

Rafrænt Öryggi

MIÐVIKUDAGUR 13. JANÚAR 2021

Kynningar: Dokobit, Taktikal, Vodafone.



Ólafur Páll Einarsson, framkvæmdastjóri Dokobit á Íslandi og Ragna Klara Magnúsdóttir, yfirmaður sölu og markaðsmála Dokobit á Íslandi, eru spennt fyrir þeim miklu breytingum á rafrænum skilríkjum sem munu fylgja tilkomu appsins frá Auðkenni á þessu ári. Þjónustan verður áreiðanlegri og hraðari í appinu, þar sem ekki verður notast við SMS skilaboð. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

Rafrænar undirskriftir: Nýtt viðmið í viðskiptum

Lausnir Dokobit gera fyrirtækjum auðvelt að innleiða rafræn skilríki í sínar eigin lausnir fyrir auðkenningar og rafrænar undirskriftir og þannig bæði tryggja öryggi og auka þægindi. ➔2

Framhald af forsiðu ➔

Segja má að á árinu 2020 hafi stafræn þróun verið á fimm-földum hraða miðað við undanfarin ár. Þjónustuveitendur hafa þurft að mæta nýjum áskorunum til að geta áfram veitt viðskiptavinum sínum þjónustu sem áður krafðist þess að þeir kæmu í eigin persónu til að undirrita ýmis skjöl. Í dag hafa flestir Íslendingar sjálfir prófað að undirrita skjöl rafrænt og þar með getað sleppt óþarfa ferðalögum. Kröfur neytenda til þjónustu hafa aukist í takt við þessar breytingar þannig að þeim finnst ekki lengur sjálfsagt að þurfa að mæta eitthvert þegar rafrænar undirskriftir eru orðnar almennari. Rafrænar undirskriftir eru að verða „standardinn“ í því hvernig fyrirtæki eiga viðskipti sín á milli og gera þeim einnig kleift að veita viðskiptavinum sínum betri þjónustu.

Dokobit er hugbúnaðarfyrrtæki sem þróar lausnir fyrir rafrænar undirskriftir og fleiri traustþjónustur. Á síðustu árum hefur uppbygging félagsins verið hröð og viðskiptin nánast fimmfölduðust á síðasta ári. Félagið er núna með skrifstofur í fjórum löndum, styður við rafræn skilríki frá 14 löndum í Evrópu og yfir milljón skjöl eru undirrituð rafrænt með Dokobit í hverjum mánuði.

„Með rafrænum undirskriftum geta fyrirtæki veitt viðskiptavinum sínum þægilegri og betri þjónustu en áður,“ segir Ólafur Páll Einarsson, framkvæmdastjóri Dokobit á Íslandi. „Rafrænar undirskriftir eru ekki einungis þægilegri, þær eru einnig öruggari en handritaðar undirskriftir, þar sem erfiðara er að falska og eiga við þær.“

Dokobit styður Auðkenni appið

„Hingað til hafa Íslendingar notað rafræn skilríki á SIM kortum og snjallkortum, en fljótlega munu neytendur sjá nýja kynslóð af rafrænum skilríkjum í appi, Auðkenni appinu, sem Dokobit mun styðja að fullu,“ segir Ólafur Páll. „Dokobit styður nú þegar þessi form skilríkja og því verður einfalt fyrir þjónustuveitendur að innleiða þessi nýju skilríki inn í sínar eigin stafrænu lausnir.

Lausnin byggir á tækni sem kölluð er „split-key technology“ sem þýðir að aðeins hluti einkalykilsins í rafrænu skilríkjunum er á handtækjum notenda og þess vegna ekki jafn mikil áhætta fólgin í að þurfa að treysta á fullkomna varðveislu skilríkja,“ útskýrir Ólafur Páll. „Með þessari tækni geta rafræn skilríki á þessu formi mætt kröfum laga fyrir „öruggan undirskriftarbúnað“ (e. QSCD – Qualified Signature Creation Device) í samræmi við lög nr. 55/2019 (eIDAS).

Fyrir neytendur þýðir þetta að þeir geta fljótlega sótt sér app í símann sinn eða spjaldtölvu og haft uppsett samtímis á fleiri en einu tæki. Í staðinn fyrir að slá inn símanúmer til að auðkenna sig nota þeir kennitölu til að innskrú sig hjá ýmsum þjónustuveitendum,“ segir Ólafur Páll. „Notkun þjónustunnar er einnig áreiðanlegri og hraðari í appi, þar sem ekki eru lengur notuð SMS skilaboð fyrir samskipti við rafrænu skilríkin.

Námsmenn og aðrir Íslendingar sem eru búsettir erlendis þurfa heldur ekki lengur að vera með íslensk símanúmer til þess að geta nálgast bankaðjónustu, opinbera þjónustu og fleira og erlendir stjórnarmenn í íslenskum fyrirtækjum geta á einfaldari hátt undirritað samþykktir og önnur viðskiptaskjöl með fullgildum rafrænum undirskriftum án þess að hafa íslenskt símanúmer,“



Appið frá Dokobit sendir tilkynningu í símann þegar undirskrift er lokið. MYND/AD-SEND



Ólafur Páll segir að kröfur neytenda til þjónustu hafi aukist í takt við hraðar breytingar og þeim finnst ekki lengur sjálfsagt að mæta eitthvert nú þegar rafrænar undirskriftir eru orðnar almennari. Þær eru að verða „standardinn“ í því hvernig fyrirtæki eiga viðskipti sín á milli og gera þeim kleift að veita betri þjónustu. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

bendir Ólafur Páll á. „Öll þessi uppbygging mun gera Ísland samkeppnishæfara og einfalda örugg, alþjóðleg viðskipti.“

Með vefþjónustu Dokobit geta þjónustuveitendur á einfaldan hátt innleitt app skilríkin í sínar eigin stafrænu lausnir til að auka öryggi og bæta upplifun notenda.

