

26 March 2020

## COVID-19 Cybersecurity | Communication for the Industry

COVID-19 poses unprecedented challenges in terms of risk for organisations, including those operating within the financial services sector. Various organisations are, for instance, reverting to contingency measures like remote working arrangements, which, if not properly and securely managed, may expose organisations unnecessarily (such as unauthorised access to, and leakage of, sensitive data).

Prominent cybersecurity sources, like [ENISA](#), [CERT-EU](#) and [EUROPOL](#) for instance, reported cases of phishing attempts referencing Coronavirus, which may give rise to ransomware, credential theft, loss of sensitive data and fraud.

Licence Holders should continue to ensure that their staff, processes and technologies remain as resilient to cybersecurity risk as possible, including by keeping abreast of any developments within the cybersecurity sphere, sustaining adequate cybersecurity hygiene, persevering with cybersecurity awareness amongst employees, and retaining the necessary cybersecurity preparedness.

For more guidance, Licence Holders may contact the MFSA Supervisory ICT Risk and Cybersecurity function via: [mirt@mfsa.mt](mailto:mirt@mfsa.mt).