hampshire Constabulary
@HantsPolice
Home
About
Page Rules
Posts
Videos
Photos
Follow @HantsPolice
YouTube
Community
Create a Page
Like Recommend Share
Contact Us
Message
View 1 more comment
Hampshire Constabulary added a new photo to the album Social Sense Status Photos.
31 August at 01:00
Never install software, visit a website or reveal your financial details as a result of a cold call or browser pop-up. #CSSFraud
Computer Software Service Fraud
How to protect yourself
Never reveal your personal or financial details as a result of a cold call.
Never install any software or visit a website as a result of a cold call.
Need professional tech support? Ask your friends or family for recommendations and look online for reviews first. Don't contact companies promoting tech support services via browser pop-ups.
Like Comment
Tracy Vale, Jacqueline Pyle, Andrea Penter and 15 others like this.
Top comments
19 shares
Mac McCarthy Do as I do, string them along for as long as possible, its costing them money. My longest so far is just over 45mins
1 · 31 August at 14:04
Vivienne Leighton We get these calls all the time! They just don't give up.
31 August at 01:06
Hampshire Constabulary added a new photo to the album Social Sense Status Photos.
30 August at 11:11
Online #sextortion involves deception, seduction and manipulation by organised criminals. In Hampshire Constabulary we help protect victims. Find out how on our website, click here: http://mymsg.eu/2nqj
Law enforcement agency
Community
See all
119,413 people like this
118,592 people follow this
About
See All
Hampshire and the Isle of Wight
101 (non emergency) Always dial 999 in an emergency.
www.hampshire.police.uk
Law enforcement agency
People
119,413 likes
People Also Like
Daily Echo
Newspaper
Meridian Tonight
TV programme
BBC South Today
Broadcasting & media production company
Pages liked by this Page
Brighton & Hove Pride - Official...


https://en-gb.facebook.com/HantsPolice/
Home Page
Hampshire Constabulary - ...
File Edit View Favorites Tools Help
OFFICIAL FACEBOOK PAGE
Hampshire Constabulary
@HantsPolice
Home
About
Page Rules
Posts
Videos
Photos
Follow @HantsPolice
YouTube
Community
Create a Page
Like Recommend Share
Contact Us
Message
Hampshire Constabulary added a new photo to the album Social Sense Status Photos.
31 August at 12:00
How much do you think a victim of Computer Software Services Fraud (CSSF) loses on average? Here's the answer with advice on how to stay safe from the fraudsters #CSSFraud
£600
Average amount of money lost by victims of computer software service fraud
Computer Software Service Fraud
Never install any software, visit a website, reveal any personal or financial details as a result of a cold call or browser pop-up.
Like Comment
Elaine Crosswell, Ryan Scott Rackett and 2 others like this.
Top comments
1 share
Mark Gotti Now I know this is a total wast of time but over in Gosport you have an in cress in boy racers that just Love to use Forton Road as a drag strip. I do know that pulling one of those cars would mean a lot of paper work as more then likely they have not told the insurance companies of the Modification done to their car. Had they done that they could not afford to run it on the roads of the UK But that is cool maybe we can just wait till another couple of kids get run down by a over zealous driver of Gosport. That's not just cars that includes Mopeds and Motorcycles.
31 August at 13:36 · Edited
Hampshire Constabulary
31 August at 09:25
We are reminding people to be extra vigilant following a report of bogus phone calls from people pretending to be police officers, and conning elderly residents out of thousands of pounds in the New Forest.
emergency.
www.hampshire.police.uk
Law enforcement agency
People
119,413 likes
People Also Like
Daily Echo
Newspaper
Meridian Tonight
TV programme
BBC South Today
Broadcasting & media production company
Pages liked by this Page
Brighton & Hove Pride - Official...
University of Southampton
KISS - Keep It Safe Southampton
English (UK) · Polski · Español · Português (Brasil) · Français (France)
Privacy · Terms · Advertising · AdChoices · Cookies · More

Hampshire County Council

Cybercrime – Cyber-Enabled Fraud' proactive scrutiny

I write with reference to the aforementioned proactive scrutiny exercise being undertaken by the Hampshire Police and Crime Panel. I am responding on behalf of Hampshire County Council Trading Standards Service only.

The specific questions posed in the call for evidence, along with any appropriate responses are below.

