



Clár an Ábhair

Leideanna chun fioscaireacht agus innealtóireacht shóisialta a aimsiú.....	2
Cur chuige i leith riosca ó ionsaithe a mhaolú	4
Moltaí chun cur le slándáil in aghaidh ionsaithe	5

Ceann de na príomhoibleagáidí faoin Rialachán Ginearálta maidir le Cosaint Sonraí (GDPR) d'eagraíochtaí atá ag próiseáil sonraí pearsanta ('rialaitheoirí'), ná nach mór dóibh é sin a dhéanamh ar bhealach a chinntíonn slándáil chúí ó thaobh sonraí pearsanta, lena n-áirítear, cosaint in aghaidh próiseáil neamhúdraithe nó neamhdhleathach (lena n-áirítear, goid, scriosadh nó damáiste nó nochtadh) agus úsáid á bhaint as 'bearta iomchuí teicniúla nó eagraíochtúla'. Tagraítear dó seo uaireanta mar an prionsabal 'sláine agus rúndachta' nó an 'prionsabal slándála'.

Is oibleagáid thábhachtach atá san oibleagáid seo, agus oibleagáid nach mór do rialaitheoir eolas a bheith acu fúithi, go háirithe iad siúd a bhaineann úsáid nó atá ag stóráil sonraí pearsanta atá íogair. Tá cibé an bhfuil nó nach bhfuil bearta iomchuí teicniúla nó eagraíochtúla i bhfeidhm ag eagraíocht chun slándáil na sonraí pearsanta atá á bpróiseáil acu a chinntiú ar cheann de na chéad cheisteanna is dóigh a bheidh á cur ag an gCoimisiún um Chosaint Sonraí (DPC) sa chás go dtarlaíonn sárú i ndáil le sonraí pearsanta nó chun cumhachtaí imscrúdaithe an DPC a fheidhmiú. Féadfaidh rialaitheoirí comhairle a fháil freisin inár [dtreoir ar shlándáil sonraí do rialaitheoirí](#) agus iad i mbun measúnaithe ar na bearta iomchuí slándála nach mór dóibh a chur i bhfeidhm.

Bealach amháin ina bhféadfadh rioscaí maidir le slándáil phearsanta a theacht chun cinn ná trí ionsaithe ar a dtugtar 'fioscaireacht' nó 'innealtóireacht shóisialta'. Sampla í fioscaireacht den innealtóireacht shóisialta a mbaintear úsáid aisti go coitianta chun úsáideoirí a chur amú. Is ionann fioscaireacht agus nuair a dhéanann duine éigin iarracht chalaoiseach le bob a imirt ar úsáideoir chun faisnéis atá íogair a nochtadh, ar nós ainm úsáideoira, pasfhocail nó mionsonraí maidir le cárta creidmheasa, ina gcuireann siad iad féin i láthair mar fhoinsé iontaofa i gcumarsáid leictreonach. Trí úsáid a bhaint as foinsé nó as ainm iontaofa nó as lógó comónta mar 'bhaoite', féadfaidh an lucht ionsaithe dul ag 'iascaireacht' d'fhaisnéis atá íogair, ar nós sonraí pearsanta.

Is féidir é seo a dhéanamh ar líon bealaí, ar nós ‘ríomhphost faoi bhréagriocht’ (ina mbaintear úsáid as seoladh ríomhphoist nó ainmneacha atá clónáilte nó as seoladh ríomhphoist atá ar an gcuma chéanna) agus úsáideoirí a chur ar strae chun faisnéis íogair a chur isteach ar láithreán gréasáin bréige (a fhéachann an-chosúil leis an láithreán gréasáin dlisteanach) nó bogearraí a fhéachann neamhdhíobhálach ach bogearraí atá mailíseach a íoslódáil (a bhíonn ceilte go minic mar cheangaltáin ríomhphoist).

