

Dokumento tipas TAISYKLĖS	Patvirtinta 2024-02-29 valdybos protokolas V-2024-10
Dokumentą rengė: Zbignevas Masovič	Įsigalioja 2024-05-21
Jungtinė centrinė kredito unija; Projektų grupė	Versija: V3

JCKU ir KU elektroninių paslaugų teikimo taisyklių

Priedas Nr.1

Internetinio banko saugumo reikalavimai

Nesiųskite el. paštu konfidencialios informacijos (prisijungimo prie elektroninės bankininkystės sistemos slaptažodžių ir pan. duomenų). Suabejoję elektroninės paslaugos ar įrenginio patikimumu, nutraukite darbą, atjunkite įrenginį nuo interneto ir nedelsdami praneškite apie tai unijai.

Kaip saugiai naudoti slaptažodį?

1. Bankininkystei naudokite unikalius slaptažodžius. Jeigu kažkas sužino jūsų daug kur naudojamą slaptažodį, jis iš karto gali patekti į visas paskyras.
2. Įsiminkite slaptažodžius, neužsirašykite jų, nesaugokite kompiuteryje (išskyrus tam skirtas ir leidžiamas programas), neatskleiskite savo asmens duomenų ar prisijungimo duomenų prie interneto banko kitiems asmenims, įskaitant šeimos narius, draugus, reguliariai keiskite slaptažodį.
3. Slaptažodžius įveskite tik tada, kai esate tikri, kad Jūsų niekas nestebi.
4. Saugokite slaptažodžius kitiems žmonėms neprieinamose vietose — ne piniginėse, rankinėse ar šalia savo kompiuterio.
5. Nepraneškite slaptažodžių telefonu, socialiniuose tinkluose, nesiųskite jų paštu ar el. paštu. Pastaruoju metu vis dažniau sukčiai slaptažodžius bando išvilioti telefonu apsimesdami, unijos, policijos, Finansinių nusikaltimų tyrimo tarnybos, Specialiųjų tyrimų tarnybos, „Sodros“ ar kitų valstybės įstaigų darbuotojais ar darbdaviais, siūlančiais patrauklų darbą. Nepasiduokite psichologiniam spaudimui — neatskleiskite telefonu konfidencialių duomenų, nes niekas neturi teisės to iš Jūsų reikalauti. Apie tokį bandymą iškart praneškite unijai ir policijai. Jeigu dvejojate, visada papildomai pasiklauskite žodžiu.
6. Sukčiai gali banko vardu siųsti jums netikrus SMS pranešimus, tam kad gautų asmens bei tapatybės patvirtinimo priemonių duomenis. Niekada neatsakykite į SMS pranešimą, kuriame prašoma pateikti slaptus duomenis.
7. Nespauskite nuorodų SMS žinutėse. Būkite itin atidūs, jeigu žinutės siuntėjai prašo atidaryti pateikiamą nuorodą. Tokiomis nuorodomis dažnai nukreipiama į netikrą interneto puslapį, skirtą duomenims surinkti.
8. Jokiu būdu nenurodykite slaptažodžių, jei prisijungiant prie elektroninės bankininkystės ar pervedant pinigus internetu Jūsų prašoma įvesti iš karto kelis slaptažodžius. Jeigu taip nutinka, vadinasi, Jūsų naudojamas kompiuteris užkrėstas — per kenksmingas programas sukčiai bando sužinoti įvestus slaptažodžius. Tokiu atveju būtinai nedelsdami:
 - baikite darbą elektroninių paslaugų sistemoje;
 - **praneškite unijai** paskambinę jos internetiniame puslapyje nurodytu kontaktiniu telefonu ir paprašykite blokuoti prieigą prie elektroninės bankininkystės sistemos.

Kokių duomenų negalima atskleisti?

1. Neatskleiskite savo paso, asmens tapatybės kortelės ar vairuotojo pažymėjimo duomenų kitiems asmenims, jeigu jie nenurodo aiškaus teisinio pagrindo šiems duomenims rinkti.
2. Nepraneškite prisijungimo prie elektroninės bankininkystės sistemos slaptažodžių telefonu, nesiųskite jų paštu ar el. paštu. Unija niekuomet nereikalauja šios informacijos pateikti minėtais būdais.

Dokumento tipas TAISYKLĖS	Patvirtinta 2024-02-29 valdybos protokolas V-2024-10
Dokumentą rengė: Zbignevas Masovič	Įsigalioja 2024-05-21
Jungtinė centrinė kredito unija; Projektų grupė	Versija: V3

3. Atminkite, kad atpažinimo kodas yra toks pat svarbus kaip jūsų asmens kodas, tad skirkite deramą dėmesį jo apsaugai.

Kaip naršyti po internetą ir naudotis teikiamomis elektroninėmis paslaugomis?

