ProCredit Bank

SIGURIA ONLINE

Si ju mbron Banka ProCredit?
Masta që mund ti merrni për t'u mbrojtur
Raportimi i mashtrimit

Në mjedisin e sotëm digjital, shumica e aktiviteteve të përditshme mbështeten në internet. Komunikimi dhe marrëdhëniet e biznesit krijohen dhe zhvillohen në këtë platformë. Kjo do të thotë se të dhënat dhe informacionet e ndjeshme shkëmbehen vazhdimisht përmes internetit.

Megjithatë, shpeshherë, interneti dhe email adresat mund të mos ofrojnë kanale të sigurta për shkëmbimin e informacionit sensitiv. Për këtë arsye, siguria në internet është një prioritet i rëndësishëm për individët si dhe për organizatat.

Si bankë, ne vazhdimisht përpiqemi të rrisim vetëdijësimin lidhur me sigurinë online të informacionit. Në këtë kontekst, ju rekomandojmë të lexoni këtë material për të marrë më shumë informacion në lidhje me:

- **Si ju mbron Banka ProCredit?**
- **Masat që mund të merrni për t'u mbrojtur**
- **Raportimi i mashtrimit**

SI JU MBRON BANKA PROCREDIT?

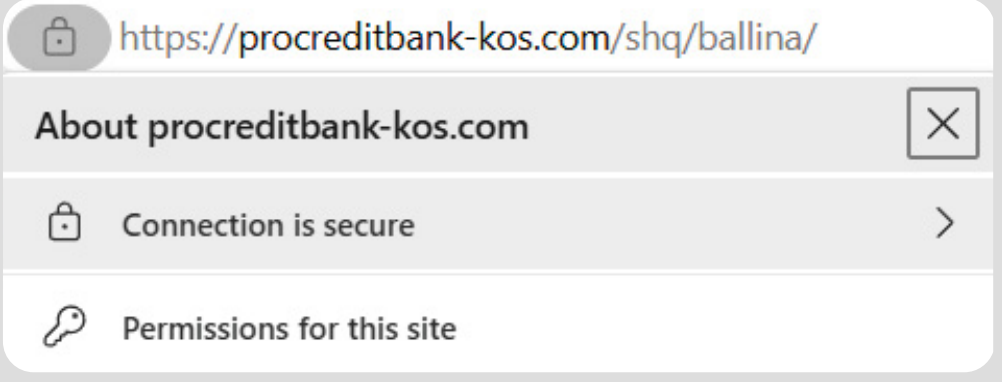
Banka ProCredit ka te implementuara masat e duhura teknike dhe administrative për të siguruar nje nivel të lartë të sigurisë në mënyrë që t'i mbrojë të dhënat sensitive te klienteve.

Infrastruktura

Ne si bankë investojmë në teknologjinë më të fundit dhe kemi vënë në zbatim masat e duhura teknike dhe administrative për të siguruar mbrojtjen e informacionit bankar të klientëve, si dhe për të identifikuar dhe parandaluar sulmet kibernetike.

Faqja e internetit e Bankës ProCredit është e siguruar me çertifikatën e sigurisë dhe për të vërtetuar autenticitetin e faqes në internet, ndiqni hapat në vijim:

Klikoni mbi ikonën e drynit/kyçit në shiritin e adresës
Konfirmoni se faqja është e siguruar me çertifikatë valide



e-Banking dhe m-Banking

- Autorizimi i pagesave mbrohet nga Autentifikimi Shumëfaktorësh për secilin transaksion që iniconi.

- Sesioni i bankimit online të klientit shkyçet automatikisht pas 15 minutave të mosaktivitetit për të shmangur përdorimin e paautorizuar të llogarisë së klientit nga të tjerët.

- Qasje e sigurtë në versionin mobil të e-Bankimit me të dhëna biometrike (tiparet e fytyrës ose gjurmët e gishtërinjve) ose fjalëkalim.

- Monitorimi i aktiviteteve për mashtrim potencial.

- Zhvillimi i aplikacioneve mobile me teknologjinë më të fundit të sigurisë.