1) *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

   Hampshire County Council Trading Standards Service does not believe it is in a position to be able to offer any view on how well the PCC, through working with the Chief Constable, has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud.

2) *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

   Hampshire County Council Trading Standards Service is a criminal law enforcement agency whose primary purpose is to protect consumers as a whole, whilst maintaining a level playing field for legitimate business to thrive. This is in relation to both High Street and online activity. Whilst this Service works with many partners in this arena, we have had no direct contact from the office of the PCC in this regard.

   All Trading Standards Services, including those operated by Portsmouth City Council; Southampton City Council and the Isle of Wight Council, would be able to enhance the partnership approach to tackling cyber fraud, in many ways including, but not limited to, the following:

   i) Complaint information received on a daily basis from the Citizens Advice Consumer Service (CACS), which can be used to identify victims of cyber fraud

ii) Links with the National Trading Standards e-Crime Team, which can be used to identify and tackle both level 2 and level 3 cyber fraud criminality and Operation Jasper.

iii) Links with the National Trading Standards Scams Team, which can offer guidance on safeguarding support for vulnerable members of the community through their role as Chair of the Victims and Vulnerability work stream of the Joint Fraud Taskforce

iv) Participation in the annual National Consumer Week education programme which, this year tied in with Cyber Monday and focussed on subscription traps and misleading subscriptions, including online subscription issues. The title of the campaign was 'Not What You Signed Up For?'. Past messaging has also included 'Know Your New Rights' in respect of new consumer rights including digital content;

v) Safeguarding support for vulnerable victims of financial abuse that may have been perpetrated through cyber fraud

vi) 'Protecting Older Persons' community engagement sessions that include cyber security as part of its content.

3) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

Hampshire County Council Trading Standards Service does not believe it is in a position to be able to offer any comment on how well the PCC has engaged with resident to enable them to recognise and, protect themselves from cyber-enabled fraud. This Service would however, encourage greater partnership working between all relevant services that are able to provide such educational messaging to consumers. This is to ensure that a consistent approach is taken and residents are not left confused as to what action they should, or could, take to prevent themselves from becoming victims of cyber fraud.

This would then, in turn, enable greater consistency with national messaging provided by Action Fraud; National Trading Standards e-Crime Team; National Trading Standards Scams Team; Citizens Advice Consumer Service (as part of the Scams Awareness Month annual campaign).

4) *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

It is the view of this Service that any priorities must fit with the Serious and Organised Crime Strategy, a Home Office initiative, in order to ensure a consistent approach to reduction of cyber-enabled crime is achieved. It is suggested that the following would be appropriate.

i) Education – increased educational campaigns but with an emphasis on those sectors who are statistically more likely to fall victim to cyber fraud or, for whom operating in a digital age is more challenging. For example, working with local charity groups such as Age UK who deliver Silver Surfers courses on digital inclusion or, working with Hampshire County Council Libraries who provide courses such as 'Getting to Know Your iPad'. This would enable such course content to not only focus on the 'how' of operating in a digital age but, give greater confidence on how to spot potential pitfalls as well. This would fit with the 'Prevent' and 'Prepare' outcomes of the Serious and Organised Crime strategy, a Home Office initiative.

ii) Intelligence sharing – greater intelligence sharing, where legally permissible, with relevant partners. Improved intelligence capabilities will help targets resources effectively and help reduce possible duplication of effort. This would fit with all four of the outcomes of the Serious and Organised Crime strategy; namely, 'Pursue', 'Prevent', 'Protect' and 'Prepare'.

iii) Improved partnership working in terms of locally; regionally and nationally. Cyber fraud is not necessarily perpetrated upon specific geographic areas but, is potentially global. It is therefore necessary to work with partners on local; regional; national and even international levels, if required, in order to reduce the threat posed within Hampshire and the Isle of Wight. This again, would fit with all four outcomes of the strategy.

