



SILWERS

SENIORS ARTIFICIAL INTELLIGENCE LEARNING
- WELL EDUCATED AND RISK SECURE



Co-funded by the
European Union

Expert fora report



University
of Economics
in Katowice



Háskólinn
á Akureyri

SecureIT



Erasmus+ KA220-ADU – Cooperation partnerships in adult education, Project No: **2024-1-IS01-KA220-ADU-000256952**

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Markmið nefndarinnar

1

Umræða um erfiðleika og áhyggjur sem þessi hópur stendur frammi fyrir varðandi nýja tækni ásamt því að greina notkunarsvið gervigreindar og tengda áhættu.

2

Greining á núverandi og framtíðarógnum á netinu fyrir fólk 55 ára og eldri.

3

Núverandiraunveruleg dæmi um atvik og ávinning af notkun gervigreindar.

4

Skilgreining á mikilvægri stafrænni hæfni fyrir fólk 55 ára og eldri.



Co-funded by the
European Union



Niðurstöður - Pólska





Mest vitnað í netógnir fyrir 55 ára og eldri

Fólk 55 ára og eldra stendur frammi fyrir einstökum áskorunum í stafræna heiminum, sem gerir það viðkvæmt fyrir ýmsum ógnum á netinu.

Að skilja algengustu og áhrifamestu hættur er nauðsynlegt til að bæta vitund þeirra um netöryggi og vernd.



Ógnanir

Ógnir sem sérfræðingarnir hafa bent á þjóna sem orðasafn fyrir eldri borgara.





Ógnir á netinu fyrir 55 ára og eldri

- Netveiðar með svksamlegum tölvupósti, SMS-skilaboðum, tenglum og símtölum
- Djúpfalsárás ræðst á falsa hljóð-/myndbönd og þykist vera fjölskyldumeðlimur
- Falskar netverslanir og svksamlegar vefsíður
- Tilfinningaleg stjórnun og félagsleg verkfræði hræðsluáætlanir
- Auðkennisþjófnaður með stolnum persónuupplýsingum



Ógnir á netinu fyrir 55 ára og eldri

- Svik gegn barnabörnunum sem þykjast vera fjölskylda í neyð
- Falskar hjálparbeiðnir í gegnum WhatsApp eða Messenger
- Ástarsvik og svik byggð á samböndum sem byggjast á netinu
- Falskar auglýsingar um fjárfestingarsvik með frægu fólki
- Skrár og viðhengi sem eru sýkt af spilliforritum og ransomware



Ógnir á netinu fyrir 55 ára og eldri

- Óstaðfest forrit og óöruggar niðurhal hugbúnaðar
- Að deila viðkvæmum gögnum með ókunnugum, myndum, upplýsingum
- Notkun úreltra tækja eða hugbúnaðar
- Fjöldaárásir með persónulegum hætti með gervigreind, sem beinast að notendasniðum
- Rangfærslur um heilsufar eða hættuleg læknisfræðileg ráð frá gervigreindartólum



Ógnir á netinu fyrir 55 ára og eldri

- Svik sem nýta sér stafræna útilokun í borgaralegri og bankastarfsemi
- Skortur á fjölþátta auðkenningaraðferðum einfaldaði lykilorð og endurnotkun
- Tap á aðgangi að mikilvægum þjónustum vegna tæknibreytinga, aðgangur eingöngu í gegnum app, takmarkaðir valkostir
- Sjálfvirk stjórnun á samfélagsmiðlum, sem veldur rangfærslum og streitu
- Lykilorð, auðkenning, líffræðileg tölfræði, 2FA



Co-funded by the
European Union



10 helstu áhyggjur samkvæmt sérfræðingum

Sérfræðingar bentu á helstu áhyggjur sem hafa mest áhrif á fólk 55 ára og eldra þegar það hefur samskipti við stafræna tækni.

Að taka á þessum áhyggjum er mikilvægt til að auka sjálfstraust þeirra og öryggi í daglegum athöfnum á netinu.



Hvatning

Þróun markvissra stuðnings- og þjálfunaráætlana.





10 helstu áhyggjur samkvæmt sérfræðingum

- **Tæknibreytingar**og flækjustig: Hraður tækniþróun gerir það erfitt fyrir eldri borgara að aðlagast, sérstaklega með uppfærslum og nýjum tækjum.
- Ótti og **tilfinningaleg meðferð** Svikahrappur nýtir sér oft tilfinningar, eins og ótta eða brýnni þörf, sem gerir eldri borgara viðkvæmari.
- **Félagsleg útilokun**og einmanaleiki: Minnkuð samskipti við fjölskyldu og vini, oft augin vegna þess að stafræn samskipti koma í stað beinna samskipta.
- **Hikaði við að biðja um hjálp**: Eldri borgarar finna oft fyrir skömm eða vandræðum þegar þeir biðja yngra fólk um aðstoð með tækni.
- **Fjárhagslegar takmarkanir** Tregða eða vanhæfni til að eyða peningum í ný tæki eða hugbúnað, sem leiðir til úreltrar og óöruggrar tækni.



10 helstu áhyggjur samkvæmt sérfræðingum

- **Stafræn útilokun** í þjónustu: Dagleg verkefni (eins og að kaupa miða, bankaviðskipti, læknisheimsóknir) eru í auknum mæli færð á netið, sem skilur eldri borgara eftir án annarra valkosti.
- **Lágt stafræn hæfni** Skortur á grunnfærni og reynslu, sem stundum versnar af því að hafa ekki fengið tölvumenntun fyrr á ævinni.
- Hvatvísi og **áhættusamar ákvarðanir** Tilhneiging til að bregðast hratt við þegar tæknileg vandamál koma upp — sem stundum leiðir til mistaka eða sviksemi.
- **Varnarleysi** rangfærslur: Erfiðleikar við að greina á milli sannra upplýsinga og stafrænnar meðhöndlunar, sérstaklega á netinu.
- Tæki og **viðhaldsvandamál hugbúnaðar** Vandamál við að uppfæra tæki, stjórna lykilorðum og skilja bestu starfsvenjur í stafrænu öryggi, sem eykur áhættu.



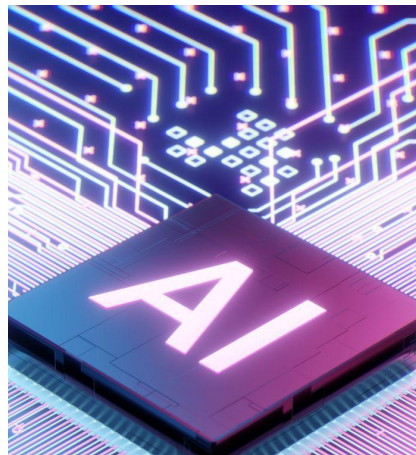
Co-funded by the
European Union



Helstu notkunarsvið gervigreindar og netáhætta

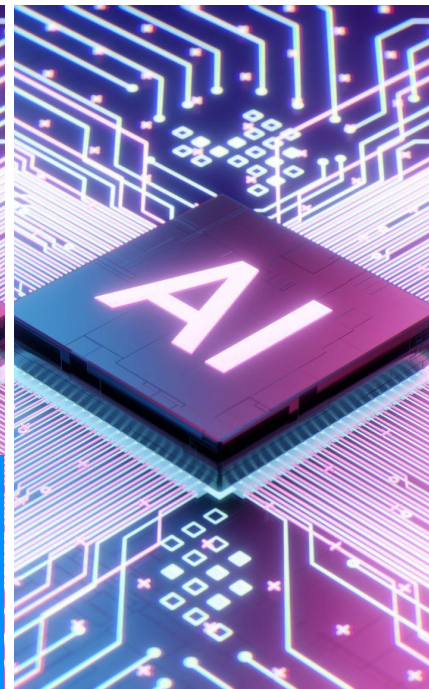
Gervigreind er í auknum mæli sambætt mörgum þáttum daglegs lífs, býður upp á verulegan ávinning en felur einnig í sér nýjar áhættur í netöryggi.