Kartelat e debitit dhe kreditit

- Menaxhimi i limitit të kartelës dhe statusit të kartelës nga vetë klienti permes kanaleve tona digjitale.

- Regjistrimi automatik i kartelave me standardet më të fundit të sigurisë, si Siguria 3-D (një protokoll i sigurisë që lejon transaksione të sigurta në internet përmes një kodi një përdorimësh i cili pranohet përmes sms në numrin e telefonit të klientit që është i rexhistruar në ProCedit Bank. Për qëllime sigurie, kodi i autorizuar njëpërdorimesh mund të përdoret vetëm për realizimin e një pagese në afat prej **180-të sekondash** dhe nuk mund të përdoret për më shumë pagesa)

- Dërgimi i mesazhit SMS për çdo transaksion online që kryen klienti me kartelë.

- Monitorimi i aktiviteteve për mashtrim potencial.

MASAT QË MUND TË MERRNI PËR T'U MBROJTUR

Përkundër masave të avancuara të sigurisë që banka ProCredit aplikon, ekziston rreziku ndaj ekspozimit të sulmeve kibernetike. Çdo individ, pavarësisht nga profesioni që ushtron, mund të bëhet viktimë e akterëve dashakeq. Këta akterë po bëhen gjithnjë e më të sofistikuar në përpjekjet e tyre për të vjedhur fjalëkalime, numra kartelash krediti, dhe për të kompromentuar pajisjet në përgjithësi. Për të shmangur këto mashtrime, është e rëndësishme të jeni të vëmendshëm në identifikimin e detajeve dhe të aplikoni masat e rekomanduara për siguri:

Fjalëkalim efektiv

Parandalimi i vjedhjes së identitetit është një prioritet i rëndësishëm. Për këtë arsye, përdorimi i fjalëkalimeve të forta dhe komplekse është thelbësor. Ja disa rekomandime për të krijuar fjalëkalime më të sigurta:

Zgjidhni fjalëkalime që janë të vështira për t'u parashikuar. Shmangni përdorimin e informacioneve të lehta për t'u identifikuar, si mbiemra, datëlindje, përvjetorë, dhe emra të zakonshëm. Mos përdorni të njëjtin fjalëkalim për llogari të ndryshme, përfshirë platformat e mediave sociale.

Evitoni ruajtjen e fjalëkalimeve në formate statike, si në letër ose materiale fizike, përveç në rastet kur ato janë enkriptuar.

Ndryshoni fjalëkalimet rregullisht dhe mos i ndani asnjëherë ID-të e përdoruesit apo fjalëkalimet me persona të tjerë, përfshirë anëtarët e familjes.

Pajisje të sigurt

Mbajeni pajisjen tuaj të sigurtë dhe softuerin të përditësuar:

Sigurohuni që keni antivirus të instaluar dhe firewall të aktivizuar

Përditësoni rregullisht sistemin operativ dhe softuerin e pajisjes suaj.

Para instalimit, skanoni çdo softuer të shkarkuar nga interneti për viruse.

Evitoni instalimin e programeve nga burime të panjohura ose të pasigurta.

Sulme të Inxhineruara Sociale

Sulmet e inxhinieruara sociale përfshijnë përpjekje për të mashtruar individët në mënyrë që të shpalosin informacion të ndjeshëm (si fjalëkalime) ose të kryejnë veprime të caktuara, si shkarkimi dhe ekzekutimi i dosjeve që duken të padëmshme, por në fakt janë të dëmshme. Kriminelët përdorin këto metoda për të fituar besimin e viktimës dhe për të mbledhur informacionin e vjedhur, që më pas mund të përdoret për mashtrim ose për të sulmuar sisteme dhe rrjete kompjuterike.

Metodat e zakonshme të sulmeve të inxhinieruara sociale përfshijnë:

Emaila Mashtrues (Phishing)
Uebfaqe të Rreme

Këto teknika janë të dizajnuara për të mashtruar dhe për të fituar qasje në informacion të ndjeshëm.

