COVID-19: FRAUD

COVID-19 Home

Fraudsters have been very quick to adapt well-known fraud schemes to target citizens, businesses and public organisations. The following is non-exhaustive and will be revised as new scams are identified:

BOGUS WEBSITES

Websites with fake news about COVID-19 or posing as charities are easily shared on social media.

But these bogus websites can do more than just spread misinformation. By asking you to create an account or log in, they gain access to your personal information and can even infect your device with malware.

What can I do?

- Don't trust information that does not come from official sources (e.g. local government, official medical entities).
- Don't spread unofficial information further. As a rule of thumb: if you can't verify it from at least two other sources, then do not share it.
- If a website asks you to fill in your personal or financial information (either through pop-up windows or a login form), think twice before doing so.
- Research before donating to charities. The WHO has a dedicated page for this.
- Use a browser that allows you to block pop-up windows.

How can I recognise them?

- Fake websites will often include text that suggests a sense of urgency.
- They are often poorly designed or only have one well-designed page.
- Pop-up windows are commonly used to gather your information.

FAKE APPS

There are currently several maps circulating online claiming to display live information on the spread of COVID-19. Some of them can be accesses in browsers and some come as downloadable apps.

Be wary of both and always check official sources – your national authorities, the WHO, ECDC and academic institutions all provide national and global statistics.

What are the risks?

If you download an app like this, you can infect your devices with mobile malware.

The malware might infect your device and could take control over your files or even lock the entire device. This is called ransomware.

What can I do?

Stick to the official statistics, like the live WHO dashboard.

Always check what permissions an app requires.

Research the app and its publishers carefully before downloading and check user reviews.

If your device is infected with ransomware, do not pay the ransom. A free decryptor may be available on No More Ransom – a Europol-backed project.

FAKE INVESTMENT OPPORTUNITIES

Investors need to be wary of COVID-19-related investment scams, such as promotions that falsely claim products or services of publicly traded companies can prevent, detect or cure coronavirus.

What can I do?

- Always get impartial financial advice before you hand over any money or make an investment.
- Reject cold calls related to investment opportunities.
- Be suspicious of offers promising a safe investment, guaranteed returns and large profits.
- Beware of future scams. If you have already invested in a scam, fraudsters are likely to target you again or sell your details to other criminals.

MONEY MULING

Criminals also use COVID-19 to recruit money mules. They create fake healthcare organisations and NGOs to lure online workers through fake job advertisements. New recruits are requested to process 'donations' to fight coronavirus, pay the money into their bank accounts, and send it on, keeping a commission for themselves.

Money muling is a type of money laundering and consequences are severe. It's not worth it.

TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other