NEWS

Cyber experts step in as criminals seek to exploit Coronavirus fears

Experts at the NCSC have revealed phishing attacks exploiting worries over COVID-19

The public are being urged to follow online safety advice as evidence emerges that criminals are exploiting the Coronavirus online.

Experts from the National Cyber Security Centre have revealed a range of attacks being perpetrated online as cyber criminals seek to exploit COVID-19.

Techniques seen since the start of the year include bogus emails with links claiming to have important updates, which once clicked on lead to devices being infected.

These 'phishing' attempts have been seen in several countries and can lead to loss of money and sensitive data.

The NCSC, a part of GCHQ created to keep the UK safe online, is urging businesses and the public to consult its online guidance, including how to spot and deal with suspicious emails as well as mitigate and defend against malware and ransomware.

In addition, in recent days the NCSC has taken measures to automatically discover and remove malicious sites which serve phishing and malware. These sites use COVID-19 and Coronavirus as a lure to make victims 'click the link'.

Paul Chichester, Director of Operations at the NCSC, said:

> "We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the Coronavirus outbreak.
>
> "Our advice to the public is to follow our guidance, which includes everything from password advice to spotting suspect emails.
>
> "In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible."

The NCSC has seen an increase in the registration of webpages relating to the Coronavirus suggesting that cyber criminals are likely to be taking advantage of the outbreak.

These attacks are versatile and can be conducted through various media, adapted to different sectors and monetised via multiple means, including ransomware, credential theft, bitcoin or fraud.

Continued global susceptibility to phishing will probably make this approach a

persistent and attractive technique for cyber criminals. Moreover, if the outbreak intensifies, it is highly likely that the volume of such attacks will rise.

There are numerous examples of cyber attacks worldwide since the Coronavirus outbreak.

On 16 February, the World Health Organisation (WHO) warned of fraudulent emails sent by criminals posing as the WHO. This followed a warning from the US Federal Trade Commission about scammers spreading phishing 'clickbait' via email and social media, as well as creating fraudulent websites to sell fake antiviral equipment.

Cyber criminals have also impersonated the US Center for Disease Control (CDC), creating domain names similar to the CDC's web address to request passwords and even bitcoin donations to fund a fake vaccine.

In January, attackers spread the Emotet banking trojan in Japan by posing as a state welfare provider to distribute infected Word documents. Similar operations have been observed in Indonesia, the US and Italy, with attackers attempting to spread the Lokibot infostealer, Remcos RAT and other malware.

Individuals in the UK have also been targeted by Coronavirus-themed phishing emails with infected attachments containing fictitious 'safety measures.' According to Proofpoint researchers, such attacks have recently become more targeted, with greater numbers focusing on specific sectors like shipping, transport or retail to increase the likelihood of success.

PUBLISHED

16 March 2020

WRITTEN FOR ⓘ

Individuals & families