Stay safe when working from home

Here are some top tips

Follow your organisation's policies, procedures and guidance.

- Your organisation will have adapted their approach to ensure that data is adequately protected. Avoid the temptation to do things in a way you think is more convenient, such as sending emails through your personal account or using the video conferencing app that you use with friends for work calls.

Only use approved technology for handling personal data.

- If your organisation has provided you with technology such as hardware or software you should use it. This will provide the best protection for personal data.

Consider confidentiality when holding conversations or using a screen.

- You may be sharing your home working space with other family members or friends. Try to hold conversations, where they are less likely to overhear you and position your screen where it is less likely to be overseen.

Take care with print outs.

- At the office, it is likely you can use confidential waste bins. At home you won't have that facility. Follow your organisation's guidance or safely store print outs until you can take them into the office and dispose of them securely.

Santander for Intermediaries

Don’t mix your organisation’s data with your own personal data.

○ If you have to work using your own device and software, keep your organisation’s data separate to avoid accidentally keeping hold of data for longer than is necessary. Ideally, your organisation should have provided you with secure technology to work with.

Lock it away where possible.

○ To avoid loss or theft of personal data, put print outs and devices away at the end of the working day if possible.

Use strong passwords.

○ Whether using online storage, a laptop or some other technology, it’s important to make your passwords hard to guess.

Be extra vigilant about opening web links and attachments in emails or other messages.

○ Don’t click on unfamiliar web links or attachments claiming to give you important coronavirus updates.

Communicate securely

○ If you need to share data with others then choose a secure messaging app or online document sharing system. If you have to use email, which isn’t always secure, consider password protecting documents and sharing the passwords via a different channel, like text.

Keep software up to date

○ If you’re using your own equipment, don’t be an easy target for hackers. Keep your security software up to date to make it more difficult for them to get in.

Intermediaries and investment professionals only: not for public distribution

Santander for Intermediaries is a brand of Santander UK plc and is not a regulated company. Santander UK plc. Registered Office: 2 Triton Square, Regent's Place, London, NW1 3AN, United Kingdom. Registered Number 2294747. Registered in England and Wales. www.santander.co.uk. Telephone 0800 389 7000. Calls may be recorded or monitored. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Our Financial Services Register number is 106054. Santander and the flame logo are registered trademarks. OCT 2020