5) *Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?*

i) Various 'Black Friday' and 'Cyber Monday' educational campaigns that operate in the run up to Christmas. These can stem from either the enforcement community or the commercial sector.

https://www.a-cg.org/newsdesk/acg-press-releases

https://www.tradingstandards.uk/news-policy/news-room/2017/know-your-rights-and-don-t-lose-out-this-black-friday-weekend

https://www.actionfraud.police.uk/calendar

http://www.tradingstandardsecrime.org.uk/citizens-advice-warns-consumers-of-trial-offers-on-facebook-and-ebay/

ii) Other all year round initiatives designed at increasing awareness of current scams/frauds and encouraging participation in the education of others including:

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

http://www.tradingstandardsecrime.org.uk/alerts/

6) *Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?*

No, although Hampshire Trading Standards Service is always content to consider how it may best answer any further questions that are put to it.

Heckfield Parish Council

1 *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

and

2 *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

Whilst we have a general understanding of the relationships between the PCC and the Chief Constable and others, we do not have any detailed information about the actual work that has been undertaken. For this reason, we do not feel we can comment on these questions.

3 *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

We are not aware of any information from the PCC sent directly to residents or to parish councils. The Heckfield Parish web site does provide links to Crime Prevention Advice pages that are relevant to our local community.

If the PCC passes data to Heckfield Parish Council, we will make sure it is available on our web site. However, we know from access statistics that, in an average month, there are usually no more than 100 visits to the web site and at least 25% of these are concerned with bookings for Heckfield Memorial Hall rather than any other information that we provide.

Access to the Crime Prevention Advice pages is very low.

4 *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

We believe that prevention is better than cure, so regular updates on current threats with advice on appropriate avoidance action is a priority. Hopefully the updates would include information on things like "telephone scams" as well as threats to computers, tablets and phones.

Even though the Heckfield parish web site is not as much used as we would like, we can publish any information we receive very quickly. Over time, we hope to persuade local residents to visit the web site more often and this should allow us to pass on warnings as soon as they are available.

We already provide "email notifications" for certain events like News Items.

5 *Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?*

None that we have identified.

6 *Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?*

Not at present.

Hythe and Dibden Parish Council

1) *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

   As a Parish council that has committed to working to improve community safety within this Parish we actively work to capacity build our community to being as resistant as possible to cyber crime. We are not aware of any operational policing plans that are targeted at cyber crime.
   Policing provision could be improved by providing 'partners' with key messages, requests for intelligence, and target hardening actions to be delivered in partnership where the partners are willing and able to assist.

2) *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

   Please see our answer to question 1. We have received no information/approaches from the PCC or his office

3) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

   We have not seen any information from the PCC so we would have to answer that the PCC has not engaged with residents in so far as we are aware. As an example on how to improve, from our view point it is probably to start working on this and starting communication.

4) *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

   - Toolkit for partners to deliver according to chronology
   - Staying safe when using social media and live apps (young people particularly)
   - Look after your family and friends who might not be as suspicious, when banking online
   - Local trends information

5) *Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?*

Yes – we operate a number of messaging systems that can reach thousands of people. If we are provided the intelligence we can warn people what to look out for

6) *Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?*

No

Police and Crime Commissioner for Hampshire and IOW

POLICE & CRIME COMMISSIONER

Serving
Hampshire
Isle of Wight
Portsmouth
Southampton

RESPONSE TO

Hampshire Police and Crime Panel's

Proactive Scrutiny

Cybercrime – Cyber-Enabled Fraud

Date	13th December 2017
Enquiries To	Office of the Police and Crime Commissioner for Hampshire, St. George's Chambers, St. George's Street, Winchester, Hampshire, SO23 8AJ – opcc@hampshire.pnn.police.uk www.hampshire-pcc.gov.uk Tel: 01962 871595

Context

The Commissioners' Police and Crime Plan outlines the strategy and intentions to be undertaken during the Commissioners' term in office. It is the Delivery Plan which outlines the different strands of work being undertaken by the office, in which cybercrime and cyber enabled fraud is to be delivered upon.

Due to the range of factors that may indicate vulnerability to cybercrimes such as personal and/or family circumstance, to economic circumstance, this generates a vast opportunity for those who wish us harm to exploit such vulnerabilities.

In order to keep our communities SAFER, a multiagency approach, while utilising community responsibility and resolve will all play a part in both tackling and in the delivery of raising awareness, protecting and preventing fraud and cybercrimes to those in Hampshire, Isle of Wight, Portsmouth and Southampton.

Traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of technology are known as cyber enabled crimes, in which cyber enabled fraud is a part of.