Hvað er rafræn undirskrift?

„Í grunninn er rafræn undirskrift rafrænt fingrafar sem notað er til að tengja á sannanlegan hátt rafrænu undirskriftina við þann sem

skrifar undir. Hægt er að undirrita skjöl rafrænt á hvaða formi sem er, en algengast er að nota PDF skjöl,“ útskýrir Ólafur Páll. „Fullgildar rafrænar undirskriftir verja skjölin á þann hátt að ekki er hægt að breyta innihaldi þeirra eftir að þau hafa verið undirrituð. Ef skjölunum yrði breytt yrði það auðmerkjanlegt þar sem undirskriftirnar brotna.“

Eru rafrænar undirskriftir löglegar?

„Fullgildar, rafrænar undirskriftir

hafa sömu réttaráhrif og handritaðar undirskriftir samkvæmt lögum númer 55/2019,“ segir Ólafur Páll. „Lögin eru innleiðing á Evrópureglugerð númer 910/2014 sem oftast er nefnd eIDAS reglugerðin. Sömu lög tryggja jafnframt að ekki megi neita að fullgild, rafræn undirskrift fái réttaráhrif af þeirri einu ástæðu að hún sé á rafrænu formi.

Dómstólar eru í dag byrjaðir að móttaka rafrænt undirrituð og innsiglið skjöl af ýmsum gerðum. Kaupsamninga, lánasamninga,

”Hingað til hafa Íslendingar notað rafræn skilríki á SIM kortum og snjallkortum, en fljótlega munu neytendur sjá nýja kynslóð af rafrænum skilríkjum í appi, Auðkenni appinu, sem Dokobit mun styðja að fullu.

þjónustusamninga, ráðningarsamninga, umboð, uppsagnarbréf, ársreikninga fyrirtækja hjá endurskoðendum, breytingar á samþykktum félaga, samþykktir á tilboðum, stefnur og greinargerðir lögmanna og ýmislegt fleira,“ segir Ólafur Páll.

eIDAS vottun Dokobit

„Dokobit er með eIDAS vottun sem fullgildir traustþjónustuveitandi í samræmi við lög númer 55/2019 fyrir fullgildar, rafrænar undirskriftir og fleiri traustþjónustur,“ segir Ólafur Páll. „Með vottuninni er staðfest að lausnir Dokobit mæta öllum tæknilegum og laga- legum kröfum sem gerðar eru til fullgildrar traustþjónustu. Dokobit er skráð á EU TSL traustlista hjá ESB sem fullgildur traustþjónustuveitandi. Vottunin tryggir áreiðanleika og réttaráhrif undirskrifa frá Dokobit.

Þjónustuveitendur á Íslandi hafa á aðáunarverðan hátt mætt miklum áskorunum á árinu með aðlögunarhæfni og tileinkað sér nýjar aðferðir og lausnir til þess að bjóða þjónustu sína. Hugarfar og kröfur neytenda eru einnig búnar að breytast og aldrei áður höfum við haft ríkisstjórn sem setur jafn mikið vægi í nýsköpun eins og í dag, sem hefur sýnt sig í fjölda aðgerða. Miðað við þá stefnu sem við höfum sett okkur held ég að næsta ár eigi eftir að verða sérstaklega spennandi og það er marga í vinnslu í okkar smiðjum sem ég hlakka til að sjá verða að veruleika á árinu,“ segir Ólafur Páll að lokum.

Hægt er að nálgast upplýsingar um lausnir Dokobit á vefnum www.dokobit.is.

Dokobit



Valur Þór Gunnarsson, framkvæmdastjóri Taktikal, segir að flestir nýti sér rafræn skilríki og það hefur aukist á tímum COVID. FRÉTTABLAÐIÐ/SIGTRYGGUR ARI

Mun fleiri nýta sér rafrænar undirskriftir á tímum COVID

Að skanna skjal er ekki lengur ásættanlegur kostur eftir COVID, en flestir kannast við að þurfa að útvega undirskriftir á mikilvæg skjöl, oft með stuttum fyrirvara, áður en hægt er að hefjast handa við verkefni eða hefja viðskiptasamband. Taktikal sérhæfir sig í rafrænum undirskriftum.

Fyrir COVID-19 voru fyrirtæki að senda skjöl sem viðskiptavinurinn þurfti sjálfur að standa í að prenta út, skanna og senda til baka með undirskrift. Að sögn Vals Þórs Gunnarssonar, framkvæmdastjóra Taktikal, telst slíkt til undantekninga í dag. Taktikal var stofnað fyrir fjórum árum og sérhæfir sig í rafrænum undirskriftum og ferlum sem byggja upp traust með rafrænum hætti.

