Eastern Region Special Operations Unit

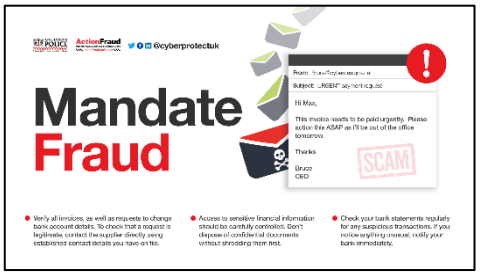
Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Friday 17th April 2020

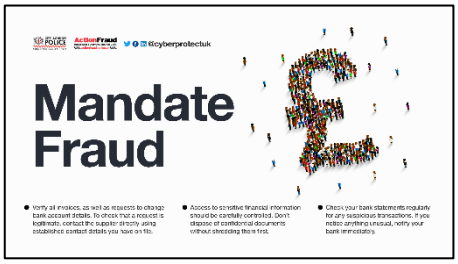
Today's topic is 'Mandate Fraud'.

How does a typical Mandate fraud occur?



- Businesses are contacted by someone pretending to be one of their suppliers and told they have changed their bank, requesting they amend the direct debit to reflect this. The genuine supplier then gets in touch to ask what happened to the monthly payments.
- Individuals are contacted by someone pretending to be from an organisation you have a mandate with and they ask you change it as they are changing their banking. Next month your products or services fail to arrive, as they did not receive their payment.
- Online bank accounts are hacked into by fraudsters and monthly payment details are altered so that the money is transferred to the fraudster's account.

Advice to avoid Mandate fraud



- Verify all invoices, as well as requests to change bank account details. To check a request is legitimate, contact the supplier directly using established contact details you have on file.
- Access to sensitive financial information should be carefully controlled. Don't dispose of confidential documents without shredding them first.
- Check your bank statements regularly for any suspicious transactions. If you notice anything unusual, notify your bank immediately.

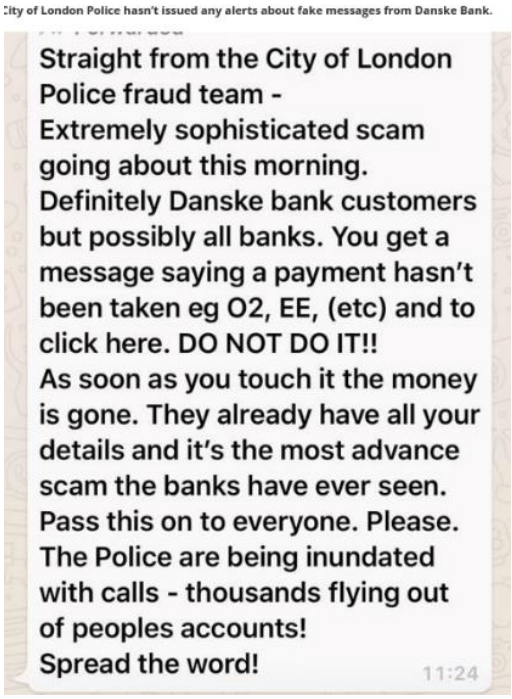
Visit Action Fraud for more information.

Trending

Eastern Region Special Operations Unit

Regional Organised Crime Unit

Action Fraud are aware of a rumour currently circulating via WhatsApp, SMS and social media which references the City of London Police Fraud Team and claims that Danske Bank customers are being targeted by a particular text message (smishing) scam. The content of this message is false.



However, smishing scams are common. Don't click on the links or attachments in any suspicious emails or texts, and never respond to messages that ask for your personal or financial details. It's important to remember that your bank would never ask you to move money out of your account, or contact you out of the blue and ask for details such as your full banking password or PIN number.

Anyone who has divulged information after receiving this type of message should contact their bank immediately.

Fraudulent websites are also being set-up, which offers an antivirus program to protect users against the coronavirus. Fraudsters trick users into downloading a remote access Trojan and install malware that could infect the user's device. Once access has been obtained, the fraudster could act as a legitimate user but use this access to steal data and seek financial gain.

Reporting

Reporting is CRUCIAL. If you think you've been a victim of fraud report this to Action Fraud either online at or by calling 0300 123 2040.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public. Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.