BONUM PUBLICUM gyvybės draudimo bendrovė	**SAUGUMO REKOMENDACIJOS**
Dokumento tipas: Rekomendacijos	**Įsigalioja:** 2019 m. birželio 21 d.

I. BENDROSIOS NUOSTATOS

1. Gyvybės draudimo UAB „BONUM PUBLICUM“ (toliau – Bonum Publicum) elektroninės savitarnos svetainės (toliau – Savitarna) saugumą užtikrina kelių lygių apsauga. Tačiau kiekvienas asmuo, sudarydamas savitarnos paslaugų sutartį (pvz., mobilus parašas, Smart ID ir kt.), turi pats laikytis saugumo priemonių – saugoti savo prisijungimo priemones, pasirūpinti, kad slaptų asmens identifikavimo duomenų nesužinotų kiti asmenys.

II. PAGRINDINĖS SAUGUMO REKOMENDACIJOS NAUDOJANTIS SAVITARNA

2. Saugokite savo savitarnos identifikavimo duomenis: Naudotojo vardą (ID), pirminį slaptažodį, prisijungimo slaptažodį, slaptažodžių PIN kortelę, generatoriaus PIN kodą, mobiliojo parašo (M. parašo) sPIN1 / sPIN2 kodus, elektroninio parašo (e. parašo) PIN kodą, „Smart-ID“ PIN1 / PIN2 kodus, telefoną apsaugokite slaptažodžiais ar kitais būdais (plačiau apie tai – čia).
3. Savo prisijungimo slaptažodžio ir kitų slaptų identifikavimo duomenų neatskleiskite niekam. Bonum Publicum darbuotojai, teisėsaugos ir kitų valstybinių įstaigų pareigūnai tokios informacijos niekada jūsų neprašys, nei telefonu, nei elektroniniu paštu, nesiteiraus socialiniuose tinkluose ar kitais būdais. Būkite budrūs ir nepasiduokite pasitaikančiam sukčių psichologiniam spaudimui.
4. Jungdamiesi prie savitarnos, atidžiai patikrinkite tinklalapį:
   4.1. svetainės adresas turi būti https://bp.sb.lt, atkreipkite dėmesį į adreso pradžią – pradžios trumpinys turi būti „https“, o ne „http“;
   4.2. puslapio saugumo sertifikatas privalo būti galiojantis – naršyklės adreso eilutėje turi būti spynelės simbolis ir žalias (arba juodas žaliame fone, priklausomai nuo naršyklės) užrašas „Siauliu Bankas AB [LT]“. Jeigu šio užrašo nėra arba naršyklė perspėja apie negaliojantį saugumo sertifikatą, nesijunkite prie savitarnos ir apie tai nedelsiant prašome pranešti Bonum Publicum.
5. Kitos saugaus naudojimosi rekomendacijos:
   5.1. rekomenduojama nesaugoti savitarnos prisijungimo duomenų naršyklės atmintyje;
   5.2. prisijungę prie savitarnos, nesinaudokite naršyklės mygtukais „Back“ ir „Forward“. Jei norite grįžti į ankstesnį langą, spustelėkite mygtuką „Grįžti“ arba rinkitės reikiamus punktus iš meniu;
   5.3. baigę darbą savitarnoje, visada atsijunkite nuo sistemos spragtelėdami mygtuką „Išeiti“ (dešiniame viršutiniame kampe) ir būtinai uždarykite naršyklę;
   5.4. pasinaudoję savitarnos sistema interneto kavinėje, bibliotekoje ar kitose viešose vietose, išvalykite naršyklės laikinąją atmintį, kad neliktų išsaugoti jokie jūsų duomenys. Taip pat rekomenduotina pasikeisti prisijungimo slaptažodį.

III. KOMPIUTERIO SAUGUMO PALAIKYMAS

6. Naudokitės kompiuteriais, kuriuose įdiegtos legalios, atnaujintos operacinės sistemos, pvz., Windows 7, Windows 8, Windows 10 ar kitų gamintojų palaikomos operacinės sistemos. Venkite neatnaujinamų ir gamintojų nepalaikomų operacinių sistemų, tokių kaip Windows XP.

7. Rekomenduojame naudoti tik naujas, gamintojų palaikomas naršyklių versijas: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Safari. Venkite nepalaikomų ir neatnaujinamų naršyklių, tokių kaip Microsoft Internet Explorer 10 ir senesnių.
8. Nuolat atsinaujinkite antivirusinę sistemą, programas, šalinančias šnipinėjančias programėles (angl. *„anti-spyware“*) bei ugniasienes (angl. *„firewall“*). Pasirūpinkite, kad ir kitos naudojamos jūsų kompiuterio programos būtų atnaujintos. Ypač atkreipkite dėmesį į programas, kurias naudoja interneto naršyklės Adobe Flash, Adobe Reader, Java.

IV. BŪKITE BUDRŪS IR ATSAKINGI

9. Nesilankykite nepažįstamuose tinklalapiuose – dažniausiai kenksmingos programėlės (šnipinėjančios, virusai ir pan.) platinamos elektroniniu paštu ir nesaugiuose tinklalapiuose, taip pat nepažįstamų žmonių žinutėse socialinių tinklų paskyrose.
10. Jūsų savitarnos slaptažodį turi sudaryti skirtingi simboliai ir skaitmenys. Slaptažodyje nenaudokite lengvai atspėjamų duomenų, tokių kaip vardas, gimimo data, augintinio vardas ar pan. Pasidomėkite plačiau, kaip susikurti saugų slaptažodį – čia.
11. Savitarnos identifikavimo priemones saugokite pašaliniams asmenims neprieinamoje vietoje, nelaikykite jų visų kartu, nerašykite savo Naudotojo ID ir / ar prisijungimo slaptažodžio ant slaptažodžių PIN kortelės ar pan., nesinešiokite šių duomenų piniginėse, slaptažodžių nesaugokite savo telefone. Savo prisijungimo bei identifikavimo duomenų niekam neatskleiskite ir neperduokite net pažįstamiems ar asmenims, prisistatantiems banko, valstybinių institucijų, teisėsaugos atstovais.
12. Atkreipiame dėmesį, kad Bonum Publicum niekada nesiunčia elektroninių laiškų, prašydama jūsų prisijungimo prie savitarnos duomenų. Gavę įtartiną laišką, nespauskite jame esančių nuorodų, neatidarykite prisegtų priedų ir nedelsdami apie tokį laišką informuokite Bonum Publicum tel.: (8 5) 236 27 23.
13. Daugiau informacijos apie tai, kaip apsaugoti savo kompiuterį, kaip išvengti situacijų, kuomet bandoma išvilioti informaciją, taip pat apie kitus nesąžiningų žmonių naudojamus sukčiavimo būdus ir kaip nuo jų apsisaugoti, galite rasti čia.