„Þetta var talsvert ferli að senda skjölin með tölvupósti sem viðskiptavinurinn prentaði út, jafnvel kallaði til votta og þurfti síðan að skanna skjalið, senda til baka afrit, sem í raun er einungis mynd af skjalinu. Frumritið gat tapast og hægt er að eiga við skjalið eftir undirritun,“ útskýrir Valur.

„Aukning í fjölda viðskiptavina sem hefur innleitt rafrænar undirskriftir á síðasta ári hefur verið gríðarleg. Hjá okkur skiptir aukningin í notkun mörgum hundruðum prósentu á milli árána 2019 og 2020,“ segir Valur. Sem dæmi um ferla þar sem rafrænar undirskriftir hafa alveg

tekið yfir, nefnir Valur skjöl tengd ráðningum nýrra starfsmanna. „Það er til dæmis þekkt í dag að ekki er hægt að hefja ýmis ferli og skráningu í kerfi fyrr en nýr starfsmaður er búinn að skrifa undir ráðningarsamning.

Í dag eru fjölmörg fyrirtæki að nýta rafrænar undirskriftir, bæði sem upplýst samþykki fyrir frekari gagnaöflun, jafnt sem við undirritun ráðningarsamninga til að flýta fyrir og uppfylla kröfur um skjölun,“ útskýrir hann.

Tímasparnaður og þægindi

„Mörg dæmi eru um að undirskriftir sem áður tók þrjá til fimm daga að safna sé núna lokið á nokkrum mínútum. Það hefur ekki bara skapað þægindi fyrir viðskiptavinum heldur eykur það þjónustustig og sparar dýrmætan tíma stjórnenda fyrirtækja. Þeir fá mun meiri tíma fyrir mikilvægustu verkefni dagsins,“ segir Valur Þór.

Auðvelt að tengja við skjalakerfi fyrirtækisins

„Lykilatriðið er að innleiðing á

Við erum heppin á Íslandi að langflestir eru með rafræn skilríki í símanum. Það gerir okkur kleift að undirrita með mikilli fullvissu og öryggi.

nýjum lausnum sé einföld og að nýjar lausnir falli vel að þeim kerfum sem fyrirtækið hefur þegar fjárfest í. Allar lausnir Taktikal eru afar sveigjanlegar og má tengja skjalakerfum sem fyrir eru og þannig auka virði þeirra, með því að tryggja sjálfvirka afhendingu rafrænna gagna að undirritun lokinni.“

Öruggar undirskriftir

„Undirskriftir Taktikal eru jafngildar undirskriftum á pappír þar sem þær byggja á fullgildum, rafrænum skilríkjum og uppfylla

kröfur um fullgildar undirskriftir samkvæmt lögum 55/2019 um rafræna auðkenningu og traustþjónustur, er tóku gildi 1. janúar 2020.

Við erum svo heppin á Íslandi að langflestir eru með rafræn skilríki í símanum. Það gerir okkur kleift að undirrita með mikilli fullvissu og öryggi um að sá sem undirritar sé sá sem hann/hún segist vera, auk þess sem skjalið er innsiglað og tímastimplað með stöðluðum hætti við undirritun. Þetta þýðir að undirritað skjal er eitt sterkasta sönnunargagnið í dag fyrir skjöl og samninga.

Allar undirritanir eru auk þess svokallaðar fullgildar langtíma-undirritanir (e. Long Term Validation) sem þýðir að hægt er að sannvotta allar undirskriftir alveg óháð kerfum Taktikal og jafnvel þó að skilríki undirritanda séu útrunnin,“ greinir Valur Þór frá.

Vitundarvottar óþarfir

Með fullgildum rafrænum undirskriftum þarf ekki lengur að kalla til vitundarvotta, þar sem vottanir fara fram með rafrænum hætti.

„Áður þurfti að kalla til aðila, alls óviðkomandi skjalinu, sem höfðu það hlutverk að votta að undirritandi væri sannanlega sá sem ritaði nafn sitt á skjalið og að hann væri eftir atvikum fjárráða. Í dag er slíkt óþarfi, þar sem einungis handhafi rafrænu skilríkjanna getur skrifað undir og lesa má aldur undirritanda úr kennitölu hans,“ segir Valur Þór.

Fjölbreyttir viðskiptavinir

Viðskiptavinir Taktikal eru fram-sækin fyrirtæki af öllum stærðum; einnig eru ríki, sveitarfélög, lögfræðistofur, fjármálafyrirtæki, tryggingafélög ásamt stofnunum sem vilja vera framarlega í stafrænni þjónustu, meðal viðskiptavina.

Frír prufuaðgangur

Nánari upplýsingar veitir Valur Þór Gunnarsson framkvæmdastjóri í síma 552-5620 eða í netfanginu hallo@taktikal.is en hægt er að skrá sig frítt og prófa rafrænar undirskriftir á slóðinni app.taktikal.is/trial eða á vef Taktikal www.taktikal.is

Rafræn samskipti gerð einfaldari

Árið 2007 var undirritaður samningur um útgáfu rafrænna skilríkja hér á landi með það í huga að einfalda rafræn samskipti. Þörfin fyrir öruggari auðkenningu á eftir að aukast á næstu árum.

Stórt skref í innleiðingu rafrænna skilríkja hér á landi var stigið árið 2007 þegar samningur var undirritaður milli fjármála- og efnahagsráðuneytisins og Auðkennis fyrir hönd fjármálafyrirtækja, um útgáfu rafrænna skilríkja.