Leideanna chun fioscaireacht nó innealtóireacht shóisialta a aimsiú

Ríomhphost faoi Bhréagriocht: Tá ríomhphost faoi bhréagriocht i gceist nuair a sheolann an t-ionsaitheoir teachtaireachtaí agus úsáid á bhaint as seoladh seoltóra atá bréagach. Mar gheall nach bhfuil meicníocht fíordheimhnithe ag croíphrótaicail theicniúla do ríomhphoist, is féidir le hionsaitheoirí úsáid a bhaint as bréagriocht leis an bhfaighteoir a chur amú maidir le bunús na teachtaireachta. D’fhéadfadh córais ar nós SSL/TLS do chriptiú ríomhphoist cuidiú ó thaobh an riosca seo a sheachaint, mar sin féin, ní bhíonn sé ar fáil nó ní bhaintear úsáid as in go leor eagraíochtaí chun na críche seo.

- Cuireann formhór na soláthróirí ríomhphoist roinnt bearta slándála ar fáil chun cosaint a thabhairt in aghaidh ríomhphoist den sórt seo, ach tá sé tábhachtach mionsonraí an tseoltóra a sheiceáil in athuair, go háirithe má tá amhras faoin ríomhphost
- Mar shampla, ba chóir a chinntiú go meaitseálann an seoladh ríomhphoist féin chomh maith le haon ainm teagmhála nó ainm atá in ábhar an ríomhphoist araon

Fioscaireacht le Sleá: Is éard atá i gceist le fioscaireacht le sleá ná foirm spriocdhírthe fioscaireachta, nuair a dhéanann an t-ionsaitheoir iarracht an t-ionsaí a chur i láthair níos dlisteanáí trína shainiúint don duine atá thíos leis. Tá sé seo coitianta ó thaobh comhaltaí sinsearach eagraíochta nó ó thaobh foireann a bhfuil freagracht orthu i réimse atá íogair. D’fhéadfadh an réamhobair a bheith déanta ag an ionsaitheoir, lena n-áirítear, ainm, teideal an phoist, seoladh ríomhphoist srl., an íospartaigh atá i gceist a bheith ceart acu.

- Tá sé tábhachtach, go háirithe, go gcuirfidh eagraíochtaí an fhoireann atá ag obair i réimsí den sórt seo ar an eolas maidir le hionsaithe spriocdhírthe fioscaireachta, agus a chinntiú go bhfuil siad ar an airdeall ó thaobh aon chomhfhreagras leictreonach nach bhfuil siad ag súil leis

Ionramháil Naisc: Is minic go mbaineann caimiléireacht theicniúil le fioscaireacht atá deartha le cuma a bheith ar nasc cumarsáide leictreonach gur le foinse iontaofa an chumarsáid. D’fhéadfadh fioscairí úsáid a bhaint as URL’na atá litrithe mícheart nó fofhearainn a fhéachann dlisteanach chun bob a bhualadh ar úsáideoir le cliceáil ar nasc. Mar shampla, d’fhéadfaí an URL ‘www.truztedsource.ie’ a úsáid chun bob a

bhualadh ar úsáideoir cliceáil ar nasc a mheasann siad a bheith do 'www.trustedsource.ie'. Mar an gcéanna, d'fhéadfadh fioscairí úsáid a bhaint as nasc ar nós 'www.trustedsource.secureinfo.ie' chun bob a bhualadh ar úsáideoirí nuair a cheapann siad go bhfuil siad ag nascadh le leathanach 'faisnéise atá slán' ar láithreán gréasáin 'foinse iontaofa', ach ina áit sin bheadh siad ag nascadh le láithreán gréasáin 'secureinfo.ie', ina bhféadfadh leathanach bréige a bheith socraithe suas ag an bhfioscaire. Uaireanta féachann an téacs atá léirithe don nasc URL dlisteanach, ach téann an nasc, nuair a chliceálann tú air, chuig áit éigin eile ar fad – mar shampla, <http://www.trustedsource.ie/> chuig 'ww.notatrustedsource.ie'. Go minic is féidir leat an fíor-nasc atá i gceist a aimsiú trí do chúrsóir a fhágáil ag crochadh os cionn an naisc ach tá sé tábhachtach a thabhairt ar aird nach féidir é sin a dhéanamh i gcónaí, ar nós mar atá an cás le formhór na bhfeidhmchlár móibíleach.

