MASA ESENCIALE TË SIGURISË ONLINE

Banka për Biznes (BPB) garanton që shërbimet e saja digjitale kanë një siguri të lartë sa i përket sigurisë kibernetike, duke përdorur praktikat më të mira dhe teknologjitë bashkëkohore që ekzistojnë në ditët e sotme në industrinë e IT-së.

Përveç kësaj, banka ka nevojë për një kontribut të rëndësishëm nga klientët e saj që gjatë përdorimit të shërbimeve elektronike bankare të kenë parasysh disa masa sigurie që i japin kuptim të plotë sigurisë kibernetike në sistemin bankar. Pra, janë disa praktika te domosdoshme që duhen patjetër klientët t'i kenë në konsideratë.

Do të ishim mirënjohës dhe do të ndihemi të sigurt nëse klientët tanë do të praktikonin udhëzimet e mëposhtme.

Rregulli i parë

- Asnjëherë mos shpalosni të dhënat tuaja personale dhe financiare nëse ju kërkohen nga burime të panjohura në çfarëdo forme (email, telefon, letër etj.) e që në fokus kanë kërkesa lidhur me llogarinë, kartelën tuaj bankare apo platformat elektronike (ebanking, m-banking etj.).

- Zyrtarët e bankës asnjëherë nuk do t'iu pyesin për informata të ndjeshme (si për shembull fjalëkalime, PIN-i të kartelës apo të dhëna tjera) të cilat mund të cenojnë privatësinë tuaj apo sigurinë e mjeteve tuaja.

- Të qenit vigjilent, mirë të informuar me zhvillimet e fundit dhe pro aktiv në mbrojtjen e të dhënave personale dhe financiare mund të zvogëlojë ndjeshëm rrezikun e vjedhjes së identitetit, të dhënave tuaja dhe mashtrimit financiar.

Kujdesuni për sigurinë e pajisjes

- Pajisja juaj duhet të jetë fizikisht e mbikëqyrur.
- Përditësoni (update) sistemin operativ dhe aplikacionet menjëherë pasi të keni njoftimin nga prodhuesit për risit e sigurisë.
- Instaloni, aktivizoni dhe përditësoni (update) *antimalware/antivirus/antispyware* ne ato pajisje që është e mundur teknikisht.
- Instaloni aplikacione vetëm prej burimeve të sigurta të prodhuesve.
- Aktivizoni murin mbrojtës (firewall) personal në pajisjet që është e mundur teknikisht.
- Praktikoni gjithmonë daljen e sigurt nga pajisja (logout/lockout/logoff/signout/signoff).
- Praktikoni ruajtjen e një kopje (backup) të konfigurimit dhe të dhënave tuaja në ndonjë disk (USB, SD, etj.) të jashtëm apo në shërbimet kloud (cloud).

Qasja në pajisje dhe aplikacione

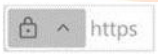
- Për qasje në pajisje të domosdoshme përdorni këto elemente: shfrytëzuesin, fjalëkalimin, PIN-in, finger print, etj.
- Mos ndani me të tjerët fjalëkalimet apo PIN-at.
- Mos përdorni detaje tuaja personale për të vendos një fjalëkalim apo PIN, si për shembull ditëlindjet, emrat tuaj apo të familjareve, numrin e telefonit, etj.
- Ndërroni fjalëkalimet apo PIN-a më shpesh.
- Vendosni fjalëkalime të gjata me karaktere të kombinuara.
- Përdorni fjalëkalime unike për secilën aplikacion.
- Përdorni siguri shtesë të qasjes me mekanizmin MFA (Multi Form Authenticator).

Qasja në rrjetet Wi-Fi publike

- Para se të qaseni në rrjetet Wi-Fi publike duhet të keni parasysh që këto rrjete janë të pasigurta.
- Provoni të verifikoni se a është legjitim rrjeti Wi-Fi në të cilin mendoni të qaseni.
- Evitoni qasjen apo të jepeni informata të ndjeshme (sensitive) derisa jeni të kyçur në Wi-Fi publike.
- Rekomandohet, nëse duheni të qaseni patjetër në shërbimet me informata të ndjeshme përdorni rrjetet mobile 3G/4G/5G në vend të atyre W-Fi publike.
- Përdorni rrjetet virtuale private (VPN) për të komunikuar sigurt.
- Rregullo qasjen në pajisje që mos të kyçet pajisja automatikisht në Wi-Fi publik.
- Shkëmbimi i dokumenteve (file-sharing) duhet të jetë deaktiv në pajisje.

