NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime

Protecting **businesses** and **communities** in the North East from common cyber attacks

GOV.UK

Created: 05/01/2021
Source: https://cfa.nhs.uk/resources/downloads/fraud-awareness/covid-19/COVID-19_SMS_and_Text_Message_Scams.pdf

COVID-19: SMS / Text message SCAMS

THREAT

The NCSC, alongside security researchers around the world, has warned users of SMS, email, and online scams using COVID-19 information as a lure. The NCSC warning lists the 'Top 4 SMS Scams' as following similar patterns: fake government (GOV.UK) links, lockdown fines, health supplements to protect against the virus, and financial support from the recipient's bank.

Scammers have launched numerous campaigns in the weeks since early December, looking to steal personal information, conduct identity theft, scam victims, and for potential financial gain. In the case of the scam leveraging the UK government, SMS were sent from UK_Gov, rather than GOV.UK.

ADVICE

1. Challenge - Could it be fake? It's ok to reject, refuse or ignore any requests that don't feel right. Check GOV.UK to ensure it's genuine.
2. Be wary of text messages that try to get you to send money, or important personal information such as bank details or passwords.
3. Take a moment to stop and think before parting with information to keep you safe or your money.
4. Use official government websites and refer to 'Contact Us' sections of websites to access information and services.

Be cyber aware https://www.ncsc.gov.uk/cyberaware/home

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime

If you have been a victim of fraud or cyber crime, report it to Action Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk