GÁTLISTI UM TÖLVUÖRYGGI

INNGANGUR

Það hefur ávallt verið forgangsverkefni íslenskra fjármálafyrirtækja að tryggja öryggi viðskiptavina sinna. Samtök fjármálafyrirtækja hafa í þessu skyni sett saman þrjá stutta gátlista með helstu atriðum sem hafa ber í huga til þess að vernda aðgangsupplýsingar. Með því að hafa þessi atriði ávalt í huga getur þú hjálpað okkur að tryggja öryggi fjármuna þinna.

1. HVAÐ BER AÐ VARAST VIÐ MEÐFERÐ AÐGANGSUPPLÝSINGA.

- Ekki skrifa niður aðgangsupplýsingar.
- Reyndu að komast hjá því að gefa upp aðgangsupplýsingar, sama hversu vel þú treystir viðkomandi.

1A. HVAÐ BER ALMENNT AÐ VARAST VIÐ MEÐFERÐ AÐGANGSUPPLÝSINGA - NÁNARI ÚTSKÝRING.

Það er aldrei hægt að fara nógu varlega með aðgangsupplýsingar s.s. notendanafn og lykilorð að heimabanka og PIN númer debet- og kreditkorta. Það eru tvö meginatriði sem hafa ber í huga við almenna meðferð þessara upplýsinga.

- Ekki að skrifa niður aðgangsupplýsingar.

Ef þú, af einhverri ástæðu, telur nauðsynlegt að skrifa niður aðgang supplýsingar er best að geyma þær á öruggum stað, t.d. í bankahólfi eða traustum öryggisskáp.

- Reyndu að komast hjá því að gefa upp aðgangsupplýsingar, sama hversu vel þú treystir viðkomandi.

Líkurnar á því að aðgangsupplýsingar komist í hendur einhvers sem þú treystir ekki, aukast hlutfallslega í samræmi við fjölda einstaklinga sem hafa þessar upplýsingar.

2. HVAÐ BER AÐ VARAST VIÐ NOTKUN TÖLVA OG MEÐFERÐ AÐGANGSUPPLÝSINGA.

- Tryggðu að hugbúnaðurinn í tölvunni sem þú notar sé ávallt búinn nýjustu öryggisuppfærslum.

- Forðast að nota tölvu sem er í eigu einhvers sem þú þekkir ekki þar sem þú getur ekki vitað hvort forrit séu uppfærð eða vírusvörn í lagi.
- Varastu að opna viðhengi eða hlekki (e. Link, URL) sem þú bjóst ekki við, hvort sem er í gegnum tölvupóst eða einhvers konar samskiptaforrit, s.s. MSN, AIM, Skype o.s.frv.
- Ekki geyma PIN númer, lykilorð o.þ.h. upplýsingar í tölvunni.
- Vertu á varðbergi gagnvart hvers konar gylliboðum sem þér berast í gegnum tölvupóst, samskiptaforrit, s.s. MSN, AIM, Skype o.s.frv. eða einfaldlega í gegnum Internetið.
- Varastu Internet glugga sem opnast sjálfkrafa (e. Pop-up window), nema þú sért örugg(ur) um að upplýsingarnar í glugganum séu frá traustum aðila.
- Læstu tölvunni með lykilorði.
- Skiptu reglulega um lykilorð.
- Passaðu upp á harða disk tölvunnar þegar líftími hennar er á enda.
- Skráðu þig inn sem venjulegan notanda þegar tölvan er notuð dags daglega.

2A. HVAÐ BER AÐ VARAST VIÐ NOTKUN TÖLVA OG MEÐFERÐ AÐGANGSUPPLÝSINGA - NÁNARI ÚTSKÝRING.

Til er ógrynni af ýmiss konar tölvuveirum og hnýsibúnaði (e. Spyware) sem hafa þann eina tilgang að komast yfir viðkvæmar upplýsingar eða valda sem mestu tjóni. Að auki eru margir sem nýta sér tæknina til þess að blekkja grandalausa einstaklinga. Þetta er alheimsvandamál sem virðist því miður vera komið til að vera. Það er erfitt að koma algerlega í veg fyrir þessa hættu. Með því að gera viðeigandi varúðarráðstafanir er þó nánast hægt að koma í veg fyrir hana.

