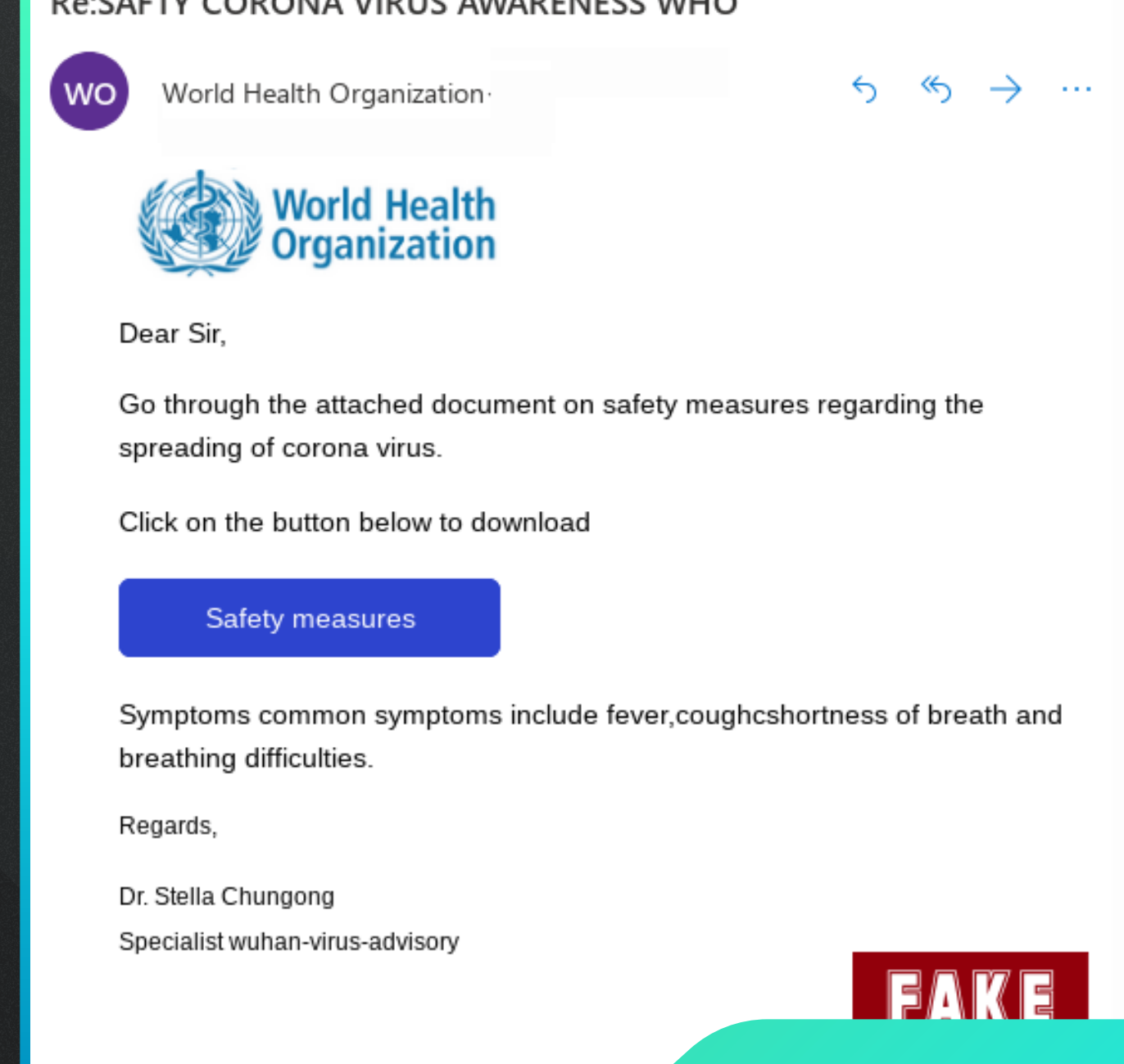


CORONAVIRUS SCAM ALERT

Criminals are using coronavirus to trick you into falling for their scams.

Stay alert to these common techniques.

