

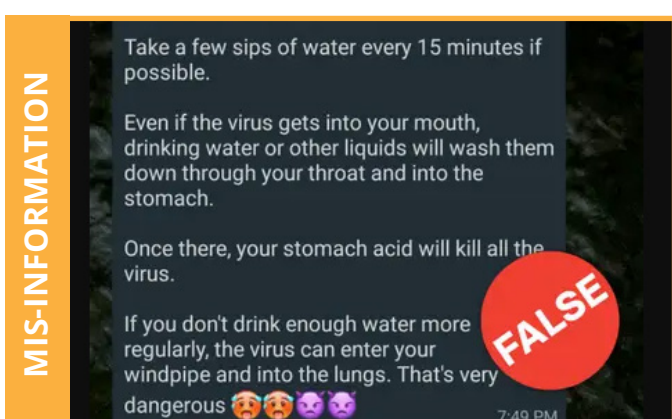
CORONAVIRUS MOBILE SCAM ALERT



for these scams arriving on your mobile devices!

There has been an increase in opportunistic criminal activity on the internet and mobile channels. The bad guys are preying on your fear and sending all sorts of scams related to the Coronavirus (COVID-19).

Below are some examples of the types of scams you should be on the lookout for on your mobile devices:



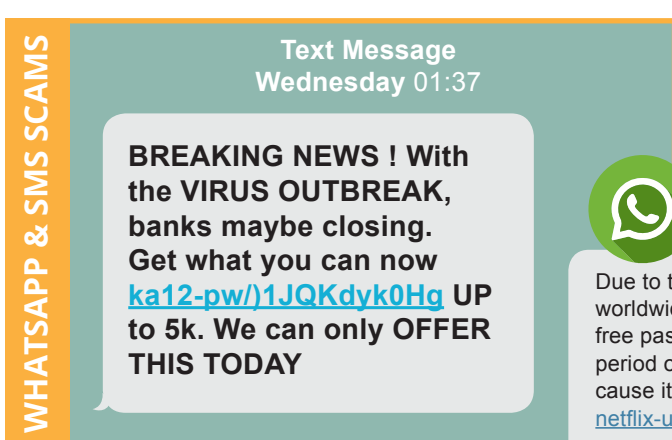
Mis-information

...Your well-meaning contact may spread fake news, misinformation, conspiracy theories and other hoaxes via chat groups like WhatsApp. Please warn your family members and do not blindly forward posts. Only trust information from reputable sources such as the WHO.



Malicious apps

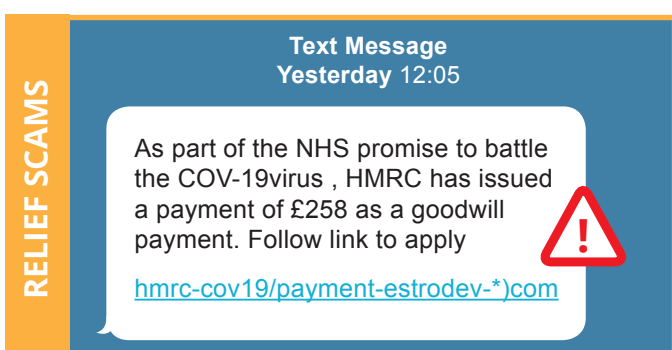
...Criminals lure victims with Coronavirus tracking mobile apps. Once installed they can gain access to your camera or microphone and can even see your text messages. Some apps even lock your device and demand a ransom in order for you to regain access. Don't get caught by malicious apps, only download reputable apps from the legit app stores.



WhatsApp & SMS scams

...Beware of fake text and WhatsApp messages talking about government checks, bank updates or Coronavirus updates in your area. Criminals are using the uncertainty around Coronavirus to trick you into clicking on the link and sharing your credentials.

No, Netflix is not offering free passes. It's a scam!



Government relief scams

...Text messages asking you to follow a link in order to receive a supposed COVID-19 relief payment from the government.



Vishing scams

...You may receive a robo-call or even a real person calling you pretending to be from your mobile operator, broadcaster or other businesses offering huge discounts or free upgrades due to Corona. Wow, you are over the moon. Then they ask for your bank details to set up a new direct debit to the scammer's account. Don't ever trust anyone asking for your personal information via the phone.



Social Media Charity Donation scams

...Social media posts asking for donations to help provide supplies or find a cure. These scams are designed to defraud residents of cash. Confirm the authenticity of any group soliciting money or goods from you before you donate.

Remain cautious! Protect yourself from scams like these:

- Never click on links from texts or emails you weren't expecting.
- Be wary of anything that triggers your emotions, good or bad.
- Avoid clicking on links in WhatsApp or other channels.
- Only trust reputable sources and if in doubt, verify.