Përdorimi i internetit nga shfletuesi (browser)

- Përdorni vetëm shfletues (browser) të sigurt nga prodhuesit e njohur.
- Evitoni ato ueb sajte që parashtrojnë pyetje rreth informatave tuaja sensitive.
- Kujdes në ueb sajte që paraqiten me *pop-up* dritare (yes/no/cancel/close).
- Gjatë përdorimit të shfletuesit(browser) ndiqeni këto udhëzime në baze të ikonave në adresë bar:



Ueb sajti është i sigurt dhe certifikata është vlefshme.

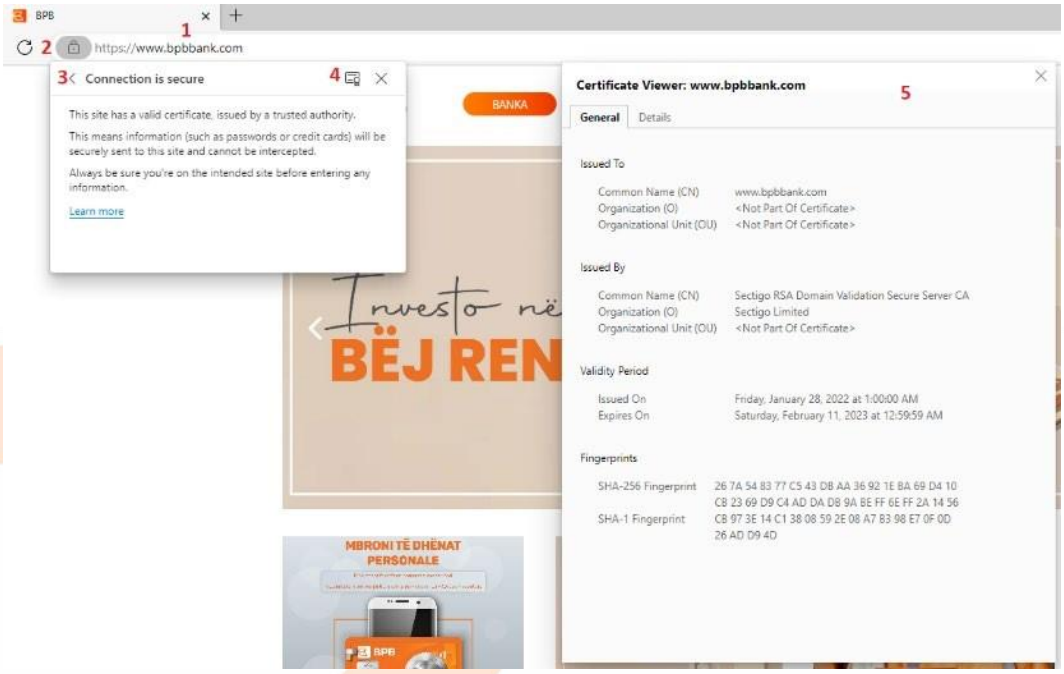
Ueb faqja nuk ka siguri të plotë. Mund të këtë rrezik në kapjen e informatave sensitive. Protokolli *http* është i pa sigurt, në vend të tij gjithmonë përdorni protokollin *https*.

Nënkupton ueb sajti nuk ka certifikatë të vlefshme, ka certifikatë të skaduar apo të vetë-caktuar. Ka rrezik potencial nga këto ueb faqe dhe duhen të evitohen gjithsesi.

Ndër ueb faqet më të rrezikshme janë me këto dy ikona. Përmbajnë rrezik shumë të lart nëse shfletohen. Mundësia është e madhe që pajisja juaj të infektohet. Mos i hapni assesi këto lloj ueb faqe.

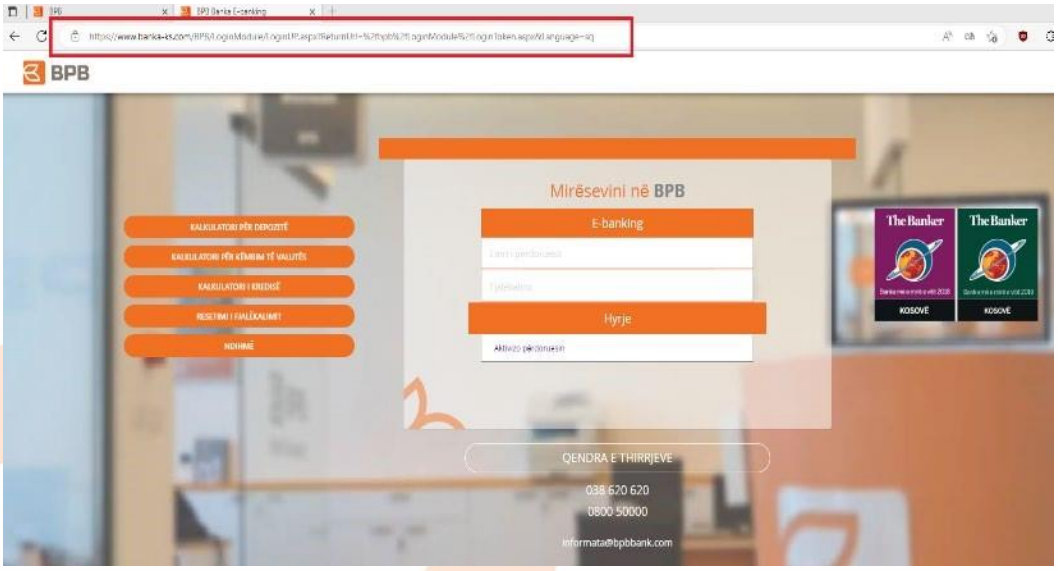
Qasja në ueb sajt dhe shërbimet e bankës BPB