Að skilja helstu notkunarsvið gervigreindar og ógnir sem þeim tengjast er nauðsynlegt til að vernda viðkvæma hópa eins og fólk 55 ára og eldra.



Stuðningur

Til að veita skilvirkan stuðning þarf að auka vitund um áhættu sem tengist gervigreind.





Helstu notkunarsvið gervigreindar og netáhætta

- **Einkaaðstoðarmenn** í sínum og tækjum (t.d. raddstýrðum aðstoðarmönnum eins og Alexa) sem styðja eldri borgara við dagleg verkefni en krefjast skilnings á friðhelgi einkalífs og öryggi.
- Gervigreind **íeftirlit með heilbrigðisþjónustu** (klæðnaðartæki, fráviksgreining í hjartslætti) sem veitir snemmbúna viðvaranir en þarfnast trausts og grunnfærni í stafrænni tækni til að starfa.
- Svik knúin af gervigreind og **uppgötvun svikamyllna** (netveiðaaauðkenning, djúpfölsunarauðkenning) til að vernda eldri borgara fyrir markvissum árásum en krefst þekkingar á að bera kennsl á grunsamlegt efni.
- Gervigreindarframleitt **persónulegar árásir** sem aðlagast hegðun og tilfinningum einstakra eldri borgara, sem gerir það erfiðara að greina ógnir á netinu.
- **Efnisframleiðsla** og rangfærslur í gegnum gervigreind (djúpfölsun, falskar auglýsingar, falsfréttir) hafa áhrif á ákvarðanir og valda ruglingi meðal eldri borgara sem skortir gagnrýna matshæfileika.



Helstu notkunarsvið gervigreindar og netáhætta

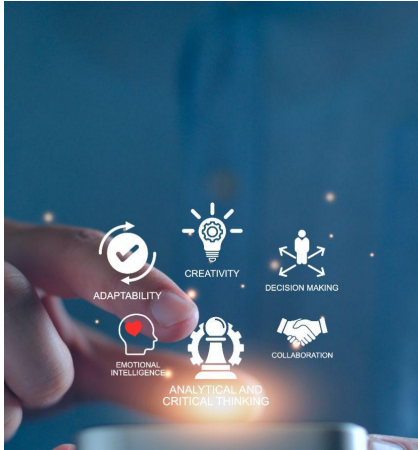
- Gervigreind í **snjallheimili** og IoT tæki sem aðstoða daglegt líf en skapa áhættu ef tækin eru óörug eða illa stjórnað.
- Ferðalög með aðstoð gervigreindar og **frístundaskipulagninga** að hjálpa til við að skipuleggja ferðir og afþreyingu, sem eykur þægindi en krefst nokkurrar stafrænnar færni til öruggrar notkunar.
- Sjálfvirk **félagsleg samskipti** Vélmanni sem herma eftir mannlegum samskiptum, oft notuð í svikum eða til að draga úr einangrun, og þurfa vitundarvakningu til að forðast blekkingar.
- Gervigreind í stafrænu formi **fjármálalögn** Sjálfvirkni viðgerð á viðskiptum og bankastarfsemi sem getur bætt aðgengi en krefst þekkingar á öryggisvenjum og svikavarnir.
- Gervigreindarverkfæri í **samskipti** með fjölskyldu og umönnunaraðilum (rauntímaeftirlit, neyðarviðvörðunarkerfi) sem eykur öryggi en krefst hæfni í uppsetningu og túlkun.



Mikilvæg hæfni fyrir eldri borgara

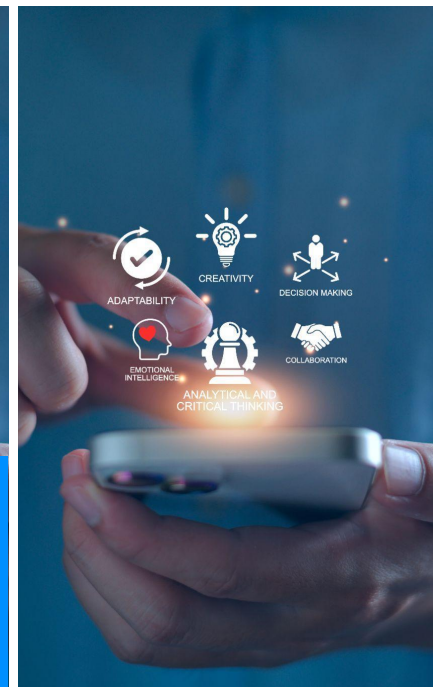
Það er mikilvægt að þróa nauðsynlega stafræna hæfni til að gera eldri borgara kleift að ferðast um netheiminn á öruggan og af öryggi.

Þessi færni hjálpar þeim að nýta tækni á skilvirkan hátt til að bæta daglegt líf sitt og seiglu gegn netógunum.



Hæfni

Gera eldri borgurum kleift að vernda sig betur og nota nútímatækni af öryggi.





Mikilvæg hæfni fyrir eldri borgara

- **Að skiljagrunnnotkun** stafrænna tækja og öryggisstillingar.
- **Viðurkenningaf** gervigreindarknúinni stjórnun og sviksamlegu efni.
- **Stafræn læsital** að eiga örugg samskipti við gervigreindaraðstoðarmenn og snjalltæki.
- **Meðvitundum** persónuvernd og gagnaverndarráðstafanir í gervigreindarforritum.
- **Hæfnitil** að leita að áreiðanlegum upplýsingum og sannreyna efni sem myndast með gervigreind.



Mikilvæg hæfni fyrir eldri borgara

- Tilfinningaþrungin **seigla** til að forðast að vera stjórnað af svikum sem knúin eru af gervigreind.
- **Þægindi** með grunn bilanagreiningu og viðhaldi stafrænna tækja.
- **Þekking** öruggar lykilorðastjórnunar og auðkenningaraðferða.
- Hæfni til **nota** Gervigreindartól fyrir heilsu, öryggi og samskipti.
- **Opinskátt** til stöðugs náms vegna hraðrar þróunar í gervigreindartækni.



Co-funded by the
European Union



Raunverulegar ógnir sem sérfræðingar hafa greint

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í algengar netógnir gervigreindar í daglegt líf aldraðra.



Ógnanir

Raunveruleg dæmi undirstrika mikilvægi þess að þekkja og draga úr netógnum.





Raunverulegar ógnir sem sérfræðingar hafa greint

- Notkun **ádjúpfölsun**Tækni til að þykjast vera fjölskyldumeðlimur: Eldri borgari fær símtal þar sem sá sem hringir, með sannfærandi hermdri rödd barnabarns eða barns, fullyrðir að hann þurfi á peningum að halda tafarlaust (t.d. vegna slyss). Eldri borgarinn, sannfærður af tilfinningalegri meðferð og kunnugleika röddarinnar, millifærir peninga, oft með BLIK eða bankamillifærslu.
- Rómantík**svik**sem felur í sér gervigreind: Eldri borgarar eru skotmark á netinu af einstaklingum (stundum spjallþjónum eða sjálfvirkum prófílum) sem mynda tilfinningaleg „sambönd“ og biðja síðan um peninga undir fölskum forsendum, nýta sér einmanaleika og traust.
- Falsahapp**drættie**ða verðlaunavinningur: Eldri borgara er upplýstur, oft í gegnum símtal eða tölvupóst með því að nota efni sem myndað er með gervigreind, um að hann hafi unnið háa peningaupphæð. Til að krefjast hennar er hann beðinn um innborgun eða persónuupplýsingar, sem leiðir til fjárhagstjóns og stundum auðkennisþjófnaðar.



