BALTIC INTERNATIONAL BANK INTERNETBANKAS UN BIB MOBILĀS APLIKĀCIJAS DROŠAS LIETOŠANAS IETEIKUMI UN PERSONĀLO DATORU, PLANŠETDATORU UN VIEDTĀLRUŅU AIZSARDZĪBAS IETEIKUMI

Interneta bankas un mobilās aplikācijas drošai lietošanai lūdzam Jūs izlasīt un ievērot personālo datoru, planšetdatoru un viedtālruņu aizsardzības ieteikumus, kā arī „Baltic International Bank" interneta bankas un BIB mobilās aplikācijas ("***B Online***") drošas lietošanas ieteikumus.

Aizsardzība personālajam datoram, kas aprīkots ar „Windows", „Mac OS", "Linux" (operētājsistēmu)

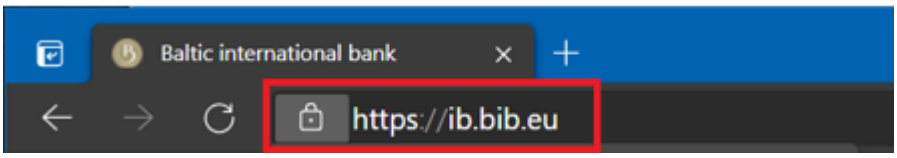
- Uzstādiet tikai tādu programmnodrošinājumu (PN), kas ir iegūts no uzticamiem avotiem;
- Piekļuves ierīcē jābūt instalētai pretvīrusu un anti-spyware programatūrai
- Aizsardzībai pret ļaunprātīgu, spiegojošu un nevēlamu programmatūru nodrošiniet, lai datorā būtu uzstādīta aktuāla antivīrusu PN versija, konfigurējiet PN tā, lai notiktu tās automātiska atjaunināšanās, un regulāri veiciet pilnu datorsistēmas pārbaudi ar antivīrusu PN. Atgādinām, ka antivīrusu PN izmantošana negarantē pilnīgu aizsardzību;
- Regulāri uzstādiet visus PN atjauninājumus, izmantojot automātiskās atjaunināšanas funkciju. Pārliecinieties, ka tiek atjaunināts viss PN, ieskaitot operētājsistēmu un lietojumprogrammas (piemēram, „Microsoft Office", „Adobe Acrobat", „QuickTime", „iTunes", Pārlūkprogrammas Chome, Edge, FireFox utl.);
- Uzstādiet atsevišķu vai operētājsistēmā iebūvētu ugunsmūri (angļu val. *firewall*), konfigurējot to tā, lai Jūsu datoram nebūtu iespējams pieslēgties no interneta;
- Piekļuvei interneta resursiem Jūsu datorā ir jāizveido lietotāju bez privilēģijām (lietotājam, kura lietotājvārdu Jūs izmantojat, lai pieslēgtos datoram, ir jābūt bez administratora tiesībām);
- Neizmantojiet „pirātisku" PN;
- Veidojiet svarīgu datu rezerves kopijas.

