



Internetinės bankininkystės saugumo reikalavimai



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

Kaip saugiai naudoti slaptažodį?

1. Įsiminkite slaptažodžius, neužsirašykite jų, niekam nesakykite, reguliariai keiskite.
2. Slaptažodžius įveskite tik tada, kai esate tikri, kad Jūsų niekas nestebi.
3. Saugokite slaptažodžius ir jų formavimo įrenginius bei priemones (slaptažodžių generatorius, korteles) kitiems žmonėms neprieinamose vietose — ne piniginėse, rankinėse ar šalia savo kompiuterio.
4. 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.
5. 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:
6. baikite darbą elektroninių paslaugų sistemoje
7. praneškite apie tai savo unijai paskambinę klientų aptarnavimo telefonu, kurį rasite užėję ant nuorodos <http://www.kreda.lt/kredito-unijos/kontaktai-darbo-laikas/> 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.

Kaip naršyti po internetą ir naudotis teikiamomis elektroninėmis paslaugomis?

1. Būkite atidūs, kai atveriate el. laiškus, naršote po internetą, kopijuojate informaciją.
2. Ypač tikrinkite nepažįstamų asmenų žinutes elektroninio pašto ir socialinių tinklų paskyrose, kuriose yra nuorodų (angl. „hyperlink“). Niekada nespauskite įtartinų nuorodų.
3. Nesilankykite nepažįstamuose tinklalapiuose — dažniausiai kenksmingos programėlės (virusai) platinamos el. paštu ir nesaugiuose tinklalapiuose.
4. Nesinaudokite elektroninėmis paslaugomis viešose vietose, jei Jums atrodo, kad esate stebimi, ar kompiuteris kelia įtarimą.
5. Viešoje vietoje pasinaudoję elektroninių paslaugų sistema, pasikeiskite slaptažodį.
6. Nesinaudokite elektroninėmis paslaugomis jungdamiesi iš nepažįstamų asmenų kompiuterių.
7. Prieš pirkdami nežinomose elektroninėse parduotuvėse, pasidomėkite jų patikimumu.
8. Nustatykite mažą operacijų, atliekamų elektroninės bankininkystės sistemoje, limitą ir didinkite jį tik tada, kai būtina.
9. Darbą elektroninėje bankininkystėje baikite spustelėdami „Baigti darbą“.
10. Dėl elektroninių paslaugų konsultuokitės tik 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 spragas. Taigi pasirūpinkite, kad Jūsų naudojama operacinė sistema ir kita programinė įranga būtų laiku atnaujinta. Nenaudokite nebeatnaujinamos programinės įrangos, tokios kaip „Internet Explorer 6“.
3. Aptikę virusą ar pasiūlymą įsidiegti įtartiną programą, iškart baikite darbą kompiuteriu ir kreipkitės į kompiuterių 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 nesklaidumus arba ilgokai matote nesibaigiančio veiksmo piktogramą, vaizduojančią besisukantį ratą, tikėtina, kad Jūsų kompiuteris yra užkrėstas virusu. Nedelsdami praneškite apie tai klientų aptarnavimo telefonu, kurį rasite užėję ant nuorodos <http://www.kreda.lt/kredito-unijos/kontaktai-darbo-laikas/>