Haraldur Bjarnason, framkvæmdastjóri Auðkennis, segir tilgang rafrænna skilríkja vera að auðvelda rafræn samskipti. Þannig verði auðkenningin einfaldari og öruggari auk möguleika til fullgildrar undirritunar. „Á Íslandi geta aðilar notað sömu skilríkin til að auðkenna sig gagnvart flestum þjónustum á netinu. Notkun rafrænna undirritana er vaxandi og eru þær aðgengilegar hjá fjölmörgum fyrirtækjum og stofnunum með tilheyrandi þægindum og hagræði.“

Langur aðdragandi

Aðdragandinn að samningnum 2007 var nokkur segir Haraldur. „Árið 2001 voru sett lög um rafrænar undirskriftir, byggð á evrópskri tilskipun. Ríkið hóf þegar þróun verkefna, enda mat aðila að almenn útbreiðsla rafrænna skilríkja væri forsenda frekari framþróunar rafrænnar stjórn-sýslu.“ Um svipað leyti var Auðkenni stofnað, meðal annars til að dreifa skilríkjum til viðskiptavina banka og sparisjóða. „Fljótlega hófust samskipti milli ríkisins og Samtaka banka og verðbréfa-fyrirtækja um mögulegt samstarf um útbreiðslu skilríkja, sem fyrst var innsiglað með viljayfirlýsingu 2005 og loks samningi sem staðfesti áframhaldandi samstarf aðila árið 2007.“ Hann segir að markmið

Árið 2001 voru sett lög um rafrænar undirskriftir, byggð á evrópskri tilskipun. Ríkið hóf þegar þróun verkefna enda mat aðila að almenn útbreiðsla rafrænna skilríkja væri forsenda frekari framþróunar rafrænnar stjórn-sýslu.

samningsins hafi verið að koma á og stuðla að, almennri dreifingu og notkun rafrænna skilríkja, bæði með uppbyggingu dreifilyklauskipulags og nýtingu á þekktum leiðum til dreifingar á rafrænum skilríkjum (debetkort). „Áætlað var að útbreiðsla yrði langt komin í lok árs 2008 en atburðir haustsins 2008 höfðu mikil áhrif á verkefnið. Fjölmargir aðilar komu að verkefninu og tók talsverðan tíma að byggja upp skipulagið. Árið 2014 var samstarf aðila ítrekað með undirritun viljayfirlýsingar milli ráðuneytisins og Samtaka fjármálafyrirtækja með það markmið að stórauka notkun rafrænna skilríkja á næstu árum og að þau yrðu megin auðkenningarleið fólks vegna margvíslegrar rafrænnar þjónustu og viðskipta á netinu.“

Hrunið tafði þróunina

Hann segir að þótt eðlilega hafi verið mismunandi skoðanir á því hvernig best væri að standa að svona verkefni hafi samstarf aðila verið talið farsælast fyrir íslenskt



Notkun rafrænna undirritana er vaxandi, segir Haraldur Bjarnason, framkvæmdastjóri Auðkennis. FRÉTTABLAÐIÐ/ERNIR

samfélag, enda nálgun okkar að mörgu leyti sambærileg öðrum Norðurlöndum og Eistlandi sem dæmi. „Flóknast var að byggja upp traustið og sannfæra almenning um tæknina.“ Ýmsar hindranir urðu á veginum sem stjórnendur verkefnisins sáu ekki fyrir segir Haraldur. „Áætlanir breyttust talsvert við bankahrunið árið 2008 sem hafði mikil áhrif á verkefnið, fjármögnun þess og forgangsroðun. Gert var ráð fyrir umtalsverðu framboði á þjónustu sem fólk og fyrirtæki gætu nýtt í samskiptum en það varð ekki raunin og var ábatinn

af nýtingu skilríkjanna því fyrst um sinn mun minni en gert var ráð fyrir. Þetta varð til þess að margir sáu ekki ástæðu fyrir því að virkja skilríkin. Að nýta skilríki á kortum reyndist einnig flókið fyrir marga og kallaði á viðbótarbúnað notenda. Tilkoma snjalltækja þar sem ekki var hægt að nýta kort hjálpaði heldur ekki. Árið 2013 hófst samstarf við fjarskiptafyrirtæki þar sem SIM kort voru nýtt fyrir rafræn skilríki og hefur sú leið reynst mjög vel.“

Fjölmörg tækifæri
Aðspurður um þróunina næstu

árin segir Haraldur að þörfin fyrir öruggari auðkenningu og undirritanir muni aukast og tæknin til þess að styðja það muni þróast í takt við þróun í heiminum. „Auðkenni er að koma á markað með Auðkennisapp sem hentar aðilum sem eru utan landsteinanna, ekki með íslensk símanúmer eða með tæki sem nýta eingöngu svokölluð eSIM. Það eru fjölmörg tækifæri fyrir rafræna þjónustu sem eykst á hverju ári. Á næstu árum munum við geta gert rafrænt alla hluti sem við gerum í dag í eigin persónu, með tilheyrandi þægindum og lækkun kostnaðar samfélagsins.“



Aukinni fjarvinnu fylgir krafa um aukið upplýsingaöryggi



PEKKING



Kristín Björk Bjarnadóttir, forstöðumaður á einstaklings-sviði Vodafone, segir að mikilvægasti þátturinn í netöryggi sé fræðsla og upplýsingagjöf. MYND/VILHELM

Netöryggi í stafrænum heimi

Internetið er hafsjór af upplýsingum og afþreyingu sem fólk notar í daglegu lífi. Netið á sér líka skuggahliðar. Vodafone leggur áherslu á að fræða viðskiptavini um öryggi í stafrænum heimi.