Under-reporting continues to obscure the full impact of cybercrime. In 2015 the Office of National Statistics (ONS) trialled the inclusion of cybercrime in the annual Crime Survey for England and Wales (CSEW) for the first time. The ONS estimated that there were 2.46million cyber incidents and 2.11million victims of cybercrime in the UK in 2015. These figures highlight the clear shortfall in established reporting, with only 16,349 cyber-dependent and approximately 700,000 cyber-enabled incidents reported to Action Fraud over the same period. In the year to September 2016 there were an estimated 1.9 million incidents of cyber-related fraud in England and Wales. The true cost of online fraud is unknown, but is likely to be billions of pounds a year. While estimates can be made on the financial cost of online fraud, the emotional impact on victims is much more difficult to assess.

Cybercrime activity is growing fast and evolving at pace, becoming both more aggressive and technically proficient. Although general cyber awareness is improving in the UK, there remains a lack of understanding of cybercrimes, including cyber enabled fraud.

Here in Hampshire, Isle of Wight, Portsmouth and Southampton from October 2016 to March 2017 there were 541 recorded fraud cases linked with online shopping and auctions. During this same time period, of cyber enabled fraud reports 28% were through the use of a phone, 14% through email and 13% via online sales.

In 2016 the Home Office set up the Joint Fraud Taskforce to improve collaboration between all bodies in tackling online fraud. With many national organisations dedicating their work to the awareness raising and prevention of fraud and cybercrimes such as Action Fraud and Take Five, fraud and cybercrimes are recognised as a priority area in which continued resource and investment is required.

1) How well has the PCC, through holding the Chief Constable to account, ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud?

The growth of the internet and advances in digital technologies have created great opportunities for innovation and economic growth, but also more opportunities for online crime.

Cyber enabled fraud is on the Constabulary's Force Control Strategy, with a dedicated team to investigate and tackle this high priority crime. As reported by the All Select Committee into online fraud, it is those more vulnerable where cyber enabled fraud can have the biggest impact, reports that elderly people can suffer real harm and stop using their computers, unplug their phones and, in the worst cases, end up in care homes because they have been victims.

It is through both formal and informal meetings with the Chief Constable where the Police and Crime Commissioner holds the Chief Constable to account, ensuring that the strategic direction is translated into frontline operational policing.

It is for the Chief Constable to deploy her resources as she sees fit, delivering upon the PCCs strategic plans for keeping our communities SAFER. Force performance is monitored, emerging issues and threats are scrutinised to allow effective and efficient responses and actions to be taken by both the Constabulary and the PCCs team.

2) How effective have the PCC and his office been in engaging with appropriate partners to ensure a joined-up approach to identifying and tackling cyber-enabled fraud?

It has been vital to gain an understanding of the work being undertaken by Hampshire Constabulary in relation to cyber and fraud, this was undertaken via a scoping exercise through the summer and autumn of this year.

The world of cyber and fraud is vast, encompassing a wide range of policing teams (under Protect, Prevent, Pursue and Prepare) and organisations both locally and nationally. Cyber enabled fraud is one fraud type amongst the many types of fraud our residents fall victim to.

It is for the PCCs office to develop partnerships and build upon our existing relationships. We recognise there is always more that can be done, casting our net as far and wide to further our joined-up approach.

Here at the PPCs office we facilitate the strand of cyber enabled fraud, we are not the leads but here to support and empower not only the Constabulary but partners and organisations, feeding into National strategy to deliver locally.

3) What efforts have been made by the PCC to educate and inform the residents of Hampshire and the Isle of Wight to recognise and protect themselves from cyber-enabled fraud?

Both Cyber and Fraud are key areas within the PCCs delivery plan in which both the Commissioner and his office are dedicated to ensure those in our communities are aware of the risks associated with such crimes, where to seek support and raise awareness in their own communities.

Hampshire Constabulary's Communications team and the PCCs Communications team are developing their working relationship to better coordinate campaigns jointly and collaboratively, developing and building upon the landscape of cyber and fraud,

including cyber enabled fraud. The first jointly developed online campaign around ‘online shopping’ and the related fraud and cybercrimes is currently underway.