Emaila mashtrues (Phishing)

Dërgimi i emailave mashtruese (phishing) është një teknikë që përdoret nga kriminelët për të fituar informacion të ndjeshëm duke u paraqitur si një biznes legjitim ose individ me reputacion në kuader te nje komunikimi elektronik, si emaila, mesazhe tekstuale (SMS), telefonata, ose mesazhe instante. Këta kriminelë shpesh përfshijnë lidhje ose shtojca që duken si burime të besueshme dhe të vlefshme, por që në të vërtetë janë faqe të dëmshme që vjedhin dhe regjistrojnë informacionin tuaj, si për shembull fjalëkalimet.

Ja disa këshilla si të mbroheni:

Gjithnjë shënojeni adresen e uebfaqes se Bankës (URL) në shfletuesin tuaj ose përdorni shenjues (bookmarks) në vend se të klikoni linqe që gjenden brenda mesazheve, edhe nëse konsideroni se mesazhi është legjitim.

Banka asnjëherë nuk ju dërgonë email për t'ju kërkuar të "konfirmoni" ose "përditësoni" fjalëkalimin tuaj apo ndonjë informacion personal duke klikuar në ndonjë link apo duke vizituar ndonjë uebfaqe.

Përpiquni të verifikoni në mënyrë të pavarur çdo detaj që jepet në mesazh direkt me kompaninë.

Të gjitha mesazhet e pakërkuara nga ju trajtojini me kujdes, kurrë mos klikoni në linqe në mesazhe të tilla për të vizituar uebfaqe të panjohura.

Emailat mashtrues zakonisht përmbajnë mesazhe urgjente apo me ton autoritativ. Sigurohuni të kontrolloni për fjalë të shkruara gabim, logo të parregullta të kompanive apo adresa emaili të çuditshme.

Shfrytëzoni ndonjë nga zgjidhjet për filtrimin e emailave SPAM që ndihmojnë kundër dërgimit të emailava mashtrues.

Uebfaqet e rreme

Uebfaqet e rreme **(spoofing)** përfshijnë krijimin e uebfaqeve mashtruese që duken të jenë identike me uebfaqet legjitime. Qëllimi i kriminelëve kibernetikë është të bëjnë që individët të besojnë se po ndërveprojnë me një kompani ose person të besueshëm, duke i manipuluar ata për të ndarë informacion të ndjeshëm ose për të shkarkuar softuer të dëmshëm në kompjuterët e tyre.

Ja disa këshilla si të mbroheni:

Kontrollojeni me kujdesë adresën e uebfaqes (URL-në). Një uebfaqe mund të duket legjitime, por URL mund të ketë ndonjë variacion në shkrim apo të përdorë domein të ndryshëm.

Sigurohuni që ka simbolin e drynit. Uebfaqet legjitime kanë simbolin e drynit ose një vijë të gjelbër në anën e majtë të adresës URL të uebfaqes që tregon se është uebfaqe e siguruar.

Mos klikoni në linqe nëpër faqet e rrjeteve sociale, dritaret që hapen, apo uebfaqe jo të besueshme. Linqet mund t'ju dërgojnë në një uebfaqe tjetër nga ajo që tregon etiketa e tyre. Alternativa më e sigurtë është që adresën ta shënoni në shfletues.

Informacionin e ndjeshëm ia jepni uebfaqes vetëm kur përdoret lidhja e siguruar. Verifikojeni adresën e uebfaqes a fillon me https:// (shkronja "s" nënkupton e "siguruar") dhe jo vetëm http://.

Kontrolloni Certifikatën e Sigurisë të Bankës ProCredit duke klikuar tek simboli i drynit që shfaqet në shfletuesin tuaj. Shmangni përdorimin e uebfaqeve kur shfletuesi juaj nxjerr gabime të certifikatës apo paralajmërime.

Bëhuni/Jini vigjilent

Kyçeni pajisjen tuaj mobile

Mbrojeni telefonin tuaj të mençur ose tabletin në mënyrë të ngjashme me mbrojtjen e një kompjuteri. Përdorni fjalëkalim, shenjën e gishtit, ose njohjen e fytyrës për të siguruar ekranin e pajisjes tuaj dhe për të mbrojtur portofolin tuaj digjital.

