

Finantsinspektsioon I Internetipanga kasutamise



Mida internetipanga kasutamisel silmas pidada?

Internetipanga teenuse turvaliseks kasutamiseks tuleb olla hoolas ning jälgida turvareegleid.

Iga internetipanga kasutaja peab jälgima, et internetipanka sisenetakse turvalisest keskkonnast, st tuleb hoolitseda oma arvuti turvalisuse eest.

Tulemüür

Iga internetti ühendatud arvuti on potentsiaalsete rünnakute sihtmärgiks. Enda arvuti kaitseks tuleks kasutada tulemüüri, see on riist- ja/või tarkvaraline lahendus, mille ülesandeks on kontrollida arvutisse sisenevat ja sealt väljuvat liiklust ning lubada ainult kasutaja poolt heaks kiidetud ühendusi.

Viirusetõrje ning programmid nuhkvara (*spyware*) eemaldamiseks

Programme, mille loomise eesmärgiks on reeglina arvutis oleva informatsiooni kahjustamine, nimetatakse pahatahtlikuks tarkvaraks. Seda terminit kasutatakse viiruste, meiliusside, Trooja hobuste jm kohta. Sellised programmid võivad häirida arvuti tööd, rikkuda kettale salvestatud andmeid, koguda ja saata edasi paroole, avada arvuti juurdepääsuks teistele isikutele, jne.

Arvutiviirused levivad internetist failide salvestamisel (nt sõnumivahetustarkvara, failivahetusprogrammid, jne), surfamisel, e-posti teel, flopiketaste ja CD-de kaudu, jne. Viiruste tõrjeks peaks igas arvutis olema installeeritud viirusetõrje tarkvara, mis aitab avastada ja kahjutuks teha enamuse levivatest viirustest. Viirusetõrjeprogrammi tuleb regulaarselt uuendada.

Nuhkvaraks nimetatakse programme, mis installeeritakse kasutaja arvutisse ilma tema teadmata ja mis võimaldavad salaja jälgida kasutaja arvutikasutamist. Nuhkvara hulka kuuluvad klahvivajutuste registreerijad ja paroolivargad, külastatavate veebilehtede ja kasutatavate programmide logerid, jne. Tihti satub nuhkvara arvutisse internetist tasuta tarkvara salvestamisel ja installeerimisel. Nuhkvara eemaldamiseks on olemas samuti spetsiaalne tarkvara, millega tuleks regulaarselt arvutit kontrollida.

Kui tegemist on koduse arvutiga, siis on selle kasutajateks tihti lapsed, kes suhtlevad jututubades ja MSN vahendusel, mängivad ja surfavad internetis, vahetavad omavahel või laevad/käivitavad internetist erinevaid faile, mille sisust ja tegevusest nad ei pruugi aru saada. Ka neile tuleb rääkida ohtudest ja hoiatada tundmatute failide salvestamise ja käivitamise eest. Kõik kahtlased ja tundmatud asjad tuleb jätta pigem puutumata.

Mõned lingid, kust saab laadida tarkvaralist tulemüüri ja viirusetõrje tarkvara:

Lehekülg	Link
Starman - Internetiga seotud kasulik tarkvara	http://helpdesk.starman.ee/est/software.htm
Elionist lisateenused: viirusetõrje ja tulemüür	http://www.elion.ee/wwwmain?screenId=html.citizen-profile.5366.13847
Viirusetõrje tarkvara	
F-Secure	http://www.f-secure.com/
Trend Micro	http://www.trendmicro.com/
Symantec	
Norton Internet Security	http://www.symantec.com/product/index_homecomp.html
AVG	http://www.grisoft.com/us/us_index.php
Tulemüür	
ZoneAlarm	http://www.zonelabs.com/store/content/catalog/products/sku_list_zs.jsp?lid=db2_free
McAfee	http://us.mcafee.com/default.asp
Programmid nuhkvara eemaldamiseks	
Ada-Ware	http://www.ada-ware.com/
Spybot S&D	http://www.safer-networking.org/

Veebilehitsejad

Operatsioonisüsteemidest ja veebilehitsejatest avastatakse erinevaid turvavigu ning seetõttu tuleks neid regulaarselt uuendada ning panna peale parandusi. Kuna vanemate versioonide puhul veaparandusi ei lisandu, tuleks jälgida, et kasutatavad veebilehitsejad ei oleks liiga vanad.

Internetis ringi liikudes ilmuvad arvuti ekraanile vahel aknad, kus küsitakse midagi või tahetakse arvutisse salvestada mõnda programmi. Enne nuppudele vajutamist tuleb see tekst läbi lugeda ja kui ei saa aru, siis võimaluse korral sulgeda üleval paremal nurgas oleva risti abil ühtegi nuppu kasutamata.

