Kingston Police and Kingston Borough Neighbourhood Watch Newsletter September 2019

A summary of Kingston Police and NHW news for the Borough as a whole. Do let us know if there are any other areas you would like future newsletters to cover by emailing Alison.J.McWhinnie2@met.police.uk

Met. Police Choir Concert!

7pm on 9th November 2019

All Saints Church, Kingston

Back by popular demand!

Delighted to be welcoming the Met. Police Choir back to Kingston for their third concert here.

Email Kingston.NHW@gmail.com today to book your places!

Kingston Borough Cyber Crime Monthly Summary – July 2019

In **July** there were **85** reports made to Action fraud by residents of Kingston borough.
The losses described over these **85** reports total **£415,758**
Meaning an average loss of **£4,891** per report.
Unfortunately, £200,000 of this was a single report for **Investment Fraud**, there were also a few high value **payment frauds** too.

The top 3 by **volume** (number of reports) type of fraud is as follows;

False Representation	19 reports	£198 lost
Online Shopping Fraud	14 reports	£11,402 lost
Advance Fee Fraud	9 reports	£1,400 lost

The top 3 by **amount** reported lost:

Investment Fraud	£201,498 lost	4 reports
Payment/Mandate Fraud	£89,715 lost	4 Reports
Push Payment Fraud	£55,008 lost	4 reports

Online Shopping

Victims are convinced into paying money for items that don't exist or are counterfeit when shopping online. E.g. fake adverts on eBay.

- Stay on the website - follow procedure / terms and conditions.
- **Never use direct bank transfers** – use the websites recommended payment methods.
- Be wary of last minute changes to delivery address or payment method. (check website terms and conditions)
- A common scam is when the fraudster 'overpays' you and asks for money back, be wary of anything **unusual** when shopping online.
- Never buy a vehicle without seeing it in person and checking its documents.
- When selling items, best practice is send via recorded delivery.
- Research the seller/buyer and bidding history- check reviews of websites/sellers.
- Seek advice from the website if unsure.
- If selling, be wary of emails stating funds have been transferred, a common scam is when a spoof email is sent claiming funds have been transferred – Always check via the official website.
- Don't click on links in emails – always go via the official website.
- **And remember if something appears too good to be true then it probably is!**

Please see our animation for more details; https://www.youtube.com/watch?v=Y-_wPFXK2m4

Investment / Share sales Fraud

Victims are pressured into making 'investments' or buying shares that don't exist or have no chance of the financial return suggested. **Genuine investment/shares companies do NOT cold call people.**
Look out for these **six warning signs:**

1. **Unexpected contact** – Traditionally scammers cold-call but contact can also come from online sources e.g. email or social media, post, word of mouth or even in person at a seminar or exhibition.
2. **Time pressure** – They might offer you a bonus or discount if you invest before a set date or say the opportunity is only available for a short period.
3. **Social proof** – They may share fake reviews and claim other clients have invested or are interested.
4. **Unrealistic returns** – Fraudsters often promise tempting returns that sound too good to be true, such as better interest rates than elsewhere.
5. **False authority** - Using convincing literature and websites, claiming to be regulated, speaking with authority on investment products.
6. **Flattery** – Building a friendship with you to lull you into a false sense of security.

To reduce the chance of falling victim to investment fraud, the Financial Conduct Authority advises consumers to, at the very least:

1. **Reject** unsolicited investment offers whether made online, on social media or over the phone.
2. Before investing, **check** the FCA Register to see if the firm or individual you are dealing with is authorised and check the FCA Warning List of firms to avoid.
3. Get **impartial advice** before investing.

The FCA's ScamSmart campaign encourages those considering investing to check its dedicated website www.fca.org.uk/scamsmart or 0800 111 6768 for tips on how to avoid investment fraud.

Push Payment Fraud

is when Fraudsters impersonate officials (normally HMRC or Bank staff) and trick victims into making payments over the phone or via internet banking.

In the **bank** scenario, fraudsters cold call (or send a text message to) the victim and state that the victims account has been compromised and they need to transfer money to a "secure" account or else their money will be stolen. In reality the "secure account" is controlled by the criminals.
The fraudsters may "spoof" their phone number to make it look like the victims' bank is calling them.

In the **Tax office** scenario, victims are called by fraudsters and informed that there is a warrant out for their arrest following non-payment of taxes. Payment is then demanded over the phone to avoid going to court. HMRC/Tax office does **not** do this. This is a scam.
HMRCs have more details on how they genuinely get in contact with you on their website.
https://www.gov.uk/topic/dealing-with-hmrc/phishing-scams

Advance Fee

Victims are encouraged to pay an advance fee for goods or services or with promise of a larger amount back in return. E.g. a scam email from the "Tax Office" stating that the victim is owed a refund for overpayment of tax, but requesting an admin fee first.

