March 2022

GREATER MANCHESTER POLICE

ECONOMIC CRIME UNIT

Scam Care Awareness Messages (SCAM)

PROTECT YOURSELF AGAINST FRAUD BY STAYING UP TO DATE WITH THE LATEST SCAMS

What is the Economic Crime Unit?

The ECU is part of the Serious Crime Division of Greater Manchester Police. We have responsibility for all economic and cyber-dependant crime (crimes that are committed using technology) in the Greater Manchester Area.

Our primary function is to ensure that the public are informed of and protected against fraud and cybercrime while bringing offenders to justice, tracing and seizing criminals assets.

Follow us at @gmpfraud on Twitter

Netflix, Apple and Spotify phishing scam: Men admit selling data

Two men who posed as Apple, Netflix and Spotify in millions of emails to steal data have pleaded guilty to selling it for cryptocurrency worth £140,000.

Gary Kelly, 32, and Craig Gorton, 30, stole information relating to at least 64,000 credit cards and 24,000 Apple IDs via a number of phishing campaigns.

Several devices were seized and found to contain stolen customer databases.

A spokesman for the North West Regional Organised Crime Unit (NWROCU) said the two men were caught after officers were alerted to the phishing, a process where a fraudster poses as a reputable company in an attempt to get bank details or passwords.

He said Kelly, of Charles Street in Farnworth, Bolton, and Gorton, of Rochdale Old Road in Bury, were responsible for a number of campaigns which involved "sending millions of emails to people portraying to be from Apple, Netflix and Spotify".

"Once the victim provided their personal and financial details, the duo sold their information on a website," he added.

Courier fraud is when a victim receives contact from a fraudster claiming to be a police officer or bank official. Criminals convince victims to either draw cash out for collection at their home address or to transfer money to a 'secure' bank account, hand over their bank cards or to purchase high value items specifically requested and then handed over such as watches, jewellery and gold (coins or bullion). Protect yourself - Your bank or the police will never make requests such as this. Hang up immediately. Check - If you need to call your bank, wait 5 minutes as fraudsters may stay on your line and use a telephone number you know to be your bank to call back. Never hand over you bank debit or credit cards to strangers, you should only ever hand to your bank if necessary. If your cards are cancelled or expired destroy them yourselves. If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at www.actionfraud.police.uk or by calling 0300 123 2040

Good News

- Fraud Triage Desk DC Mason located a sum in the region £600k for a victim of Mandate fraud, this week they were unaware had been set aside for return. The victim said 'it was the best phone call he had ever had in his life'. He is now able to contact his bank and complete an indemnity process to obtain the return of his funds

Upcoming Events

Crucial Crew is a multi-agency safety event aimed at Year 5/6 primary school children (10 to 11 year olds). It has been designed to provide children with life skills that will, in the future, help to keep themselves and others safe.
GMP Cyber Protect Officer (along with other members of the Cyber Crime Team) attends events (across numerous Greater Manchester boroughs) and provide 12 x 15 minute sessions each day, often over the 3 week period.
They cover topics on; Passwords, updates, Social media, privacy & location settings, and bullying.
They also included 4 age appropriate prevent slides on CMA, consequences, and tech opportunities.

Follow us at @gmpfraud on Twitter

Cyber Security tips

- Never give an unsolicited caller remote access to your computer.
- Clicking Without Thinking Is Reckless
- Make sure your computer is protected with regularly updated anti- virus and anti-spyware software, and a good firewall.
- Be careful and exercise caution when installing apps, browsing the web, and following instructions
- Back up your data regularly
- If you have given fraudsters access to your computer you should consider resetting your computer

➢ Microsoft error and warning messages never include phone numbers.