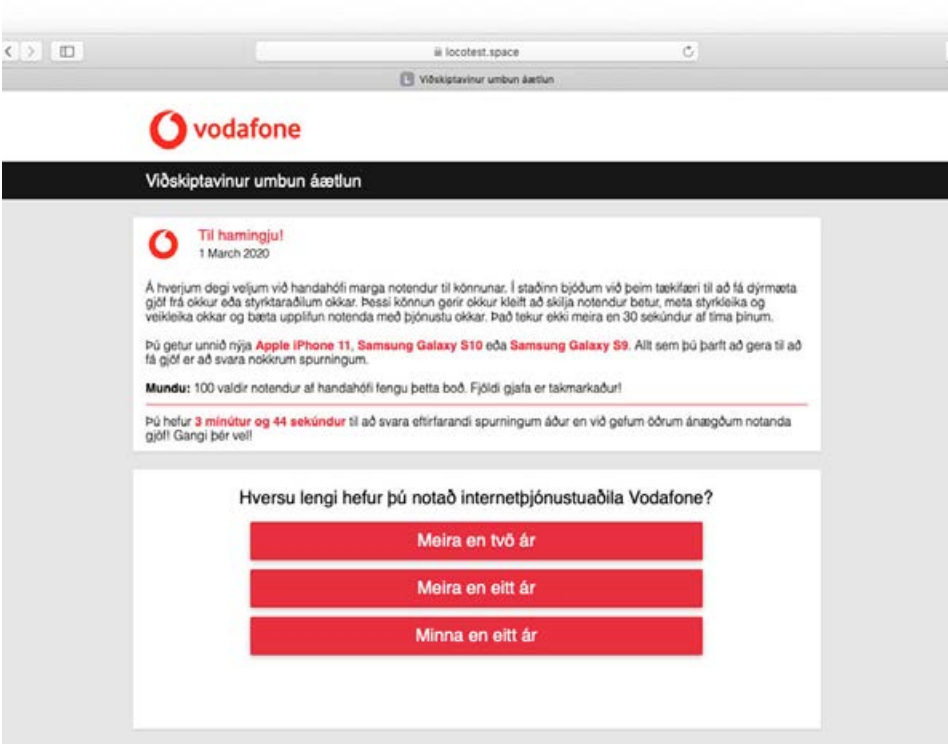
Vodafone hefur lagt áherslu á fræðslu í gegnum samstarf við SAFT sem er vakningaráttak um jákvæða og örugga tölvu- og nýmiðlanotkun barna og unglunga á Íslandi sem og með beinni fræðslu til sinna viðskiptavina.

„Möguleikarnir á netinu eru óteljandi og hafa breytt mörgu til hins betra, en það á einnig sínar skuggahliðar sem þarf að varast,“ segir Kristín Björk Bjarnadóttir, forstöðumaður á einstaklings-sviði hjá Vodafone. „Mikilvægasti þátturinn í netöryggi er fræðsla og upplýsingagjöf,“ bætir hún við. „Það getur reynst mikil áskorun fyrir fjölskyldur að halda í við þá öru tækniþróun sem er að eiga sér stað og þar skiptir helst máli að foreldrar axli ábyrgð og aðstoði börn og unglunga við að læra á netið, snjalltæki, smáforrit og annað sem fylgir þessari öru þróun“ upplýsir Kristín.

„Fyrir foreldra sem eru smeykir við YouTube notkun ungra barna sinna höfum við bent á áskriftaveituna okkar Hopster, sem er bæði aðgengileg fyrir áskrifendur í Vodafone Sjónvarp, sem app í snjallsímann eða spjaldtölvuna og er sérsníðið fyrir börn á aldrinum 2-6 ára,“ segir Kristín.

„Allt efni Hopster er yfirfarið af teymi sérfræðinga, uppeldisfræðinga og sálfræðinga í Bretlandi og þarf að uppfylla strangar reglur áður en það er vottað „KidSAFE“ eða barnvænt og fer í loftið. Hopster er öruggt og auglýsingalaust umhverfi fyrir börn,“ nefnir Kristín.

„Bæði börn og fullorðnir verða að tileinka sér meðvitaða varkárni í umgengni sinni við internetið og í því samhengi viljum við einnig nefna netsvindl í gjafaleikjum þar sem stöðugt er reynt að hafa fé af



Netsvindl er varasamt en það er hægt að forðast með góðri fræðslu.

Hér er dæmi um hvernig netsvindl getur litið út.

» Möguleikarnir á netinu eru óteljandi og hafa breytt mörgu til hins betra, en það á sínar skuggahliðar.

