trešdiena, 2018. gada 15. augustā 10:09

Ieteikumi datora aizsardzībai

1. Lietojot internetbanku, ieteicams nodrošināt datoru vai mobilo ierīci, caur kuru veicat darbības, ar pretvīrusu programmām.
Gadījumā, ja pretvīrusa programma ir instalēta, tad ir nepieciešama pretvīrusa atjaunināšana.

Tāpat ieteicams instalēt ugunsmūra programmas (firewall) un/vai citus rīcībā esošos aparāta līdzekļus, tādus kā - kaitīgā koda piekļuves novēršanas sistēma, konfidenciālās informācijas pieejamības kontroles sistēma utt. (IPS/IDS, DLP).

Ugunsmūris (firewall) — programma datora aizsardzībai no uzbrukuma un nesankcionētas piekļuves tiešsaistes režīmā.

IPS – tīkla un datora drošības programmatūras vai aparatūras sistēma, **kas konstatē ielaušanos vai drošības pārkāpumus un automātiski pasargā** no tiem.
IDS – programmatūras vai aparatūras līdzeklis, lai **atklātu faktus** par nesankcionēto piekļuvi datorsistēmā vai tīklā vai par datorsistēmas vai tīkla nesankcionētu vadību galvenokārt caur Internetu.
DLP - **konfidenciālās informācijas noplūdes novēršanas tehnoloģijas no informācijas sistēmas ārpusē**, kā arī tehniskas ierīces (programmatūras vai programmatūras-aparatūras), lai novērstu šāda veida informācijas noplūdes.
Lietderīgi resursi:

- http://www.esidross.lv/ - drošības informācijas portāls
- http://windows.microsoft.com/lv-lv/windows/security-essentials-download — pretvīruss no Microsoft
- http://www.antivirus.lv/ - Kaspersky pretvīruss
- https://www.avira.com — Avira pretvīruss
- http://avg.com – AVG pretvīruss
- https://www.virustotal.com — bezmaksas pārbaude uz vīrusiem tiešsaistē
- http://secunia.com/ - datora drošības audits
- http://www.zonealarm.com/ - pretvīruss ugunsmūris (firewall)
- www.zemana.com – anti key-logger cīņai ar programmām – spiegiem
- www.malwarebytes.org — rīks, lai atrastu un izdzēstu ļaunprātīgu programmatūru

2.Datora vai mobilās ierīces aizsardzība, izmantojot paroli.
Gadījumā, ja nepieciešams atstāt datoru bez uzraudzības, jāizmanto ekrāna bloķēšanas iespēja ar paroli. Datoros ar operētājsistēmu Windows, ekrāna bloķēšana notiek uzspiežot taustiņus Win (taustiņš ar Windows logo, starp Alt un Ctrl) +L.

3. Ierīcei ar kuru notiek darbs internetbankā, regulāri jāatjaunina programmatūra — operētājsistēma, pārlūkprogramma, pretvīrusu programmatūra.

4. Ierobežot trešo personu pieeju pie ierīces, ar kuru notiek darbs internetbankā.
Nav ieteicams izmantot publiski pieejamas ierīces – datorus interneta kafejnīcas, viesnīcās, bibliotēkās. Ja jums tomēr nācās izmantot publiski pieejamo datoru, tad pēc darba pabeigšanas savā internetbankā nepieciešams iziet to tās, nospiežot pogu “Iziet” un aizvērt interneta pārlūku.

5. Izmantojiet datora lietotāju tiesību sadalīšanas iespēju.

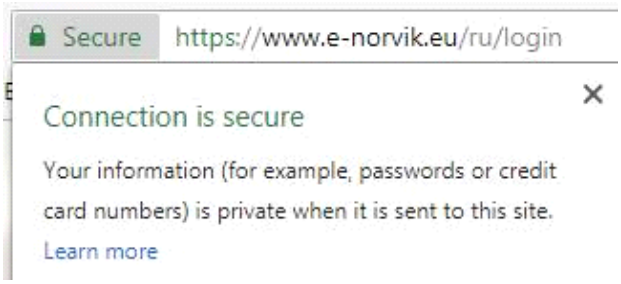
Datora lietotāju tiesību sadalīšana ļauj lietotājam ar administratora tiesībām atļaut/aizliegt datora programmu un resursu izmantošanu. Ikdienas darbā nav ieteicams izmantot lietotāju ar administratora tiesībām, jo šim lietotājam ir pilna piekļuve datora resursiem: programatūras instalēšana (t.sk. arī ļaunprātīga programmatūra), programmu dzēšana (t.sk. arī pretvīrusu), programmu atslēgšana (pretvīrusi, ugunsmūris), piekļuve citu datora lietotāju datiem. Ikdienas darbā iesakām izmantot lietotāju ar ierobežotām piekļuves tiesībām: ir aizliegta programatūras instalēšana, aizliegta iespēja atslēgt pretvīrusu programmu. Gadījumā, ja nepieciešams instalēt kādu programatūru, var pārslēgties uz lietotāja ar administratora tiesībām profilu.

