**NTK article COVID-19 Malicious cyber attacks**

Following on from last weeks NTK article on phishing and fraudulent emails (<https://ntk.eastamb.nhs.uk/news/stay-alert-for-covid-19-fraudulent-emails.htm>) the United Kingdom’s National Cyber Security Centre (NCSC) and the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) have released a joint advisory document detailing information on cyber attacks and exploitation by cyber criminals during the COVID-19 global pandemic. (<https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory>)

Since the COVID-19 outbreak the number of cyber attacks using COVID-19 related themes has increased and continues to grow. Cyber criminals rely on social engineering methods to take advantage of the curiosity of the user around the COVID-19 response, which includes clicking on links or downloading apps which pose as an outbreak tracker or vital information when actually it is a malicious app or link which downloads the users details.

It has been noted that cyber criminals are sending fraudulent communications, which appear to come from WHO to create the impression of authenticity around their attack.

The NCSC have provided guidance how to spot fraudulent emails:

* **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 concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.
* **Current events** - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you. (<https://www.ncsc.gov.uk/guidance/suspicious-email-actions#section_3>)

Cyber criminals are seeking to exploit the increased use of popular communications platforms (such as Zoom or Microsoft Teams) which more people have downloaded due to working from home during the COVID-19 response and lockdown. The criminals send phishing emails and include malicious files with names such as ‘zoom-us-zoom\_##########.exe’ and ‘microsoft-teams\_V#mu#D\_##########.exe’ (# representing various digits that have been reported). The attackers have been able to hijack teleconference calls that have been set up without security controls (e.g. passwords) or with unpatched versions of the communications platform software.

**Tips when using Microsoft Teams:**

* Do not make the meetings public.
* Do not share the link to people other than those invited to join the meeting
* Manage screensharing options

If you receive an email which you believe to fraudulent, please forward it to phishing@eastamb.nhs.uk and delete it from your mailbox. It is vital that you do not click on any of the links/open any attachments. If you are unsure about the validity of an email, you should go straight to the source of the information (e.g. going to the WHO or the government website directly, rather than using the link, if it appears to be suspicious).