Enamkasutatavad veebilehitsejad Internet Explorer ja Netscape pakuvad kasutajale võimalust salvestada erinevatele veebilehtedele sisenemiseks kasutatavad paroolid. See valik tuleks maha võtta või kasutada seda äärmiselt tähelepanelikult.

Paroolide salvestamise võimaluse kõrvaldamiseks:

Internet Explorer

Internet Exploreri korral menüüst *Tools* valida Internet *Options*. Valida menüü *Content* ning otsida üles nupp *AutoComplete*. Valiku *User names and passwords on forms* juures olevast kastist tuleks ära võtta linnuke. Nupp *Clear Passwords* kustutab juba salvestatud paroolid.

Internet Explorer'i puhul võiks kontrollida, et oleks paigas märgend, mis keelab krüpteeritud lehekülgede salvestamise arvuti kettale. Selleks tuleks menüüst *Tools* valida Internet *Options*. Sealt teha valik *Advanced* ning allpool avanevas *Settings* aknas otsida üles sõna *Security*. Valiku *Do not save encrypted pages to disk* ette tuleks märkida linnuke.

Netscape (7.1,...)

Netscape (7.1 ...) paroolide salvestamist ning lehekülgi, millede kohta on kasutajatunnused salvestatud, saab näha menüüst *Edit* valiku *Preferences* kaudu. Vasakul avanevast menüüst tuleb otsida üles osa *Privacy&Security* ning sealt *Passwords*. Kui eemaldada linnuke *Remember Passwords* eest kastist, siis paroole enam ei salvestata. Veebilehekülgi, millede kasutajatunnused on salvestatud ning lehekülgi, millede kohta kunagi kasutajatunnuseid ei salvestata, on võimalik näha ning vajadusel eemaldada vajutades nupule *Manage Stored Passwords*.

Internetipanka sisenemine ja väljumine

Internetipanka sisenemine

Internetipanga aadressi sisestamisel luuakse ühendus arvuti ja internetipanga vahel kasutades SSL-protokolli (krüpteeritud ühendus), st interneti aadress peab algama `https://...`

Veebilehitseja alumises parempoolses servas peab olema suletud tabaluku kujutis, topeltklõpsuga kujutisel avaneb sertifikaat, mis peab kuuluma vastavale pangale.

Võimalusel ärge kasutage internetipanka avalikest arvutitest, mille turvalisuses Te kindel pole. Kui kasutasite internetipanka mõnest ühiskasutusega arvutist, siis võiks tühjendada arvuti vahemälu (*cache*) — mälu, kuhu salvestatakse ühenduse jooksul näidatud leheküljed.

Vahemälu tühjendamine enamkasutatavate veebilehitsejate korral:
Netscape erinevate versioonide korral leiab vahemälu kustutamise käsud tehes menüüst *Edit* valiku *Preferences*. Avanevatest kategooriate nimekirjast valida *Advanced* ning *Cache*. Olenevalt kasutatavast versioonist tuleks klikkida nupule *Clear Memory Cache*, *Clear Disk Cache*, või *Clear Cache*.

Internet Explorer'i korral tuleks olenevalt kasutatavast versioonist kas menüüst *View* või *Tools* leida valik *Internet Options*. Otsida üles märksõna *Temporary Internet Files* ning vajutada nupule *Delete Files*.

Internetipangast väljumine

Peale internetipangas töö lõpetamist tuleb sealt väljuda, vajutades vastavale lingile ning sulgeda seejärel kindlasti veebilehitseja aken. Mingil juhul ei tohi arvuti juurest lahkuda, olles internetipanka sisse loginud ning jättes arvuti avatuks.

Internetipanga kasutajatunnused ja paroolid

Kasutajatunnus ja püsiparool

Internetipanga lepingu sõlmimisel väljastatakse Teile kasutajatunnus ja püsiparool (salasõna). Püsiparool antakse turvaümbrikus või saab selle ise välja mõelda ning seda ei tohi teada mitte keegi teine peale Teie enda.

Esimesel sisenemisel internetipanka võiks püsiparooli ümber muuta ning edaspidi tuleks püsiparooli regulaarselt vahetada. Püsiparooli ei tohiks kasutada paroolina (või muu kasutajatunnusena) mitte üheski teises süsteemis ning teda ei tohi öelda mitte kellelegi teisele.

Koodikaart

Lisaks kasutajatunnusele ja püsiparoolile on internetipanga kasutamiseks reeglina vaja veel koodikaarti. Kui sama koodikaart on kasutusel olnud juba pikemat aega, siis võiks ta pangakontoris vahetada uue vastu.

