Kingston Borough Cyber Crime Monthly Summary – October 2019

Fraud Type	Amount of Offences	Amount Lost
Misc. (False Representation)	17	£0
Cheque, Plastic Card and Online Bank Accounts (Banking Fraud)	15	£117,941
Online Shopping and Auctions	15	£3,155
Computer Software Service Fraud	8	£21,870
Push Payment	7	£83,981

Fraud Type	Amount Lost	Amount of Offences
Mandate Fraud	£300,300	3
Other Financial Investment	£200,000	1
Cheque, Plastic Card and Online Bank Accounts (Banking Fraud)	£117,941	15
Push Payment	£83,981	7
Dating Scam	£40,839	3

Total Number of offences	101
Total loss	£858,399
Average per victim	£8,499

Online Shopping

Victims are convinced in to paying money for items that don't exist or are counterfeit when shopping online. E.g. fake adverts on eBay. Criminal convince their victims by offering cheaper deals, or discounts if they transfer the money directly to their bank account, rather than using the recommended payment method.

How to stay safe

- Stay on site!
- Be wary of offers that look too good to be true.
- Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.
- Research the seller/buyer and any of their bidding history.
- Don't be convinced by the sellers' profile pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com/ or https://reverse.photos/
- Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.
- Never buy a vehicle without seeing it in person. Ask to see the relevant documentation for the vehicle to ensure the seller has ownership. If you are selling online, be wary of any emails stating funds have been sent.
- Log in to your account via your normal route (not via link in email) to check this.
- Watch our video on Online Shopping Fraud at www.met.police.uk/littlemedia.

Remember

Never pay via direct bank transfers, always use the websites recommended payment method.
If it's too good to be true, it probably is!

Push Payment Fraud

Online banking makes managing money easier for the general public, however criminals are taking advantage of this ease of banking and using it to defraud the public.

Criminals can pretend to be from somewhere official, for example, your bank, or the tax office. They contact you via email, phone or social media, and then warn you of fake suspicious or criminal activity on your bank account. They state that they've set up a safe account for you to transfer your funds into. However, this is actually their account.

How to protect yourself

- Be suspicious of a call out of the blue from someone claiming to be from a position of authority.
- Take down the person's details (name, authority, department, branch etc.) and verify using independent source contact details.
- A genuine official from the Police, your bank, HMRC or any other trusted authority will **NEVER** call you to ask you to verify your personal banking details, PIN or password or threaten you with arrest.
- Never transfer money into another account unless you are 100% certain of the owner of the account.
- Your bank will never set up a "safe" account for you.
- If you are a victim, contact your bank *as soon as possible*, as they may be able to help stop the transfer.
- Watch our video on Impersonation Fraud at www.met.police.uk/littlemedia.

Remember

Your bank will never set up a "safe account" and the HMRC conducts the majority of correspondence by letter, and will never call and threaten arrest. No reputable company will demand you pay money over the phone, or purchase items (like vouchers)

Computer Software Service Fraud.

Where fraudsters phone the victims and claiming that they were internet providers, (E.g. Talktalk, BT, EE) Microsoft or similar and state there is an issue with their computer/internet/router and either demand money to prevent their internet being shut off, or offer to help the victim "fix" the problem by getting the victim to install "team viewer" (or similar) a program which gives the fraudster remote access to the victims computer. Once the fraudster has access to the victms computer they will see what they can find or steal to defraud the victim or demand payment for their services. This, is a scam.
So remember

- Your service provider will never contact you out of the blue because of unusual activity on your computer.
- Never give someone remote access to your computer.

Please watch our video for more information:
https://www.youtube.com/watch?v=aJA-eyVtOW4

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.**