SECURITY GUIDANCE:

COVID-19 Leveraged Cyber Attacks

As users around the UK and the rest of the globe try to adjust to the current health concerns surrounding COVID-19 and the rapid changes it has introduced to their daily working structure, cyber criminals are quickly taking advantage of the extensive online communications around coronavirus by leveraging it for their own malicious email campaigns.

Researchers have already noted an alarming number of COVID-19 related spear phishing attacks, which have risen by over **600%** between January and March.

137	*detections in January*
1,188	*detections in February*
9,116	*detections in March*

ADVICE FOR DETECTION & PREVENTION:

Carefully Check Email Addresses
Always look for subtle misspellings of names and the use of incorrect domains, such as public domains (e.g. @gmail.com) used in seemingly corporate campaigns.

Hover Over Links
Make sure to always hover your cursor over links before clicking through - this will display the true source of the URL, allowing you to research whether it should be trusted.

Avoid Opening Attachments
Many phishing attacks will include a malicious payload in their emails, often embedding them in 'urgent' attachments.

Never Give Out Personal Data
With campaigns impersonating government bodies or financial organisations, such as HM Revenue and Customs or banks, attackers will often ask you to confirm confidential information like credit card or tax details.

TOP 3 OBSERVED TACTICS:

Scamming attacks completely falsify information for their campaigns, including company names, domains, and web addresses, making it difficult for targets to fact-check their claims.

COVID-19 scams to look out for:

- Claim to be selling cures for the virus, or protective equipment like face masks.
- Request payment under the guise of either charity donations or investment into vaccine development.

Brand Impersonation attacks rely on tricking targets into believing they are a trusted source, like a service provider or government organisation, through the imagery, domains and links used in their messaging.

COVID-19 impersonations to look out for:

- Service providers like Netflix claiming to offer free subscriptions or products.
- Government organisations like WHO sending safety guidance via attachments.

Blackmail attacks use various threats to demand bitcoin payments from their targets, typically claiming to have obtained compromising footage of them by hacking webcams, or insisting they have access to vital account credentials.

COVID-19 blackmails to look out for:

- Attackers claiming to know your location with threats of intentional viral infection.