ProCredit Bank

Part of the ProCredit Group

Securitatea serviciului ProCredit Mobile Banking

În ceea ce privește securitatea **ProCredit Mobile Banking** nu ai de ce să-ți faci griji. **ProCredit Bank România** te protejează folosind cele mai moderne măsuri de Securitate. Totuși te sfătuim:

- Să nu divulgi nimănui, în nici un fel, elementele de autentificare. Acestea sunt confidențiale;
- Să îți schimbi parola la intervale regulate de timp, cel puțin de 2 ori pe an;
- Să nu dai curs niciunei solicitări prin care se cere furnizarea unor date confindențiale și să contactezi în cel mai scurt timp Banca la numerele de telefon disponibile, în orice situație care ți se pare suspectă.

ProCredit Bank România **NU** a trimis și **NU** va trimite niciodată, sub niciun pretext, mesaje prin care să solicite date confindețiale de acces la aplicația **Mobile Banking** prin mesaje de eroare web/e-mail/telefonic.

Smartphone/Tabletă

Protejaţi accesul la smartphone-ul sau tableta dumneavoastră folosind una din opţiunile de securitate disponibile (PIN, parola, sau “semn grafic”). În cazul în care echipamentul este pierdut sau furat informaţiile aflate pe el sunt protejate împotriva accesului neautorizat.

Atunci când este posibil actualizaţi sistemul de operare de pe smartphone-ul sau tableta dumneavoastră (Android, iOS, Windows). În general producătorii de echipamente care utilizează sistemul de operare Android oferă versiuni personalizate ale acestuia (Samsung, LG, HTC, etc). În cazul în care Google (producătorul Android) publică o actualizare de securitate care remediază o problemă de securitate, actualizarea nu se va instala automat pe echipamentele ce utilizează versiuni personalizate ale sistemului de operare. De aceea este important să urmăriţi când apar noi update-uri şi să le instalaţi manual. Aceste vulnerabilităţi pot fi remediate doar când producătorul echipamentului (Samsung, LG, HTC, etc) publică o nouă versiune personalizată a sistemului de operare Android.

Instalaţi aplicaţii (Apps) doar din magazinele de aplicaţii oficiale (Google Play, Apple App Store, Microsoft Store). Aplicaţiile care provin din “magazine” necunoscute pot conţine şi cod maliţios (malware) care vă poate infecta şi compromite securitatea echipamentului.

De exemplu, împreună cu aplicaţia descărcată instalaţi şi un malware de tip tojan care poate fura credenţialele aplicaţiei de mobile banking, precum şi codurile OTP (One Time Passcode) primite prin SMS necesare pentru autorizarea plăţilor 3D Secure.

Pentru a evita pe cât posibil infectarea cu malware se recomandă să vă protejaţi telefonul sau tableta cu o aplicaţie antivirus. Este recomandat de asemenea să verificaţi şi “permisiunile” pe care aplicaţiile le solicită la instalare. Aplicaţiile maliţioase vă pot cere permisiuni suplimentare care poate afecta securitatea dispozitivului dvs.

Dezactivaţi opţiunile de conectivitate (Wi-Fi, Bluetooth, NFC, etc) pe care nu le utilizaţi în mod curent. Eliminaţi astfel posibilele canale de intruziune pe care un potenţial atacator le-ar putea utiliza, în plus, economisiţi resursele bateriei şi prelungiţi durata de funcţionare a echipamentului.

Evitaţi operaţiuniile de “jailbreak” (iOS) sau “root” (Android). Este posibil ca în urma acestui proces sistemul de operare să nu mai funcţioneze în parametrii normali (se poate bloca mai des), bateria să se consume mai rapid, aplicaţiile malware să fie mai uşor instalate iar actualizările de securitate şi suportul producătorului să nu mai fie disponibile pentru acest terminal.

Evitaţi să lăsaţi echipamentele portabile (telefoane, tabelete, laptopuri) nesupravegheate în spaţii publice (cafenele, restaurante, aeroporturi) sau la vedere în maşină (suport de bord sau pe scaune).

Ori de câte ori este posibil securizaţi date păstrate pe echipamentele mobile prin aplicarea unui mecansim de criptare. Păstraţi cu grijă cheile de criptare deoarece fără ele puteţi risca să nu mai recuperaţi informaţiile păstrate în aceste echipamente.