CORONAVIRUS PHISHING



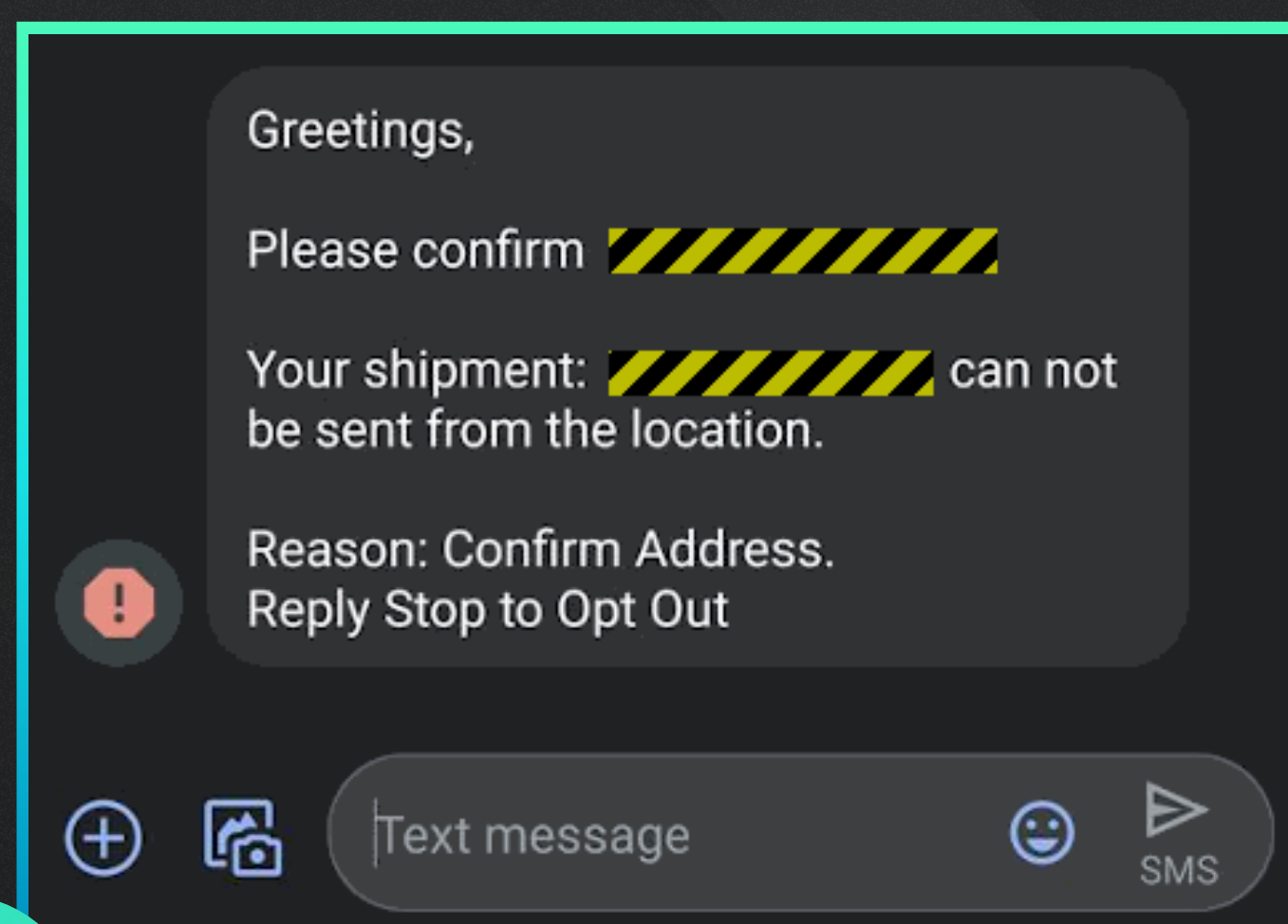
Beware of emails, SMS, and WhatsApp messages from unknown sources with information on coronavirus. Often crooks impersonate legitimate organizations and people to make their messages more believable. Their goal is to trick you into clicking links, sharing personal data, and even sending money to their 'worthy cause.'

Be extra suspicious of messages about coronavirus. If you don't know and trust the source, don't click, don't share, don't reply.

Always look at the email address used to send the email and not just the display name. On mobile devices, click on the display name to reveal the real email address.

