Cazenove Capital

Important Information

To safeguard your PIN and one-time passcode

Important information to safeguard your PIN and one-time passcode

At Schroders, we have implemented measures to safeguard your account information. However, to ensure that your online security, account access and information are not compromised, we recommend that you adopt the following eService security guidelines.

1. Before entering your WebUserID and PIN, you should always ensure that the website you are visiting belongs to Schroders. This can be verified by the URL displayed in your browser as well as the Bank's name in its digital certificate. This precaution will ensure that you are not revealing your Schroders eService Access Code and PIN to a website other than Schroders.
2. Important tips on how you can safeguard and protect your PIN, passcode and account information:
   (a) PINs should be at least 6 digits.
   (b) PINs should not be based on WebUserID, personal telephone number, birthday or any other guessable personal information.
   (c) PINs must be kept confidential and not be divulged to anyone.
   (d) PINs must be memorised and not be recorded anywhere.
   (e) PINs must be changed regularly. When there is any suspicion that the PIN has been compromised or impaired, change it immediately and notify Schroders.
   (f) The same PIN should not be used for different websites, applications or services, particularly when they relate to different entities.
   (g) Please do not keep your WebUserID, PIN and/or security token together.
   (h) Please do not select the browser option for storing or retaining user name and password.
   (i) Please check that the bank's website address changes from 'http://' to 'https://' and a security icon that looks like a look or key appears when authentication and encryption is expected.
   (j) Please do not allow anyone to keep, use or tamper with your security token.
   (k) Please do not reveal the one-time passcode generated by the security token to anyone.
   (l) Please do not divulge the serial number of your security token to anyone.
   (m) Please check your bank account balance and transactions frequently and report any discrepancy.
3. Please install anti-virus, anti-spyware and firewall software in your personal computers.
4. Please update the anti-virus and firewall products with security patches or newer versions on a regular basis.
5. Please remove file and printer sharing in your computers, especially when you have internet access via cable modems, broadband connections or similar set-ups.
6. Make regular backup of critical data.
7. Consider the use of encryption technology to protect highly sensitive data.
8. Clear browser cache after the online session.
9. Log off the online session and turn off the computer when not in use.
10. Do not install software or run programs of unknown origin.
11. Delete junk or chain emails.
12. Do not open email attachments from strangers.
13. Do not disclose personal, financial or credit card information to little known or suspect websites.
14. Do not use a computer or device which cannot be trusted.
15. Do not use public or internet cafe computers to access online banking or perform financial transactions.

The above mentioned information on security precautions and good practices is not intended to be exhaustive or static.

Please do not hesitate to contact us if you have any questions or require assistance.

Cazenove Capital