Fighting Back Against Fraudsters

It's almost too much to bear: hundreds of thousands are losing their lives, millions are losing their jobs and unknown numbers of us are dealing with innumerable other stresses triggered by Covid-19. To make matters worse, there are opportunistic cyber-criminals taking advantage of our insecurities as well as the goodwill that is inherent within the majority of us.

From the early days of remote working, hacking events have surged as compromised technology and weakened security have allowed easier access to network systems. Further, cyber criminals are exploiting human frailties.

Our natural fears and anxieties are being used against us as criminals seek to offer us fraudulent PPE, home-testing kits and cures. The appeal is all too obvious.

These fraudulent activities are carried out via email, phone scams (e.g. offering free home testing kits or the promotion of bogus cures), or hoax texts (including one that offered a $30,000 "relief" package from "The Financial Care Center" and another that informed recipients that they must take a mandatory online Covid-19 test; both attempts to obtain banking and other personal information).

The majority of these scams are technology-based but sadly, there are also "doorstop criminals", who cold-call at the homes of older and vulnerable residents.

Equally repugnant are the fraudulent attempts to prey on our generosity of spirit - that spirit clearly evident in our nation's response to Captain Tom Moore's heroic efforts. Bogus websites have been set up posing as charities to channel funds into cyber-criminals' bank accounts.

While spotting a phishing email is becoming increasingly difficult, the National Cyber Security Centre (NCSC) has put together a list with some common signs to look for:

- **Authority** - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.
- **Current events** - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

The overriding message is: Don't trust information that doesn't come from official sources and be suspicious of messages coming from a company from which you don't normally receive communications.

The other message is: Let's fight back.

The NCSC has launched a suspicious email reporting service and is encouraging the public to use it. The NCSC's automated scanning system has the ability to scan and remove criminal sites.

The NCSC has, in the last month, removed:

- 471 fake online shops selling fraudulent coronavirus-related items
- 555 malware distribution sites set up to cause significant damage to visitors
- 200 phishing sites seeking personal information such as passwords and credit card details
- 832 advance-fee frauds where a large sum of money is promised in return for a set-up payment

Further, the UK government is asking that scam text messages are forwarded on to 60599 (albeit at standard network rates). Scam phone calls should be reported to the HMRC's phishing team.

We have been given the opportunity to use technology against the criminals – to turn the tide. Let's use it.

For further details please contact:

Vanessa Cathie | Account Executive,
Global Professional & Financial Risks

E vanessa.cathie@uk.lockton.com
T +44 (0) 20 7933 2478