- Vegëza (URL) e qasjes në ueb faqe të bankës BPB është:
  "***https://www.bpbbank.com/"***
- Verifikoni qasjen në ueb faqe përmes këtyre hapave:
  - Verifikoni mirë që adresa e bankës është saktësisht si në pikën **1**, në ilustrimin e më poshtëm.
  - Sigurohuni që komunikimi ka statusin si në piken **2** të ilustrimit. Për më shumë është sqaruar më lart se çfarë ueb sajti e konsiderojmë të sigurt. ○ Pika **3** duhet të ketë pamjen dhe përshkrimin si në ilustrim.
  - Nëse klikojmë në pikën **4**, na tregon që ka certifikatë për siguri të komunikimit.
  - Përfundimisht, pika **5** në ilustrim, na jep detaje si të duket një certifikatë digjitale e bankës BpB.



- Verifikoni qasjen në e-banking përmes këtyre hapave:
  - Hap ueb faqen me vegëzën (URL) "***https://www.bpbbank.com/"***

  - Kliko në ikonën  o Do të shfaqet ueb aplikacioni për e-banking.



- Vini re, ueb aplikacioni e-banking funksionon me një vegëz (URL) tjetër që është në shfrytëzim nga banka BPB, gjithashtu. Kjo vegëz (URL) është legjitime dhe është pjesë e domenit "***banka-ks.com***": ***"https://www.banka-ks.com/BPB/Account/Login"*** o Për më shumë ndihmë rreth përdorimit të e-banking mund të gjeni edhe në vegëzat tjera si më poshtë:

  Për individ:
  "https://www.bpbbank.com/individ/#bankingu-elektronik" Për biznes:
  "***https://www.bpbbank.com/bizneset/#bankingu-elektronik"***

Përdorimi i e-mailit (pranimi i e-mailave nga banka BPB)

- Familjarizohuni me teknikat (phishing, spoofing dhe spam) të mashtrimit që përmes e-mailit, janë kudo në internet.
- Verifikoni mirë dërguesin e-mailit. Mund ta verifikoni edhe përmes telefonit.
- Të keni kujdes në hapjen e vegëzave (URL) tek e-mailat e dyshimtë nëse kanë arrit në emër të bankës.
- E-mailat e dyshimtë mund të duken zyrtar dhe me përmbajte bindëse, por kujdes.
- E-mailat e dyshimtë mund të kenë defekte drejtshkrimore dhe gramatikore.
- Mos hapni dokumentet e bashkangjitura në e-mailat e dyshimtë që përmenden shërbime bankare.

Shembull i përgjithshëm

Sot ka shumë mashtrime në internet që mundësojnë domenet të duken sikur ato origjinale dhe shpeshherë shfrytëzuesit bien pr e këtyre mashtrimeve. Të marrin një shembull:

Mashtruesit (keqdashësit, hakerët) e internetit përdorin emra të ngjashëm me domenet origjinale, për shembull: "***bpbbanka.com***" Në shikim të parë dhe të shpejt duket që është domen zyrtar, por mashtruesit vendosin vetëm një karakter ndryshe që e dallon atë. Në këtë rast është shtuar vetëm një "**a**". Me këtë karakter shtesë mund të na dërgoj në ueb faqen e mashtruesve (keqdashësve, hakerëve) dhe nga aty do të na marrin të dhënat personale dhe do të keqpërdorin informatat në kuptimin e krimit kibernetik, apo do të iniciohet ndonjë sulm kibernetik. Andaj, lusim për vëmendje dhe bashkëpunim.

Raportimi

Nëse dyshoni për ndonjë aktivitet të paautorizuar, pranoni e-email, mesazh, apo njoftim të dyshimtë për të cilat nuk e dini burimin e saktë në lidhje me shërbimet e bankës, ju lutem raportoni ato menjëherë në BPB, përmes kanaleve tona të komunikimit:

dataprotection@bpbbank.com
sherbimiperkliente@bpbbank.com
0800 50 000, 038 620 620