Raunverulegar ógnir sem sérfræðingar hafa greint

- **Meðhöndlun** gegnum falsa netverslanir: Aldraðir kaupa óafvitandi vörur af vefsíðum sem eru næstum eins og löglegar verslanir (með smávægilegri stafsetningarbreytingu á heimilisfangi eða nafni). Þeir borga fyrir vörur sem aldrei berast og verða þannig fórnarlömb háþróaðra gervigreindartengdra vefveiðasíðna.
- Læknisfræði með gervigreindrangfærslurEldri borgarar leita ráða hjá gervigreindarspjallþjónum eða nettólum til að fá heilsufarsráð. Stundum eru ráðleggingarnar villandi og valda því að þeir sleppa því að ráðfæra sig við lækni eða jafnvel taka rangar lyf, sem geta verið hættuleg heilsu þeirra.



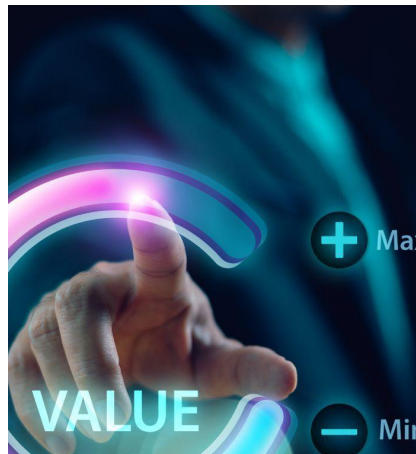
Co-funded by the
European Union



Raunverulegir ávinningar sem sérfræðingar hafa bent á

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í ávinninginn gervigreindar á daglegt líf aldraðra.



Kostir

Raunveruleg dæmi varpa ljósi á Ávinningur gervigreindar til að bæta lífsgæði og daglega virkni eldri borgara.





Raunverulegir ávinningar sem sérfræðingar hafa bent á

- Eldri borgari notaði ferðataeki knúið af gervigreind **skipulagningtöl** til að skipuleggja ferð, tilgreina dagsetningar og persónuleg áhugamál (eins og söfn eða útivist), fá ítarlega, sérsniðna ferðaáætlun — sem gerir ferðina auðveldari og skemmtilegri.
- Gervigreindarknúin læknisfræði **greiningar** Verkfæri greindu snemma viðvörðunarkerki um heilsufarsvandamál (eins og óreglulegan hjartslátt hjá sjúklingum með gangráða og sykursýki), sem leiddi til tímanlegrar læknisaðstoðar og bættrar vellíðunar.
- Eldri borgarar nýttu sér gervigreinda **aðstoðarmenn** (eins og Alexa) fyrir daglegar áminningar (t.d. lyfjatökutíma og tímapantanir), heimilishald og félagsleg samskipti, draga úr einmanaleika og auka sjálfstæði.



Raunverulegir ávinningar sem sérfræðingar hafa bent á

- Dæmi um snjalltækiklæðanleggtæki (úlnliðsbönd knúin gervigreind) sem fylgdust stöðugt með helstu heilsufarsmælingum aldraðra sem búa einir og gerðu umönnunaraðilum eða neyðarþjónustu sjálfkrafa viðvart ef upp kæmu frávik eða neyðarástand.
- Gervigreindarmyndviðurkenning og leit hjálpaði eldri manni að bera kennsl á óþekkta plöntu í garðinum sínum, veitti tafarlaugar leiðbeiningar um umhirðu og jók þannig garðyrkjukunnáttu og sjálfstraust.



Co-funded by the
European Union



Niðurstöður - Tékkland





Mest vitnað í netógnir fyrir 55 ára og eldri

Fólk 55 ára og eldra stendur frammi fyrir einstökum áskorunum í stafræna heiminum, sem gerir það viðkvæmt fyrir ýmsum ógnum á netinu.

Að skilja algengustu og áhrifamestu hættur er nauðsynlegt til að bæta vitund þeirra um netöryggi og vernd.



Ógnanir

Ógnir sem sérfræðingarnir hafa bent á þjóna sem orðasafn fyrir eldri borgara.





Ógnir á netinu fyrir 55 ára og eldri

- Netveiðarárásir, þar á meðal tölvupóstar, SMS og símtöl þar sem árásarmenn þykjast vera bankar eða traustar stofnanir til að stela viðkvæmum gögnum.
- Falskar netverslanir og svik sem beinast að eldri borgarum með sviksamlegum tilboðum og vefsíðum.
- Auðkennisþjófnaður, þar sem persónuupplýsingar eru misnotaðar til að afla sér fjár eða þykjast vera fórnarlambið.
- Meðferð með stuttum myndböndum og rangfærslum, þar á meðal uppspunnum fréttum og undirmeðvituðum skilaboðum.



Ógnir á netinu fyrir 55 ára og eldri

- Ófullnægjandi viðhald upplýsingatækni, svo sem úreltur vélbúnaðarhugbúnaður og hunsaðar öryggisuppfærslur, sem leiðir til viðkvæmra kerfa.
- Svik sem nýta sér einmanaleika — svindlarar hefja falskar vináttubönd eða ástarsambönd.
- Óörugg samstilling milli tækja og óörugg geymsla lykilorða í vöfrum.
- Vaxandi ógn af svikum sem knúin eru af gervigreind, þar á meðal klónuðum röddum sem þykjast vera ættingja til að fá brýna fjárhagsaðstoð.
- Vaxandi áhætta vegna gervigreindar í vírusvarnarforritum, sem gerir stillingar og örugga notkun mikilvæga fyrir eldri borgara.



Co-funded by the
European Union



10 helstu áhyggjur samkvæmt sérfræðingum

Sérfræðingar bentu á helstu áhyggjur sem hafa mest áhrif á fólk 55 ára og eldra þegar það hefur samskipti við stafræna tækni.

Að taka á þessum áhyggjum er mikilvægt til að auka sjálfstraust þeirra og öryggi í daglegum athöfnum á netinu.



Hvatning

Þróun markvissra stuðnings- og þjálfunaráætlana.





10 helstu áhyggjur samkvæmt sérfræðingum

- **Erfiðleikar við að halda í viðmeð flækjustigi og hraðri þróun tækni.**
- **Ótti við að missa aðgang að persónuupplýsingum eða fjármálum og verða fórnarlömb svikamyllna.**
- **Vandræðieða missa sjálfstraust þegar ekki er hægt að nota tækni fyrir framan fjölskylduna.**
- **Ósjálfstæði á aðra (ættingja eða tæknimenn) sem hindrar að byggja upp sjálfstæði.**
- Öryggi almennings Wi-Fi, oft notað af eldri borgurum án **öryggisvitund**.



10 helstu áhyggjur samkvæmt sérfræðingum

- **Óöruggt lykilorðgeymslu**, eins og að nota vafra í stað lykilorðastjóra.
- **Stafræn samskiptikoma** í stað verðmætra samskipta augliti til auglitis, sem leiðir til félagslegrar einangrunar.
- Að slökkva á uppfærslum eða öryggiseiginleikum vegnaskortur á **skilningi**, sem gerir tæki berskjölduð fyrir veikleikum.
- Í **erfiðleikum með að breyta kerfinu**útlit, tákni eða óvæntir nýir eiginleikar.
- Vanhæfni til að þekkja **grunsamlegt eða breytt efni**, sem gerir eldri borgara viðkvæmari fyrir blekkingum.



