

# PRIMARY SAFETY MEASURES



Ensure your devices have the latest **internet browsers** and **security software** installed

## Use your own personal computer or cell phone

Shared or public devices pose a threat as they may have spyware installed that captures your credentials without your knowledge



## Safe online transaction behaviours



When transacting online, **check that the URL you are using begins with 'https'** and not 'http'. The 'https' creates a secure encrypted connection to ensure your data is protected



**Always log out of your online profile**, regardless of the device you used, as soon as you've completed your transaction



**Never share your personal or account information** via email, SMS or telephone

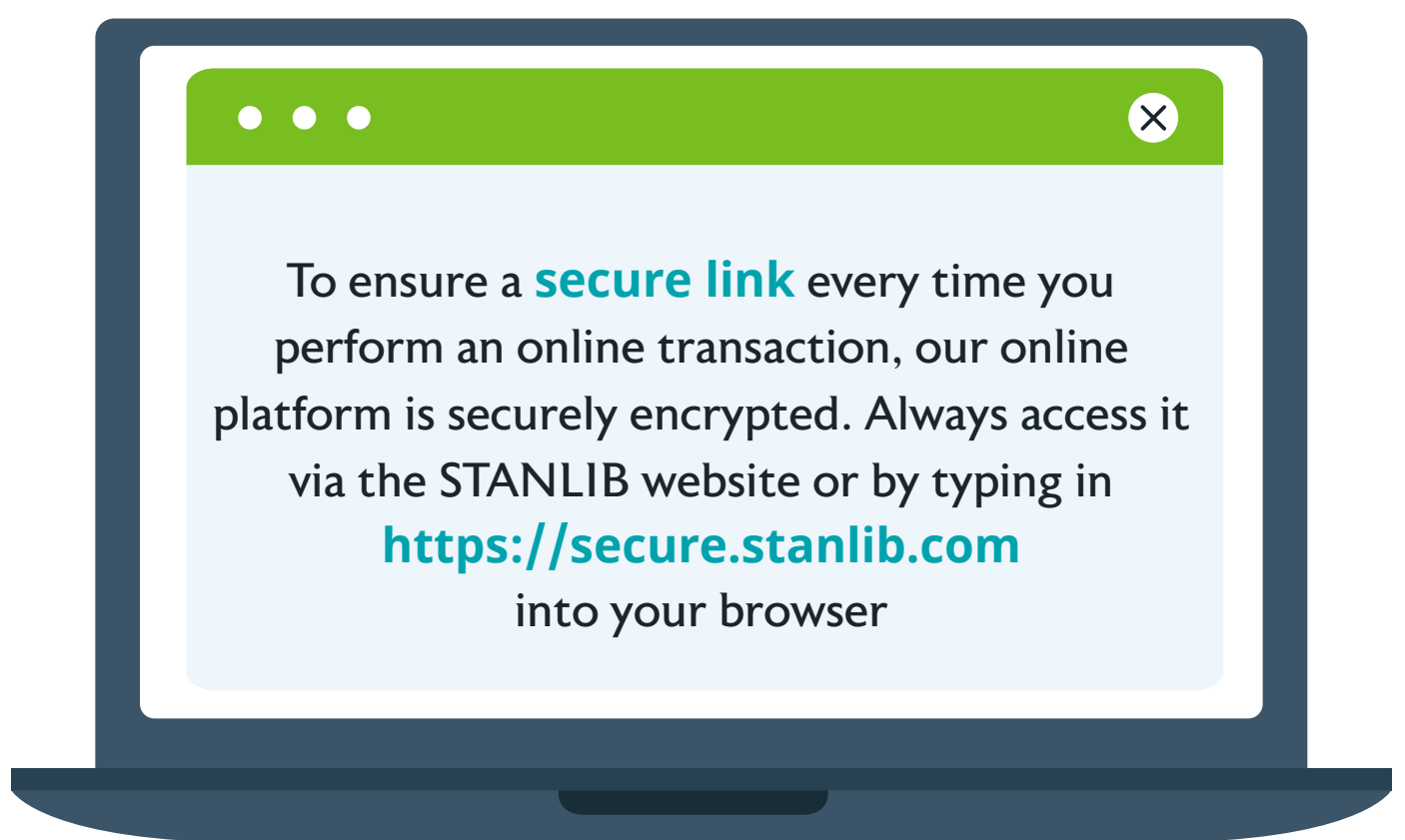


**Never access our online platform via a link or attachment**



**Keep your password strong and change it regularly**

## HOW STANLIB IS PROTECTING YOUR ONLINE SAFETY



If you receive a suspicious email or if you believe you may have accidentally clicked on a link in a phishing email, please email [infosec@stanlib.com](mailto:infosec@stanlib.com)



For more information about safe and secure online transacting and email practices, visit [www.stanlib.com](http://www.stanlib.com)