How to recognise phishing emails

	How to recognise coronavirus-themed phishing emails?	What to do?
Online requests for personal information	An email, with a "Corona-virus" subject / title, that seeks personal information such as your Social Security number and/ or login information is a phishing scam. Legitimate public and private bodies will never ask for that information over an email or even on the phone.	Never respond to the email with your personal data.
Check the email address or link	You can inspect a link by hovering your mouse button over the URL to know where it leads. Sometimes, it is obvious that the web address is not legitimate. But please be mindful that phishers can create links that are almost perfect lookalikes to legitimate addresses.	Should you not be 100% sure of the authenticity of the redirection link, do not click on it.
Watch out for spelling and grammatical mistakes	If an email includes spelling, punctuation, and grammar errors, it is very likely that it is a phishing email.	Do not action on the email until you have a way to cross check and confirm its authenticity.
Look for generic greetings	Phishing emails are unlikely to use your name. Greetings like *"Dear Sir or Madam"* indicate that an email might not be legitimate.	Do not action on the email until you have a way to cross check and confirm its authenticity.
Avoid emails that insist you to "act now" or provide a sense of urgency in any way during this period	Phishing emails often try to create a sense of urgency or demand that you take an immediate action. The goal is to get you to click on a link and provide personal information on the spot.	Never disclose any personal information over such type of emails and flag such emails as "spam" in your mailbox.

COVID-19: Phishing Email Scams

Examples of SCAM emails which you may receive during this pandemic period:

Email Alerts

Emails that appear to be from organisations such as the CDC (Centers for Disease Center), or the WHO (World Health Organisation) where they might falsely claim to link to a list of COVID-19 cases in your area.

Health advice emails

Phishers have sent emails that offer purported medical advice to help protect you against the COVID-19. The emails might claim to be from medical experts near Wuhan, China, where the outbreak started.

Such emails might mention:

- "This little measure can save you"
- "Use the link below to download Safety Measures."

Workplace policy emails

Cybercriminals have targeted employees' workplace email accounts.

Phishing emails might mention the name of "AfrAsia Bank" giving you the impression that the email comes from the Bank.

An example might be "All, Due to the COVID-19 outbreak, AfrAsia Bank is actively taking safety precautions by instituting a Communicable Disease Management Policy." If you click on the fake company policy, you might download malicious software.

LIVE COVID-19 Maps

Maps that pretend to track the virus outbreak is actually a manipulation tactic by hackers to inject malwares onto your workstations, which will help them to steal your personal data.