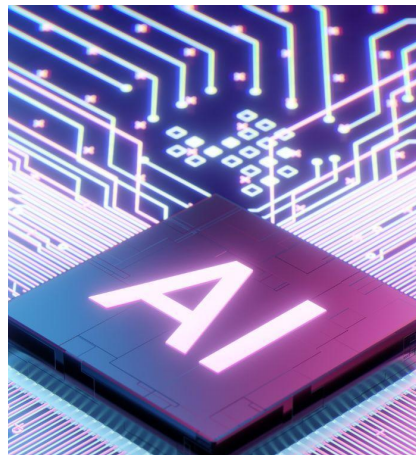
Co-funded by the
European Union



Helstu notkunarsvið gervigreindar og netáhætta

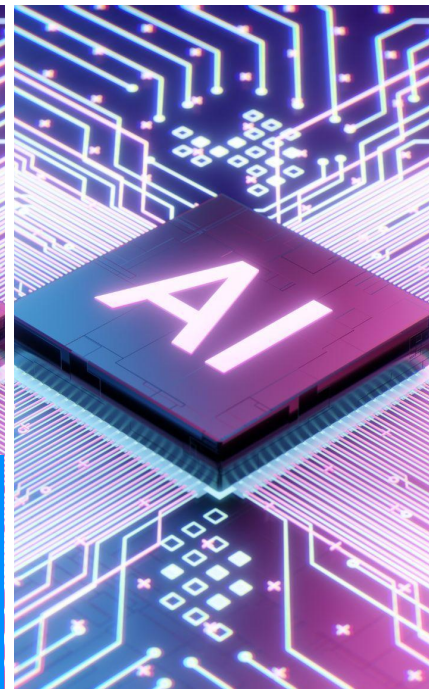
Gervigreind er í auknum mæli sambætt mörgum þáttum daglegs lífs, býður upp á verulegan ávinning en felur einnig í sér nýjar áhættur í netöryggi.

Að skilja helstu notkunarsvið gervigreindar og ógnir sem þeim tengjast er nauðsynlegt til að vernda viðkvæma hópa eins og fólk 55 ára og eldra.



Stuðningur

Til að veita skilvirkan stuðning þarf að auka vitund um áhættu sem tengist gervigreind.





Helstu notkunarsvið gervigreindar og netáhætta

- **Gervigreind í heilbrigðisþjónustu:** Fjarlæknisfræði, heilsufarseftirlit og þýðing fyrir samskipti við fjölskyldu.
- **Daglegur stuðningur:** Raddaðstoðarmenn gervigreindar, snjalltæki fyrir heimili, vírusvarnartól.
- Hætta á **gagnameðhöndlun**, djúpfölsunarárásir og dreifing rangupplýsinga.
- Gervigreindarvirktraddklónunað þykjast vera ættingja, sem leiðir til fjársvika.
- **Of mikil traust á gervigreindarverkfæri**án þess að skilja takmarkanir þeirra — gervigreind ætti að líta á sem verkfæri, ekki óskeikulan vald.



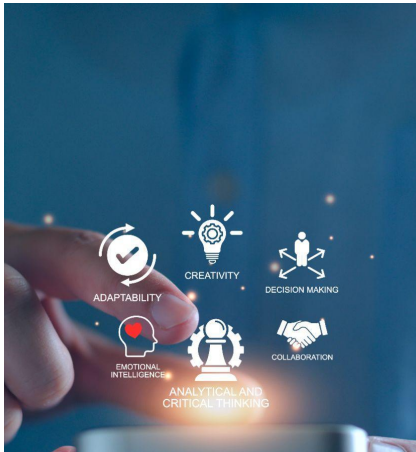
Co-funded by the
European Union



Mikilvæg hæfni fyrir eldri borgara

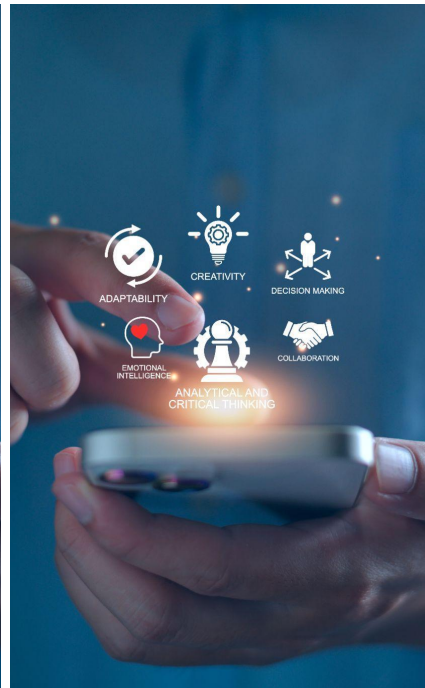
Það er mikilvægt að þróa nauðsynlega stafræna hæfni til að gera eldri borgara kleift að ferðast um netheiminn á öruggan og af öryggi.

Þessi færni hjálpar þeim að nýta tækni á skilvirkan hátt til að bæta daglegt líf sitt og seiglu gegn netógnum.



Hæfni

Gera eldri borgurum kleift að vernda sig betur og nota nútímatækni af öryggi.





Mikilvæg hæfni fyrir eldri borgara

- Að koma á fót sterkum, einstökum lykilorðum og **öryggisstjórnun** (forðastu geymslu í vafra, notaðu lykilorðastjóra).
- Virkjun **tvíþátta auðkenning** til að tryggja reikninga.
- Að skilja ogað **stilla vírusvarnarforrit**, sérstaklega verkfæri sem byggja á gervigreind.
- **Að viðurkennagrunsamlegt**, manipulerað eðasviksamlegt efni á netinu.
- **Að nota gervigreindaraðstoðarmenn** í reynd en samt sem áður gagnrýninn á niðurstöðurnar.
- Grunnatriði **stafræn læsi**: uppfærsla tækja, örugg vafratökn, örugg notkun Wi-Fi.
- **Að byggja upp sjálfstraust** til að draga úr ósjálfstæði gagnvart öðrum og styðja við áframhaldandi stafræna menntun.



Co-funded by the
European Union



Raunverulegar ógnir sem sérfræðingar hafa greint

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í algengar netógnir gervigreindar í daglegt líf aldraðra.



Ógnanir

Raunveruleg dæmi undirstrika mikilvægi þess að þekkja og draga úr netógnum.





Raunverulegar ógnir sem sérfræðingar hafa greint

- Dæmi: Eldri kona varð fyrir svikum þegar símtalandi notaði djúpfölsunartækni til að klóna rödd barnabarns hennar og bað um reiðufé sem hún afhenti sendiboða.
- Ástar- eða vináttusvindl sem nýta sér tilfinningatengsl, oft í gegnum skilaboð eða símtöl.
- Rangfærslur dreifast í gegnum myndbönd eða stutt skilaboð, sem gerir eldri borgurum erfitt fyrir að staðfesta áreiðanleika þeirra.
- Léleg viðhald upplýsingatækni eða notkun óöruggra neta sem leiðir til raunverulegra brota.



Co-funded by the
European Union



Raunverulegir ávinningar sem sérfræðingar hafa bent á

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í ávinninginn gervigreindar á daglegt líf aldraðra.



Kostir

Raunveruleg dæmi sýna fram á ávinning gervigreindar við að bæta lífsgæði og daglega virkni eldri borgara.





Raunverulegir ávinningar sem sérfræðingar hafa bent á

- 72 ára gömul kona notaði raddstýrðan gervigreindaraðstoðarmann til að þýða, sem gerði henni kleift að taka þátt í og skilja myndsímtöl fjölskyldunnar og finna sig hluti af alþjóðlegum samræðum.
- Eldri borgarar nota gervigreind til áætlanagerðar (t.d. ráðleggingar um Windows, heimagerðu hluti) eða spjallþjóna á Alzheimersdeildum.
- Gervigreind býður upp á persónulega ráðgjöf og styður við daglegt sjálfstæði, en virkar best þegar hún er notuð ásamt sterkum grunnfærni.



