OPERATION REPEAT

Reinforcing Elderly Persons Education at All Times

COVID-19 SCAMWISE

The current situation is a wonderful opportunity if you are a criminal. Already we are seeing new twists to old themes appearing on our computers, mobiles and landline telephones. The doorstep doesn't escape either, with cold callers offering their new concept to get you to hand over money.

City of London Police recently reported a 400% increase in criminal scams as a result of coronavirus related fraud. Action Fraud reports 862 victims lost £2,120,870.00 having also received over 5000 coronavirus related phishing emails. Those are the ones that have been reported. As you know all such incidents are under-reported and the figures could easily be ten fold on this number and as we stay in this un-precedented situation, it will only get worse.

The following items relate to known incidents reported *[sources listed below]* since the outbreak of coronavirus but will by no means encompass every variation of scam being attempted across the crime enablers of Doorstep, Telephone, Mobile or Computer. This list is designed to give a general conception of the lengths that criminals have already gone to in such a short space of time to up their game and take advantage of this horrendous situation.

We ask that you take a moment or two to read and digest the information. By doing so you will have more knowledge and remember, **#KNOWLEDGE is KEY in #PREVENTION.**

The Scam list:

Doorstep:

- Cold Calling Doorstep Criminals have been pitching up and offering to go shopping for older / vulnerable people. But, as shops aren't accepting cash, they will need your card and PIN in order to pay for your groceries.
- Others are purporting to be from organisations such as British Red Cross, coming to check your temperature to see if you have Coronavirus. In this instance they will also require you to pay them a fee for the test.
- Bogus Health Workers also cold calling offering fake COVID-19 home testing kits and sanitisers, some of which contain glutaral (or glutaraldehyde, which was banned for human use in 2014.) again with payment required on the doorstep.
- Doorstep and driveway cleansing services to keep the virus away.
- Criminal Tradesmen cold calling offering to finish off work that genuine tradespeople have had to leave, claiming the lockdown does not apply to them!
- Up front payment to ensure your black waste bin is emptied.

Telephone:

- Calls claiming to be from Amazon, stating your account has been hacked and requesting your details to open new account.
- Your bank /HMRC requesting personal details including PIN or account login information or asking you to move money to 'safe account'.
- Your phone provider needs to update your account and requires your payment details.

Mobile:

- Fake text message issuing a Government fine for breaching the 'lockdown' rules.
- HMRC refund text, requiring your bank details.
- 'Tap Here' to receive £458.00 Government refund text.

Online:

- Fake Government email claiming to be collecting donations for NHS.
- HMRC refund email, with link to 'click' to receive money.
- Fake supermarket vouchers with link to 'click' to receive your voucher.
- DWP email requesting 'update' of your personal details.
- Fake Paypal message 'declining' your last transaction, with 'recovery' button within text of email.
- False Coronavirus maps, delivering malware onto your computer.
- Free school meal, requiring details of your bank account to be forwarded.

Other:

- Social media attempts to get you to supply personal details, which in turn can be used for 'social engineering' by criminals (such as #gettoknowyou challenge).
- New friend requests from people you do not know.
- Chain letter type request on behalf of 'NHS' member or similar, asking for 10 friends to forward post on – usually with some heartfelt message, but, allows access to all those friends who have not set privacy correctly.

And as time moves on there will be other variations of the above, all aimed at taking your money!

Simple messages to REPEAT:

- **DON'T DEAL WITH COLD CALLERS!**
- **DON'T TALK MONEY ON THE PHONE!**
- **DON'T CLICK THAT LINK or ATTACHMENT!**
- **DON'T RESPOND to UNSOLICITED EMAILS!**
- **UPDATE YOUR SOFTWARE!**
- **DON'T FORGET ANTIVIRUS PROTECTION FOR MOBILE's & TABLETS!**

We know under the current conditions you are going to be under enormous pressure in completing your normal work and activities. But we also know your training with Operation REPEAT will have alerted you to much of what is going on in the big wide world. This note is a reminder at how quickly the 'professional criminals' seize a situation and turn it to their advantage.

The good thing is, they don't know about **YOU!**

They don't know how professional **YOU** are at making sure those around you know about **SCAMS** and how to prevent them.

They don't know that **YOU** can **SPOT** their **SCAMS** a mile off and send them packing and, how good **YOU** are at sharing this information with all those you do come into contact with.

To that end, we thank you for helping to **KEEP PEOPLE SAFE**!

Keep up the good work.
We are proud of what you are achieving in very difficult circumstances.

Reg Burrell (Director)

OPERATION REPEAT
Reinforcing Elderly Persons Education at All Times

[Sources: Action Fraud; CTSI; NCA; NTS]