Tölvuöryggisfræðsla – í nútíð og framtíð

Ari Kristinn Jónsson
AwareGO

Tölvuöryggi er lykilviðfangsefni

Allt er stafrænt í dag

- Stjórn innviða samfélags
  - Rafmagn, vatn, gas, olía,...
  - Samskipti, gagnamiðlun,...
- Eignir og réttindi
  - Skráning fasteigna, verðbréfa,...
  - Réttindi, leyfisveitingar,...
- Heilbrigðiskerfi
  - Nútíma tæki á spítölum
  - Stjórnun mannafla og aðgerða
  - Sjúkragögn einstaklinga
- Persónulegt líf
  - Minningar, afþreying,...

Afleiðing: Stafræn glæpastarfsemi

- Upphaflega: Hakkarar
  - Einstaklingar að hakka kerfi
  - Forvitni, illvilji, sýna hvað þau geta
- Í dag: Skipulögð glæpastarfsemi
  - Hugbúnaður og kerfi til staðar
  - Skipulagðar stórar árásir
  - Marglaga starfsemi í gróðaskyni
- Í dag: Stafrænn hernaður og njósnir
  - Rannsóknir og þróun
  - Skipulögð innbrot og árásir
  - Leið til að stela upplýsingum
  - Leið til að veikja andstæðinga

Tölvuöryggi er lykilviðfangsefni

Skaði vegna tölvuglæpa vex hratt

- Flest fyrirtæki eru tengd við internetið
- Tölvukerfi eru yfirleitt tengd innbyrðis
- Það þarf bara einn notenda með aðgang til að hleypa inn spilliforriti
- Tjón vegna tölvuglæpa er í dag yfir **$1.000.000.000.000 á ári**
- 945 milljarðar dollara árið 2020 – McAfee Vex hratt ár frá ári

Tölvuöryggi er lykilviðfangsefni

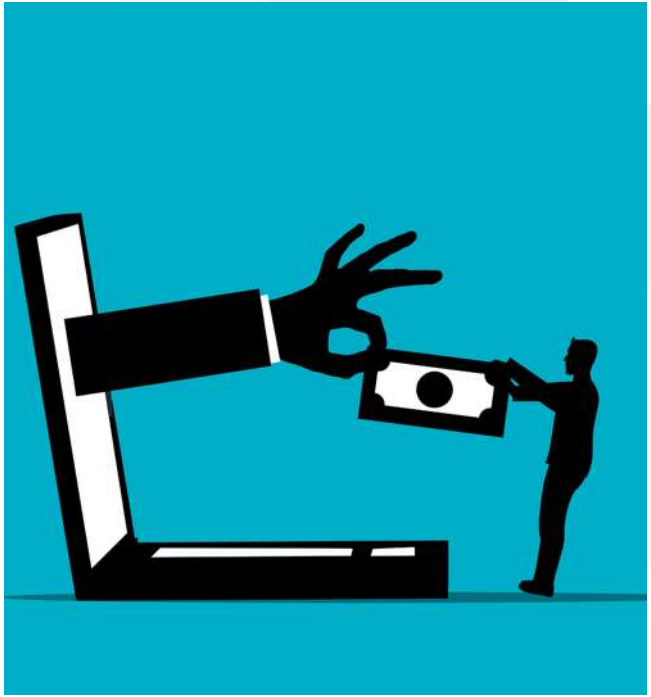
Starfsfólkið er lykillinn að tölvuöryggi

- Tæknilegar lausnir hafa verið til í áratugi
  - Eldveggir, vírusavarnir, o.fl.
- 85% innbrota nýta sér starfsfólk fyrirtækjanna
  - Hlaða niður spilliforritum/njósnaforritum
  - Millifæra fjármuni á fölskum forsendum
  - Veita aðgang að viðkvæmum gögnum
  - Gefa upp aðgangsorð
  - o.s.frv.
- Af hverju að eyða tíma í að hakka vel varin kerfi þegar hægt er að fá starfsfólk til að hleypa sér inn?