Co-funded by the
European Union



Úrslit - Ísland





Mest vitnað í netógnir fyrir 55 ára og eldri

Fólk 55 ára og eldra stendur frammi fyrir einstökum áskorunum í stafræna heiminum, sem gerir það viðkvæmt fyrir ýmsum ógnum á netinu.

Að skilja algengustu og áhrifamestu hættur er nauðsynlegt til að bæta vitund þeirra um netöryggi og vernd.



Ógnanir

Ógnir sem sérfræðingarnir hafa bent á þjóna sem orðasafn fyrir eldri borgara.





Ógnir á netinu fyrir 55 ára og eldri

- **Djúpfölsuð svik**með fölsuðum myndum og myndböndum, sérstaklega á WhatsApp, þar sem glæpamenn þykjast vera fjölskyldumeðlimir sem fullyrða að þeir þurfi á peningum að halda.
- Háþróað**phishing**þróaðist yfir í félagsverkfræði í gegnum skilaboðaforrit með sannfærandi fölsuðum símtölum og skilaboðum.
- **Ástarsvindlá** stefnumótasíðum sem beinast að einmana eldri borgara um allan heim, þar á meðal á Íslandi, sem leiðir til fjárhagslegs og tilfinningalegs tjóns.
- Líkamleg**teftirlíkingar af glæpamönnum**að þykjast vera tæknideildarfulltrúar eða fulltrúar bankans sem heimsækja heimili aldraðra.



Co-funded by the
European Union



10 helstu áhyggjur samkvæmt sérfræðingum

Sérfræðingar bentu á helstu áhyggjur sem hafa mest áhrif á fólk 55 ára og eldra þegar það hefur samskipti við stafræna tækni.

Að taka á þessum áhyggjum er mikilvægt til að auka sjálfstraust þeirra og öryggi í daglegum athöfnum á netinu.



Hvatning

Þróun markvissra stuðnings- og þjálfunaráætlana.





10 helstu áhyggjur samkvæmt sérfræðingum

- Erfiðleikar með flókininnskráningarferli þar á meðal kröfur um lykilorð og tíðar endurstillingar.
- Ruglingur og viðnám gegn tveggja þátta auðkenningu meðal eldri notenda.
- Léleg þekking á tölvupóstihindrar endurheimt lykilorðs.
- Lítil leturstærð og eldri símar sem takmarka notagildi og öryggiseiginleika.
- Skortur á skýrum leiðbeiningum frá þjónustu sem krefst rafrænna skilríkja eða svipaðrar auðkenningar.



10 helstu áhyggjur samkvæmt sérfræðingum

- Eldri borgararendurnýta **lykilorð** á mikilvægum síðum, sem gæti leitt til þess að reikningar verði í hættu.
- **Lénsvillur** að búa til sannfærandi falsa vefsíður til að stela viðkvæmum gögnum.
- Stöðugt óséðurmálamiðlanir um **persónuskilríki** frá eftirliti með dökka vefnum.
- **Almennt vantrausteða** misskilningur á ógnum í netöryggi sem hafa áhrif á viðbrögð eldri borgara.
- Hindranir skapaðar **aftækniflækjustigað** draga úr sjálfstrausti og sjálfstæði.



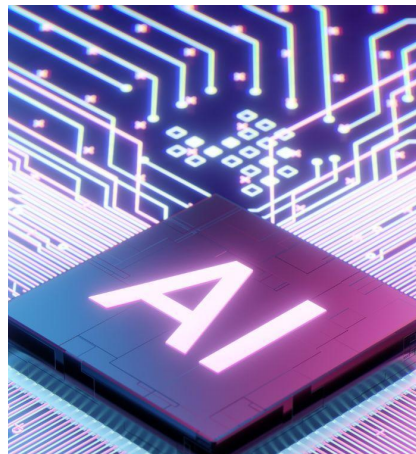
Co-funded by the
European Union



Helstu notkunarsvið gervigreindar og netáhætta

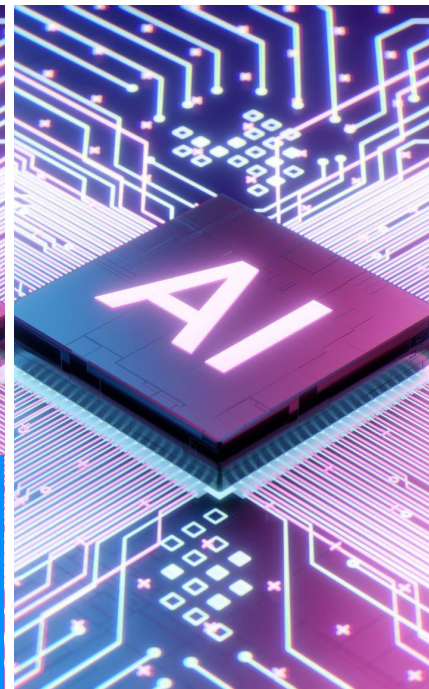
Gervigreind er í auknum mæli sambætt mörgum þáttum daglegs lífs, býður upp á verulegan ávinning en felur einnig í sér nýjar áhættur í netöryggi.

Að skilja helstu notkunarsvið gervigreindar og ógnir sem þeim tengjast er nauðsynlegt til að vernda viðkvæma hópa eins og fólk 55 ára og eldra.



Stuðningur

Til að veita skilvirkan stuðning þarf að auka vitund um áhættu sem tengist gervigreind.





Helstu notkunarsvið gervigreindar og netáhætta

- **Menntunum** hættuna á fölsuðu netefni sem gervigreind framleiðir, sérstaklega myndböndum sem fullyrða að neyðarástand sé í fjölskyldunni.
- **Ráðgjöf**dri borgarar að staðfesta áriðandi skilaboð með því að hringja beint í fjölskylduna og leggja áherslu á að raunveruleg neyðartilvik fela yfirleitt í sér símtöl, ekki smáskilaboð.
- **Meðvitundað** gervigreind geti hermt eftir hvaða gögnum sem er, þar á meðal myndböndum og myndum, sem krefst efasemda og annarra staðfestinga.
- Áhætta af völdum **ofdeilingu persónuupplýsinga** í gervigreindarspjallþjónum og tólum eins og ChatGPT, þar sem gögn eru geymd.
- Áhersla á **viðhalda gagnrýninni hugsun** og staðfesta upplýsingar í gegnum aðrar samskiptaleiðir.



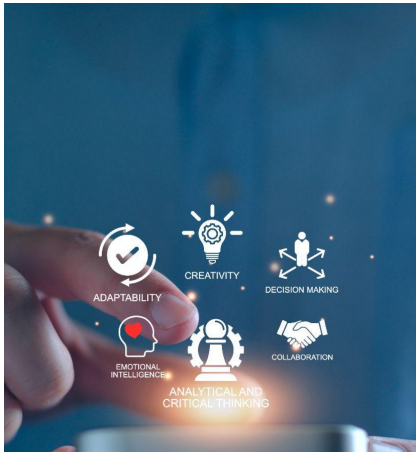
Co-funded by the
European Union



Mikilvæg hæfni fyrir eldri borgara

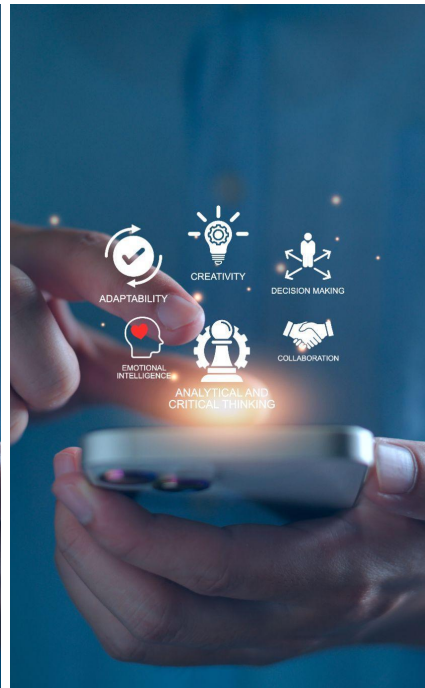
Það er mikilvægt að þróa nauðsynlega stafræna hæfni til að gera eldri borgara kleift að ferðast um netheiminn á öruggan og af öryggi.