- Tryggðu að hugbúnaðurinn í tölvunni sem þú notar sé ávallt búinn nýjustu öryggisuppfærslum.

Nánast ómögulegt er fyrir hugbúnaðarframleiðendur að koma í veg fyrir alla öryggisgalla í hugbúnaði sínum. Á hverju ári eyða hugbúnaðarframleiðendur miklum tíma og fjármunum í að finna mögulega galla í hugbúnaði sínum og koma með úrlausnir í formi öryggisuppfærslna. Með því að fylgjast vel með og passa að hugbúnaðurinn í tölvunni sé ávallt búinn nýjustu öryggisuppfærslum, er hægt að lágmarka hættuna á að utanaðkomandi aðilar komist inn í tölvuna.

- Vertu á varðbergi þegar þú notar tölvu sem er í eigu einhvers sem þú þekkir ekki.

Til er ýmiss konar hugbúnaður sem getur afritað allar aðgerðir sem framkvæmdar eru á tölvu. Þetta er mjög áríðandi að hafa í huga þegar þú notar tölvu sem er ekki í þinni eigu, því slíkur hugbúnaður er oft nýttur til að nálgast persónulegar (m.a. fjárhagslegar) upplýsingar. Sýna ber sérstaka varkárni þegar fenginn er aðgangur að tölvu erlendis og varast að fara inn á netbankann í almenningstölvum, t.a.m. á kaffihúsum og öðrum stöðum þar sem þú ert ekki örugg(ur) um hvernig öryggismálum er háttað.

- Varastu að opna viðhengi eða hlekki (e. Link, URL) sem þú bjóst ekki við, hvort sem er í gegnum tölvupóst eða einhvers konar samskiptaforrit, s.s. MSN, AIM, Skype o.s.frv.

Öll viðhengi og hlekkir geta verið smituð af óæskilegum hugbúnaði, sem getur t.d. stolið upplýsingum af tölvunni eða afritað aðgerðir sem framkvæmdar eru á henni. Í flestum tilfellum kemur þetta frá einhverjum sem þú þekkir ekki og þá er öruggast að eyða skeytinu strax. Í sumum tilfellum kann hins vegar að virðast sem þetta komi frá einhverjum sem þú treystir. Ef þú bjóst ekki við pósti eða skilaboðum frá þessum aðila er öruggast að eyða skeytinu strax, eða hafa samband við viðkomandi og ganga úr skugga um að hann/hún hafi í raun sent það.

- Ekki geyma PIN númer, lykilorð o.þ.h. upplýsingar í tölvunni.

Það er aldrei að vita hverjir eiga eftir að komast í tölvuna, t.d. er mögulegt, ef viðeigandi ráðstafanir eru ekki gerðar, að brjótast inn í tölvur sem tengdar eru við Internetið og skoða upplýsingar sem þar er að finna. Auk þess mun tölvan líklega fara í viðgerð a.m.k. einu sinni á líftíma hennar, þar sem viðgerðarmaður mun hafa fullan aðgang að öllum þeim upplýsingum sem er að finna í henni.

- Vertu á varðbergi gagnvart hvers konar gylliboðum sem þér berast í gegnum tölvupóst, samskiptaforrit, s.s. MSN, AIM, Skype o.s.frv. eða einfaldlega í gegnum Internetið.

Þó svo að þessi gylliboð geti virst fullkomlega traustsins verð, þá er að öllum líkindum eitthvað ólöglegt á bakvið þau. Hætta er á að verið sé að reyna að komast yfir fjárhagslegar upplýsingar þínar eða að koma illa fengnum peningum úr landi. Ef þú færð skeyti, sem þú telur að eitthvað ólöglegt búi að baki, er skynsamlegast að áframsenda það á lögreglu á netfangið svik@rls.is og eyða því svo.

- Varastu Internet glugga sem opnast sjálfkrafa (e. Pop-up window), nema þú sért örugg(ur) um að upplýsingarnar í glugganum séu frá traustum aðila.