Internetipanka sisenemiseks kasutatavaid turvaelemente (kasutajatunnus, püsiparool, koodikaart) ei tohi anda mitte kellelegi, ka mitte pereliikmetele. Soovi korral saab teistele isikutele anda õigused oma konto kasutamiseks ning nad saavad pangast personaalsed turvaelemendid. Püsiparooli ja kasutajatunnust ei tohi kirjutada koodikaardile või hoida paberil komplektis koodikaardiga.

ID kaart ja PIN kalkulaator

Kasutajad, kes soovivad internetipanka kasutada turvalisemate autentimisvahendite abil, peaksid võtma koodikaardi asemel kasutusse ID-kaardi või PIN kalkulaatori.

ID kaart ehk isikutunnistus on Eestis esmane isikuttõendav dokument, mille abil saab enda isikut tõendada ka elektrooniliselt. Kui panga poolt on antud vastav võimalus, siis saab ID kaarti kasutada koodikaardi asemel internetipanka sisenemiseks. ID kaardi kasutamiseks peab olema arvuti juurde muretsenud kaardilugeja ning arvuti seadistatud. Kaart tuleb lugejasse sisestada enne teenuse valikut ning peab jääma lugejasse kogu internetipangas viibimise ajaks. Peale internetipangast väljumist tuleb sulgeda kõik veebilehitseja aknad ning eemaldada lugejast kaart. Kunagi ei tohi arvuti juurest lahkudes jätta ID kaarti kaardilugejasse.

Täpsemat infot ID kaardi kasutamise ja arvuti seadistamise kohta saab järgmistelt veebilehtedelt:

<http://www.pass.ee>

<http://www.id.ee>

PIN-kalkulaator on väike elektrooniline seade, mis genereerib ajas muutuvaid koode. Genereeritud koodi saab internetipanka sisenemiseks kasutada ainult teatud aja vältel, seejärel kood aegub. Pangast kalkulaatori saamisel on ta kaitstud esmase PIN-koodiga, mis tuleb kasutajal esimesel kasutamisel vahetada. Uueks PIN-koodiks tuleks valida raskesti arvatav numbrikombinatsioon, valitud kood tuleb jätta meelde ning seda ei tohi mingil juhul hoida üleskirjutatuna koos PIN-kalkulaatoriga.

Limiidid

Internetipanga lepingut sõlmides on seal tavaliselt määratud vaikimisi päeva- ja kuulimiidid. Kui need limiidid on võrreldes Teie igapäevaste tehingutega liiga suured, võiks vaikimisi limiitide asemel määrata endale sobivad. Vajadusel saab limiite alati suurendada, kuid parajate piirangutega on potentsiaalset kahju võimalik vähendada. Keskmisest suuremate limiitide kasutamisel võiks kasutada ka panga poolt pakutavat tugevamat autentimisvahendit, nt ID kaarti või PIN kalkulaatorit.

Internetipanga teenuse blokeerimine

Kui Teil on tekkinud kahtlus, et salasõna või koodikaardi koodid on saanud teatavaks teistele isikutele või kadunud, siis ärge oodake, vaid helistage viivitamatult panka ning peatage internetipanga kasutamise teenus. Internetipanga teenuse blokeerimine on kõigis pankades võimalik ööpäevaringselt. Teenuse taastamiseks tuleb pöörduda panka, kust saab uue salasõna ning koodikaardi.

Pankade veebilehtedel on avaldatud soovitusel kasutajatele internetipanga turvalisuse suurendamiseks ning toodud panga kontaktandmed:

- AS Hansapank
Klienditoe tel: 6310 310; www.hanza.net
- AS Eesti Ühispank
Klienditoe tel: 6655 100; www.eyp.ee
- AS Sampo Pank
Klienditoe tel: 6800 800; www.sampo.ee
- AS Eesti Krediidipank
Pangakaartide ja internetipanga sulgemise tel: 6616 039; 08004 050;
www.krediidipank.ee
- Nordea Bank Finland Plc Eesti filiaal
Internetipanga teenuse blokeerimise tel: 6283 283; www.nordea.ee
- Tallinna Äripanga AS
Tel: 6 688 040; 6688 000; www.tbb.ee

* Finantsinspeksioon ei võta kohustust tulevikus käesolevas materjalis teatavaks tehtud informatsiooni värskendada või eraldi teatada selles toimunud muudatustest. Käesolevas materjalis toodu ei ole konkreetses varalises küsimuses teabe või arvamuse andmine. Konkreetses varalises küsimuses soovitame konsulteerida vastava valdkonna spetsialistidega.

