Dear Teachers, Parents and Carers,

I am writing to you with warning of a highly lucrative Snapchat scheme (although not limited to), which takes advantage of children's bank accounts 16-18, offering them money for taking part in a wider money laundering scam.

What is money muling and why do criminals target children?

Organised Crime Gangs (OCGs) and criminals need to make proceeds from their wrongdoings as difficult to trace as possible, so they can avoid being linked to a particular crime. This is why they recruit - usually unsuspecting people - into assisting them, with the promise of 'free and easy' money.

The idea here is that the target (child) moves the money along between bank accounts, very quickly, which reduces the chances of being traced - as an incentive, the child is promised a small cut. 9 times out of 10 they don't receive that cut but the larger gangs may choose to pay up as this either keeps the recipient quiet, or it helps recruit their friends too. Children are an easy target because most don't have means of earning money themselves. With social media advertising the latest gadgets and designer clothes, it can be difficult for a child to say no to this money, and most of the time they don't even realise it's a crime.

OCG's use social media to recruit people, using the likes of Instagram, Facebook and Snapchat, saying something along the lines of 'instant cash'. It draws the attention of the reader and before they know what's happening, they are in on it. It is normal for there to be some aspect of social proof, like a text message or photo, which again makes it seem like a legitimate process.

Some recruiters even go the extra mile and advertise money muling jobs on search sites like Reed and Indeed, but under an obscure name like "currency controllers".

So what happens if they say yes?

1. They will ask the child for bank account details so they can transfer over a large amount of money

2. Ask them to transfer the money on to another account. In some cases, they may ask the child to withdraw the money in cash from an ATM and deposit it into their friends account – cash makes it even more difficult to trace back and adds an extra person to the scheme

3. They may or may not get a percentage, but they then also become a criminal too.

Consequences of being a mule

Becoming part of a money laundering scheme, whether or not the recipient is aware of what's happening has serious consequences.

The banks may detect the recipient is moving fraudulent money and choose to close their account immediately. They may choose to add the recipient to a fraud database, which could make it very hard to open another account.

If they are without a bank account, it may be very difficult to get a job and be put on a payroll. It could also make it difficult for them to access credit, so things like a mortgage, credit card or over draft, mobile contract or car finance could all be out of reach.

If reported, the account holder is the one who will be questioned by the police, whereas the offender/recruiter or perpetrator, who has totally used the account holder, gets to remain anonymous and not linked to the crime.

The recipient of the laundered money could held accountable. **I should point out that money laundering offences carry a term of up to 14 years imprisonment.**

How do we stop more children falling victim

Most children have absolutely no idea of why someone wants to use their account in exchange for money. All they want is to be able to buy a new pair of shoes or game for their PlayStation/Xbox. They really do not know the long terms effects of being part of a money laundering scheme, so we must educate them. If they handover their banking information and receive a sum of money, they are assisting criminals to get away with awful crimes like, terrorism, human trafficking, modern slavery and your everyday fraud.

We need to take a common sense approach. If it sounds too good to be true, then it usually is! A person should never willingly handover their banking information to someone they don't know – once they do they have absolutely no protection if it inevitably turns out to be fraud. Sensitive personal information like someone's DOB, home address and name are extremely difficult to change – they are not like usernames, email address and passwords. If a criminal has all a child's personal information, which they gave up voluntarily, then it can be very easy for them to impersonate them. They can do things like open credit or put debt in their name. This causes unwanted and unnecessary stress for their future. Children MUST protect their personal information at all times!

Resources

Please find below some useful websites that will provide assistance with securing your digital life and online presence:

- https://twofactorauth.org/ - Set up 2FA.
- https://takefive-stopfraud.org.uk/ - how to protect yourself against fraud.
- https://www.ncsc.gov.uk/cyberaware/home - Cyber Aware information.
- https://www.getsafeonline.org/ - Safety tips for online usage.
- https://howsecureismypassword.net/ - Check the strength of a password.
- https://www.howtogeek.com/ - Technology explained.
- https://www.lifewire.com/ - Something technical, explained in a non-technical way.

Finally, if someone has fallen victim to a scam/fraud then it should be directly reported to the social media platform, if applicable, and most importantly to Action Fraud - https://www.actionfraud.police.uk/

If you require additional assistance, please contact me on the details provided below.

Sincerely,

Drew Jefferies

Cyber Protect Officer

Tel: 077802874715

Email: drew.jefferies@avonandsomerset.police.uk