July
2018

Cyber Update – July 2018

Bringing you latest cyber crime & scam news from Hampshire & the Isle of Wight

Cybercrime Trends– latest reporting period

- Between October – March 2018, the most common type of cyber-enabled crime was **cheque and online fraud** (most of it reported by banks); second was application fraud – people using other people's stolen details to apply for bank accounts.
- We have seen an increase in **'romance fraud'** or dating website scams, which are also seeing the highest losses. If you use a dating app or website, please be **very wary** of anyone asking for money. This is an increasingly common scam and people are parting with huge amounts of cash.
- Recent Hampshire cases include:
- Woman in her 50s 'met' a man online via the Elite Singles site, and quickly moved onto Whats App chat. She believed she was in a relationship with him and parted with £50,000 on request. She never did meet him.
- 52 year old woman 'met' a man on the Christian Café dating forum. Chatted with him for a period of time via email and phone call. He asked for £2,000 to enable him to move to the UK (transport his furniture from the US). The visit never happened. Fortunately, the would-be victim smelled a rat, did not part with any cash and reported to police.
- 57 year old woman 'met' a man via the Words With Friends online gaming app – contact them moved to Instant Messenger. He told her he worked on an oil rig in the North Sea and needed £1270 to get home. Then said he was stopped by Customs and needed more money. Luckily, again, victim was suspicious – did not hand over any cash, and reported to police.
- Most common reasons for 'needing money' by dating scammers reported to us:
  - Travel/to get home or get to them;
  - So they can send stuff;
  - Medical/urgent operations needed;
  - Help out family;
  - Help with job;
  - Pay for a visa to enable visit;
  - Help out with an orphanage.
- For more information on a Hampshire case and advice, please visit: https://www.youtube.com/watch?v=G3uDrNG_SAc

Cybercrime – latest news & developments

Lloyds Bank customer? Did you know that Lloyds is implementing new policy that you won't be refunded if you voluntarily give your details away as part of a scam – such as an online phishing scam or, vitally, our most commonly reported scam **Computer Service Software Fraud**. Other banks are starting to follow suit.

CSSF – or 'phone call fraud' as we like to call it, will form part of a major campaign we will be running from September this year. The campaign will be targeted at members of our Hampshire & Isle of Wight communities who are aged 60+, as research shows this is the most vulnerable demographic.

We are working alongside the Office of The Police & Crime Commissioner, which is running a fraud-busting campaign throughout the autumn, and partners helping us with this vital work include Citizens Advice Bureau, Trading Standards, the Blue Lamp Trust and Hampshire Fire and Rescue Service.

Read on for more details about 'phone call fraud'…and what to do if you are a victim.

Focus on… CSSF – ‘phone call fraud’

Computer Software Service Fraud (CSSF) is a cyber-enabled crime in which fraudsters attempt to gain access to your computer by pretending to be from an Internet Service Provider or a well-known company like Microsoft or Apple. We have known cases where they also pretend to be other well-known service providers including Talk Talk and Sky.

Typically, someone calls you pretending to be from a legitimate company. They will tell you there is a problem with your computer or that it has a virus that needs fixing. Often they will say they can fix it for a fee or that they need to validate your software by asking for your credit card details; they may ask you to install some software or visit a particular website where you can enter payment details. They may well ask for access codes to your account which they will then use to get into your accounts and steal your money.

All the while they are trying to get you to give them remote access to your computer so they can grab your personal data and your payment details.

Key advice:
If it happens to you - don’t panic
Report it - we won’t think you are foolish for being tricked
We can get you help

See next page for prevention & reporting advice….

Focus on… CSSF – ‘phone call fraud’

How to prevent falling victim to ‘phone call fraud’…

HANG UP if you don’t know the caller, put the phone down.
SSSHHH never give out any personal or financial details to anyone cold calling you
NEVER give anyone remote access to your PC, install software or visit a website as the result of a call
DO NOT call them back

If you think you may have fallen victim:
UNPLUG disconnect your computer from the internet/network as soon as you realise you were tricked
REPORT straight away to your bank if you think remote access may have been gained
REPORT to Action Fraud ASAP on 0300 123 2040 or via www.actionfraud.police.uk/report_fraud
REPAIR Get your computer checked out & cleaned by a trusted IT technician before using it again.

Protect Yourself:

Speak to your telephone provider about the Telephone Preference Service (TPS) which can help block some unwanted calls;
Install anti-virus software on all devices and make sure it is kept up-to-date.
Computer firms do not send unsolicited emails or make unsolicited calls to request personal information or to fix your computer.

