



Naudas e-sardze pilnveidojas

Ik gadu arvien biežāk naudas lietas kārtotam attālināti no savas bankas ar interneta pieslēgumu starpniecību un kādu ierīci jeb e-vidē. Vai tas būtu dators vai moderns viedtālrunis – mūsu finanšu pakalpojumu iespējas attīstās un tehnoloģijas attīstās, diemžēl pilnveidojas arī šīs vides blēžu un ļaundaru spējas. Tam visam seko banku nozares atbildīgās organizācijas, tāpēc atbilstoši Eiropas Banku iestādes pamatnostādņiem FKTK ir mainījusi tirgus dalībnieku informācijas sistēmu drošības noteikumus, prasot pilnveidot maksājumu drošību internetā. Pārejas periods tuvākajos mēnešos beigsies, un 1. aprīlis ir tas datums, kurā ikvienai bankai jābūt risinājumiem, t. s. stingrajai jeb divu faktoru klientu autentifikācijai maksājumu veikšanai e-vidē.

VAI TAS ESI TU?

Autentifikācija ir personas attālināta atpazīšana. Proti, Tava banka, pirms dot atļauju veikt finanšu darījumu personai, kura klausvē pie durvīm Tavu finanšu e-vidē, noskaidro – vai tiešām tas esi Tu? Tev jāieraksta, jāievieto, jāuzrāda kaut kas tāds, kas zināms vai pieejams tikai Tev vienīgajam. Atpazīšanas līdzekļi balstās uz kādu no trim faktoriem:

- Tu kaut ko zini (paroli vai PIN kodu),
- Tev kaut kas pieder (karte, viedkarte, kodu kalkulators u. c.),
- Tavas biometriskās īpašības (balss, pirkstu nospiedumi u. c.).

Ja ar to bija pietiekami līdz šim, tad no 1. aprīļa būs nepieciešama stingrā jeb divu faktoru atpazīšana, kurā tiks izmantoti divi no pieminētajiem atpazīšanas faktoriem, turklāt vienam no šiem elementiem ir jābūt unikālam un otrreiz neizmantojamam. Tikai Tava parole un kods no kodu kartes turpmāk nav uzskatāms par stingro autentifikāciju (atpazīšanu).

DROŠĪBAS RĪKI



Katra banka Latvijā ir izveidojusi savus rīkus stingrajai autentifikācijai, līdz ar to šo risinājumu klāsts ir gana daudzveidīgs. Ja esi klients vairākās bankās, tad vajadzēs iepazīt vairākus no tiem. Piemēram, risinājums var būt Tava parole un:

- kodu kalkulatora ģenerēts vienreiz lietojams kods;
- Tava viedtālruna lietotnes (aplikācijas) ģenerēts unikāls kods;
- ar izsiņu (SMS) tālruni atsūtīts vienreiz lietojams kods;
- viedkartē saglabāts sertifikāts u. c.

Banku izstrādātie risinājumi klienta stingrajai atpazīšanai vienmēr būs atkarīgi no katras bankas biznesa modeļa, no tās klientu pro-

fila un to klientiem raksturīgajiem veiktajiem maksājumiem.

NB – IZŅĒMUMI! Turklāt saskaņā ar FKTK noteikumiem ir pieļaujams, ka klienta maksājumiem nelielās summās un vispārzināmiem pakalpojumu sniedzējiem var būt arī parastā līdz šim izmantotā atpazīšanas procedūra:

- t. s. Taviem mikromaksājumiem līdz 30 eiro vienam maksājumam, kamēr sasniegti 150 eiro;
- Taviem maksājumiem zināmiem saņēmējiem, kas iekļauti iepriekš izveidotā bankā apstiprināto maksājumu t. s. baltajā sarakstā;
- darījumiem starp Taviem diviem kontiem vienā un tajā pašā bankā;
- maksājumiem citam klientam vienas bankas ietvaros.

Vai šie izņēmumi būs spēkā Tavā bankā, tas būtu laikus jānoskaidro.

MANA BANKA= MANS TĀLRUNIS



Skaidrs, ka tehnoloģiju attīstības laikmetā arvien pieaug mūsu tālrunu un viedtālrunu loma finanšu pakalpojumu saņemšanā. Ja Tavs tālrunis būs vienīgā ierīce, kas iesaistīta Tevis kā bankas klienta atpazīšanas procesā (lietotne, izsiņas, mobilais kalkulators u. c.), tad bez tā nebūs iespējams izmantot finanšu pakalpojumus. Lieki teikt, ka tas jāglabā kā acuraugs, vienmēr laikus jāuzlādē un jānoslēdz piekļuve Tavai bankai lietotnēm ar parolēm, jāizvairās no ļaunatūru lejuplādes. Tomēr ir vēl daži būtiski aspekti – cik drošs ir interneta savienojums, visbiežāk Wi-Fi, kuru izmantojam finanšu pakalpojumu saņemšanai? FKTK eksperti zina teikt – ja Tev tiek nodrošināta individuāli veidota parole, lai pieslēgtos šifrētam Wi-Fi tīklam, tad Wi-Fi lietošana ir droša. Savukārt par nedrošu uzskatāms tāds koplietošanas Wi-Fi tīkls, kurš brīvi pieejams ikvienam un bez paroles vai arī Wi-Fi tīkls, kura paroli var izmantot daudzi lietotāji. E-vides blēdis, uzzinot šo koplietošanas paroli no restorāna viesmīles vai biroja administratores, tādā nedrošā tīklā, vismaz teorētiski, var realizēt Tavu privāto datu, t. sk. paroles un citu šifru un kodu zādžību piekļuvei gan Tavam e-pas-tam gan interneta bankām un citām lietotnēm. Tāpēc finanšu pakalpojumu jomā Tavs e-drošības līmenis būs krietni augstāks, ja izmantosi mobilās lietotnes (aplikācijas), jo tās ir speciāli veidotas tā, lai šifrētu pārraidāmos datus, un tie būtu aizsargāti neatkarīgi no tā, vai izmanto drošu šifrētu Wi-Fi vai brīvi pieejamu nedrošu Wi-Fi tīklu.

Vairāk par šiem e-drošības jautājumiem un arī dažādu jēdzienu skaidrojumu atradīsi arī KLIENTU SKOLAS – ābecē B līmenī: <http://www.klientuskola.lv/lv/abece/aktivs-klients.html>.

Jautājiet par tematiem saistībā ar finanšu pakalpojumiem –
FKTK eksperti jums atbildēs šajā slejā!