- Ní mór d'eagraíochtaí a chinntiú go bhfuil an fhoireann airdeallach ó thaobh cliceáil ar naisc chuig láithreáin gréasáin sheachtracha, go háirithe ar ghléasanna móibíleacha.
- Ní mór d'eagraíochtaí bearta slándála teicniúla a fheidhmiú a d'fhéadfadh cuidiú ó thaobh ionramháil naisc a bhrath agus cosaint a thabhairt ina choinne.

Innealtóireacht Shóisialta: Is iomaí cineál innealtóireachta sóisialta a d'fhéadfadh a bheith ann agus de ghnáth, baintear úsáid as teicnící síceolaíochta atá caolchúiseach le húsáideoirí a chur amú le gníomh áirithe a dhéanamh. D'fhéadfadh sé go ndéanfaí úsáideoirí a ghríosú chun cliceáil ar chineálacha éagsúla ábhar nach rabhthas ag súil leis, ar nós naisc nó ceangaltáin, ar chúiseanna éagsúla gairmiúla, teicniúla nó sóisialta. D'fhéadfaí ríomhphost a sheoladh chuig bosca isteach oibre agus é marcáilte 'Tábhachtach!' nó 'PRÁINNEACH', le teideal agus foclaíocht lena ndéantar iarracht bob a bhualadh ar an fhoireann leis an gceangaltán a oscailt go tapa nó cliceáil ar nasc. D'fhéadfaí iarracht a dhéanamh trí mhír aníos slándála atá bréagach úsáideoir a scanrú le cliceáil ar nasc trína chur ar na súile dóibh go bhfuil siad faoi réir ag ionsaí bogearraí atá mailíseach nó nach mór dóibh a gcuid bogearraí slándála a thabhairt cothrom le dáta. Nó d'fhéadfaí fógra nó ríomhphost an duine a ghríosú le cliceáil ar nasc trí chur i gcéill go bhfuiltear ag nascadh le cabaireacht áite oibre atá thar a bheith spéisiúil nó le ceannlíne nuachta a théann thar fóir.

- Is féidir le heagraíochtaí an dainséar a bhaineann le cumarsáid leictreonach a fhreagairt fiú nuair atá cuma phráinneach ar an gcumarsáid sin a mheabhrú don fhoireann
- Ní mór d'eagraíochtaí bearta teicniúla nó eagraíochtúla a bhreithniú maidir leis na naisc gur féidir leis an fhoireann cliceáil orthu nó ceangaltáin a d'fhéadfadh an fhoireann a íoslódáil, nuair is cuí.

D'fhéadfadh fioscaireacht agus cleachtais innealtóireachta sóisialta eile a bheith mealltach agus riosca tromchúiseach a bheith ag gabháil leo d'eagraíochtaí, go háirithe áiteanna oibre ina bhfuil go leor foirne agus/nó go leor trealamh cumarsáide leictreonach. Tá sé tábhachtach, mar chuid dá mbeartas ginearálta slándála sonraí, go mbreithneoidh eagraíochtaí cibé an bhfuil siad i mbaol ó thaobh ionsaithe den sórt sin,

agus na 'bearta teicniúla nó eagraíochtúla cuí' is féidir leo tabhairt fúthu chun aon bhaol a d'fhéadfadh a bheith ann a laghdú.

