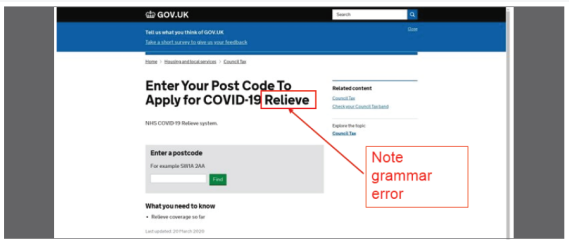
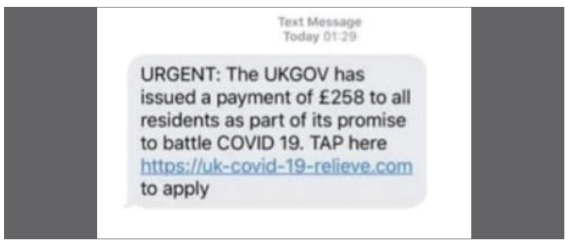
CORONAVIRUS (COVID-19) AND CYBER RISK

Remote working threats and scams

It's been a couple of weeks since many parts of the world went into lockdown to prevent the spread of COVID-19, forcing many workers into remote working. Unsurprisingly, cyber criminals are taking advantage of the current situation and increased number of vulnerable targets.



Website scam (impersonating UK GOV.UK domain).

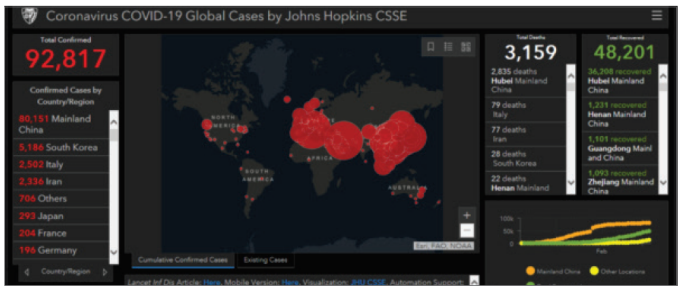


SMS phish purporting to be from GOV.UK.

Below are some of the common attacks we have seen in the last week

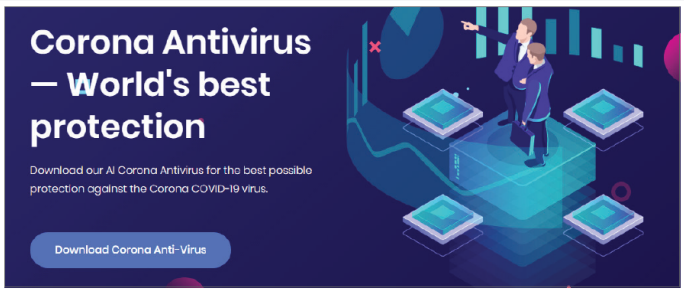
1. COVID-19-themed phishing attacks have been on the increase with all sorts of campaigns ranging from government relief to health information supposedly from the World Health Organisation (WHO).

2. Cyber criminals are preying on people's fears and vulnerable state by developing apps that appear to provide essential and timely information, such as where to buy N95 face masks or how to track recorded cases in real-time.



Fake COVID-19 tracker app providing users with tracking and statistical information about COVID-19 and heatmap visuals.

3. Scammers have launched a website containing a digital anti-virus – Corona Antivirus – that promises to protect its users against the actual COVID-19 virus. This malicious software posing as an anti-virus, once downloaded, turns the device into bot. A bot is zombie computer awaiting commands from a command-and-control server operated by a malicious actor.



Malicious Corona Antivirus website.

What can businesses or individuals do to protect themselves from the above scams?

- We urge business to alert their employees on potential incoming phishing emails. Employees should be trained to spot and manage phishing emails. Our partner cyber insurers are currently offering a free cyber awareness training to all of its cyber insurance customers. The platform also contains helpful modules such as 'bring your own device (BYOD) and 'remote and mobile working'.
- Anti-malware software, IDS/IPS (intrusion detection/ prevention software) etc. should be up-to-date.
- Use only applications recommended/vetted by the business on work devices. On personal devices, users should download apps recommended by relevant bodies such as the WHO or the government and this should be from their official websites. Many of these malicious apps can be found in Android stores.
- Enable multi-factor authentication (MFA) on user accounts, especially administrator accounts.

For further advice on protecting your business against scams, please email our team at info@hamiltonleigh.com

Hamilton Leigh, Unit 1 Capital Business Park, Manor Way, Borehamwood, Hertfordshire WD6 1GW
Tel: 020 8236 5350
Email: info@hamiltonleigh.com