Further Support:
www.actionfraud.police.uk
www.citizensadvice.org.uk
www.hampshire.police.uk

Current Cyber Protect focus

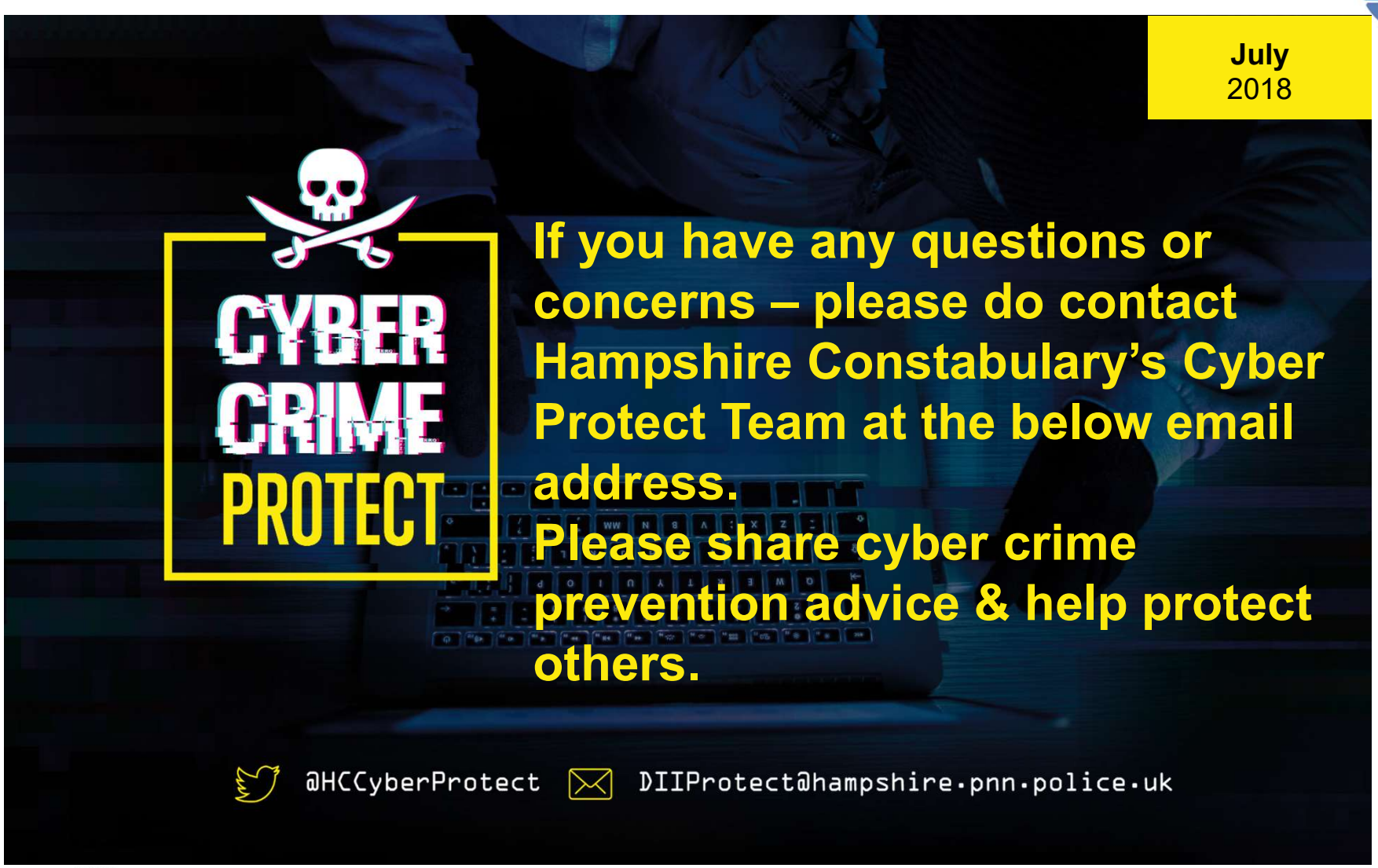
- Three key vulnerable groups (based on victimology):
  - Older users (50 – 69 and above)
  - Children and young people
  - Local businesses, organisations and voluntary sector;

  Key areas of concern:
  - Social media and online safety/safeguarding;
  - Those with great threat, harm and risk including cyber stalking, sextortion, and more serious cases featuring exploitative images of children;
  - Computer Software Service Fraud;
  - Educating and upskilling police teams and partner agencies to improve response and victim care for victims of cyber-enabled and cyber-dependent crime.

Reporting cybercrime & fraud

If you or someone else is in immediate danger or risk of harm dial 999 now.

If you are suffering a live cyber attack that is in progress, call now on 0300 123 2040 to report, do not report using the online tool. This service is available 24 hours a day, 7 days a week for businesses, charities and organisations. Advisors are also available 24/7 on web chat if you have any questions - http://www.actionfraud.police.uk/report-a-fraud-including-online-crime


July
2018
CYBER
CRIME
PROTECT
If you have any questions or concerns – please do contact Hampshire Constabulary's Cyber Protect Team at the below email address.
Please share cyber crime prevention advice & help protect others.
@HCCyberProtect
DIIProtect@hampshire.pnn.police.uk