Rekomenduojamos apsaugos priemonės Jūsų kompiuteriui

Ţemiau išvardinti patarimai skirti siekiant maksimaliai uţtikrinti saugų naudojimąsi internet banko paslauga Multinet.

1. Jungdamiesi prie Multinet sistemos patikrinkite ar tikrai prisijungėte prie tikrosios svetainės, kuri priklauso AS „Meridian Trade Bank" (www.multinetbank.eu). Įsitikinkite ar yra elektroninių duomenų protokolas HTTPS, o taip pat elektroninis svetainės tapatumo sertifikatas, kurį Bankui suteikė sertifikavimo įmonė VeriSign.

2. Siekiant uţtikrinti savo konfidencialumą dirbant Multine sistema (www.multinetbank.eu), patikrinkite ir esant reikalui pakeiskite savo naršyklės nustatymus taip, kad Jūsų slaptaţodis, vartotojo vardas sistemoje MultiNet ir kiti duomenys, būtini tapatybės nustatymui, nebūtų išsaugomi Jūsų kompiuteryje.

3. Nesinaudokite MultiNet sistema, jei nesate įsitikinę kompiuterio saugumu (viešose bibliotekose, interneto kavinėse). Svetimuose kompiuteriuose gali būti kenkėjiškos programos, kurių pagalba galima suţinoti Jūsų slaptaţodį ir MultiNet sistemos prisijungimo kodus.

4. Jokių būdu neatsakykite į tokius laiškus, kuriuose prašoma atskleisti informaciją apie Jūsų sąskaitas arba informaciją, kuri reikalinga prisijungimui prie MultiNet sistemos (kliento ID, slaptaţodis, kodai iš kodų kortelės). Bankas niekada neprašo atsiųsti tokio tipo informacijos elektroniniu paštu!

5. Apsaugokite savo kompiuterį slaptaţodţiu, o taip pat rekomenduojama naudoti ekrano uţsklandą su slaptaţodţiu. Tai panaikins galimybę pašaliniam asmeniui prisijungti ir dirbti Jūsų kompiuteriu. Jokiu būdu, nepalikite savo kompiuterio be prieţiūros, kai dirbate su MultiNet sistema (www.multinetbank.eu).

6. Baigdami darbą MultiNet sistemoje (www.multinetbank.eu), visada spauskite „Išeiti", kad tinkamai baigtumėte savo prisijungimo sesiją ir pašalinis asmuo negalėtų tęsti darbo po Jūsų.

7. Saugokite visus savo slaptaţodţius! Labai daţnai, būtent nesilaikant slaptaţodţio saugojimo taisyklių, reikšmingai padidėja nesankcionuoto prisijungimo rizika. Kad apsaugotumėte savo slaptaţodţius, Jums būtina laikytis šių reikalavimų:

- Slaptaţodţiui sudaryti naudokite tik Jums ţinomus ţodţių junginius, didţiąsias ir maţąsias raides, skaitmenis ir simbolius;
- Jokiu būdų slaptaţodţio nekurkite naudodami savo vardo, pavardės, vaikų, giminaičių ar naminių gyvūnų vardų, automobilio numerio, asmens kodo ar kaţkokios kitos lengvai atspėjamos simbolių kombinacijos;
- Slaptaţodis turi būti ne trumpesnis nei 8 simboliai;
- Pastoviai keiskite savo slaptaţodį (ne rečiau kaip kartą per du mėnesius);
- Jokiu būdu neuţsirašinėkite slaptaţodţių ant popieriaus lapukų, ar kitų dokumentų ir nepalikite jų kitiems prieinamoje vietoje;
- Niekam neatskleiskite savo kompiuterio, MultiNet sistemos ar kitų slaptaţodţių;
- Jei įtariate, kad pašaliniai asmenys gali pasinaudoti Jūsų slaptaţodţiais ar MultiNet sistemos kodų kortele, nedelsiant praneškite apie tai telefonu +371 67019341;

8. Papildomam saugumui savo kompiuteryje naudokite antivirusines programas ir ugniasienes (software firewall):

- Antivirusinė programa uţtikrins Jūsų kompiuterio apsaugą nuo įvairių kenkėjiškų programų (kompiuterinių virusų, šnipinėjimo programų, „trojanų", nereikalingų reklaminių programų ir kt.). Pasirenkant antivirusinę programą įsitikinkite, ar ji gali tikrinti ir vidinės atminties įrenginius ir išorinės atminties kaupiklius (USB atmintines, CD ir DVD diskus ir kt.), o taip pat visą informaciją, kuri patenka į Jūsų kompiuterį iš kitų kompiuterių per tinklą (el. paštas, interneto svetainės, duomenų apsikeitimas ir kt.). Įsitikinkite, ar Jūsų antivirusinės programos nustatymai uţtikrina pastovų programinį atnaujinimą.

- Ugniasienė padės papildomai apsisaugoti nuo pavojų esančių interneto tinkle. Ši programa leis daryti tik tuos sujungimus tarp kompiuterio ir interneto, kurie reikalingi Jūsų poreikiams. Bet kurie kiti sujungimai ar bandymai jungtis, kuriems nedavėte sutikimo, bus blokuojami. Ši programa stipriai sumažina riziką, kad piktavaliai asmenys per interneto tinklą suras Jūsų kompiuterio silpnas vietas ir gaus prieigą prie jame esančios asmeninės informacijos.

9. Pasirūpinkite, kad tiek Jūsų kompiuterio, tiek prie jo jungiamų įrenginių operacinė sistema būtų atnaujinama ir saugumo atnaujinimai būtų instaliuojami joje savalaikiai.

Banko rekomenduojamos papildomos saugumo priemonės

1. Naudokite tokius dienos limitus, kuriuos viršijus, reiktų papildomos autorizacijos (pranešimas bankui; vartotojui patariama taip pat naudoti dvigubą operacijos autorizaciją)
2. Naudokite įrenginius užtikrinančius didesnį identifikavimo saugumą - kodų generatorių, kuris generuoja unikalius, vienkartinius kodus galiojančius ribotą laiką.
3. Naudokitės Banko pasiūlymu paskambinti klientui, jei pervedimo suma viršija tam tikrą limitą.

Kontroliuokite finansines operacijas savo sąskaitose

1. Nuolatos tikrinkite pinigų likučius ir įvykdytas finansines operacijas savo sąskaitose.
2. Naudokitės galimybe gauti trumpuosius pranešimus – („SMS pranešimo“ paslauga).

Kilus įtarimams būtinai susisiekite su Banku

Jei kyla įtarimai dėl kažkokio sandorio, laiško, elektroninio laiško ar skambučio, būtinai susisiekite su Banku ir įsitikinkite jo tikrumu (tel.: +371 67019341).

Įsidėmėkite, kad Bankas niekada neprašo klientų atskleisti duomenis, kurie reikalingi naudotis elektroninėmis paslaugomis.