Për sigurinë tuaj

1- Sigurohuni që të ndryshoni fjalëkalimin tuaj rregullisht.

2- Mos i jepni emrin e përdoruesit dhe fjalëkalimin tuaj personave të tjerë.

3- Fjalëkalimet dhe kodet e sigurise duhet të mbahen sekret. Këto nuk duhet të shkruhen diku apo tu jepen njerëzve të tjerë për tu përdorur, e as të jepen nëpërmjet telefonit ose nëpërmjet email-it. Sigurohuni që askush nuk mund tiu shohë ndersa jeni duke shkruar fjalëkalimin apo PIN-et tuaja. Fjalëkalimet duhet të jenë të zgjedhura në mënyrë që të mos jenë të lehta për tu gjetur apo marrë me mend, si dhe duke shmangur informacione standarde personale si psh: ditëlindjen tuaj, emrin tuaj apo të afërmve tuaj etj.

4- Mos lejoni njerëz te tjerë qe të përdorin kartat tuaja. Mbajini ato në një vend të sigurtë dhe kontrollojini periodikisht nëse janë në rregull.

5- Asnjëherë mos jepni të dhëna konfidenciale ose personale me postë elektronike ose me ndonjë mjet tjetër, edhe nëse kërkesa ngjan sikur është bërë nga një burim i ligjshem i besueshëm. BKT nuk do tiu kerkojë kurrë të dhënat tuaja personale pa qënë të pranishëm.

6- Mos jepni informacione të tjera konfidenciale pa konfirmuar se faqja zyrtare është e sigurtë. Kontrolloni nëse adresa fillon me https:// ndjekur nga emri përkatës i faqes së kërkuar dhe se faqja tregon një dryn në shiritin e saj diku poshtë apo më sipër.

7- Mos lejoni asnjë person tjetër të përdorë pajisjen tuaj ndërkohë që ju jeni të loguar në Internet/Mobile Banking.

8- Instaloni software kundër viruseve dhe mbajeni të përditësuar gjatë gjithë kohës. Nëse nuk është i përditësuar është e njësoj sikur të mos keni fare.

9- Përdorni një firewall për të filtruar trafikun e internetit për hyrjet dhe daljet në kompjuterin tuaj.

10- Qëndroni vigjilentë për përditësime të sigurisë të ofruara nga prodhuesit e besueshëm të software-ve dhe zbatojini ato në përputhje me udhëzimet e ofruara.

11- Mos hyni në linqe apo çdolloj faqe që kërkon nga ju që ti jepni informacione sensitive personale apo konfidenciale ose ju lejon ju të kryeni transaksione bankare. Gjithmonë shkruani adresën e plotë të faqes që ju dëshironi për të hyrë në shfletuesin përkatës (browser).

12- Mos e hapni mesazhet e postës elektronike pa kontrolluar identitetin e dërguesit dhe subjektit. Nëse keni ndonjë dyshim në lidhje me origjinën e mesazhit e fshini atë menjëherë dhe mos hapni asnjë skedar apo dokument të bashkëngjitur që mesazhi i postës elektronike mund të përmbajë.

13- Ju lutem mos bëni asnjë transaksion bankar në kompjuterat e hapura për publikun (psh internet kafe). Lloje të ndryshme të programeve mundësojnë hakerat për të hyrë në të dhënat tuaja të llogarisë dhe të dhëna personale përmes kompjuterëve të cilat janë të hapura për publikun.

14- Ju lutem tregoni vemendje që të mos përdorni faqet e internetit të cilat janë të hapura përmes postës elektronike ose platformave të tjera. Mos hyni në Internet Banking tuaj nëpërmjet ndonjë faqeje tjetër.

15- Pasi keni hyrë në Internet / Mobile Banking ju do të informoheni për datën dhe kohën tuaj të fundit të hyrjes në faqen kryesore. Nga ky informacion mund të kontrolloni nëse llogaria juaj është përdorur nga ndonjë person tjetër, pas përdorimit tuaj të fundit.

16- Mbani nën vëzhgim llogarinë tuaj. Kontrolloni llogarinë tuaj të paktën çdo dy deri në katër javë. Nëse ju jeni mësuar me mënyren tradicionale dhe pasqyrën e llogarisë e merrni në letër, ju rekomandohet ta lexoni brenda dy javëve pas mbërritjes.

17- Mbani pajisjet që ju përdorni për të hyrë në online banking të siguruara mirë. Siguroni çdo pajisje (tabletë, smartphone, PC, laptop, etj) që përdoren për të hyrë në online banking janë të perditesuar nga ana e sigurisë. Kjo përfshin software të tille si anti-malware\anti-virus\firewall etj. Mos perdorni software piratë. Mbyllini pajisjet tuaja me një fjalëkalim, dhe sigurohuni që keni dalë nga faqja nëse keni përfunduar veprimet bankare online.

18- Raportoni çdo incident apo ndonjë dyshim që keni, pranë bankës.Njoftoni menjëherë BKT-ne në qoftë se ju mendoni se ka diçka të gabuar apo te dyshimtë, dhe ndiqni udhëzimet e dhëna.

19- Në rast se ju përdorni Aplikacionin Mobile Banking BKT Smart

a. Aktivizoni kodin e bllokimit të pajisjes tuaj. (PIN LOCK apo te ngjashem)
b. Mos i ruani të dhënat tuaja të tilla si PIN, OTP,CIF, PAN, Credit/Debit Card, Fjalekalime etj, në pajisjen tuaj smart phone. Gjithmonë mbajeni me kujdes smart phone tuaj kështu që askush nuk mund të shohë të dhënat tuaja ndërsa ju hyni në BKT Smart.
c. Përdorni vetëm versionin e përditësuar të sistemit të pajisjes tuaj. IOS/Android.
d. Nëse është e mundur nga prodhuesi i smart phone tuaj, përdorni software të përditësuar të anti viruseve dhe një firewall personal.

20- Pasi keni përfunduar veprimet tuaja bankare, ju lutem klikoni në butonin dalje të sigurt dhe duke mbyllur shfletuesit tuaj të bankingut online (E-Banking/BKT Smart).

21- Për një përdorim të sigurt të aplikacioneve ju rekomandojmë të mos përdorni aparate rooted/jailbroken, që kanë thyer garancinë e prodhuesit.