Pop-up gluggum fylgir oft ýmiss konar óæskilegur búnaður, sem getur t.d. stolið upplýsingum af tölvunni eða afritað aðgerðir sem framkvæmdar eru á henni. Það er vissara að loka glugganum og ekki skoða innihald hans frekar, nema að þú sért fullkomlega viss um að þú getir treyst þeim sem ber ábyrgð á honum.

- Læstu tölvunni með lykilorði.

Hægt er að læsa tölvum þannig að í hvert sinn sem kveikt er á þeim þurfi að slá inn lykilorð. Það er alltaf möguleiki á því að óæskilegir aðilar geti komist yfir tölvuna þína. Ef það þarf lykilorð til þess að komast inn í hana, eru minni líkur á að viðkomandi komist í upplýsingar sem þar er að finna.

- Skiptu reglulega um lykilorð.

Þó svo að allt sé gert til þess að passa upp á lykilorð, er ávallt sá möguleiki fyrir hendi að óæskilegir aðilar komist yfir þau, jafnvel án þinnar vitundar.

- Passaðu upp á harða disk tölvunnar þegar líftími hennar er á enda.

Það er í flestum tilfellum hægt að nálgast upplýsingar af harða disk tölvunnar þó svo að tölvan sjálf sé ónothæf. Því er vert að hafa í huga að þegar tölvunni er hent sé harða disknum haldið eftir eða að hann eyðilagður sérstaklega.

- Skráðu þig inn sem venjulegan notanda þegar tölvan er notuð dags daglega.

Ef þú ert skráð(ur) inn í tölvuna þína sem almennur notandi, en ekki sem umsjónarmaður (e. Administrator), er ekki hægt að breyta uppsetningu á stýrikerfi.

- Hvaða búnað er ráðlagt að hafa í tölvunni til þess að vernda hana fyrir tölvuþrjótum?

Til að verjast þessari nýju hættu er til ýmiss konar hugbúnaður. Sá hugbúnaður sem til er á markaðnum er hins vegar misgóður og því er mikilvægt að vanda valið. Hafa verður einnig í huga að á hverjum degi líta dagsins ljós nýjar leiðir til þess að komast inn í tölvur einstaklinga. Því er mjög mikilvægt að fylgjast vel með og passa að sá búnaður sem notaður er sé ávallt búinn nýjustu öryggisuppfærslum.

3. HVAÐA BÚNAÐ ER RÁÐLAGT AÐ HAFA Í TÖLVUNNI TIL ÞESS AÐ VERNDA HANA FYRIR TÖLVUÞRJÓTUM.

Búnaður sem nauðsynlegt er að hafa í öllum tölvum

- Veiruvarnarforrit.

- Forrit sem verja tölvuna fyrir hnýsibúnaði (e. Anti Spyware program).

- Eldveggur (e. Firewall).

Búnaður sem æskilegt er að hafa í öllum tölvum.

- Vörn gegn síðum sem opnast sjálfkrafa (e. Pop-up Blocker).

- Tölvupóstsía.

3A. BÚNAÐUR SEM NAUÐSYNLEGT ER AÐ HAFA Í ÖLLUM TÖLVUM - NÁNARI ÚTSKÝRING

- Veiruvarnarforrit

Nýjar tölvuveirur koma fram á hverjum degi og er því nauðsynlegt að tölvan sé búin góðri vörn gegn þess háttar ógnun.

- Forrit sem verja tölvuna fyrir hnýsibúnaði (e. Anti Spyware program)

Hnýsibúnaður er líkt og tölvuveira óæskilegt forrit sem sett er inn í tölvuna án vitundar notandans. Þessi búnaður leitast við að safna upplýsingum um, það sem er í tölvunni fyrir, eða það sem framkvæmt er á tölvunni, og koma þeim upplýsingum til þess sem bjó búnaðinn til. Því er mikilvægt að hafa í tölvunni gott varnarforrit til þess að verja hana fyrir þess háttar búnaði.

- Eldveggur (e. Firewall)

Góður eldveggur ver tölvuna fyrir bæði utanaðkomandi forritum, sem reyna að ná aðgangi að upplýsingum sem í henni er að finna, sem og óæskilegum forritum sem hafa komið sér fyrir í tölvunni og eru að reyna að senda upplýsingar út á netið. Hafa ber þó í huga að ekki er nóg að eldveggur sé í tölvunni, heldur verður að passa að kveikt sé á honum.