Monitoroni aktivitetin e llogarisë tuaj

Kontrollojeni aktivitetin e llogarisë shpesh për të zbuluar ndonjë mashtrim sa më herët. Rekomandojmë që llogarinë tuaj të e-bankimit ta kontrolloni çdo javë. Raportoni menjëherë tek Banka ProCredit çdo aktivitet të dyshimtë apo mashtrues.

Kur jeni në lëvizje, bankoni në mënyrë të mençur

Shmangni përdorimin e bankimit mobil dhe dërgimin e emailave ose mesazheve të ndjeshme kur jeni të lidhur në Wi-Fi publike ose pajisje të pasigurta. Jini të kujdesshëm kur përdorni pajisje që nuk janë të juaja dhe mbi të cilat nuk keni kontroll të plotë. Banka ProCredit rekomandon të shmangni përdorimin e pajisjeve të tilla, pasi ato mund të kenë të instaluar programe monitorimi të dëmshme.

Fshijeni rregullisht memorien e pajisjes tuaj

Është praktikë e mirë të fshini informacionin e ruajtur në kompjuterin tuaj pas çdo sesioni të bankimit online. Shfletuesi juaj mund të ruajë automatikisht kopje të uebfaqeve që keni vizituar dhe të fjalëkalimeve që keni përdorur në to. Ju lutemi, kontrolloni dhe fshini çdo informacion të ruajtur në memorien e shfletuesit tuaj.

Masa të tjera proaktive

- Shkarkojini aplikacionet vetëm nga dyqanet zyrtare të aplikacioneve: Apple iTunes dhe Google Play Store. Shkarkimi i aplikacioneve falas nga burime jozyrtare ose të panjohura mund ta infektojë me virus pajisjen tuaj.

- Shmangni përdorimin e shërbimit e-Banking në kompjuterë publik apo Wi-Fi publike

- Tregoni mosbesim në rast të dritareve të dyshimta apo të papritura që shfaqen gjatë sesionit të bankimit online. Në rast dyshimi, ju lutemi ta kontaktoni direkt Bankën ProCredit.

- Asnjëherë mos i shenoni PIN-in e kartelës, fjalekalimin apo të dhënat e tjera personale konfidenciale sensitive në fletore, notes, etj

- Asnjëherë mos u largoni nga kompjuteri ndërkohë që jeni të kyçur në bankimin përmes internetit.

- Përkunder afatit të caktuar të shkyçjes automatike, preferohet që të shkyçeni manualisht pasi të keni përfunduar bakimin online.

RAPORTIMI I MASHTRIMIT

Nëse pranoni ndonjë mesazh apo email që përmend Bankën ProCredit në ndonjë mënyrë ose ndonjë element të marrëdhënies suaj me Bankën, ju rekomandojmë të njoftoni menjëherë Bankën ProCredit.

Njoftimin mund ta dërgoni në email adresat:
kos.contactcentre@procredit-group.com
kos.abuse@procredit-group.com

Në njoftim të përfshini një "screenshot" të mesazhit të dyshimtë dhe përshkrimin e dyshimeve tuaja mbi mesazhin e pranuar. Personeli i autorizuar i bankës do të analizojë më tej detajet përkatëse.

Për më tepër, mund të kontaktoni Bankën ProCredit përmes Qendrës sonë të Kontaktit në numrat **038-555-555** ose **049-555-555**, ose duke kontaktuar Këshilltarin tuaj të Klientit.

Për më shumë burime rreth Sigurisë Kibernetike, ju lutemi t'i referoheni:

Njësia Vendore për Sigurinë Kibernetike në Kosovë
https://www.kos-cert.org/en/index.php/home

Aleanca Vendore për Sigurinë Kibernetike
http://www.staysafeonline.org

Agjencia e BE-së për Sigurinë Kibernetike
https://www.enisa.europa.eu/

Njësia Vendore për Sigurinë Kibernetike në Kosovë -
Home kos-cert.org

Aleanca Vendore për Sigurinë Kibernetike -
http://www.staysafeonline.org

Agjencia e BE-së për Sigurinë Kibernetike -
https://www.enisa.europa.eu/