How to avoid being a victim of this type of fraud:

- **Never** give your bank details or personal information following an unsolicited email. If claiming to be a government affiliated organisation (e.g. DVLA, Tax office, Council etc.) Confirm with the organisation via a pre-established contact method (i.e. the phone number on the company's website).
- **Check that the advertisement is genuine** – Search for the website of the Company using tools such as Google. Do not rely upon links provided in e-mails received from organisations. Research the company and look for reviews.
- **Carry out checks on telephone numbers on-line**. The internet is a useful tool for identifying scams. Consider using numbers identified from your own searches rather than any provided in e-mails e.g. Check telephone directories with respected providers.
- **Be aware of advertisements with e-mail addresses provided free** (e.g. Hotmail, Gmail etc) whilst some smaller organisations may use e-mail facilities from these sources, this is much less common with larger businesses.
- **Be cautious if you are ever asked to pay up front fees**.
- **Be very cautious if you are asked to pay fees by e-money** or via money transfer bureaus. This allows the scammers easy access to the funds and often makes it very difficult to trace their identity.
- **Seek advice or a second opinion before engaging with the organisations.**

Payment Fraud

Payment or **Mandate** Fraud is when fraudsters **get a victim to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation they make regular payments to, for example a subscription, membership or a business supplier. Normally this is done via email where one of the email accounts is hacked and emails containing "new" bank account details are sent.**

- Always **verify** requests for amended payments to an organisation directly using established contact details.
- If a call seems suspicious, hang up and call the organisation using established contact details.
- Never leave invoices, regular payment mandates or similar information unattended for others to see.
- Check bank statements carefully and report anything suspicious to your bank.
- Make sure colleagues, particularly those in a finance function, are aware of the risks
- Avoid using public Wi-Fi systems to check emails when house purchases are being made. Fraudsters can easily hack into vulnerable Wi-Fi systems.
- Avoid posting on social media about buying/selling your house or getting a mortgage. Fraudsters may get hold of this information and know the next step is a large financial transaction.
- Make sure you have strong passwords for your accounts and have anti-virus installed on your devices. To create a strong password, simply choose three random words. Numbers and symbols can still be used if needed.

Please see our video for more details; https://www.youtube.com/watch?v=O1tktyF0-Tg

Remember, criminals can spoof their number, i.e. they can change their number to be anything they like, such as the number on the back of your bank card.
Caller ID is NOT proof of idenitity.

Your bank, the police, tax office, or any other legitimate organisation will never ask you to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers. This is a scam.

Whenever you get unsolicited contact from a business, take 5 minutes to verify their claims via a trusted method. Never use the number given in an email, text or call.

1. **Hang up** (Never give details or money following a cold call)
2. **Take 5** (Seek a second opinion, tell someone what has happened)
3. **Verify** (if concerned, contact the company via a pre-confirmed method)

Please help us share this information, tell your family, friends and neighbours as people are still falling victim to these types of fraud.
All of our videos and electronic leaflets can be found on the following link;
www.met.police.uk/littlemedia

Always report, Scams fraud and cyber crime to Action Fraud,
either online at **www.actionfraud.police.uk** **or by telephone on 0300 123 2040.**

More than £900,000 confiscated from cyber hacker

A prolific hacker who carried out cyber-attacks on more than 100 companies worldwide has been ordered to pay back £922,978.14 of cryptocurrency he had stashed away.

Grant West, 26 (15.02.1992) of Ashcroft Caravan Park, Sheerness, Kent, was subject to a confiscation order under the Proceeds of Crime Act at Southwark Crown Court on Friday, 23 August.

The confiscation of the cryptocurrency, which West did not contest, follows a lengthy police investigation, codename 'Operation Draba', into the criminal activities of West, who was operating on the Dark Web under the moniker of 'Courvoisier'.

The cryptocurrency will now be sold, and the victims will receive compensation for the damage caused by the organised criminality committed by West.

West was responsible for attacks on more than 100 companies worldwide. He predominately used ‘phishing’ email scams to obtain the financial data of tens of thousands of customers. West would then sell this personal data in different market places on the dark web.

He would then convert the profit made from selling financial details online into cryptocurrency, and store these in multiple accounts.

West was jailed on Friday, 25 May at Southwark Crown Court for 10 years’ and eight months’.

Officers from the Met’s Police Cyber Crime Unit (MPCCU) arrested and charged West in September 2017 following a two-year investigation. He was identified as the head of an Organised Crime Network (OCN) which predominantly targeted London-based organisations.

Throughout the course of the investigation detectives discovered evidence of West conducting cyberattacks on the websites of 17 major firms including Sainsbury’s, Nectar, Groupon, AO.com, Ladbrokes, Coral Betting, Uber, Vitality, RS Feva Class Association 2017, Asda, the British Cardiovascular Society, Mighty Deals Limited, Truly Experiences Ltd, T Mobile, M R Porter, the Finnish Bitcoin exchange, and Argos.