Tölvuöryggi er lykilviðfangsefni

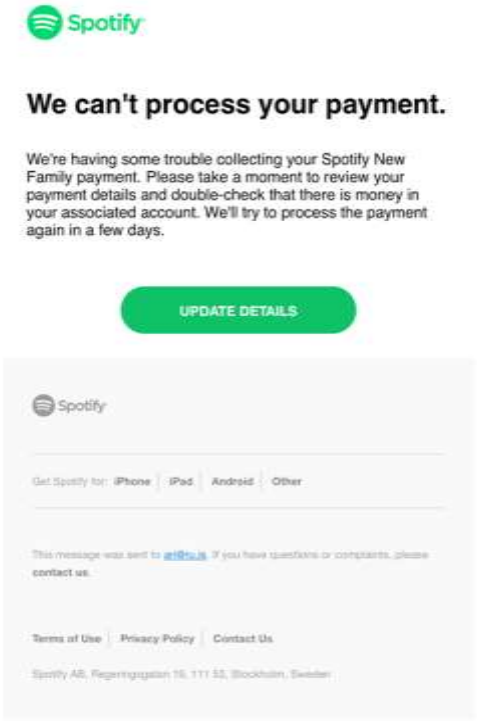
Nokkur nýleg dæmi

- Colonial Pipeline
  - Komust líklega inn með svikatölvupósti
  - Stálu gögnum og lokuðu kerfum
  - Fengu 4,4 milljónir dollara í lausnargjald
  - Dæmi um „phishing“
- Toyota Boshoku Corporation
  - Notuðu veiðipósta á valið starfsfólk
  - Plötuðu til að millifæra 37 milljónir dollara
  - Dæmi um „spear phishing“
- FACC
  - Komust líklega inn í tölvupósthólf forstjóra
  - Sendu tölvupósta á fjármáladeild í nafni forstjóra og óskuðu eftir millifærslum
  - Samtals 42 milljónir evra töpuðust
  - Dæmi um „CEO Scam“



Hvernig er verið að “hakka” fólk?

“Phishing” er klassíska dæmið

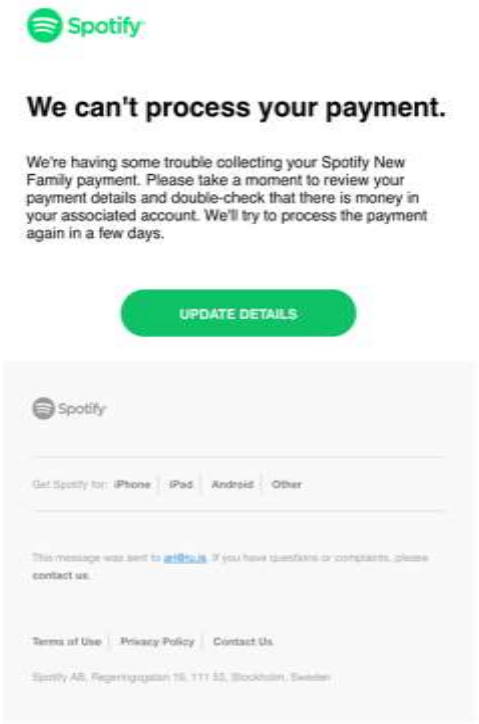


Þetta er raunverulegur
og réttur póstur frá Spotify

awarego

Hvernig er verið að “hakka” fólk?

“Phishing” er klassíska dæmið



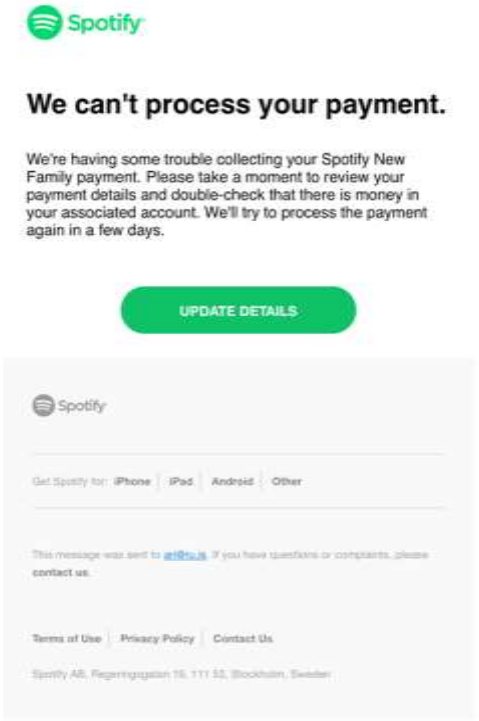
Þetta er raunverulegur
og réttur póstur frá Spotify

Þetta er “phishing” póstur
sem ég fékk – augljóst!