Þessi færni hjálpar þeim að nýta tækni á skilvirkan hátt til að bæta daglegt líf sitt og seiglu gegn netógnum.



Hæfni

Gera eldri borgurum kleift að vernda sig betur og nota nútímatækni af öryggi.





Mikilvæg hæfni fyrir eldri borgara

- Að skilja **mikilvægi staðfestingar** áður en brýnum beiðnum er svarað í gegnum stafræna miðla.
- Grunnatriði **stafræn færni** þar á meðal örugg lykilorðastjórnun og vitundarvakning um áhættur gervigreindar.
- **Hæfni til að spyrja spurninga** og staðfesta óvænt eða tilfinningaþrungin skilaboð, sérstaklega þau sem virðast áríðandi eða kvíðvænleg.
- **Efahyggja** gagnvart áreiðanleika efnis á netinu, sérstaklega fjölmiðlum sem eru framleiddar með gervigreind.
- Að efla traustsbyggingu við fjölskyldumeðlimi fyrir **bein samskipti** og hjálp.



Co-funded by the
European Union



Raunverulegar ógnir sem sérfræðingar hafa greint

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í algengar netógnir gervigreindar í daglegt líf aldraðra.



Ógnanir

Raunveruleg dæmi undirstrika mikilvægi þess að þekkja og draga úr netógnum.





Raunverulegar ógnir sem sérfræðingar hafa greint

- Dæmi um fórnarlömb sem tapa sparnaði vegna djúpfölsunar ástarsvindla með því að nota gervigreindarframleiddar myndir af frægu fólki.
- WhatsApp-svik sem fela í sér falsa skilaboð um veika ættingja sem þurfa peningainnborgun, stundum stöðvuð með íhlutun fjölskyldunnar.
- Ástarsvindl á samfélagsmiðlum og stefnumótaforritum sem leiða til þess að eldri borgarar borga fyrir falska heilbrigðisþjónustu eða ferðast til útlanda fyrir maka sem ekki er til.
- Atvinnusvik þar sem kreditkortaupplýsingar eru stolnar með raddklónuðum sviksamlegum atvinnutilboðum.
- Dæmi um einstaklinga sem eru viðkvæmir og birta óvart skaðlegt efni á netinu án þess að skilja afleiðingarnar.



Co-funded by the
European Union



Raunverulegir ávinningar sem sérfræðingar hafa bent á

Sérfræðingar deildu raunverulegum dæmum sem sýndu bæði áhættu og ávinning af stafrænni tækni fyrir fólk 55 ára og eldra.

Þessi dæmi veita verðmæta innsýn í ávinninginn gervigreindar á daglegt líf aldraðra.



Kostir

Raunveruleg dæmi sýna fram á ávinning gervigreindar við að bæta lífsgæði og daglega virkni eldri borgara.





Raunverulegir ávinningar sem sérfræðingar hafa bent á

- Gervigreind aðstoðar eldri borgara við hagnýt ráð í daglegu lífi, svo sem þrif, viðgerðir á heimilum og skjót vandamálalausn.
- Gervigreindarspjallþjónar veita tilfinningalegan stuðning og félagsskap, eru tiltækir allan sólarhringinn til að lina kvíða og til að spjalla almennt.
- Notkun gervigreindartækja eins og ChatGPT til að staðfesta grunsamleg tölvupóst eða skilaboð sem tengjast netöryggi.
- Árangur innleiðingar gervigreindar er mjög breytilegur og fer eftir tæknifærni og trausti aldraðra á tækni.



Co-funded by the
European Union



Ógnir á netinu fyrir 55 ára og eldri - orðalisti





Netveiðar (sviksamleg tölvupóstskeyti, SMS, tenglar, símtöl)

Netveiðar eru tegund netárásar þar sem glæpamenn senda falsa tölvupósta, textaskilaboð, símtöl eða tengla sem þykjast vera einhver sem þú treystir, eins og banki eða vinur. Markmið þeirra er að blekkja þig til að gefa upp mikilvægar persónuupplýsingar eins og lykilorð, kreditkortanúmer eða bankareikningsupplýsingar. Þessi falsa skilaboð líta oft mjög raunveruleg út og reyna að fá þig til að bregðast hratt við með því að skapa tilfinningu fyrir brýnni þörf eða ótta. Árásarmennirnir vilja stela peningunum þínum eða sjálfsmynd með því að blekkja þig til að smella á hættulega tengla eða deila viðkvæmum gögnum. Til að vera öruggur skaltu alltaf tvíathuga hver sendi skilaboðin, forðast að smella á grunsamlega tengla og aldrei deila persónuupplýsingum nema þú sért alveg viss um að þær séu öruggar.



Djúpfölskunarárásir (falsað hljóð/myndband, að þykjast vera fjölskyldumeðlimur)

Djúpfalsaárásir fela í sér að búa til falsa hljóð- eða myndbandsupptökur með gervigreind sem líta út og hljóma mjög raunverulegar. Í þessum árásum herma glæpamenn eftir rödd eða andliti einhvers sem þeir þekkja, oft fjölskyldumeðlims, til að blekkja fólk til að trúa því að það sé að tala við ástvin. Til dæmis gæti svindlari notað djúpfalsatækni til að hringja símtal sem hljómar nákvæmlega eins og barnabarn sem biður um peninga áriðandi. Þessar falsu upptökur eru mjög sannfærandi og geta blekkst jafnvel varkára einstaklinga. Djúpfalsaárásir eru hættulegar vegna þess að þær nýta sér traust og tilfinningar, sem gerir það erfitt að átta sig á blekkingunni fyrr en það er of seint. Til að vernda sjálfan þig skaltu alltaf staðfesta óvenjulegar beiðnir með því að hafa samband við viðkomandi beint í gegnum mismunandi samskiptaleiðir áður en þú grípur til nokkurra aðgerða.



Falskar netverslanir og svik (falsaðar vefsíður)

Falskar netverslanir og svindl eru svikamyndir sem eru hannaðar til að líta út eins og lögmætar verslanir en eru í raun búnar til til að blekkja fólk til að kaupa vörur sem eru ekki til eða eru af lélegum gæðum. Þessar falsu verslanir afrita oft lógó, vörulýsingar og myndir frá raunverulegum fyrirtækjum til að virðast sannfærandi. Svindlarar nota þessar síður til að stela peningum og persónuupplýsingum frá grunslausum viðskiptavinum. Þeir lokka kaupendur með loforðum um mjög lágt verð eða sértíðboð sem virðast of góð til að vera sönn.