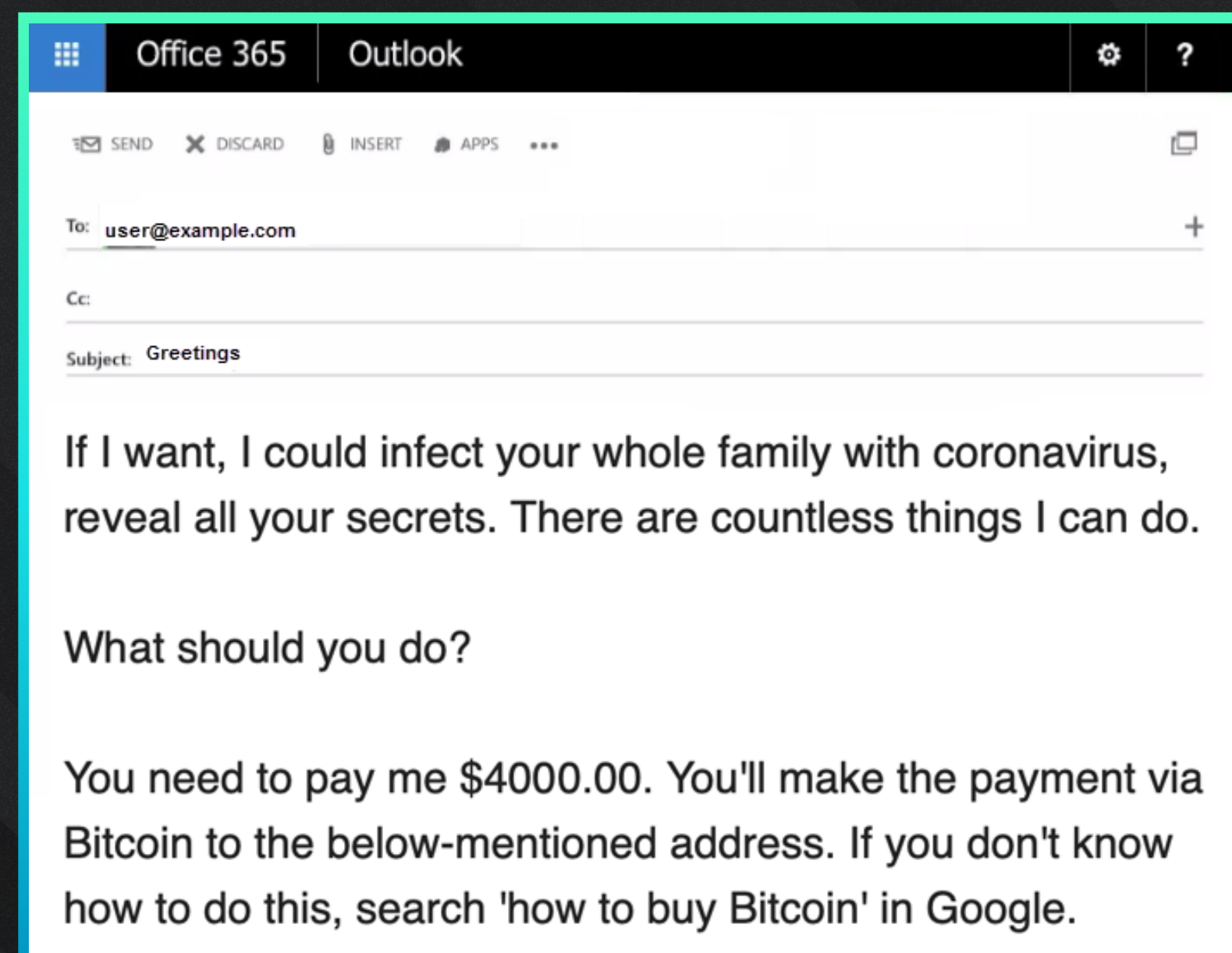
HOME DELIVERY PHISHING

With many people waiting on home delivery of essential items, criminals are impersonating delivery services. Their goal: to trick you into clicking malicious links or con you into paying extra 'delivery' fees.



Remain vigilant, even if you're expecting a delivery. And treat SMS as notifications, not links.

