Mobile User Education

It is vital that credit union management educate members utilizing mobile banking in order to mitigate security risks to the users. The credit union will educate membership by including the following information within documentation provided once home banking is enabled.

a) Instruct users that mobile applications should be downloaded from trusted sources only
b) Password protect the mobile device
c) Members should not store usernames and passwords on devices
d) Users should not text confidential information
e) Instruct users to obtain virus and malware protection for mobile devices
f) Refrain from enabling the “install from unknown sources” feature in mobile banking platforms using the Android operating system
g) Secure mobile devices at all times when not in use
h) Ensure confidential data is not stored on the device
i) Delete text messages promptly after receiving them from the credit union
j) Notify the credit union and carrier immediately if the mobile phone is lost or stolen to ensure it is deactivated
k) Frequently check account activity and notify credit union of any unauthorized transactions
l) Do not open attachment or click on links contained in emails received from unfamiliar sources