Þessar vefsíður gætu haft undarleg vefslóðir, innihaldið stafsetningarvillur eða skortir réttar tengiliðaupplýsingar. Eftir að viðskiptavinir hafa greitt fá þeir oft aldrei pöntunina sína eða fá falsaðar vörur. Til að vernda þig skaltu alltaf kaupa frá traustum verslunum, skoða umsagnir um vefsíður, forðast tilboð sem virðast óraunhæft ódýr og aldrei deila greiðsluupplýsingum á grunsamlegum síðum. Ef eitthvað virðist ekki rétt er betra að athuga það vel áður en þú kaupir.



Tilfinningaleg meðferð og félagsverkfræði (hræðsluátak)

Tilfinningaleg meðferð og félagsverkfræði fela í sér að blekkja fólk með því að spila á tilfinningar þess til að fá það til að hegða sér á þann hátt sem það myndi venjulega ekki gera. Netglæpamenn nota aðferðir eins og hræðslusögur, áríðandi hegðun, falskt vald eða góðvild til að skapa tilfinningu fyrir ótta, trausti eða skyldu. Til dæmis gætu þeir látið eins og þeir séu bankastarfsmaður sem varar þig við vandamáli með reikninginn þinn og hvatt þig til að bregðast hratt við, þannig að þú gefur viðkvæmar upplýsingar án þess að hugsa. Þessar aðferðir nýta sér náttúruleg mannleg viðbrögð - ótta, traust, forvitni eða hjálpssemi - sem gerir það erfitt að standast. Besta vörnin er meðvitund: að þekkja þessi tilfinningalegu brögð og stoppa til að staðfesta hver er í raun að biðja um upplýsingar áður en svarað er.



Auðkennisþjófnaður (með því að nota stolnar persónuupplýsingar)

Auðkennisþjófnaður þýðir þegar einhver stelar persónuupplýsingum þínum án þíns leyfis og notar þær til að bykjast vera þú. Þeir gætu notað nafn þitt, kennitölu, bankaupplýsingar eða aðrar upplýsingar til að opna reikninga, taka lán eða kaupa í þínu nafni. Þetta getur valdið miklum fjárhagsvandræðum og skaðað mannorð þitt.



Svik „á barnabarninu“ (svikarar þykjast vera fjölskylda í neyð)

Svik „á barnabarninu“, einnig þekkt sem „ömmu- og afasvindl“, er algeng aðferð sem glæpamenn nota þegar þeir þykjast vera fjölskyldumeðlimur – oftast barnabarn eða barn – í neyð. Þetta gerist venjulega í síma, þar sem svindlarinn hringir í eldri einstakling og fullyrðir að viðkomandi sé í alvarlegum vandræðum, svo sem að hafa lent í slysi, verið handtekinn eða þurfi á brýnni fjárhagsaðstoð að halda. Sá sem hringir biður oft um að peningar séu sendir fljótt og krefst þess að fórnarlambið haldi því leyndu, til dæmis með því að segja: „Ekki segja mömmu frá því, hún mun hafa áhyggjur.“

Þetta svindl spilar á tilfinningar eins og ást og umhyggju fyrir fjölskyldumeðlimum, sem fær viðkomandi til að vilja hjálpa strax án þess að stoppa til að hugsa. Í auknum mæli nota svindlarar tækni eins og gervigreind til að herma eftir rödd raunverulegs barnabarns, sem gerir símtalið mjög sannfærandi.



Falskar „hjálp“ beiðnir í gegnum WhatsApp eða Messenger

Falskar „hjálp“ beiðnir í gegnum WhatsApp eða Messenger eru svindl þar sem einhver þykist vera vinur eða fjölskyldumeðlimur í brýnum vandræðum og biður um peninga eða persónuupplýsingar. Þessi skilaboð koma oft óvænt frá óþekktum eða dulbúnum tengiliðum. Svindlarinn gæti sagt að hann hafi týnt símanum sínum, verið læstur úti af reikningnum sínum eða þurfi á neyðarfjárhagsaðstoð að halda. Þeir reyna að skapa tilfinningu fyrir brýnni þörf og trausti til að fá fórnarlömb til að bregðast hratt við án þess að athuga hvort það sé satt.



Ástarsvik og svik byggð á samböndum sem byggjast á netinu

Ástarsvindl eru tegund svika þar sem glæpamenn búa til falsa netprófíla og þykjast hafa ástarsamband við einhvern. Þeir byggja upp traust og tilfinningatengsl með tímanum, sem fær fórnarlambið til að halda að það sé í raunverulegu sambandi. Þegar þeir hafa öðlast traust, búa svindlarar til neyðarástand eða brýnar fjárhagslegar þarfir - svo sem læknisreikninga eða ferðakostnað - og biðja fórnarlambið um peninga eða gjafir.

Þessir svindlarar eru mjög færir í að virðast umhyggjusamir og traustir og forðast oft fundi augliti til auglitis eða myndsímtöl með því að afsaka sig. Þeir nýta sér einmanaleika og tilfinningalega varnarleysi, sem gerir fórnarlömb líklegri til að gefa þeim peninga.



Fjárfestingarsvik (falskar auglýsingar með frægu fólki)

Fjárfestingarsvik sem fela í sér falsa auglýsingar með frægu fólki er tegund svindls þar sem glæpamenn nota myndir, myndbönd eða nöfn frægs fólks til að láta fjárfestingartækifæri virðast lögmætt og traustvert. Stundum innihalda þessar auglýsingar djúpfölsk myndbönd sem sýna frægt fólk mæla með fjárfestingu, eða þær þykjast vera fréttir sem tengja frægt fólk við fjárhagslegan árangur á ákveðnum kerfum.

Svindlararnir blekkja fólk til að trúa því að það geti grætt hratt og mikinn hagnað, oft í dulritunargjaldmiðlum eða gjaldeyrisviðskiptum. Þeir lokka fórnarlömb til að stofna reikninga, leggja inn peninga og biðja síðan um meiri fjármuni til að greiða fölsuð gjöld eða skatta. Snemmbúnað endurgreiðslur geta verið sýndar til að öðlast traust, en þegar fórnarlömb reyna að taka út peningana sína eru þau lokuð og beðin um stórar viðbótargreiðslur.



Spilliforrit og ransomware (sýktar skrár, viðhengi)

Spilliforrit eru skaðleg forrit sem geta sýkt tölvuna þína eða símann og valdið skaða, svo sem að stela persónuupplýsingum þínum, skemma skrár eða taka stjórn á tækinu þínu. Ransomware er sérstök tegund af spilliforritum sem læsir eða dulkóðar skrárnar þínar og gerir þær óaðgengilegar þar til þú greiðir lausnargjald - venjulega í dulritunargjaldmiðli - til árársarmannsins. Ransomware getur komist inn í tækið þitt í gegnum sýkt tölvupóstviðhengi, illgjarnar vefsíður eða óörugg niðurhöl.

Þegar vírusinn hefur smitast kemur hann í veg fyrir að þú getir notað mikilvægar skrár og stundum krefst hann peninga til að endurheimta aðgang. Að greiða lausnargjaldið tryggir ekki að gögnin þín verði afhent og það hvetur glæpamenn til að halda áfram þessum árásum.



Óstaðfest forrit og óöruggar niðurhal á hugbúnaði

Óstaðfest öpp og óörugg niðurhal hugbúnaðar eru netógnir þar sem fólk hleður niður og setur upp forrit eða skrár frá óþekktum eða óáreiðanlegum aðilum. Þessi öpp eða niðurhal geta innihaldið falinn spilliforrit, vírusa eða njósnahugbúnað sem getur skaðað tækið þitt, stolið persónuupplýsingum eða veitt tölvuþrjótum óheimilan aðgang.

Þar sem þessi forrit eru ekki skoðuð eða samþykkt af traustum kerfum geta þau truflað öryggi tækisins, valdið hrunum eða gert þig berskjaldaðan fyrir svikum. Falsuð forrit geta litið út eins og raunveruleg, en þegar þau eru sett upp geta þau safnað gögnum þínum eða dreift skaðlegum hugbúnaði.



