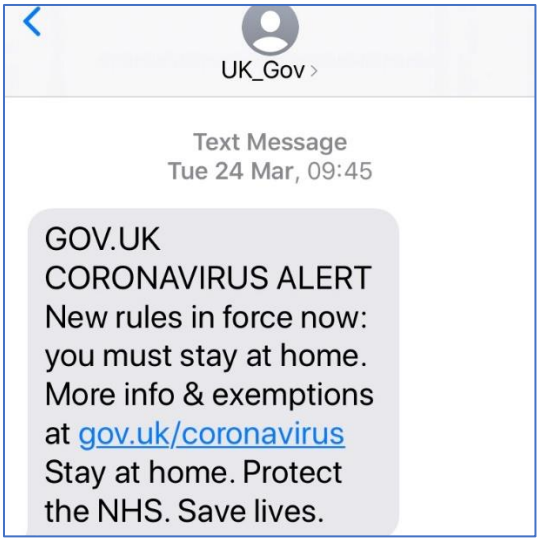
Working from home or furloughed: the risk from fraud is probably greater than ever.

With the Covid-19 "lockdown" affecting everyone's lives, and the massive changes in our work, domestic, and travel arrangements, it wasn't going to take fraudsters long to adapt to the new conditions. In many ways fraudsters act exactly like a virus: they rely on human interaction to transmit their disease, and they will adapt to the environment to try and achieve their aim – which is to suck life from you!

One of the most well-known methods is the email or text message which pretends to be a trusted person: a member of your team, a manager, a client, or even a government department. Within a few hours of the (genuine) text message sent from the Cabinet Office to every mobile phone in the country giving advice about the Covid-19 emergency, fraudsters were targeting mobile phone numbers with their own version. And, like the official advice, the messages had a hyperlink to a website. The genuine message you will have received is shown below:



The fake messages will look very similar to this, but you can check the hyperlink without opening it. On a smartphone, hold your finger over the hyperlink until a box opens, which will show the address that it will direct to. In this case it is http://gov.uk/coronavirus Note that, although it's a .gov.uk address it doesn't use a secure protocol: http stands for HyperText Transfer Protocol, whereas the secure version is https, which stands for HyperText Transfer Protocol Secure. You can, in fact, go to a secure version of exactly the same webpage: https://gov.uk/coronavirus

Fraudulent versions will either be a misspelled version of this, or will direct you to a different page by editing the hyperlink. The first may look something like this:

http://gov.uk_/coronavirus (this one won't connect to anything – but if you hover your mouse over it you'll see there's an underscore after uk).

The alternative is where the fraudster has edited another hyperlink to make it look exactly the same as the real one. So, I can make this hyperlink (which, in a shameless bit of advertising, goes to my business website!) look as though it's the genuine one:

http://gov.uk/coronavirus

Hover your mouse over the hyperlink and you will see where it directs you!

You may receive emails or WhatsApp messages that apparently come from someone you trust: perhaps a customer. These may tell you that, because of the Coronavirus they have had to change their bank account details. Check the email address in exactly the same way, because they can be falsified in the same way that is described above. Ask yourself if they are use a company email address and, if it looks like one, check it. Your trusted customer may not be the person you know:

Your-trusted-customer@trusted.com (hover your mouse over this email address to see what its real address is!)

This is where some open-source research can really help you. Firstly, use a trusted site to search (I generally use the DuckDuckGo search engine, rather than Google). You might try searching for a phrase in the email that you think is suspicious: in this case put it in speech marks ("suspicious phrase") to make the search specific. You may well find that someone has posted exactly the same text on a scam reporting website. There are trusted sources of information about scams. The UK Government has a webpage with useful links:

https://www.gov.uk/report-suspicious-emails-websites-phishing

And *"Which"* have recently published a useful guide to Coronavirus scams:

https://www.which.co.uk/news/2020/04/coronavirus-scams-how-to-spot-them-and-stop-them/

These types of fraud are commonly referred to as "phishing" attacks – if you identify one and it hasn't been successful (you haven't lost money or data) then you can report it online to the national Action Fraud system (https://www.actionfraud.police.uk/report-phishing). If you have been a victim of fraud, and have lost money or data (leaving aside for a moment any GDPR issues!) then you can report it to Action Fraud as a crime (https://reporting.actionfraud.police.uk/login).

I would always recommend that, if you do make a report, you register with the system rather than reporting it as a "guest." The reason for doing this, although it takes about a minute longer, is that you can provide updates to the report, track its progress and ask for updates about what is being done.

Finally, we all know that in most cases where the fraud has been successful the money is lost forever. Going back to my analogy of fraudsters as a virus, we are all being told to take part in a huge collective effort to prevent Covid-19 from spreading: we need to adopt the same way of thinking to stop the spread of fraud. If that online deal on PPE looks too good to be true, it is! Instead of keeping a two-metre distance from people in the street or a shop, keep an online distance from fraudsters by not following a hyperlink until you're certain of it. Because, if Covid-19 is fatal in 2% of cases and hospitalises 30% of those who contract it, fraud can be as fatal to businesses – and you don't want to be in either the 2% or the 30% group.

Stay safe!

Stephen at Ventham Consulting