Cuir chuige i leith riosca ó ionsaithe a mhaolú

Is féidir le heagraíochtaí go leor céimeanna a ghlacadh chun iad féin a chosaint ó rioscaí i ndáil le slándáil sonraí ar nós fioscaireacht agus innealtóireacht shóisialta, ar nós anailís mionsonraithe agus rialta a dhéanamh; athbhreithniú a dhéanamh ar bheartais chumarsáide agus IT inmheánacha; agus bearta slándála fisiciúla agus teicniúla agus oiliúint foirne a chur i bhfeidhm.

Ní mór d'eagraíochtaí breithniú a dhéanamh ar scoth na mbeart teicniúil agus eagraíochtúil agus costais agus comhréireacht bearta áirithe a fheidhmiú – ní mór go dtabharfaidh an cinneadh san áireamh, ní hamháin an teicneolaíocht infheidhme is cuí, ach saghas agus nádúr araon na heagraíochta chomh maith le méid agus nádúr na sonraí pearsanta atá a stóráil agus á bpróiseáil.

Ní mór d'eagraíochtaí na hoibleagáidí maidir le slándáil agus le hionracas aon phróiseáil sonraí atá á déanamh ag lucht próiseála sonraí thar a gceann a thógáil san áireamh freisin, lena n-áirítear, cibé an bhfuil na comhaontuithe próiseála sonraí ag tabhairt clúdach leordhóthanach ó thaobh slándáil agus ionracas na próiseála agus cad ba cheart a dhéanamh ó thaobh eachtra slándála nó sárú i ndáil le sonraí pearsanta.

D'fhéadfadh seirbhísí áirithe a mbaineann eagraíochtaí úsáid astu, ar nós seirbhís ríomhphoist néalbhunaithe go leor buntáistí a chur ar fáil d'eagraíochtaí. D'fhéadfadh siad, áfach, laigí sláinte teicniúla a chur i láthair freisin, nach mór d'eagraíochtaí a aithint. D'fhéadfadh sé, má chlistear rialuithe slándála agus comhlíonadh cuí a chur i bhfeidhm, go gcuirfear leis an riosca i ndáil le sárú sonraí pearsanta ó ionsaithe fioscaireachta nó innealtóireachta sóisialta. Ní mór d'eagraíochtaí frithbhearta a chur i bhfeidhm chun cosaint a thabhairt in aghaidh na mbagairtí seo, go ginearálta agus go sonracha araon trí bhogearraí agus seirbhísí a mbaineann an eagraíocht úsáid astú, ar nós, rochtain neamhúdairithe chuig sonraí pearsanta, fuadach cuntais, bradaíl aitheantais, cibear-chalaois agus haiceáil.

Cuireann 'grúpearraí' néalbhunaithe (bogearraí a chuidíonn le grúpaí comhghleacaithe comhoibriú agus a gcuid gníomhaíochta a eagrú), d'fheidhmeanna ríomhphoist agus d'fheidhmeanna gairmiúla eile, ar nós, Microsoft Office 365 agus Sraith G Google ardsocruithe agus réitigh ar fáil, atá in ann cuidiú le heagraíochtaí a bheith slán agus troid in aghaidh na mbagairtí seo. Cuireann soláthróirí ríomhphoist, sa chuid is mó de chásanna, treoir dea-chleachtais ar fáil d'eagraíochtaí freisin chun seirbhís ríomhphoist a choinneáil slán.

Taobh le bearta slándála teicniúla cuí, tá oiliúint foirne ar cheann de na bealaí is fearr chun cur ar chumas eagraíocht a leochaileacht ó thaobh fioscaireacht agus innealtóireacht shóisialta a laghdú. Is féidir le hoiliúint- taobh le bearta slándála teicniúla cuí – trína chinntiú go mbíonn tuiscint ag an bhfoireann, go háirithe an

fhoireann atá ag obair le faisnéis atá íogair ar nós sonraí pearsanta, ar na rioscaí agus go mbíonn siad ábalta rioscaí den sórt sin a sheachaint araon, ar nós gan ríomhphoist ó sheoltóirí nach bhfuil aithne acu orthu a oscailt agus trí chliceáil ar naisc a bhíonn i ríomhphost a sheachaint mura mbíonn a fhios acu go díreach cá bhfuil an nasc sin ag dul.

