Covid-19 Phishing Scams

An increasing number of malicious cyber criminals are exploiting the current COVID-19 pandemic for their own objectives. Below we want to give you an understanding of the ways criminals are exploiting the current situation to attack both personally and professionally.

Due to the current pandemic a lot of these cyber criminals are mirroring websites and text messages, very professionally, from the World Health Organisation and Government Agencies similar to the below.

Figure 1 – UK Government themed SMS phishing

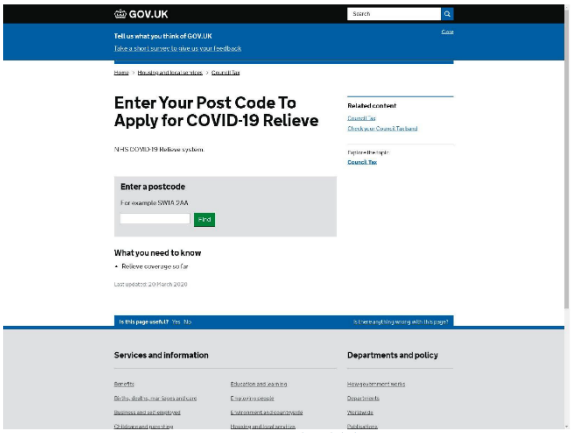

Figure 2 - UK Government themed phishing page

From these phishing attempts two of the most common ways that cyber criminals try and get data from you is:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware.
    - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install 'CovidLock' ransomware on their device.

- Open a file (such as an email attachment) which contains malware.
    - For example, email subject lines contain COVID-19 related phrases such as 'Coronavirus Update' or '2019-nCov: Coronavirus outbreak in your city (Emergency).'

Phishing attempts often show some key indicators that can allow you to spot them and cyber attacks often utilise these 4 aspects to force you into their trap:

- 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 money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

The main thing is to be consciously aware of what you are doing and accessing when online and if something does not feel right then it probably isn't.

If via your FA account you believe you may have fallen victim to one of these activities then please contact our IT Support team immediately.