Drošība darbā ar DIGIPASS ierīci

Kas ir DIGIPASS? – DIGIPASS DP 260 ar unikālu ciparu kombināciju ļauj klientam identificēt sevi internetbankā, veikt maksājumus un citas nepieciešamās darbības. DIGIPASS izmantošana pieejas un autorizācijas kodu ģenerēšanai nodrošina īpaši augstu drošības līmeni darbā ar internetbanku.

Darbam ar DIGIPASS DP 260 nepieciešams ievadīt 5 zīmju PIN kodu. Pirmajā lietošanas reizē jāievada Bankas izsniegtais PIN kods. Klients atbild par šī koda maiņu uz personīgo PIN kodu. Katrs ģenerētais identifikācijas un paraksta kods ir unikāla ciparu kombinācija, kas ir atkarīga no ierīces veida un ģenerēšanas laika. Katrs kods ir izmantojams tikai vienu reizi.

A/S „Meridian Trade Bank" atgādina, ka savu DIGIPASS iekārtu jāglabā drošā, svešām personām nepieejamā vietā un neizpaudiet nevienam savu PIN kodu. DIGIPASS kalkulatoru aizliegts izjaukt. Ja DIGIPASS ierīce ir fiziski bojāta, tā izslēgsies un kļūs lietošanai nederīga. Ja DIGIPASS baterija ir izlādējusies, un Jūsu rīcībā nav citu autorizācijas līdzekļu (piemēram, kodu kartes), Jūs zaudējat sava konta vadības iespējas izmantojot MultiNet sistēmu līdz Jūs nebūsiet saņēmis citu DIGIPASS ierīci. Ja esat pazaudējis DIGIPASS vai ierīce ir nozagta, nekavējoties ziņojiet par to Bankai. Lai saņemtu jaunu DIGIPASS ierīci, Jums jāierodas Bankā.

A/S „Meridian Trade Bank" iesaka mainīt ierīces PIN kodu ne retāk kā reizi divos mēnešos.

Pin koda nomaiņa. Kā to izdarīt?
PIN koda maiņa
1. Kad kalkulators ir ieslēgts un ekrānā redzams APPLI_ , nospiediet un turiet, līdz ekrānā parādīsies _ _ _ _ _ NEW PIN.
2. Ievadiet jauno PIN kodu. Kad ekrānā parādās_ _ _ _ _ PIN CONF, apstipriniet PIN kodu, ievadot to atkārtoti. _ _ _ _ _ NEW PIN CONF apliecinās veiksmīgu PIN koda nomaiņu.

Risinājumus Jūsu datora aizsardzībai

AS „Meridian Trade Bank" iesaka papildus drošības pasākumus.

Darbā ar Multinet sistēmu (www.multinetbank.lv) iesakām ievērot sekojošus ieteikumus:

1. Beidzot darbu Multinet sistēmā (www.multinetbank.lv), vienmēr nospiediet pogu „Izeja".
2. Lai sasniegtu maksimālu drošības pakāpi darbā ar MultiNet (www.multinetbank.lv), pārbaudiet un nepieciešamības gadījumā izmainiet pārlūkprogrammas uzstādīšanas (browser) parametrus; paroli, lietotāja kodu un citu informāciju nekādā gadījumā nedrīkst saglabāt.
3. Bieži vien iemesls, nepiederošo piekļuvei Jūsu datoram, ir nepietiekama paroles drošība.
Lai to novērstu, vajadzētu:

- Parolei izmantot tikai Jums zināmu vārdu salikumus, speciālus simbolus, piemēram, ciparus, simbolus un lielos burtus. Parole nekādā gadījuma nedrīkst būt paša lietotāja vārds, uzvārds, bērnu, radinieku vārdi, mājdzīvnieku vārdi, automašīnas numurs utt.;
- Izvēlēties paroli ne mazāku par 8 simboliem;
- Regulāri mainiet paroli (ne retāk kā reizi divos mēnešos);
- Paroles nepierakstiet uz papīriem un to neatstājiet citiem pieejamās vietās;
- Nevienam neuzticiet savas datora, internetbankas un citas paroles;

- Ja Jums ir aizdomas par nepiederošu personu piekļuvi Jūsu parolēm vai kodu kartei, nekavējoties ziņojiet to pa telefonu(+ 371 67019341).