Following West’s arrest, approximately £1 million worth of cryptocurrency was seized from a number of his accounts. Taking currency fluctuations into account the currency is today valued at £922, 978.14.

West started trading on the dark web in March 2015 and completed more than 47,000 sales from an online "store". As well as financial data, he also sold cannabis which he shipped to customers, and ‘how to’ guides instructing others how to carry out cyberattacks.

Between July and December 2015, West perpetrated a phishing scam masquerading as online takeaway service Just Eat, in an attempt to obtain the personal details of 165,000 people. Although no financial information was obtained, his actions cost the firm approximately £200,000.

West carried out the attacks from a laptop belonging to his girlfriend, Rachael Brookes. He also stored personal financial information, also known as "fullz", belonging to more than 100,000 people on the device.

Officers also recovered an SD card from West’s home address in Kent and discovered approximately 78 million individual usernames and passwords as well as 63,000 credit and debit card details stored on it.

As well as selling information online, West also regularly used stolen credit card details to pay for items for himself, including holidays, food, shopping and household goods.

Throughout the course of the investigation £25,000 cash and half a kilogram of cannabis was seized from storage units rented by West across Kent.

Grant West, 26 (15.02.1992) of Ashcroft Caravan Park, Sheerness, Kent, pleaded guilty to the following offences at Southwark Crown Court on 14 December 2017.

2 x conspiracy to defraud;

2 x possession of criminal property;

1 x unauthorised modification of computer material;

1 x possession of a Class B drug with intent to supply;

1 x possession of Class B drug

1 x attempting to supply a controlled drug;

1 x offering to supply a Class B drug, and;

1 x concealing/removing criminal property from England and Wales, Scotland or Northern Ireland.

Head of the Met's Cyber Crime Unit, Detective Chief Inspector Kirsty Goldsmith, said: "The MPS is committed to ensuring that individuals who are committing criminality on the Dark Web are identified, prosecuted and their criminal assets are seized.

"I wish to thank our partners within the MPS and in both public and private industry who have all assisted with this investigation which was incredibly complex and lengthy. I am very proud of my team for bringing this offender to justice and ensuring we have secured this order."

To reduce your chances of being a victim of cybercrime, it is important to use strong passwords, preferably three different words and numbers and symbols.

Detectives investigating a murder in Chessington have made a fifth arrest.

A 17-year-old male [E] was arrested on suspicion of murder on Monday, 26 August and later released under investigation.

Police were called to a car in collision with a man on Moor Lane in Chessington at 00:13hrs on Friday, 26 July.

The driver did not stop and the man was dragged under the car for some distance. Officers attended along with the London Ambulance Service.

Liam Dent, 25, from Chessington, was pronounced dead at the scene, and his next of kin continue to receive support from specialist officers.

A post-mortem examination held at Kingston Mortuary on Saturday, 27 July established cause of death as injuries consistent with a collision.

The car believed to have been involved in the incident, a Ford S Max, was found burnt out on Cyclamen Way in Epsom, approximately one mile from the crime scene. Since then a further two vehicles have been recovered.

On Thursday, 1 August, a 17-year-old male [A] was arrested on suspicion of murder by officers in Surrey on behalf of the Met, and taken to a local police station. He has since been bailed to a date in September.

A 22-year-old man [B] was arrested on suspicion of murder on Thursday, 8 August, at an address in Epsom. He has been released on bail to a date in September.

On Thursday, 15 August, officers arrested two people as part of the investigation. A 19-year-old man [C] was arrested on suspicion of murder. He has been bailed to a date in

September.

A 17-year-old girl [D] was arrested on suspicion of assisting an offender. She has since been bailed to return on a date in mid-September.

Any witnesses, or anyone with information that may assist police, should call the incident room number on 020 8721 4622 or 101 quoting CAD 96/26July. To remain anonymous, call Crimestoppers on 0800 555 111.

Appeal – Can you Help?

Driver of a white Fiat Dobio van to Contact police

Officers are appealing for a van driver who drove off from the scene of a serious collision in Kingston to come forward. They also wish to speak with witnesses to the collision.

Police were called at around 15:50hrs on Tuesday, 27 August, to a van in collision with a cyclist in Queen Elizabeth Road near the junction with Hardman Road, Kingston.

Officers attended along with London Ambulance Service. The cyclist – a 41-year-old man – was taken to hospital, where his condition is life-threatening.

The driver of the van, a white Fiat Dobio, stopped briefly at the scene and spoke with the injured cyclist before driving off. Police are now appealing for this van driver to come forward and speak with officers.