- Óskað er eftir kreditkortaupplýsingum í gjafaleik
- Það eru stafsetningar- og mál-farsvillur í textanum
- Verðlaunin í leiknum eru of góð til að geta verið sönn
- Það er farið fram á að brugðist sé strax við tilboðinu eða gjöfinni sem viðkomandi fær sendar upplýsingar um
- Almennt gefa fyrirtæki ekki upp IP tölu í samskiptum sínum við viðskiptavini

Upptalningin er vissulega ekki tæmandi og hvetur Kristín viðskiptavini Vodafone til að hafa samband ef grunur er um netsvindl í nafni Vodafone. Hægt er að hafa samband við okkur í síma 1414, á netspjalli á vodafone.is eða á samfélagsmiðlum Vodafone,“ segir hún.

„Þrátt fyrir að internetið hafi verið hluti af okkar daglega lífi undanfarna áratugi erum við sem notendur stöðugt að læra að umgangast það, bæði hvað varðar tímann sem fólk notar á internetinu, mörk sem það setur í samskiptum sínum í gegnum internetið og áreiðanleika gagna sem það finnur þar. Internetið er sístækkandi hluti í þeirri þjónustu sem fólk sækir, hvort sem um er að ræða bankaviðskipti, að kaupa í matinn eða horfa á sjónvarpið, það er því mikilvægt að netöryggi og þær leiðir til þess að gera enn betur á því sviði séu ávallt í skoðun og að samtalið við neytendur sé lifandi.“

fólki,“ upplýsir Kristín og nefnir nokkra punkta sem gætu gefið í skyn að um netsvindl sé að ræða.

„Almennt óska fyrirtæki ekki eftir kreditkortaupplýsingum án aðkomu öruggra greiðslusíðna á borð við Valitor og Borgun hér heima á Íslandi. Það er þrautinni þyngra að sporna við svindlpóstum eða vefsíðum eins og þessum á myndinni þar sem klókir svindlarar eiga auðvelt með að setja upp tímabundnar falskar heimasíður og netföng. Hjá Vodafone Ísland erum við í stöðugu samstarfi við Vodafone Global að reyna að uppræta þessa starfsemi,“ segir Kristín.

Hér má sjá nokkra punkta sem geta bent til þess að um netsvindl sé að ræða:

Hættulegustu spilliforritin

Spilliforrit valda ómældum skaða, en þessi háþróaði hugbúnaður sýkir tölvur í alls kyns vafasömum tilgangi. Þrjú hættulegustu spilliforritin bera ábyrgð á stórum hluta af netárásum.

Oddur Freyr
Þorsteinsson
oddurfreyr@frettabladid.is

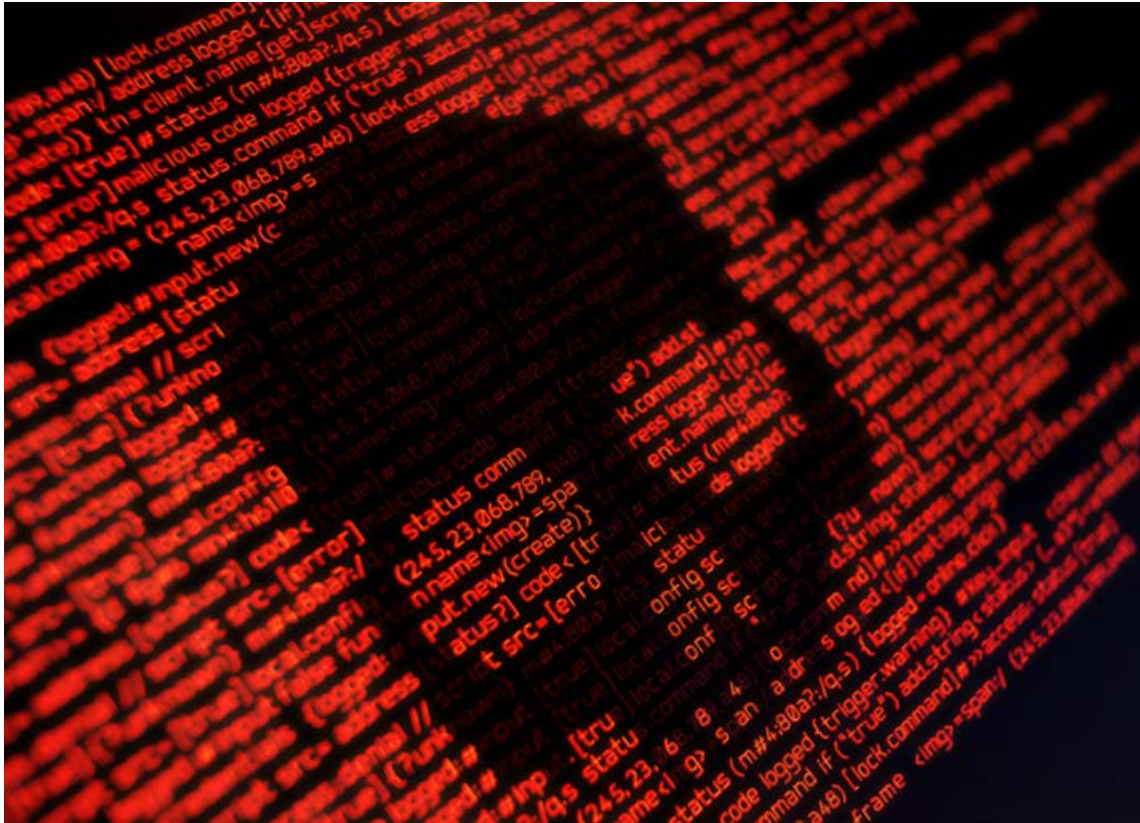


Á hverjum degi eru gerðar ótal netárásir um allan heim og það þarf stöðugt vopnakkaphlaup við tölvuþrjóta til að koma í veg fyrir að þessar árásir valdi enn meiri skaða en raun ber vitni, en þær kosta fyrirtæki og stofnanir gríðarlega fjármuni. Netöryggisfyrirtækið Check Point tekur saman tölur yfir netárásir og gaf nýlega út lista yfir hættulegustu spilliforritin í desember 2020.