Our Communications and Engagement team share online national and local messages around raising awareness of fraud and cybercrimes. While attending recent older person’s fayres in Hayling Island, Fareham, Gosport and the older drivers awareness event in West End, we engaged with local communities specifically around fraud and cyber enabled crimes. Here we gathered volunteers for focus groups who are keen to support the development of resources and campaigns, being targeted to vulnerable groups such older people in relation to fraud and cyber enabled crimes. As an office we will develop resources appropriate to the demand we hear from our local communities, to reach a wide range of our communities and the diverse needs of our residents.

We are jointly working with Hampshire Constabulary in the public launch of Operation Signature in March 2018. This operation is currently active across the force, seeking to protect those falling victim to fraud. This will include cyber enabled fraud.

4) What are the key priorities which need to be considered by the PCC to reduce the threat posed to the residents of Hampshire and the Isle of Wight through cyber-enabled fraud?

The PCC will continue to consult and engage with the residents of Hampshire, Isle of Wight, Portsmouth and Southampton. Fraud and Cyber enabled crimes effect and impact a wide range of our communities, not just those traditionally targeted for such crimes.

It is the extensive under reporting of fraud and cyber enabled crimes which has led us to invest in developing a cyber survey to help shape the priorities of both the PCCs office and the Constabulary, providing evidence of the impact of cybercrimes upon both adults and children across our 14 districts. With the evidence of where there are gaps in knowledge, support services and partner engagement across differing demographics, we can best utilise the resources available to us.

5) What best practice exists which could also be considered by the PCC in his approach to preventing and tackling cyber-enabled fraud?

The PCC continues to encourage Hampshire Constabulary to work with Action Fraud in preventing and tackling the ever increasing types of fraud and cyber crimes, including cyber enabled fraud.

There is the evolving need to recognise the value the PCC can bring to developing the communications and campaign support with the Constabulary, to extend and be diverse in our messaging, to reach as many of our residents as possible, raising awareness to keep SAFER.

We continue to watch the All Select Public Accounts Committee into ‘The growing threat of online fraud’ published 6th December 2017. With a number of recommendations put forward by the All Select Committee, we watch with significant interest.

Public replies

How effective do you feel the current policing provision is, within Hampshire and the Isle of Wight, in response to cyber-enabled crime? Can you identify any areas where the PCC could work with the Chief Constable to improve the current approach?

A1. Unfortunately, I have no knowledge at all of any action(s) that the PCC/HCC are doing to seek out the root causes/sources of the numerous Cybercrimes in our area.

A1. a. Therefore, an obvious area for improvement is multi-directional communications strategy, plan and a very timely and effective implementation. Not a long-winded study to reinvent the wheel, there must be similar communication strategies within HCC/PCC that can be emulated/piggy backed onto.

A1. b. A quick efficient non-complicated/non bureaucratic system/method for residents to communicate potential or actual attempts at Cyber Fraud is desperately needed. Getting in touch with the Action Fraud Office is a nightmare.

2. How well do you feel the PCC and his office have worked with partners to identify and tackle cyber-enabled fraud, and seek solutions to prevent and reduce the impact this has upon members of the community? Can you identify any opportunities for further partnership working in the future?

A2. As above unfortunately, I have no knowledge at all of any action(s) that the PCC are doing with partners to seek solutions and prevent cybercrime in our area.

A2. a. Most cyber crime is carried out via telecommunications/broadband internet. The Carriers must be encouraged/shammed into doing their bit to prevent these crimes being carried out using their networks: Computer generated fictional telephone numbers being used by telephone fraudsters like those in the Microsoft and HMRC scams.

A2. b. Communication.

3. How well has the PCC communicated with you and other local residents to enable you to recognise and protect yourself from cyber-enabled fraud? Can you suggest how the PCC could improve his interaction with local communities in the future?

A3. Not well at all. See response to Question 1 above.

4. What actions do you think should be a priority to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?

A4. As a priority implement a system/method whereby residents can very quickly communicate attempted or actual cyber crimes and have procedures in place that will react immediately to this “live” intelligence data. Implement an effective communications plan/system that will get to all residents, do not totally rely on IT. 2

5. Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you are aware of, either within Hampshire and the Isle of Wight or in other areas?

A5. Not sure at all about the success of the following examples as feedback is non-existent: The high-street banks do regular communications on potential and actual threats via their internet banking system. Action Fraud are doing their bit but with no feedback or follow up on reported attempted/actual cybercrimes.

6. Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?

