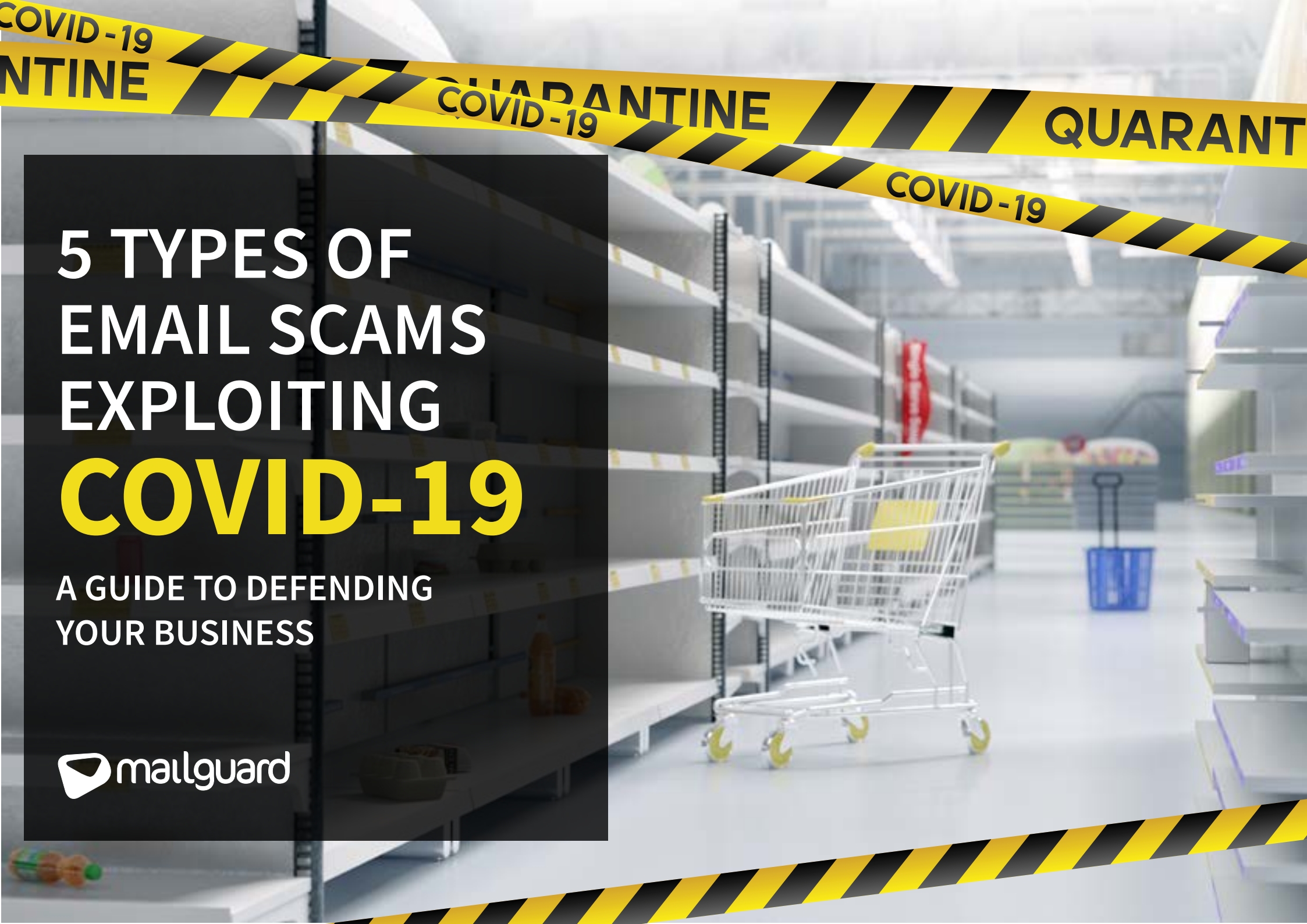


5 TYPES OF EMAIL SCAMS EXPLOITING COVID-19

A GUIDE TO DEFENDING YOUR BUSINESS

mailguard

The worldwide pandemic of Coronavirus (officially known as COVID-19) has gripped all of us. It's trending everywhere – from news publications to social channels. The hashtag #COVID19 is trending on Twitter with millions of tweets.

Global fears about the spread of the virus, combined with a lack of clarity about how to prevent it have made the topic irresistible – and cybercriminals have noticed too. Interpol has reported that cybercriminals have exploited the Coronavirus already to scam millions($) from hapless victims who are fearful about the growing pandemic.

5 real examples of cyber-attacks exploiting fears around Coronavirus

At MailGuard, we have intercepted several email scams centred around Coronavirus. In this guide we highlight 5 of the most common so far. Share them with your business and networks to increase their awareness and to make them more cyber resilient during this global health emergency.

1. THE EDUCATIONAL GUIDE

This scam tries to trick users who are seeking more information about surviving the pandemic, claiming to offer tips to avoid being afflicted by it, like boosting your “immunity”.

The emails often masquerade as ‘learning material’ sent from reliable sources – material often leads to malicious links and/or attachments.