Eftir fjöldapóstaherferð yfir jól og áramót sem beindist gegn yfir 100 þúsund notendum á dag, tryggði forritið Emotet sér þann vafasama heiður að vera hættulegasta spilliforrit heims í desembermánuði, samkvæmt greiningu Check Point. Samkvæmt henni var Emotet notað til að gera árásir á 7% af fyrirtækjum og stofnunum heims í mánuðinum.

Brýnt að þekkja ógnina

Forritið, sem á uppruna sinn í Rússlandi, hefur verið í notkun síðan árið 2014 og er reglulega uppfært af höfundum sínum til að það haldi áfram að gera óskunda. Forritið var upprunalega hannað til að stela bankaupplýsingum en hefur nú mun viðtækara hlutverk. Það opnar bakdyr að sýktum tölvum sem eru svo seldar öðrum netþrjótum til að þeir geti sýkt tölvurnar með öðrum spilliforritum, þar á meðal forritum sem læsa tölvum og krefja notendur þeirra svo um lausnargjald, svokölluð gagnagisling.



Spilliforritin Emotet, Trickbot og Formbook eru algengustu og hættulegustu spilliforritin um þessar mundir. Sérfræðingar segja að það sé mjög mikilvægt að vera á varðbergi gagnvart slíkum forritum. FRÉTTABLAÐIÐ/GETTY

Emotet getur dreift sér með því að færa sig yfir í aðrar tölvur sem eru tengdar sama neti og tölvan sem upprunalega sýktist, en henni er líka dreift með gabbpóstum. Forritið er svo mjög gott í að halda áfram virkni sinni á sama tíma og það forðast að vera uppgötvað, þannig að förnarlömb eru oft ekki meðvituð um sýkinguna fyrr en of seint.

„Emotet hefur þróast með tím-

anum og er nú talið ein kostnaðarsamasta og skaðlegasta útgáfan af spilliforriti,“ sagði Maya Horowitz, forstöðukona áhættugreininga og rannsókna hjá Check Point. „Það er brýnt að fyrirtæki og stofnanir séu meðvituð um ógnina af Emotet og að þau hafi öflug öryggiskerfi til staðar til að koma í veg fyrir að óþrúttir aðilar geti brotist inn í gögn þeirra. Það ætti líka að þjálfa starfsfólk þannig að það sé fært um

að bera kennsl á þá gerð tölvupósta sem dreifa Emotet.“

Mikilvægt að uppfæra

Næstalgengasta spilliforritið er Trickbot, sem kom fyrst fram árið 2016, og var upphaflega hannað til að stela bankaupplýsingum. Líkt og Emotet hefur það fengið stöðugar uppfærslur, sem gefa því alls kyns nýja notkunarmöguleika svo það hentar í allar gerðir

„Ein besta leiðin fyrir fyrirtæki og stofnanir til að vernda gögnin sín er að tryggja að nýjustu öryggisuppfærslur séu alltaf virkar á öllu netkerfinu svo tölvuþrjótar geti ekki nýtt þekkta veikleika.

netárása og rétt eins og Emotet er það oft notað til að opna bakdyr að tölvum svo hægt sé að taka gögn í gislingu.

Spilliforritið Formbook, sem safnar persónuupplýsingum, var þriðja algengasta spilliforritið sem greindist í desember. Það er selt á spjallsvæðum á myrkranetinu og gefur tölvuþrjótum öll nauðsynleg verkfæri til að stunda stórfelldan þjófnað á persónuupplýsingum. Það tekur notendanófn og lykilorð frá vöfrum, safnar skjaskotum og fylgist með og skráir hvern einasta áslátt á lykilorð, ásamt fleiru.

Samkvæmt tölunum frá Check Point gerðu Trickbot og Formbook, hvort í sínu lagi, árásir á 4% af netsvæðum allra fyrirtækja og stofnana heims í desembermánuði.

Ein besta leiðin fyrir fyrirtæki og stofnanir til að vernda gögnin sín er að tryggja að nýjustu öryggisuppfærslur séu alltaf virkar á öllu netkerfinu svo að tölvuþrjótar geti ekki nýtt þekkta veikleika í tölvukerfum. Starfsfólk ætti svo aldrei nokkurn tímann að smella á hlekki í tölvupóstum sem það er ekki 100% visst um að séu öruggir.

BYRJADU DAGINN MEÐ FRÉTTABLAÐINU

Lestu Fréttablað dagsins í snjalltækinu þínu, hvar og hvenær sem er!



• Þú sækir appið frítt í Appstore eða Googleplay.

• Opnar blað dagsins.

• Lest þegar þér hentar!

Sæktu Fréttablaðsappið frítt!