A 6. Only the following; as senior citizens my wife and I have been repeatedly targeted by scams designed to access our bank accounts: Microsoft, HMRC, not selling surveys etc. We have requested the help of our network provider with exceedingly little success, we have purchased and installed number blockers, however the computer randomly generated telephone number facility gets through. I would therefore like to request the Panel to consider all legal ways to encourage cajole the network providers to use/improve their technology/Customer Service to attack this prevalent and “foul” crimes.

Thank you for this opportunity to share my opinions

Item 6) Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?

The one obvious thing you should do support free speech by abandoning the pathetic "Hate Crime" concept.

Stop acting as Orwellian Thought Police suppressing any opinion that does not accord with politically correct dogma.

As a town councillor in Petersfield I received the invitation to provide some feedback to the Hampshire Police and Crime Panel’s proactive scrutiny of ‘Cybercrime – Cyber-Enabled Fraud’

I fear I have to say I am unaware of any initiatives or advice provided to residents on this topic which would lead me to thinking that the efforts, which I am sure are being made, are not fully effective in getting the message across.

I have just read through the report on Cybercrime what would be useful to councillors and residents alike is that if there was a dedicated mail box that receivers could send elicit spoof emails to for the police to help monitor it would give all a greater understanding of on line fraud. I often get spoof emails from persons claiming to represent PayPal these I direct to spoof@paypal.com others are from various banks

even from banks I have no connection with so if links was made readily available for residents to redirect spoof or suspicious emails to this would I feel help reduce cybercrime and not put the entire responsibility on the Police.

The other is constant calls from persons claiming to represent Microsoft and saying I have a computer error or fault if there was a way of collecting the numbers these are sent from then emailing them to the police that would help to in building up the data needed to identify where the calls are coming from and then through international partners tackle them head on..

South West Police Regional Organised Crime Unit

- *How well has the PCC, through holding the Chief Constable to account, ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud?*

  The South West Regional Organised Crime Unit have Cyber Crime as a force priority. The Police and LEA's have recognised it is a key threat to safety of the residents in their force areas and take appropriate actions to address this threat risk.

- *How effective have the PCC and his office been in engaging with appropriate partners to ensure a joined-up approach to identifying and tackling cyber-enabled fraud?*

  All Partner agencies and key stakeholder are invited to attend tasking meetings within the SW ROCU. Those meetings will review disruptions taken to counter this threat and review bids for pending operations to make the most efficient use of available resources.

- *What efforts have been made by the PCC to educate and inform the residents of Hampshire and the Isle of Wight to recognise and protect themselves from cyber-enabled fraud?*

  I cannot answer this question

- *What are the key priorities which need to be considered by the PCC to reduce the threat posed to the residents of Hampshire and the Isle of Wight through cyber-enabled fraud?*

  I would say that the General public need to be made aware of the threat of cyber -crime, what it looks like to the man in the street and how they can tighten up personal security to help stop being a victim of Cyber crime

- *What best practice exists which could also be considered by the PCC in his approach to preventing and tackling cyber-enabled fraud?*

  Organised and resourced teams that specifically target Cyber-Criminals. Making vulnerable people and businesses aware of the current threats and malware programmes. Press releases on recently detected attacks and what the general public should look for.

7) *Through working with the Chief Constable, how well do you feel the PCC has ensured that operational policing plans are sufficiently robust to meet the strategic threat posed by cyber-enabled fraud? Can you identify any areas where the policing provision within Hampshire and the Isle of Wight could be improved?*

   I cannot answer this question

8) *How effective do you feel the PCC and his office have been in working with partners to ensure a joined-up approach in identifying and tackling cyber-enabled fraud? What opportunities do you feel exist to enhance this partnership approach?*

   See above

9) *How well has the PCC engaged with residents to enable them to recognise and protect themselves from cyber-enabled fraud? Can you identify further examples of how the PCC might improve this communication in future?*

   I cannot answer this question

10) *What do you think should be the priorities for action to reduce the threat posed by cyber-enabled crime within Hampshire and the Isle of Wight?*

    See above

11) *Are there any examples of successful approaches to preventing and tackling cyber-enabled fraud which you or your organisation are aware of, either within Hampshire and the Isle of Wight or in other areas?*

    See above

12) *Is there anything further that you can provide to the Panel that will assist us with our proactive scrutiny of this topic?*

    Not at this time