Ieteikumi drošam darbam internetbankā

Drošs darbs internetbankā ir abpusēji atbildīgs, no vienas puses – *Norvik Banka*, no otras – internetbankas lietotājs.
Visaugstāko drošības līmeni var sasniegt tikai darbojoties kopā!
Lūdzu atcerieties, ka banka nekad nelūgs paziņot internetbankas autorizācijas datus pa e-pastu, tālruni vai jebkādā citādā veidā. Nevienam neatklājiet internetbankas paroli, autorizācijas rīku kodus. Gadījumā, ja jūsu identifikācijas tabula, kodu kalkulators, mobilā ierīce (SMS-pin/ Google Authenticator autorizēšanai) kļuvuši pieejami citām personām un jums ir aizdomas par drošības apdraudējumu, nekavējoties ziņojiet bankas drošības dienestam (+371) 6704 1100.

Mūsu ieteikumi, lai darbs internetbankā vienmēr būtu drošs:

1. Strādājot ar internetbanku, jāpārliecinās ka autentiskuma sertifikāts (SSL) ir derīgs. Derīgam sertifikātam adreses daļa https adreses joslā ir zaļā krāsā.



Tāpat arī nosaukumam adreses joslā jāsakrīt ar jūsu ievadīto adresi — www.e-norvik.eu.
Autentiskuma sertifikāta ailē *"Izsniegts kam"* (Issued to:) jābūt nozīmei www.e-norvik.eu, ailē *"Izsniedza"* (Issued by:) jābūt nozīmei thawte Extended Validation SSL CA.
Autentiskuma sertifikāts (SSL) arī nodrošina šifrētu savienojumu starp klientu un internetbanku.

Gadījumā, ja adreses daļa https: ir iekrāsota sarkanā krāsā vai pārlūkprogrammā paradījās SSL sertifikāta kļūda, tas nozīmē iespējamo drošā savienojuma apdraudējumu. Tādā gadījumā jāvēršas pie bankas drošības dienesta (+371) 6704 1100.

2. Ieteicams regulāri kontrolēt bankas maksājumu vēsturi un kontu atlikumus. Izmantojiet iespēju kontrolēt darbības internetbankā ar SMS īsziņu starpniecību.

3. Lai ieietu internetbankā, izmantojiet kombinētās paroles, kuras sastāv no 8 līdz 16 simboliem. Parolē jābūt lieliem un maziem burtiem, cipariem, speciāliem simboliem. Neizmantojiet parolei viegli uzminamus jēdzienus, tādus kā vārds, uzvārds, automašīnas numurs, dzīvnieku vārdi, pilsētu nosaukumi, dzimšanas datums, uzņēmuma reģistrācijas numurs utt. Nepierakstiet savu paroli uz papīra vai kodu kartes. Ja mainīsiet paroli, neizmantojiet savu iepriekšējo paroli kā jaunu. Gadījumā, ja rodas aizdomas, ka jūsu parole varēja tikt nozagta, sazinieties ar bankas drošības dienestu (+371) 6704 1100, nomainiet paroli, veicot paroles maiņu no cita datora vai ierīces.

4. Pēc darba beigām internetbankā , jānospiež taustiņš *"Iziet"*. Un jāaizver pārlūks. Ja nācies izmantot publiski

pieejamo datoru, jānotīra kešatmiņa, jāizdzēš failus ar konta izrakstiem vai citus no internetbankas lejupielādētos failus.

Galvenie draudi lietotājam, izmantojot internetbanku

1. **Viltus vēstules, zvani**

Kā vispopulārākais veids jāmin „Phishing" – viltus vēstuļu izsūtīšana vai zvanu veikšana bankas vārdā ar lūgumu sniegt savus autorizācijas datus. Tāpat ļaundari cenšas iegūt kredītkaršu datus (kartes numuru, CCV2, PIN kodu, kartes derīguma termiņu) vai klienta personīgos datus. Viltus vēstulēs var tikt atdarināts bankas korporatīvais stils.

2. **Viltus vietnes**

Nereti viltus vēstulēs izmanto saites ar piedāvājumu autorizēties internetbankā vai saņemt papildinformāciju, šīs atsauces pāradresē lietotāju uz viltotām vietnēm, līdzīgām internetbankas vietnei, ar kuru palīdzību mēģinot piekļūt lietotāja autorizācijas datiem. Viltotās vietnes var saturēt kaitīgas programmas, kuras var inficēt lietotāja datoru ar vīrusu vai spiegošanas programmu.

3. **Viltus autentiskuma sertifikāts**

Viltus autentiskuma sertifikātus (SSL/https) izmanto, lai traucētu šifrēto datu pārraides kanālu vai pāradresētu lietotāju uz viltus vietnēm. Gadījumā, ja lietotājs piekritis izmantot neautentisko sertifikātu, var tikt ne tikai pārtverti un atšifrēti lietotāja nosūtāmie dati, bet arī mainīti šie dati. Strādājot internetbankā, ir jāpārliecinās, ka autentiskuma sertifikāts ir īsts.

Gadījumā, ja saņemat vēstules, zvanus ar lūgumu sniegt rekvizītus darbam internetbankā, uzreiz jāziņo bankas drošības dienestam (+371) 6704 1100.