The best way to distinguish malicious emails from legitimate ones is by checking for any grammatical or formatting errors – errors not likely included in authentic notifications sent by authorities.

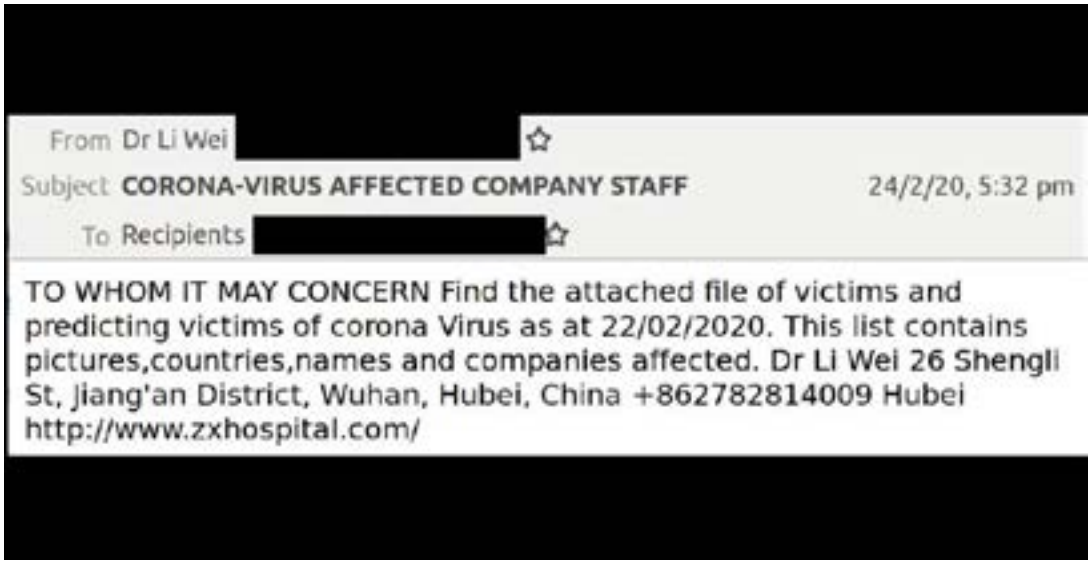
2. MERCHANDISE OFFERS

Another Coronavirus-themed email scam is for the sale of pandemic related merchandise and prevention measures. For example selling hand sanitizers, toilet paper, soaps, etc.

The example to the right is for the sale of face masks. As you're probably aware, face masks are in high demand and in many places, are in limited supply. Preying on people's fear, cybercriminals hope recipients will ignore any concerns about the legitimacy of the email before clicking.

3. MEDICAL CORRESPONDENCE

Coronavirus is ultimately a health pandemic, and any information or updates on this relatively unknown and evolving emergency are naturally considered valuable. And that's what cybercriminals hope to leverage in the email scam on the right. The email claims to contain a list of 'pictures, countries, names and companies affected' by Corona-virus – information that many users would like access. This link to the list is actually for a malicious payload designed to infect the system of any unsuspecting recipient who opened it. The email was supposedly sent from a medical practitioner called "Dr. Li Wei".


From Dr Li Wei [redacted]
Subject CORONA-VIRUS AFFECTED COMPANY STAFF 24/2/20, 5:32 pm
To Recipients [redacted]

TO WHOM IT MAY CONCERN Find the attached file of victims and predicting victims of corona Virus as at 22/02/2020. This list contains pictures,countries,names and companies affected. Dr Li Wei 26 Shengli St, Jiang'an District, Wuhan, Hubei, China +862782814009 Hubei http://www.zxhospital.com/

4. FEAR OF THE ECONOMIC DOWNTURN

Fear is a powerful emotion, especially when centred around a rapidly spreading, devastating global health emergency.

This scam for example, taps into the economic ramifications of the crisis, and the fears of business owners about the effect of the virus on their companies.

China is “the workshop of the world” and the disruption caused by the widespread presence of the virus in the country is likely to disrupt business operations worldwide.

5. OFFICIAL ANNOUNCEMENTS

Cybercriminals aren't just stopping at impersonating random individuals, they're also spoofing authorities.

Phishing emails have been intercepted claiming to be from the Centre for Disease Control and Prevention and the World Health Organization, attempting to steal sensitive credentials.

Additionally, researchers with IBM X-Force reported that cybercriminals are spreading the Emotet trojan via emails purporting to be from a disability welfare service provider in Japan.

Defending your business

Coronavirus scams are no different to other email-borne cyberattacks, other than the heightened level of fear and uncertainty that is sweeping across our communities.

Avoid clicking links in emails that:

- Are not addressed to you by name, have poor grammar or omit personal details that a legitimate sender would include. Most Coronavirus-themed emails that MailGuard has intercepted didn't address the recipient directly
- Are from businesses you're not expecting to hear from
- Ask you to download any files, and
- Take you to a landing page or website that does not have the legitimate URL of the company the email is purporting to be sent from.

For additional information or support protecting your business against cybercriminals, please reach out to expert@mailguard.com.au

Brought to you by

mailguard

Gold Microsoft Partner

Microsoft