YH ROCU

Yorkshire & Humber
REGIONAL ORGANISED CRIME UNIT

TRENDING

ZOOM Video Security

The video conferencing application ZOOM has rapidly gained popularity during the current situation, however, there have been several reports in the media, both mainstream and Cyber, raising doubts about the security of ZOOM.

To avoid any potential issues, we recommend that users review the recommended security settings within the application.

There are currently no warnings about the use of the app from the NCSC.

Top tips for video users:

- Think about location - what can be seen in the background?
- Do you have Alexa, Siri or Google Assistant listening in the background?
- Sharing your screen - think about what else can be seen when you "share"

- A new COVID related scam reported involves calling business owners, purporting to be from Trading Standards and accuse the business of operating illegally during lockdown and risking a fine. The Fraudsters then follow up with a second call purporting to be from HMRC, issuing a fine and a link on WhatsApp to pay the fine.

- Suspicious callers are said to have been knocking on doors of elderly and vulnerable residents in various parts of the UK, saying that they are health officials doing door-to-door testing.

ACTION FRAUD REPORT DETAILS

https://takefive-stopfraud.org.uk/advice/general-advice/

Latest update from NFIB as of 23.59hrs on Sunday 05 April 2020

Total reports to Action Fraud = 577
Total losses = £1,665,558
Total reports of phishing to Action Fraud = 2,442

Currently COVID-19 related fraud makes up 3-5% of all fraud reports received to Action Fraud Reported scams include:

- Suspect incorporating the COVID-19 epidemic into push payment frauds.
- Suspect asking for a donation to tackle COVID-19, normally via emai, or pretending to be from a charity which is assisting vulnerable people during the outbreak.
- Suspect calling purporting to be victim's bank, saying account was compromised/there had been unusual activity. Victim advised to open new account/transfer money there and then. Victim told they should not visit their branch because of COVID-19.
- Suspect persuades victim to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property.The property does not exist or the suspect is not in a position to rent it.

Phishing/Smishing

Some more tactics being used in phishing emails and texts include:

• Emails being sent to recipient claiming to be from Argos and offering free vouchers to help support people during the outbreak. The email features a link for recipients to claim their voucher.

• Emails claiming to be from Hotmail and Microsoft Outlook advising recipient that their account has been deactivated. There is a malicious link for the recipient to verify their details to reactive and secure their accounts which allows attackers to steal email passwords and personal details.