EXTORTION EMAILS

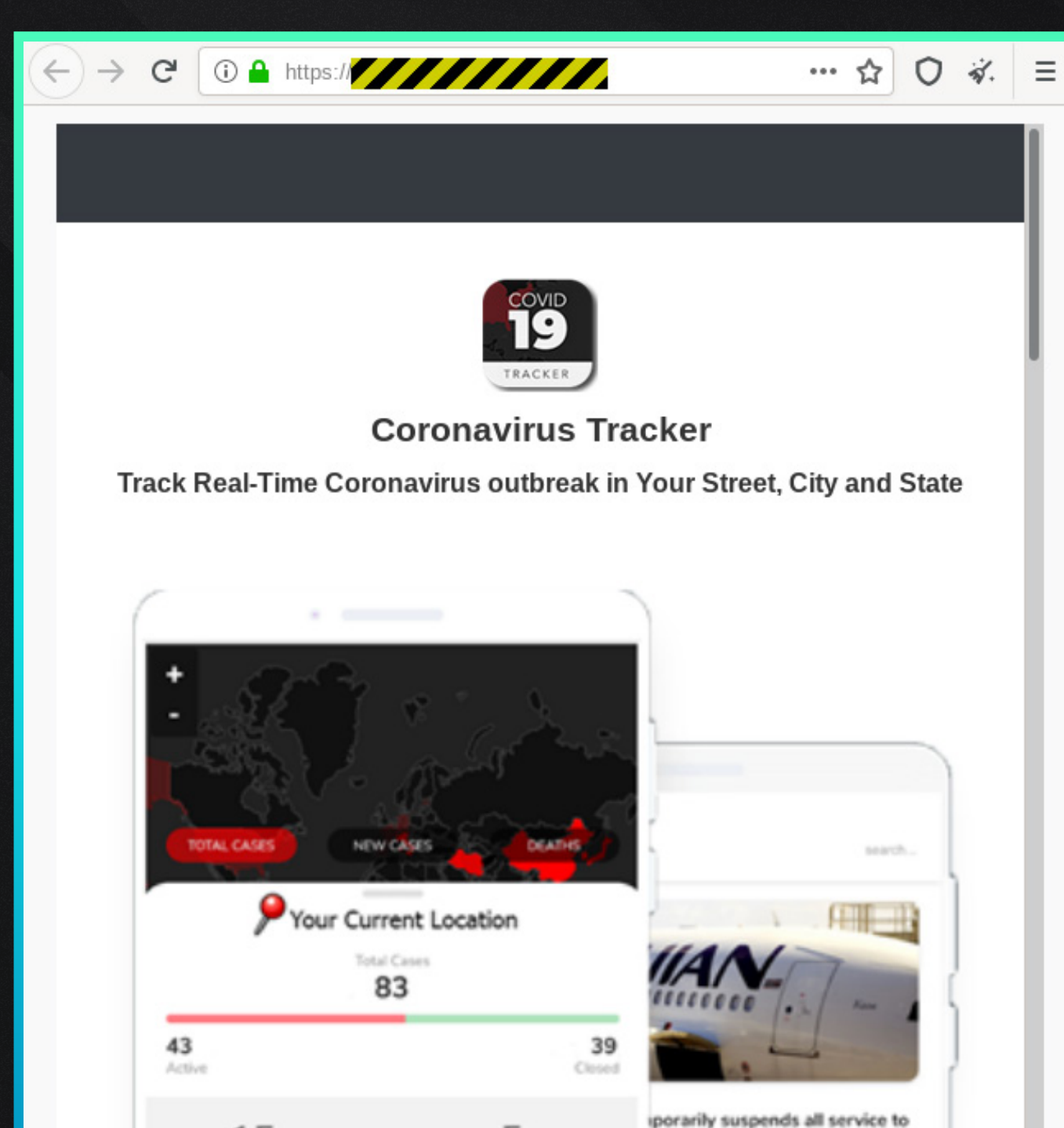


Attackers threaten to infect someone with coronavirus unless you pay them. Often these threats include a small piece of personal information to make them more believable.

Don't send any money. Don't reply. Don't worry – it's all lies.