Að deila viðkvæmum gögnum með ókunnugum (myndum, upplýsingum)

Að deila viðkvæmum gögnum með ókunnugum, svo sem myndum eða persónuupplýsingum, er netógn þar sem fólk gefur upp persónuupplýsingar til óþekktra eða ótreysta einstaklinga á netinu. Þetta getur virst skaðlaust, eins og að deila mynd, en þessar upplýsingar geta verið misnotaðar til að stela persónuupplýsingum þínum, fremja svik eða skaða mannorð þitt.

Myndir geta afhjúpað heimili þitt, staðsetningu eða persónulegar venjur án þess að þú takir eftir því. Ókunnugir geta notað þessar upplýsingar til að blekkja þig eða til að svindla á þér. Til að vera öruggur skaltu aðeins deila persónuupplýsingum og myndum með fólki sem þú treystir, hugsa þig vel um áður en þú birtir á netinu og stilla persónuverndarstillingar til að takmarka hverjir geta séð upplýsingarnar þínar.



Gögn leka úr notkun úreltra tæki eða hugbúnað

Notkun úreltra tækja eða hugbúnaðar er netógn því gamlar útgáfur skortir oft nýjustu öryggisuppfærslur. Þessar uppfærslur sem vantar skapa veikleika, kallaða öryggisgalla, sem tölvuþrjótar geta auðveldlega nýtt sér til að fá aðgang að persónuupplýsingum þínum eða stjórna tækinu þínu. Þetta getur leitt til gagnaleka, þjófnaðar eða sýkingar af völdum spilliforrita.

Úreltur hugbúnaður hægir einnig á tækinu þínu og gæti hætt að virka með nýrri forritum, sem gerir dagleg störf erfiðari. Til að vernda þig er mikilvægt að uppfæra tækið og hugbúnaðinn reglulega með nýjustu uppfærslum og öryggisleiðréttingum. Þetta lokar öryggisgötum, heldur gögnunum þínum öruggari og tryggir að tækið þitt virki snurðulaust.



Fjöldaárásir með persónulegum hætti með gervigreind, sem beinast að notendasniðum

Fjöldaárásir með gervigreind eru netógnir þar sem árásarmenn nota gervigreind til að búa til mjög sérsniðin og sannfærandi skilaboð sem beinast að einstaklingum út frá persónuupplýsingum þeirra. Gervigreind greinir upplýsingar af samfélagsmiðlum, tölvupósti og opinberum aðilum til að búa til skilaboð sem virðast mjög kunnugleg og traustvekjandi fyrir skotmarkið.

Þessar árásir geta falið í sér persónulega netveiðatölvupósta eða skilaboð þar sem nafn fórnarlambsins, starf, nýleg athöfn eða áhugamál eru nefnd. Markmiðið er að blekkja fólk til að smella á illgjarn tengla, afhjúpa lykilorð eða millifæra peninga. Þar sem gervigreind lærir stöðugt og aðlagast verða þessar árásir áhrifaríkari og erfiðari að greina.



Rangfærslur um heilsu eða hættuleg læknisfræðileg ráð frá gervigreindartólum

Rangfærslur um heilsu eða hættuleg læknisfræðileg ráð frá gervigreindartólum eru netógn þar sem gervigreind býr til rangar, villandi eða skaðlegar heilsufarsupplýsingar. Fólk getur treyst gervigreindarspjallþjónum eða nettólum fyrir læknisfræðileg ráð, en stundum framleiða þessi kerfi rangar greiningar, leggja til óöruggar meðferðir eða dreifa fólkskum fullyrðingum um sjúkdóma.

Þessar rangfærslur geta leitt til þess að fólk fresti viðeigandi lækni meðferð, noti árangurslausar aðferðir eða grípi til skaðlegra aðgerða. Efni sem myndast með gervigreind getur hljómað mjög fagmannlegt og sannfærandi, sem gerir það erfitt að segja til um hvort ráðleggingarnar séu áreiðanlegar.



Svik sem nýta sér stafræna útilokun í borgaralegri og bankastarfsemi

Svik sem nýta sér stafræna útilokun í borgaralegri og bankastarfsemi eru ógnir sem beinast að fólki sem hefur takmarkaðan aðgang að eða þekkingu á stafrænni tækni. Þessi svik notfæra sér fólk sem á erfitt með að nota þjónustu ríkisins eða banka á netinu, stundum vegna þess að það skortir tæki, aðgang að internetinu, stafræna færni eða sjálfstraust.

Glæpamenn blekkja þessa einstaklinga með því að bjóða upp á falsa aðstoð við netferli eða með því að senda sviksamleg skilaboð sem líkja eftir opinberum stofnunum í von um að fórnarlömb deili viðkvæmum gögnum eða sendi peninga. Þar sem þetta fólk hefur minni úrræði eða stuðning til að bera kennsl á svikamyllur eru þau berskjaldaðri.



Skortur á fjölþátta auðkenningaraðferðum (einfölduð lykilorð, endurnotkun)

Skortur á fjölþátta auðkenningu (MFA) þýðir að aðeins er notað lykilorð – oft einfalt eða endurtekið á mörgum síðum – til að vernda netreikninga. Þetta er áhættusamt því ef einhver stelur eða giskar á lykilorðið þitt getur viðkomandi auðveldlega komist inn á reikningana þína.

Fjölþátta auðkenning bætir við auka öryggislagi með því að krefjast tveggja eða fleiri gerða auðkenningar. Til dæmis, eftir að þú hefur slegið inn lykilorðið þitt gætirðu slegið inn kóða sem sendur er í símann þinn eða notað fingrafaraskannan. Þetta gerir það mun erfiðara fyrir tölvuprjóta að fá aðgang að reikningnum þínum, jafnvel þótt þeir hafi lykilorðið þitt.



Tap á aðgangi að mikilvægum þjónustum vegna tæknibreytinga (aðgangur eingöngu í gegnum app, takmarkaðir valkostir)

Aðgangur að mikilvægri þjónustu tapast vegna tæknibreytinga þegar mikilvægar opinberar eða bankaðjónustur færast yfir í stafrænt form, svo sem öpp eða netgáttir, án þess að auðvelt sé að nota þær. Þetta þýðir að fólk sem ekki býr yfir snjallsíma, tölvum eða stafrænni færni getur átt erfitt með eða ekki fengið aðgang að nauðsynlegri þjónustu eins og heilbrigðistíma, lífeyrisréttindum eða bankaviðskiptum.

Þessi stafræna breyting getur útilokað marga, sérstaklega eldri fullorðna eða þá sem hafa takmarkaðar auðlindir, sem gerir þá háða öðrum eða ófæra um að klára mikilvæg verkefni.



Sjálfvirk stjórnun á samfélagsmiðlum, sem veldur rangfærslum og streitu

Sjálfvirk stjórnun á samfélagsmiðlastrauma er netógn þar sem tölvuforrit, kölluð vélmenni, og gervigreind stjórna því hvaða efni þú sérð á samfélagsmiðlum þínum. Þessi kerfi greina hvað þér líkar, deilir eða skrifar athugasemdir við og sýna þér síðan fleiri svipaðar færslur til að halda þér við efnið.

Því miður er hægt að nota þetta til að dreifa rangfærslum, falsfréttum eða öfgafullu efni sem veldur streitu, ótta eða reiði. Bots geta óeðlilega aukið vinsældir slíkra færslna með því að líka við, deila eða skrifa athugasemdir, sem gerir það að verkum að margir eru sammála þeim.