S 6.2.2 A FSP shall inform financial consumers of the importance of reading and understanding the terms and conditions for e-banking services, particularly those terms relating to the consumers' responsibilities in using the e-banking services.

S 6.2.3 A FSP shall clearly inform financial consumers of their responsibilities, which include the obligation to-

a. abide by the terms and conditions and use the e-banking services in a responsible manner;
b. take reasonable steps to keep the security credentials such as access identification (ID) and passcode as well as any security device[25] secure at all times. These include-
   i. not to keep a record of the security credentials in a manner that is easily recognisable and accessible to any other person;
   ii. not to disclose the security credentials to a third party;
   iii. not to allow anyone to use the consumer's e-banking services; and
   iv. not to disclose the security credentials to any unsolicited email or SMS and on any website or mobile application other than the FSP's official website to access the e-banking services;
c. notify the FSP as soon as reasonably practicable after having discovered that the security credentials or security device for accessing the e-banking services have been compromised, lost or stolen, or that an unauthorised transaction has occurred on the e-banking account;
d. notify the FSP immediately upon receiving a transaction alert if the transaction was unauthorised; and
e. notify the FSP when there is a change in the financial consumer's contact number that receives transaction alerts.

S 6.2.4 A FSP shall raise awareness on the safety measures that financial consumers must undertake to prevent unauthorised use of their e-banking services which shall include the following-

a. create a strong pass code that cannot be easily predicted such as one that uses a mixture of alphabets, numbers and symbols as well as to regularly change the pass code;
b. access the e-banking services only via the FSP's legitimate website or mobile application and not to access the FSP's website through hyperlinks from emails or other websites;
c. ensure that the device being used to perform e-banking transaction has installed an updated anti-virus software and to update the device's browser and operating system to the latest version;
d. check all transaction alerts in a timely manner and report to the FSP as soon as practicable of any unauthorised transaction;
e. verify the authenticity of messages sent by FIs and take appropriate action upon detecting that such message is fraudulent;
f. check their e-banking account transactions regularly and report any suspicious transaction to the FSP without delay;
g. regularly read security tips or warnings posted on the FSP's banking website or mobile banking apps;
h. only download the FSP's mobile banking apps from a trusted app store;

[25] "Security device" refers to a token or other devices that generate a passcode.