Verið velkomin í skýið hjá dk

Eitt vinsælasta bókhalds- og sölukerfið

Yfir 7.000 fyrirtæki nýta sér þjónustu dk hugbúnaðar í dag. Það gerir dk að einu stærsta hugbúnaðarfyrirtæki landsins. Lítil sem stór fyrirtæki eru með bókhaldið í skýinu hjá dk og nýta sér þannig fjölbreytta þjónustu þess í hugbúnaðar- og hýsingarlausnum. Bókhaldskerfi, birgðakerfi, innkaupakerfi, sölukerfi, sjálfsafgreiðsla, rafrænar lausnir ásamt tengingum við banka og opinbera aðila hérlandis. Hafið samband við okkur og fáið kynningu á þeim fjölbreyttu lausnum sem dk hugbúnaður hefur fyrir ykkar fyrirtæki.



FYRIRMYNDAR
FYRIRTÆKI 2020



dk hugbúnaður
510 5800 | dk@dk.is | dk.is
Smáratorgi 3 | 201 Kópavogi
Hafnarstræti 53 | 600 Akureyri



Rafræn innsigli eru að taka við af þeim hefðbundnu í Peking, höfuðborg Kína. FRÉTTABLAÐIÐ/GETTY

Rafræn innsigli taka við í Kína

Í síðasta mánuði gáfu yfirvöld í Peking, höfuðborg Kína, út fyrirmæli um reynsluprófanir á rafrænum innsiglium eða stimplum. Borgaryfirvöld ætla að hvetja til notkunar á rafrænum innsiglium til að skrifa undir vottorð, samþykktir, samninga og annað rafrænt efni. Reynslutíminn stendur yfir út þetta ár en á því næsta á þessi tækni að fara í notkun í öllum víðeigandi geirum.

Í Kína eru innsigli notuð á sama hátt og undirskriftir eru notaðar á Vesturlöndum. Rafrænar undirskriftir og innsigli hafa sama lagalega gildi og hefðbundin innsigli og ríkisstjórnin hefur lagt áherslu á að nýta þessa tækni í sinni þjónustu, en samt sem áður þarf fólk enn að leggja fram pappírsgögn með hefðbundnum innsiglium fyrir ýmis konar stjórnsýslu.

Nýlega jók ríkisstjórn Kína áhersluna á þjónustu á internetinu, meðal annars vegna COVID-19 faraldursins, og til að bæta þjónustugetu og minnka kostnað.

Þetta reynslutímabil í Peking er til marks um mikilvægt skref í tilraunum Kínverja til að koma rafrænum innsiglium í almenna notkun og þau eiga eftir að taka við í rafrænum viðskiptum þar.



Það er alltaf skynsamlegt að gæta fyllsta öryggis í viðskiptum á netinu. MYND/GETTY

Góð ráð við skoðun á vefsíðum

Neytendur eiga að sýna varfærni og varast netverslanir sem reyna að svindla á þeim. Það geta þeir gert með því að skoða vel heimasíður sem selja vörur eða þjónustu, áður en þeir gera pöntun eða eiga þar viðskipti og gefa upp persónuupplýsingar.

- Athugið hvort seljandi veiti nægar upplýsingar um sjálfan sig – þar á meðal heimilisfang.
- Athugið hvort verðupplýsingar séu skýrar, svo og farið vel yfir sölu- og afhendingarskilmála.
- Athugið hvort greiðslur séu öruggar og gerðar með tengingu þar sem notuð er dulkóðun.
- Kannið hvort verslunin hefur aflað sér traustleikamerkis sem táknar að hún hefur skuldbundið sig til að tryggja réttindi neytenda í viðskiptum.
- Leitið að nafni vefverslunarinnar á internetinu og hvort þar finnist færslur um reynslu annarra neytenda af viðskiptum við hana.
- Notið Hávörð sem getur aðstoðað við könnun á áreiðanleika vefverslunar.

Heimild: neytendastofa.is

Öruggt lykilorð

Til að tryggja öryggi á netinu er mjög mikilvægt að velja sterk lykilorð. Lykilorð eru veikur hlekkur í netöryggi en því miður eru oft ekki aðrar leiðir í boði. Gallinn við lykilorð er að fólk hefur tilhneigingu til að velja einföld lykilorð sem auðvelt er að muna, eins og 1234 eða LykilOrd. Það neikvæða við þessi lykilorð er að netþjófvar eiga auðvelt með að komast að þeim. Þegar lykilorð er valið þarf að hafa í huga að finna orð sem netþjófarnir finna ekki

auðveldlega en þú manst samt. Það er best að blanda saman hástöfum og lágstöfum, tölustöfum og táknum. Dæmi um lykilorð er að nota upphafsstafi úr setningum sem bara þú þekkir og nota tákni í staðinn fyrir bókstafi þar sem það er hægt. Til dæmis: Sigga vinkona mín á fimm börn og býr í Hveragerði. Lykilorðið gæti þá verið: \$vMa5B0b1#. Það er ekki auðvelt að átta sig á hvað þessi stafaruna merkir, en auðvelt að muna fyrir þann sem þekkir merkinguna.



Öruggt lykilorð eru mikilvæg.

Það er hægt að
Ötryggja sig fyrir
netglæpum!

MEIRIHLUTI
FYRIRTÆKJA
Á ÍSLANDI
ERU ALGERLEGA
VARNARLAUS

Ötryggja

Stórhöfða 23 / 110 Reykjavík & Skipagata 16 / 600 Akureyri / 414 1999 / tryggja@tryggja.is / www.tryggja.is