3B. BÚNAÐUR SEM ÆSKILEGT ER AÐ HAFA Í ÖLLUM TÖLVUM - NÁNARI ÚTSKÝRING.

- Vörn gegn síðum sem opnast sjálfkrafa (e. Pop-up Blocker)

Hægt er að koma í veg fyrir að síður á Internetinu opnist sjálfkrafa með svokölluðum pop-up blocker. Þess háttar búnaður kemur í veg fyrir að síðan opnist, þ.e. notandinn fær val um hvort hann vilji að glugginn opnist eða ekki.

- Tölvupóstsía

Ein algengasta leiðin til þess að dreifa óæskilegum hugbúnaði er í gegnum tölvupóst. Til að lágmarka þessa hættu er æskilegt að sía póstinn í gegnum svokallaða tölvupóstsíu, áður en hann kemur í tölvuna.

VIÐAUKI A. RÁÐLEGGINGAR UM MEÐFERÐ LYKILORÐA

Lykilorð eru notuð til þess að verja aðgang að öllu mögulegu þegar kemur að tölvum og Internetinu. Í þessu felst það vandamál að til þess að geta nýtt sér alla þá þjónustu sem í boði er, er nauðsynlegt að muna ógrynni af lykilorðum.
Hér að neðan eru nokkrar hugmyndir um hvernig hægt er að auðvelda meðferð lykilorða.

a. Fjöldi lykilorða

- Því fleiri lykilorð sem þú treystir þér til að muna því betra. Góð regla er að notast við ekki færri en 3 persónuleg lykilorð.
- Það fyrsta getur verið tiltölulega einfalt. Það er fyrir hinar ýmsu síður sem krefjast lykilorðs en skiptir ekki miklu máli hvort einhver utanaðkomandi komist þar inn.
- Það næsta þarf að vera leynilegt. Það er notað til að vernda upplýsingar sem skipta máli en geta ekki valdið neinu fjárhagslegu eða tilfinningalegu tjóni ef einhver kemst yfir það, t.d. netpóstur o.þ.h.
- Það þriðja þarf að vera það leynilegt að enginn geti komist yfir það. Það er notað til þess að vernda hvers konar upplýsingar sem þú vilt ekki undir neinum kringumstæðum að einhver komist yfir, t.d. heimabankinn o.þ.h.

b. Að búa til lykilorð

- Forðastu að nota hvers konar orð eða númer sem tengjast þér persónulega og hægt er að giska á með tiltölulega einföldum hætti. t.d.:
- Nafn, kennitala, heimilisfang eða afmælisdagur þinn, náins vinar eða fjölskyldumeðlims, bíltegund, gæludýr, o.s.frv.
- Æskilegt er að lykilorð byggist upp af samblandi af háum og lágum bókstöfum auk tölustafa. Hversu flókið sambland þessara atriða er æskilegt fer eftir mikilvægi þess, samanborið við flokkana sem nefndir eru hér að ofan. Þannig gæti lykilorðið verið sambland af tveim eða jafnvel öllum þessum atriðum. Dæmi:

1. kEysari

2. keysari123
3. keysAri123

c. Hversu oft er æskilegt að breyta lykilorðum

- Góð viðmiðunarregla er að því viðkvæmari sem upplýsingarnar eru, sem lykilorðið verndar, því oftar er æskilegt að breyta því. Ef horft er til þeirra lykilorða sem tilgreind eru í lið 1.1 hér að framan, þá eru eftirfarandi góð viðmiðun.
- Ef það verndar lítt mikilvægar upplýsingar - breyta á 1-3 ára fresti.
- Ef það verndar mikilvægar upplýsingar aðrar en fjárhagslegar eða mjög persónulegar - breyta á 6 til 12 mánaða fresti
- Ef það verndar mjög persónulegar (m.a. fjárhagslegar) upplýsingar - breyta ekki sjaldnar en á 2-3 mánaða fresti.
- Þar sem æskilegt er að breyta lykilorðinu reglulega, getur verið gott að koma sér upp einhvers konar kerfi varðandi það hvernig því er breytt hverju sinni.