







# CYBER SECURITY – BASICS

| DO  |  | DON'T  |
|---|--|--|
| <ul style="list-style-type: none"> <li>✓ Use long passwords with special characters, avoiding common or dictionary words.</li> <li>✓ If your firm has approved digital safes, use them to generate random passwords and hold them.</li> <li>✓ Regularly change your password even when not prompted to do so.</li> </ul>  |  <p><b>PASSWORDS</b></p>          | <ul style="list-style-type: none"> <li>✗ Share your account details with anyone.</li> <li>✗ Reuse passwords between business and personal accounts.</li> <li>✗ Use your corporate email for login or accounts unrelated to your firm's.</li> <li>✗ Circumvent your firm's security controls.</li> </ul>  |
| <ul style="list-style-type: none"> <li>✓ Ensure updates and security patches are applied regularly by connecting your device to your firm network regularly.</li> <li>✓ Only install corporate and packaged software that is approved by your firm.</li> </ul>  |  <p><b>CORPORATE DEVICES</b></p>  | <ul style="list-style-type: none"> <li>✗ Circumvent, modify or disable your device's settings or programmes.</li> <li>✗ Connect unauthorised devices to your firm's network or devices</li> <li>✗ Leave Wifi and Bluetooth options activated on my corporate smartphone or device when not in use.</li> </ul>  |
| <ul style="list-style-type: none"> <li>✓ Stay vigilant to unsolicited requests from email, social networks, calls or meeting proposals.</li> <li>✓ Select the recipients to email carefully limiting them to only those who need the information – Be careful of distribution lists and auto complete functionality.</li> <li>✓ Ensure you follow your firm's operational procedures to help avoid fraud attempts.</li> </ul> |  <p><b>EXTERNAL THREATS</b></p> | <ul style="list-style-type: none"> <li>✗ Click on attachments or links in suspicious messages (including emails and or SMS).</li> <li>✗ Provide information on your firm and its clients to unknown or unauthorised individuals.</li> <li>✗ Share information related to your firm on social media platforms unless permitted by your firm.</li> </ul> |
| <ul style="list-style-type: none"> <li>✓ Follow your firm's classification policies to ensure information is stored appropriately</li> <li>✓ Only use solutions approved by your firms to exchange or share data.</li> </ul>  |  <p><b>DATA</b></p>             | <ul style="list-style-type: none"> <li>✗ Share, use or publish documents if you do not have approval from your firm to do so.</li> <li>✗ Take photos of your firm's information (documents or information on screens</li> </ul>  |
| <ul style="list-style-type: none"> <li>✓ Check the sender email.</li> <li>✓ Think before acting: were you expecting the email?</li> <li>✓ Check what the link looks like.</li> <li>✓ Be wary of any implied urgency?</li> </ul>   |  <p><b>EMAILS</b></p>           | <ul style="list-style-type: none"> <li>✗ Respond to emails where the sender's identity is not confirmed or known.</li> <li>✗ Use your work email address on external websites or forums.</li> <li>✗ Do not open files attached to emails or hyperlinks from unknown sources.</li> </ul>  |
| <ul style="list-style-type: none"> <li>✓ Only use your firm's approved remote access solutions to connect to your firm's network</li> <li>✓ Use a VPN if in public.</li> <li>✓ Keep your corporate equipment with you or in a secure location.</li> <li>✓ Alert your firm immediately if your equipment is lost, stolen or seized.</li> </ul>   |  <p><b>REMOTE WORKING</b></p>   | <ul style="list-style-type: none"> <li>✗ Connect to unknown or untrusted networks, especially to public Wi-Fi networks.</li> <li>✗ Carry unnecessary data and confidential documents in hard copy.</li> <li>✗ Charge your firm's equipment using public USB ports.</li> </ul>  |