Officers are also appealing for any witnesses to call them on 020 8543 5157.

Taser Q and A, Monday 9th September 7-8pm, Guildhall, Kingston

Doorcam


SHOP NOW
RESPONSE @ ERA
ERA
ERA
BE IN...
EVEN WHEN YOU'RE OUT
DOORCAM
THE SMART WAY TO ANSWER YOUR DOOR
The DoorCam smart doorbell means you will never miss a caller at your door, even when you're out. Using HD video with zoom capability and a 180 degree fish eye lens, DoorCam delivers excellent video quality so you can see, hear and talk to the caller through your smartphone, wherever you are.
With adjustable motion detection, video recording and snapshots all managed through an easy to use smartphone app, you can know who is at your door before they even press the button, giving you convenience and security in one.
You can choose to either simply wire to existing doorbell wiring or use with the plug adaptor for use in a standard UK socket. The package includes a plug-in WiFi Chime, so even when you are home, you can hear the doorbell.
No hassle. Just simple smart security.

Travelling by Train?

Did you know you can discreetly text British Transport Police if something concerns you? Tell them what happened and where by text 61016.

Contact Details for Safer Neighbourhood Teams

ALEXANDRA	**020 8721 2516** KingstonAlexandra.SNT@Met.police.uk
BERRYLANDS	**020 8721 2002** Berrylands.SNT@Met.Police.uk
BEVERLEY	**020 8721 2750** Beverley.SNT@Met.Police.uk
CANBURY	**020 8721 5882** Canbury.SNT@Met.Police.uk
CHESSINGTON NORTH	**07342 713970** Chessington.SNT@Met.Police.uk
CHESSINGTON SOUTH	**020 8721 2011** Chessingtonsouth.snt@met.police.uk
COOMBE HILL	**020 8721 2804** Coombe.Hill.SNT@Met.Police.uk

COOMBE VALE	**020 8721 2515** **CoombeVale.SNT@Met.Police.uk**
GROVE	**020 8721 2588** **Grove.SNT@Met.Police.uk**
NORBITON	**020 8721 2000** **Norbiton.SNT@Met.Police.uk**
OLD MALDEN	**020 8721 2517** **OldMalden.SNT@Met.Police.uk**
ST JAMES	**020 8721 2595** **StJames.SNT@Met.Police.uk**
ST MARKS	**020 8721 2044** **StMarks.SNT@Met.Police.uk**
SURBITON HILL	**020 8721 2518** **SurbitonHill.SNT@Met.Police.uk**
TOLWORTH	**020 8721 2045** tolworth.snt@met.police.uk
TUDOR	**020 8721 2580** **Tudor.SNT@Met.Police.uk**

Easyfundraising

Did you know that whenever you buy anything online - from your weekly shop to your annual holiday - you could be raising a free donation for Kingston Borough Neighbourhood Watch? There are nearly 3,000 retailers on board ready to make a donation, including Amazon, John Lewis, Aviva, thetrainline and Sainsbury's – it doesn't cost you a penny extra!

It's really simple, all you have to do is:

1. Join.
Head to http://www.easyfundraising.org.uk/causes/kingstonboroughneighbourhoodwatch/ and sign up for free.

2. Shop.
Every time you shop online, go to easyfundraising first, pick the retailer you want and start shopping.

3. Raise.
After you've checked out, that retailer will make a donation to your good cause for no extra cost whatsoever!

Co Op Home Insurance Discount

Neighbourhood Watch 10% discount offer

All new Co-op Insurance customers who are active members of a Neighbourhood Watch Scheme and purchase a home insurance policy directly from Co-op Insurance over the phone will receive a 10% discount for the first year of their policy. In order to claim this offer you will need to telephone their customer contact centre for a quote. An active member of a valid Neighbourhood Watch Scheme is someone who is designated as such by Neighbourhood Watch. The terms and conditions of this promotion do not alter or vary the terms and conditions of any Co-op Insurance home policy which may be purchased. The Co-op reserve the right to decline any application for any insurance policy in their absolute discretion and they are not obliged to disclose any reason for rejection. Please visit www.ourwatch.org.uk/exclusions-and-limitations/ for Exclusions and Limitations for this offer. A new customer is someone who has not had an Insurance policy of the same type with Co-op Insurance in the last 12 months. Home insurance lines are open from 8am- 8pm weekdays, 8am-5pm Saturdays and 9am-4pm Sundays. Applicants for insurance are subject to normal underwriting criteria.

Call the Co-op on 0800 781 1390 and quote code NHW10

Social Media

Kingston Police, Neighbourhood Watch and Business Watch are all on social media. We would love you to follow us:

@mpskingston

@KingstonNHW

@KBBusinessWatch

/mpskingston

/KingstonNHW

/KingstonBoroughBusinessWatch