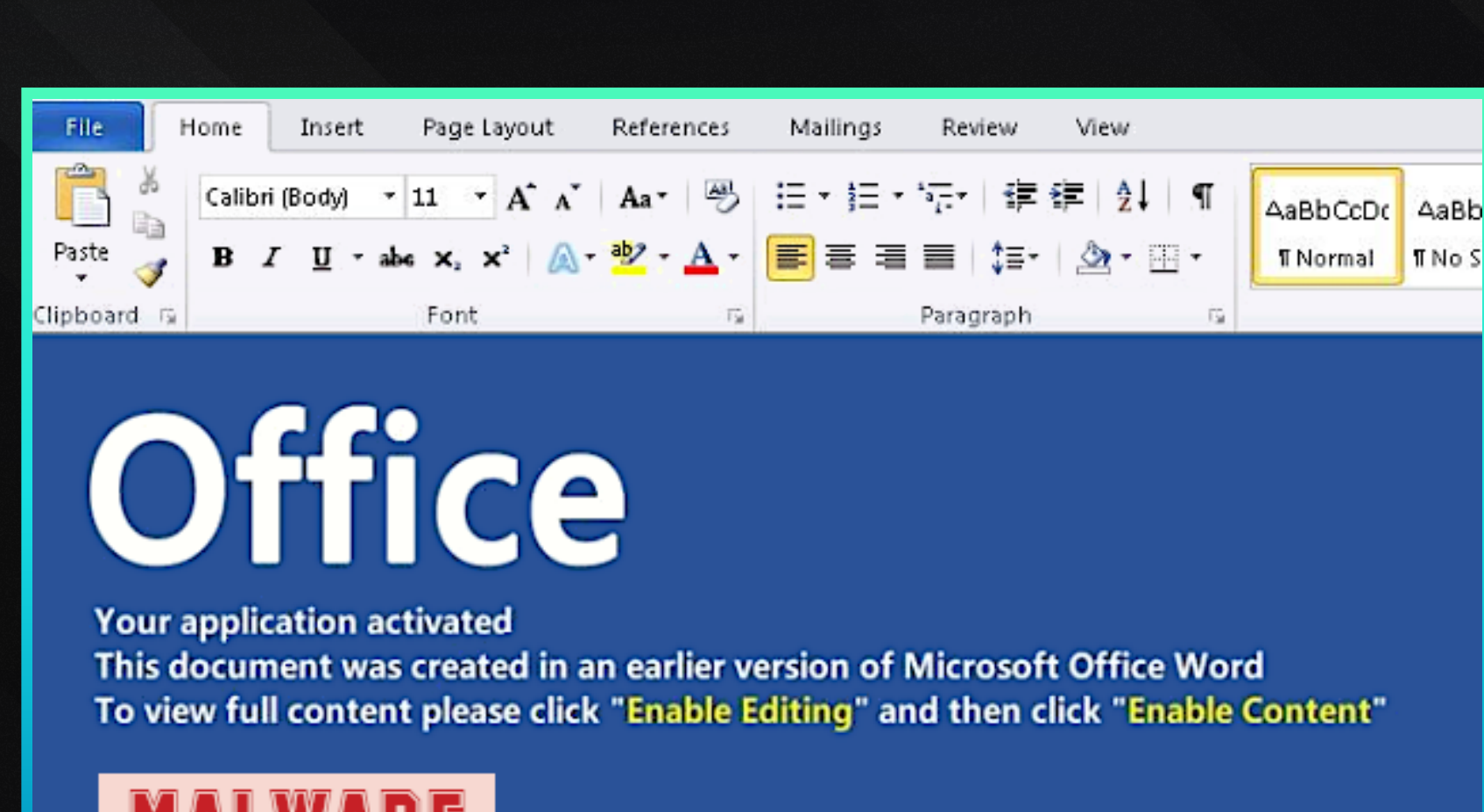
MALICIOUS APPS

Criminals offer coronavirus-related apps. Once installed, the apps enable the crooks to access all the information on the device – and even hold you to ransom.



Only download reputable apps from official app stores.

MALICIOUS DOCUMENTS



Crooks create documents claiming to contain coronavirus-related information. Upon opening the document, you're asked to 'enable editing' and 'enable content.' Doing so installs malicious software onto your computer.

Never click 'enable content' just because the document tells you to. Microsoft blocks it by default because it's used so often to spread cyberattacks.

There is lots of great information available about coronavirus, but there are also a lot of scams. Criminals are busy exploiting our desire to get the latest news, information, and updates.

During this time, stay extra vigilant and think before opening, clicking, or sharing anything.