Déanann cur chuige sraithaithe i leith slándála maolú ar riosca go gclisfeadh ar bheart slándála aonair a bhféadfadh sárú i ndáil le sonraí pearsanta a bheith mar thoradh air don eagraíocht.

Moltaí chun cur le slándáil in aghaidh ionsaithe

D'fhéadfadh na moltaí seo a leanas cuidiú le heagraíochtaí agus iad i mbun breithnithe ar na bearta teicniúla agus eagraíochtúla is gá a chur i bhfeidhm chun slándáil agus ionracas sonraí pearsanta atá á bpróiseáil acu a chinntiú agus cosaint a thabhairt in aghaidh ionsaithe fioscaireachta agus innealtóireachta sóisialta. Ní bheidh gach moladh ábhartha do gach eagraíocht ach ní mór iad a bhreithniú i gcomhthéacs na hoibre atá á déanamh ag eagraíocht agus na cineálacha próiseála sonraí a bhfuil an eagraíocht rannpháirteach ann, chun na bearta is fear a oireann a fheidhmiú i ngach cás:

- Athbhreithniú a dhéanamh ar aon socruithe slándála réamhsocraithe, lena n-áirítear, pasfhocail agus faisnéis aitheantais, a chuireann seirbhís nó earraí grúpa ar fáil a mbaineann an eagraíocht úsáid astu.
- Fíordheimhniú ilfhachtóra a chur i bhfeidhm d'úsáideoirí láithreán-bhunaithe nó cian-úsáideoirí ríomhphoist, bunachar sonraí nó córais eagraíochta, lena n-áirítear, aon chomhpháirtí seirbhíse bainistithe nó riarthóirí.
- Rialacha a chur i bhfeidhm le ríomhphoist lena mbaineann amhras agus/nó turscar a scagadh agus a bhrath.
- Rialacha nua a chruthú maidir leis an mbealach le teachtaireachtaí agus ceangaltáin a láimhseáil bunaithe ar choinníollacha ar nós cineál comhaid nó méid na teachtaireachta.
- Iniúchadh a chasadh air chun a chinntiú go mbíonn log iniúchta ar fáil chun gníomh an úsáideora ar an gcóras ríomhphoist a rianú.
- A chinntiú go mbíonn na ceadanna ríomhphoist ról-bhunaithe ceart – maidir leis na cearta córais, bainistíochta nó leagan amach.
- Cianrochtain nó rochtain láithreán-bhunaithe chuig ríomhphost, bunachar sonraí nó chuig córais eile don fhoireann atá lonnaithe san oifig go príomha a dhíchumasú.
- Rialuithe a chur i bhfeidhm chun cosc a chur ar úsáideoirí ríomhphost/ríomhphoist a sheoladh ar aghaidh go huathoibríoch chuig seoltaí ríomhphoist seachtracha.

