

Coronavirus COVID-19 Cyber Security Information

During these trying times, scammers are taking advantage of fears surrounding the Coronavirus. They're setting up websites to sell fake products, and using fake emails, texts, and social media posts as a way to take your money and get your personal information.

The emails and posts may be promoting awareness and prevention tips, and fake information about cases in your neighbourhood. They also may be asking you to donate to victims, offering advice on unproven treatments, or contain malicious email attachments. Below are a couple of examples to be on the lookout for.

Spam emails and Phishing attempts

The overwhelming amount of news coverage surrounding the novel coronavirus has created a new danger, phishing attacks looking to exploit public fears about the sometimes-deadly virus.

Cybercriminals send emails claiming to be from legitimate organizations with information about the coronavirus. The email messages might ask you to open an attachment to see the latest statistics. If you click on the attachment or embedded link, you're likely to download malicious software onto your device. They might even ask you to enter usernames and passwords to access the content.






Malicious websites

Since January there have been thousands of websites registered that contains the word 'corona' and many of those are suspicious. Most of these websites spread malware and tries to trick users into providing personal information.

The screenshot shows a website with a dark header containing the text 'CORONAVIRUSTEST' and navigation links: 'Главная', 'Доставка и оплата', and 'Контактные данные'. Below the header is a shopping cart table with the following items:

Товар	Цена	Количество	Итого
 Тест для определения вируса 2019-ncov	р.19,000.00	1	р.19,000.00

Below the table are buttons for 'Код купона', 'Применить купон', and 'Обновить корзину'. A summary section titled 'Сумма заказов' shows:

Подытог	р.19,000.00
Итого	р.19,000.00

A large red button at the bottom says 'Оформить заказ'. The footer contains the text '© vaccinecovid-19.com'.

Fake internal communication

This spam campaign poses as information that the recipient needs to know about their company's business continuity operations during Lockdown etc. The attachments usually have malware or will try to access usernames and passwords.

The screenshot shows an Outlook email window. The subject line is 'UPDATE : BUSINESS CONTINUITY PLAN ANNOUNCEMENT 2020 DUE TO CORON...'. The email body contains the following text:

Dear Partner,
A MUST READ!!!
Please find in the attached everything you need to know about our business continuity plan for the year (2020) due to management of the deadly Coronavirus COVID 19 as published by the World Health Organisation (WHO).
Endeavour to read through so as to keep you enlightened on all updated necessary information about our operations.

The email includes an attachment named 'Business continuity plan_pdf.gz (434 KB)'. The interface shows standard Outlook navigation and action buttons.



Fake charities

There are multiple scammers out there trying to take advantage of good-hearted people, please be vigilant who you donate money too.

If you would like to donate, we advise donating to the official government Solidarity fund.
<https://www.solidarityfund.co.za>

Some useful DO's and DON'T's

- DO: Second guess anyone looking for any personal information.
- DO: Be vigilant of any websites you visit.
- DON'T: Open any email/attachments or click on any links that you are not expecting or requested or if you do not recognize the sender.
- DON'T: Enter your email or laptop password on any website that is out of the ordinary.
- DON'T: Believe everything you read. There are a couple of official channels where legitimate Coronavirus information is sent from. There's so much information out there that can be very confusing and problematic. This is the official government information page that should be referenced for any information: <https://sacoronavirus.co.za>

Please feel free to contact us if you are unsure about anything or require any assistance.

Follow the links below for more information.

<https://www.welivesecurity.com/2020/03/13/beware-scams-exploiting-coronavirus-fears/>

<https://www.theguardian.com/money/2020/mar/29/coronavirus-social-disease-fraudsters-adapt-old-scams/>

<https://blog.knowbe4.com/piling-on-exploiting-the-coronavirus-for-fraud-and-profit>



Email: support@absol.co.za

Tel: +27 (012) 365 2142