5. Sava datora aizsardzībai, izmantojiet sekojošas programmas: **Firewall**, **Spyware** un **Antivirus**.

Liela nozīme datora aizsardzībai ir sekojošām programmām:

Firewall – ir programma, kas nodrošina aizsardzības barjeru starp Jūsu datoru un virtuālo pasauli. Hakeri izmanto programmas, kuras ir speciāli aprīkotas interneta skenēšanai un neaizsargātu datoru meklēšanai. Šādas programmas datoram sūta nelielu informācijas daudzumu un gadījumā, ja tam nav uzinstalēta Firewall programma, tas automātiski uz šāda veida paziņojumu (ziņu) atbild, kas attiecīgi dod iespēju sistēmu uzlauzt. Firewall programma šāda veida gadījumus atpazīst un uz tiem neatbild, tādējādi hakeri nemaz nevar uzzināt, ka Jūsu dators ir pieslēgts tīklam.

Dažas Firewall programmas:

- Network ICE BlackICE Defender
- Zone Labs ZoneAlarm и ZoneAlarm Pro
- Symantec Norton Internet Security, Norton Personal Firewall u.c.
- Spyware – programma, kura aizsargā no programmspiegiem, nevēlamas reklāmas, „trojas zirgiem", klaviatūras spiegiem, personīgo datu zagšanas, izspiegošanas draudiem, krāpnieciskām programmām, nevēlama programmnodrošinājuma, „fišinga" , izlecošiem logiem un nevēlamām mājas lapām.

Dažas Firewall programmas:

- Spyware Doctor 6 for Windows
- Anti-Spyware

Antivīrusu programmas

Antivīruss – programma, kura atpazīst un likvidē datorvīrusus. Lai cīnītos ar datorvīrusiem, ir izstrādātas ļoti daudz speciālas antivīrusu programmas, tā saucamās programmas-skeneri. Antivīrusu skeneru darbības princips ir, skanējot cieto disku un pārnēsājamos datu nesējus (USB flash), atrast inficētos failus. Antivīruss spēj atrast tikai tam zināmus vīrusus un, ja pēc skenēšanas antivīruss neko nav fiksējis, tas vēl nenozīmē, ka vīrusu nav. Vēlams ir pēc iespējas biezāk atjaunot antivīrusa datu bāzes.

Izplatītākās antivīrusu programmas:
AVG Internet Security
Dr Solomon's Anti-Virus Toolkit
F-Prot Professional
IBM AntiVirus
McAfee VirusScan
Norton AntiVirus
ThunderByte Anti-Virus Utilities
TouchStone PC
Cillin
Kaspersky un citi

Noderīgas Web adreses:
Kaspersky Lab - www.antivirus.lv
Symantec - www.symantec.com

VeriSign - www.verisign.com
ZoneAlarm Pro - www.zonelabs.com
McAfee - www.mcafee.com
www.networkassociates.com
WatchGuard - www.watchguard.com
PC World Communications - www.pcworld.com/downloads

Cīņai pret spiegošanas programmām:
spychecker.com
www.pcworld.com/downloads
Pret tastatūras ierakstītājiem - www.anti-keyloggers.com un citi.

Praktiski padomi

Datora drošība. Regulāri kontrolējiet datorsistēmu, kuru izmantojat elektronisko pakalpojumu veikšanai:

- rūpīgi sekojiet tam, kurš izmanto Jūsu datoru,
- izmantojiet ekrānsaudzētāju (screensaver) ar paroli savā prombūtnes laikā,
- izmantojiet vairākus datoru informācijas aizsardzības līdzekļus - pieejas paroles, jaunākos interneta aizsardzības rīkus un regulāri atjaunojiet pārlūkprogrammas,
- regulāri atjaunojiet antivīrusu programmas,

Bankas piedāvātie drošības risinājumi

- Izmantojiet dienas limitus, pēc kuru pārsniegšanas jāveic papildu autorizācija (ziņojums bankai, lietotājiem ieteicams lietot arī dubulto darījumu autorizāciju).
- Izmantojiet augstākas drošības pakāpes identifikācijas līdzekļus – kodu kalkulatorus, kuru ģenerētie kodi ir derīgi noteiktu laiku un neatkārtojas.
- Izmantojiet bankas piedāvāto iespēju atzvanīt klientam, ja maksājuma summa pārsniedz noteikto limitu.

Kontrolējiet finanšu kustību kontos

- Regulāri kontrolējiet savu kontu atlikumus un informāciju par darījumiem bankā.
- Izmantojiet iespēju saņemt īsziņu par notikušajiem darījumiem ar mobilās bankas palīdzību.

Aizdomu gadījumā obligāti sazinieties ar banku

- Ja rodas šaubas par kādu darījumu, vēstuli, e-pastu vai zvanu, obligāti sazinieties ar banku un pārliecinieties par to patiesumu. (Tel.: + 371 67019341).
- Atcerieties, banka nekad nelūgs no klienta rekvizītus, kuri ir nepieciešami elektronisko pakalpojumu izmantošanai.