Planšetdatoru un viedtālruņu aizsardzība

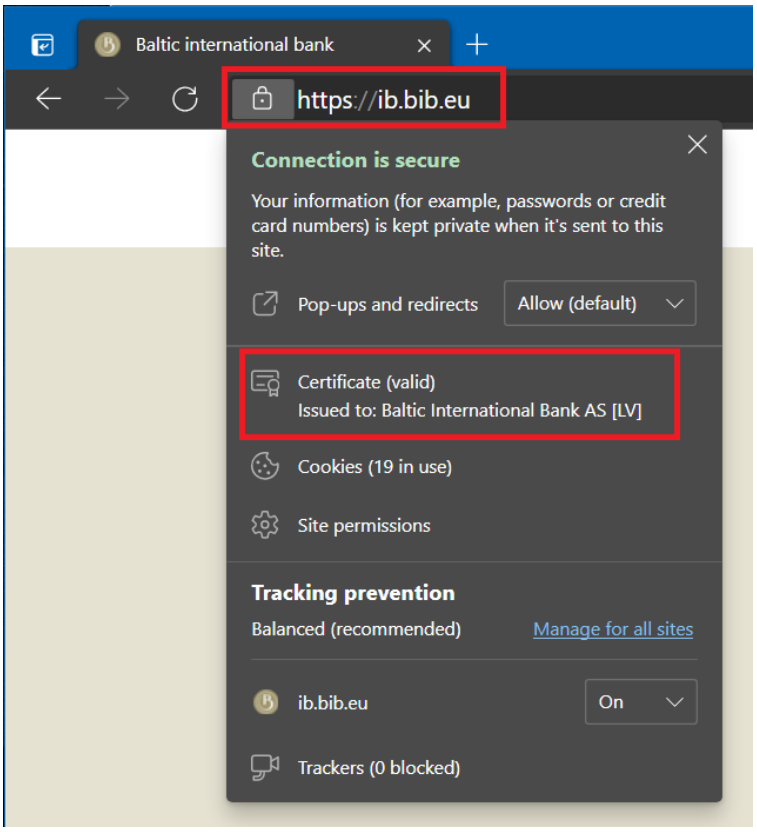
- PN jāuzstāda, izmantojot atļautos programmu avotus („iPad" un „iPhone" ierīcēm – „Apple App store" interneta veikalu, „Android" ierīcēm – „Google Play" interneta veikalu);
- Ieslēdziet Jūsu ierīces automātiskas PN atjaunināšanas funkciju, sekojiet līdzi un regulāri atjauniniet Jūsu ierīces operētājsistēmu uz jaunāko versiju;
- Neveiciet savā ierīcē neatļautas izmaiņas (angļu val. *jailbreake*, *root*), lai apietu ražotāja noteiktos ierobežojumus un aizsardzības līdzekļus;
- Aktivizējiet aizsardzību pret piekļuvi Jūsu personālajām ierīcēm (PIN kods, biometrija);
- Veidojiet visas ierīces datu rezerves kopijas.

Baltic International Bank internetbankas un BIB mobilās aplikācijas(“*B Online*”) drošas lietošanas ieteikumi

- Pirms pieejas kodu ievadīšanas pārliecinieties, ka Jūs atrodaties īstajā „Baltic International Bank” internetbankas lapā. Tās adresei ir jāsākas ar https://ib.bib.eu.
- Savienojumam jābūt šifrētam, par to liecina slēdzenes piktogramma:



- Sertifikāta īstumu var pārbaudīt, noklikšķinot uz slēdzenes piktogrammu. Tagad sertifikāta izdevējs ir firma „DigiCert”:



- Neizmantojiet publiskās vietās pieejamus datorus (piemēram, bibliotēku, Interneta kafejnīcu u.c. datorus);
- Nepieslēdzieties ar portatīvajām ierīcēm pie bezmaksas un nezināmiem bezvadu (Wi-Fi) tīkliem;
- Neapstipriniet tīmekļa pārlūkprogrammas vai citu sistēmu piedāvājumu saglabāt lietotāja piekļuves vārdus un paroles;
- Darba seanss internetbankā ir jāpabeidz pareizi. Ar vienkāršu aktīvā loga aizvēršanu nepietiek, izmantojiet izvēlnes punktu „IZIET”;
- Neizmantojiet personālo datoru/planšetdatoru/viedtālruni darbam ar interneta banku ar trešajām personām (kā arī ar radiniekiem un bērniem) ;

- Piekļuvei interneta bankas tīmekļa vietnei nekad neizmantojiet hipersaites; neizmantojiet ar meklēšanas programmām atrastas vai pa elektronisko pastu saņemtas hipersaites;
- „Baltic International Bank" **nekad** un nekādā gadījumā nepieprasa saviem klientiem paziņot pieejas kodus, paroles, PIN kodus pa elektronisko pastu, ar īsziņu vai MMS ziņu, pa tālruni vai kaut kadiem citiem veidiem;
- Neizpaudiet lietotāja vārdu, paroli, PIN kodu un citu Jūsu identifikācijas informāciju nepiederošām personām;
- Glabājiet interneta bankas autorizācijas līdzekļus (lietotāja vārdu, „Digipass" kodu kalkulatoru, PIN kodu, aktivizācijas atslēgas) drošībā;

Gadījumā, ja Jums rodas aizdomas par neatļautu internetbankas izmantošanu vai neatļautu piekļuvi Jūsu autorizācijas līdzekļiem un citai Jūsu identifikācijas informācijai no trešo personu puses, nekavējoties informējiet par to savu personīgo baņķieri.