- ☑ Athbhreithniú rialta a dhéanamh ar aon rialacha maidir le cur ar aghaidh a chumasú do ghrúpearra ar mhaithe lena chinntiú nach mbíonn aon rialacha ann nach bhfuil riachtanach nó nach bhfuil ceadaithe.
- ☑ Beartais a leagan amach le rabhadh (leid amhairc) a thabhairt nuair a sheoltar ríomhphost chuig teagmhálaí nó eagraíocht sheachtrach (m.sh leideanna sábháilteachta Oifig 365).
- ☑ Beartais a leagan amach le foláireamh a sholáthar maidir le hiompar síniú isteach ar nós rochtain geoshuíomh neamhrialta.
- ☑ Beartas cosc maidir le cailliúint sonraí a leagan amach le haon fhaisnéis atá íogair (m.sh. mionsonraí bainc) a bheith á seoladh go dtí seoltaí seachtracha a aithint agus monatóireacht a dhéanamh orthu go huathoibríoch.
- ☑ Athbhreithniú rialta a dhéanamh ar bheartais rochtana láithreáin (scagadh) le rochtain chuig láithreáin gréasáin (fioscaireacht) mhailíseacha nó neamhchuí a chosc.
- ☑ Próiseas rialaithe a chur i bhfeidhm chun gach gaireas a bhíonn ag rochtain ríomhphoist a cheadú agus a dhaingniú.
- ☑ Beartais rochtana ríomhphoist chuí a chruthú do réimsí ar nós Beir Leat do Ghléas Féin (BYOD).
- ☑ Bainistiú a dhéanamh ar ghléasanna móibíleacha trína gclárú ar réiteach bhainistíochta do ghléas móibíleach (a d'fhéadfadh iad a aimsiú, a chur faoi ghlas nó a ghlanadh má chailltear iad).
- ☑ Liosta a choinneáil agus a athbhreithniú ar bhonn rialta, de ghléasanna móibíleacha atá ceadaithe le ríomhphost a rochtain agus chun fáil réidh le haon ghléasanna nach dteastaíonn níos mó.
- ☑ Plean freagartha i leith eachtra a fhorbairt chun creat a chur ar fáil ó thaobh bainistíochta a dhéanamh ar aon eachtra/eachtraí slándála.
- ☑ A éileamh go ndéantar ríomhphoist a tharchur trí cheangal slán (criptithe) ar nós TLS 1.2.
- ☑ Aon bheartais cartlannaithe ríomhphoist a athbhreithniú chun méid na faisnéise atá laistigh de bhoscaí poist a laghdú.
- ☑ Criptiú a chur i bhfeidhm don chuid eile de na boscaí poist.
- ☑ Uasdátú ábhartha a eisiúint don fhoireann maidir lena bheith airdeallach ó thaobh iarrachtaí maidir le hinnealtóireacht shóisialta trí ríomhphost nó trí veicteoirí ionsaithe eile. An t-uasdátú sin a chomhtháthú i bpróiseas oideachais leanúnach maidir le cibearshlándáil agus bagairtí gaolmhara.
- ☑ A chinntiú go mbíonn ar chumas na foirne teagmháil a dhéanamh le duine éigin, ar nós bainisteoir nó saineolaí seachtrach IT, sa chás go mbíonn údar imní acu maidir le rioscaí i ndáil le sonraí, ar nós cumarsáid amhrasach, nasc, ceangaltán nó mír aníos.

- ☑ Breithniú a dhéanamh ar mhodhanna cosanta sofaisticiúla ríomhphoist a fheidhmiú ar nós Creatbheartas Seoltóra ([SPF](#)), DomainKeys Ríomhphost sainaitheanta ([DKIM](#)), Fíordheimhniú Teachtairreachta Bunaithe ar Fhearann ar Thuairisciú agus ar Chomhréireacht ([DMARC](#)).

Meabhraítear d'eagraíochtaí nach mór dóibh sárúithe i ndáil le sonraí pearsanta a thuairisciú faoin GDPR do na heagraíochtaí maoirseachta ábhartha sa chás go bhfuil riosca ann don duine aonair atá faoi thionchar. Ní mór d'eagraíochtaí an méid sin a dhéanamh laistigh de 72 uair an chloig ó fhaigheann siad amach faoin sárú. Sa chás go mbeidh ardriosca ann do na daoine aonair atá faoi thionchar, ní mór d'eagraíochtaí na daoine aonair sin a chur ar an eolas gan mhoill mhíchuí. Tá tuilleadh [treorach i ndáil le fógraí sárúithe](#) le fáil ar láithreán gréasáin an DPC.