CORONAVIRUS SCAM ALERT

Watch out for these scams!

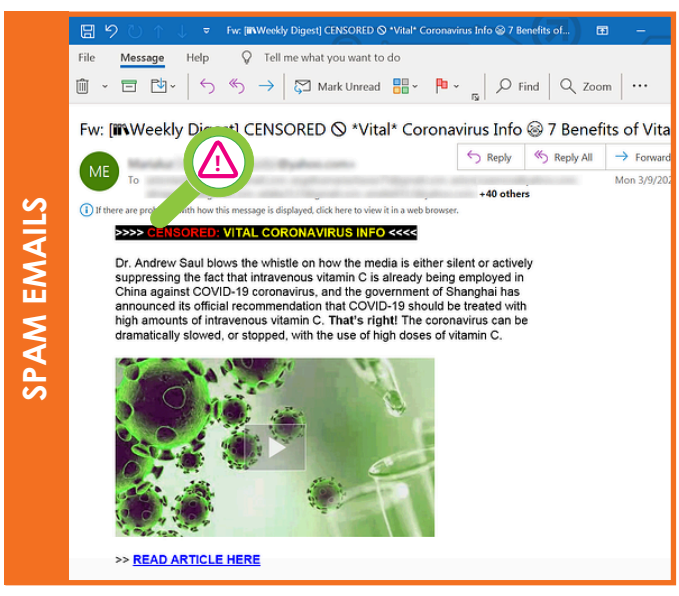
When natural disasters or pandemics like Covid-19 occur, there is often an increase of opportunistic criminal activity on the internet.

Criminals 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:

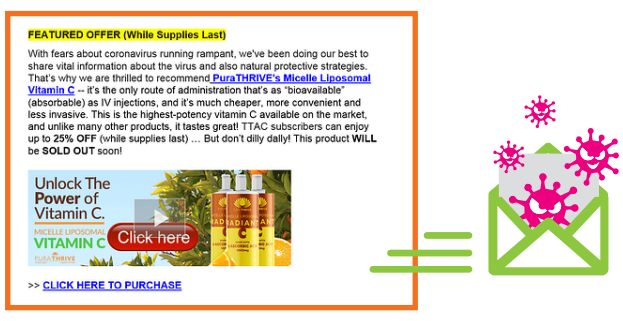
01 Malicious websites

...with the purpose of infecting your device with malware. Watch out for sites such as coronavirus(.)com or corona-virus-map(.)com. Since January there have been thousands of websites registered containing the word 'corona' and many of those are suspicious. Some of these websites distribute malware.



02 Spam emails

...trying to grab your curiosity by using conspiracy themed catchphrases, such as "censored", to try and sell information (paid-for videos) or goods that are now in high demand, such as masks, hand sanitisers or vitamins, for example.

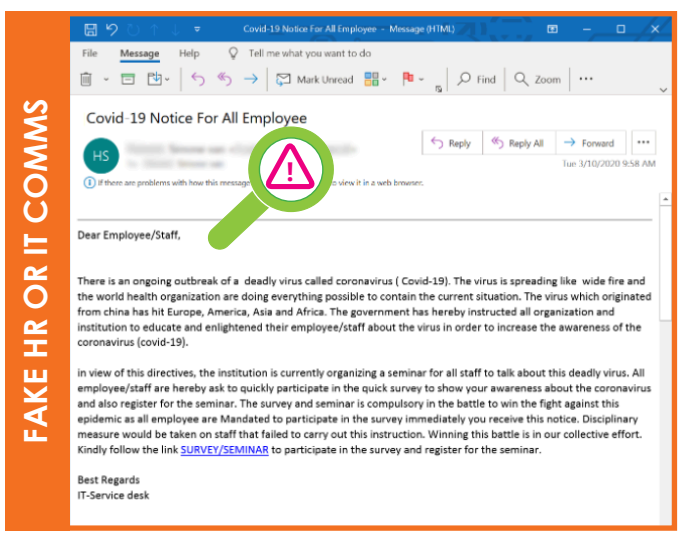


03 Phishing scams

...that appear to come from organisations such as the CDC (Centers for Disease Control) or the WHO (World Health Organisation). The scammers have crafted emails that appear to come from these sources, but they actually contain malicious phishing links or dangerous attachments. There are also emails that claim to have a "new" or "updated" list of cases of coronavirus in your area. These emails contain dangerous links.

04 Fake charities

...emails and websites that ask you for charity donations for studies, doctors, or victims that may have been affected by the Covid-19 coronavirus. Scammers often create fake charity emails after global disasters or pandemics like the Covid-19 outbreak.



05 Fake internal HR or IT communication

...such as coronavirus surveys impersonating your HR or IT department - the objective here is to steal your username and password.

To access the 'document' or 'survey', the recipient has to provide their Office 365 credentials on a fake site – thus compromising their Office 365 account.

Remain cautious! Protect yourself from scams like this:

- **Avoid clicking on links or open attachments** from an email that you weren't expecting.
- **Be aware of suspicious emails that appear to come from an official organisation** such as the WHO or the South African Department of Health.
- If you want to make a charitable donation, go to the charity website of your choice to submit your payment. **Type the charity's web address in your browser** instead of clicking on any links in emails or other messages.

Finally, be cautious of anyone knocking on your door, dressed up as a health official wanting to perform Covid-19 tests – they could be there to rob you! Verify with their employer first before you let them into your home.

Stay cyber safe and report any suspicious online activity to:
Call 0800 22 21 17 or visit – www.tip-offs.com