MFSA MALTA FINANCIAL SERVICES AUTHORITY

Circular

26 March 2020

COVID-19 Cybersecurity | Communication for Consumers

Technology has been crucial for the world in its fight to control the spread of COVID-19 in various ways. It has provided the opportunity for people to observe social distancing whilst remaining connected and continuing with their professional and personal lives.

Our increased dependence on technology means that we need to be careful because the current situation can be capitalised upon to use technology for malicious purposes.

The following are some useful cybersecurity tips for consumers of Financial Services:

1. Information about COVID-19. Seek information from authoritative sources such as public authorities within the health sector and the World Health Organisations (WHO). Be careful about opening emails that claim to have the latest news on Coronavirus, information about locations where the virus persists or medicine that cures Coronavirus. Be cautious about any clickable links including on emails, internet sites and social media.

2. Cybersecurity Education and Awareness. Follow developments within the cybersecurity sphere by following cybersecurity news and updates from authoritative and reliable sources such as CERT-EU, EUROPOL and ENISA. These sources provide a wealth of knowledge in different languages and at different levels and have joined forces together with the European Commission to fight against COVID-19 related threats.

3. Passwords. Change default passwords, especially those of internet-connected devices. Use different passwords for different systems and applications. Employ strong passwords and change them regularly. Adopt multiple factors of authentication (for example password + one-time PIN) where possible.

4. Software and Applications. Keep your software and applications up-to-date, by installing the relevant updates when these become available. Use security software, such as antivirus software, and ensure that it is up-to-date. Be careful about the software and applications that you install and about the permissions that you allow these on your devices and data.

5. Devices. Secure your electronic devices, including your mobile phone, with passwords, PINS and/or biometrically. Configure your devices to lock down automatically.

6. Connecting to a network. Be careful about which network/s you connect to. Networks and connections that are not secure may give rise to unauthorised access to information that you send or receive over that network.

7. Backing Up. Back up your data regularly on a separate data storage device. Backup software can help to facilitate and automate this. Protect your backed-up data. Verify that your backup process is working correctly by restoring data from your backup and checking it.