1. Junkitės prie internetinės bankininkystės sistemos tik per oficialius unijų puslapius arba surinkę adresą: <https://e.kreda.lt/>. Norėdami prisijungti prie internetinės bankininkystės turite naudotis naujausiomis Internet Google Chrome, Mozilla Firefox arba Explorer naršyklių naujausiomis versijomis
2. Būkite atidūs, kai atveriate el. laiškus, naršote po internetą, kopijuojate informaciją.
3. Ypač tikrinkite nepažįstamų asmenų žinutes elektroninio pašto ir socialinių tinklų paskyrose, kuriose yra nuorodų (angl. „hyperlink“ (//bit.ly)). Niekada nespauskite įtartinų nuorodų.
4. Jeigu gavote elektroninį laišką iš unijos, kuriame prašoma prisijungti arba suvesti asmens duomenis, slaptažodžius, eikite į unijos interneto puslapį ne per nuorodą, o prisijunkite rankiniu būdu, kaip paprastai.
5. Nesilankykite nepažįstamuose tinklalapiuose — dažniausiai kenksmingos programėlės (virusai) platinamos el. paštu ir nesaugiuose tinklalapiuose.
6. Jei sąskaitoje yra daugiau pinigų, negu jums reikia kasdienėms išlaidoms, nustatykite operacijų apribojimus. Sudarant internetinės bankininkystės paslaugų sutartį, iš anksto nustatoma didžiausia pinigų suma, kurią galima išleisti naudojantis interneto banku. Jei norite pakeisti apribojimus arba pervesti didesnę sumą, atvykite į artimiausią unijos skyrių.
7. Nesinaudokite elektroninėmis paslaugomis viešose vietose, jei Jums atrodo, kad esate stebimi, ar kompiuteris kelia įtarimą.
8. Viešoje vietoje pasinaudoję elektroninių paslaugų sistema, pasikeiskite slaptažodį.
9. Nesinaudokite viešais tinklais (kavinės, parduotuvės ar kitu nesaugiu WIFI) bankinėms transakcijoms.
10. Nesinaudokite internetine bankininkyste iš svetimo kompiuterio. Svetimame ar viešai naudojamame kompiuteryje gali būti įdiegta kenkėjiška programinė įranga, renkanti asmeninius duomenis ar registruojanti klaviatūros paspaudimus. Tokiu atveju rizikuojate tretiesiems asmenims atskleisti savo asmeninius duomenis bei slaptažodžius.
11. Pirkite tik patikimose parduotuvėse. Prekes ir paslaugas visada saugu pirkti žinomose, gerą reputaciją turinčiose Lietuvos ir užsienio el. parduotuvėse. Nežinomus pardavėjus vertinkite kritiškai, pasidomėkite jų veikla. Pasidomėkite viešai internete pateikiamais atsiliepimais apie konkrečią el. parduotuvę.
12. Jei suabejojote dėl internetinės bankininkystės atvaizdavimo ar sistemos veikimo, iš karto nutraukite veiksmus. Baikite darbą internetinėje bankininkystėje ir apie tai informuokite uniją.
13. Nustatykite mažą operacijų, atliekamų elektroninės bankininkystės sistemoje, limitą ir didinkite jį tik tada, kai būtina.
14. Darbą elektroninėje bankininkystėje baikite spustelėdami „Baigti darbą“.
15. Dėl elektroninių paslaugų konsultuokitės tik su unijos darbuotojais.

Kaip apsaugoti kompiuterį?

1. Įsidiekite patikimą legalią antivirusinę programą, reguliariai atnaujinkite programinę įrangą ir naudokite naujausias naršyklių versijas.
2. Dažnai aptinkama operacinių sistemų ir kitos programinės įrangos saugumo spragų, leidžiančių sukčiams neteisėtai patekti į svetimus kompiuterius ir prisijungti prie sistemų. Šiomis spragomis naudojasi įsilaužėliai, todėl gamintojai, siekdami užtikrinti įrangos saugumą, nuolat ją koreguoja, šalina aptiktas

Dokumento tipas TAISYKLĖS	Patvirtinta 2024-02-29 valdybos protokolas V-2024-10
Dokumentą rengė: Zbignevas Masovičius	Įsigalioja 2024-05-21
Jungtinė centrinė kredito unija; Projektų grupė	Versija: V3

spragas. Taigi pasirūpinkite, kad Jūsų naudojama operacinė sistema ir kita programinė įranga būtų laiku atnaujinta. Rekomenduojame nustatyti automatinius nustatymus.

3. Aptikę virusą ar pasiūlymą įsidiesti įtartiną programą, iškart baikite darbą kompiuteriu ir kreipkitės į specialistus.

4. Domėkitės ir naudokitės informacinių technologijų saugumo specialistų patarimais.

5. Jei elektroninės bankininkystės sistemos registracijos lange įvedus atpažinimo kodą ir slaptažodžius, nepavyksta prisijungti, rodomas pranešimas apie techninius nesklandumus arba ilgokai matote nesibaigiančio veiksmo piktogramą, vaizduojančią besisukantį ratą, nedelsdami praneškite apie tai unijai paskambinę jos internetiniame puslapyje nurodytu kontaktiniu telefonu.

6. Puslapis <https://www.kreda.lt/> yra apsaugotas autentiškumą patvirtinančiu sertifikatu. Naršyklėje, šalia puslapio adreso atsiranda spynelė, kuri patvirtina puslapio tikrumą. Dauguma naršyklių taiko papildomus perspėjimus, jeigu sertifikatas nėra autentiškas.

7. Daugiau informacijos, kaip apsaugoti savo įrenginį ir kaip saugiai naudotis kitomis paslaugomis internete, rasite šioje svetainėje: <https://www.esaugumas.lt/lt>