Varnostna priporočila uporabnikom mobilne banke mSberbank SI

1. Vsako krajo naprave, ki jo uporabljate za mobilno bančništvo, takoj prijavite banki, kjer bodo onemogočili dostop do vašega računa.
2. Svojo napravo zavarujte s PIN kodo ali geslom, ki je drugačen od gesla, ki ga uporabljate za mobilno bančništvo. Pri kreiranju PIN kode upoštevajte priporočila za kvalitetno geslo (8 znakov, velike in male črke, številke….), auto lock, passcode in vključite podobne tehnologije.
3. Po zaključeni uporabi mobilne banke se vedno se odjavite.
4. Ne shranjujte osebnih informacij in informacij o mobilni banki na svoji napravi (gesla in druge informacije)
5. Ne pošiljate osebnih informacij in informacij o mobilni banki z elektronsko pošto ali SMS sporočili. Prestrezanje takih informacij je enostavno.
6. Ne uporabljajte funkcije »auto-fill« na svojih napravah za vpisovanje uporabniškega imena in gesel za svojo mobilno banko.
7. Ne klikajte na nobeno povezavo ali drugo obliko teksta, ki ste ga prejeli z e-pošto ali v SMS obliki in je videti kot bi ga poslala vaša banka.
8. Ne odgovarjajte na e-pošto in SMS sporočila, ki jih niste pričakovali od vaše banke. Napadalci pogosto uporabljajo tehnike pošiljanja lažnih elektronskih sporočil s katerimi želijo pridobiti informacije o bančnem računu, gesla in podobno.
9. Ne uporabljajte »jailbroken« ali »rooted« naprav za mobilno bančništvo. Omenjeni tehniki (proces vdora v operacijski sistem mobilne naprave) izpostavljata naprave naprednim oblikam napadov (prestrezanje vnašanja podatkov, dostop do zavarovanih lokacij naprave in podobno).
10. Pri uporabi mobilne banke se povezujte samo z zaupanja vrednim WiFi omrežji. Ne uporabljajte mobilne banke na odprtih nezavarovanih omrežjih.
11. Ko ne uporabljate WiFi omrežja, uporabo WIFI omrežja na napravi onemogočite (enako Bluetooth).
12. Nadgrajujte vaše naprave z varnostnimi popravki, ki so priporočljivi in na voljo za vašo napravo.
13. Uporabljajte varnostne funkcije, ki jih omogočajo vaše naprave. Uporabite enkripcijo, oddaljeno brisanje, »location tracking« in podobne tehnologije. Uporabljajte dodatne varnostnih tehnologije in antivirusno programsko opremo za vašo napravo.
14. Nameščajte mobilne aplikacije samo z zaupanja vrednih lokacij (Apple App Store, Google Play…). Ne nameščajte aplikacij, ki so vam bile poslane z e-pošte ali ste kako drugače dobili povezavo do njih.
15. Pri nameščanju mobilnih naprav upoštevajte **princip dobre prakse** in se prepričajte kaj aplikacija na sistemu izvaja (poseg do drugih podatkov, klici, SMS sporočila…). Android naprave so zaradi svoje odprte platforme pogosto tarča nameščanja zlonamerne kode in s tem povečanja varnostnega tveganja za uporabnika.
16. Ne delite podatkov o svoji mobilni banki z drugimi uporabniki.
17. Ob zamenjavi in prehodu na novo napravo zbrišite vse podatke na stari napravi, ki ste jo uporabljali za mobilno bančništvo.

Sberbank d.d.