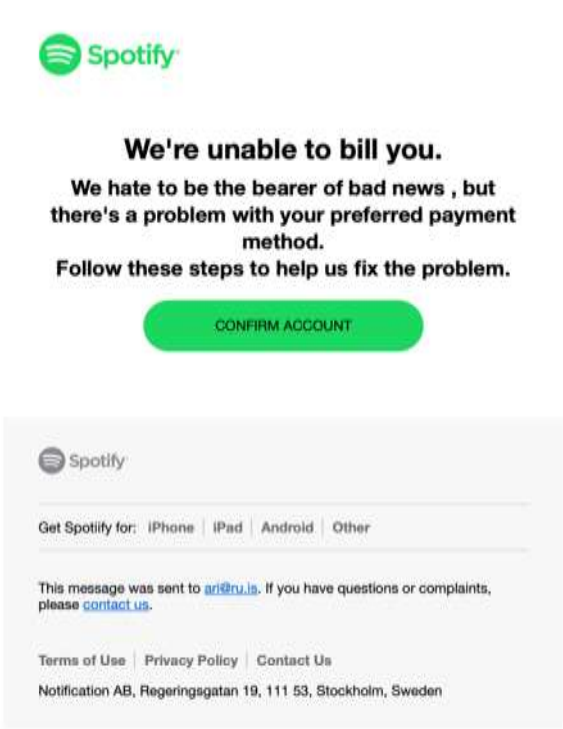
awarego

Hvernig er verið að “hakka” fólk?

“Phishing” er klassíska dæmið



Þetta er raunverulegur
og réttur póstur frá Spotify



Þetta er líka “phishing” póstur
sem ég fékk – alls ekki augljóst!

awarego

Hvernig er verið að “hakka” fólk?

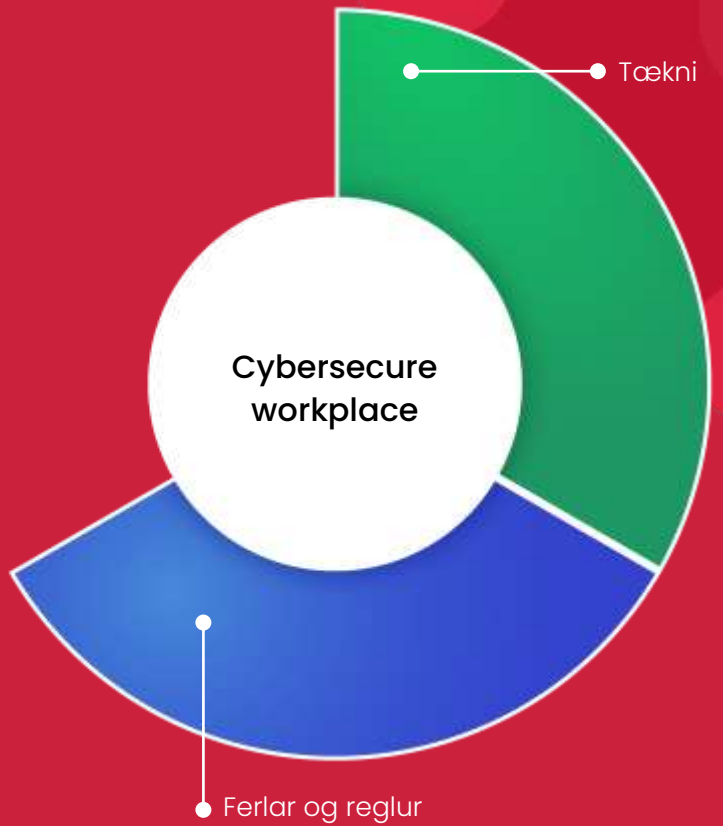
Það er svo margt fleira til

- “Spear Phishing”
- “Pretexting”
- “Scareware”
- ”CEO scam”
- “Website masking/hacking”
- “Spyware”
- “Ransomware”
- “USB drops”
- “Fake WiFi”
- ”WiFi Sniffing ”
- “Unattended computers”
- “Mixed work”

Vandamálið

Áhersla á tækni og reglur

- Treystum um of á tæknina
  - Eldveggi
  - Póstsíur
  - Vírusvarnir
  - o.s.frv.
- Treystum of mikið á reglur
  - Form lykilorða
  - Líftími lykilorða
  - Aðgangsstýringar
  - o.s.frv.
- Dugar því miður ekki til

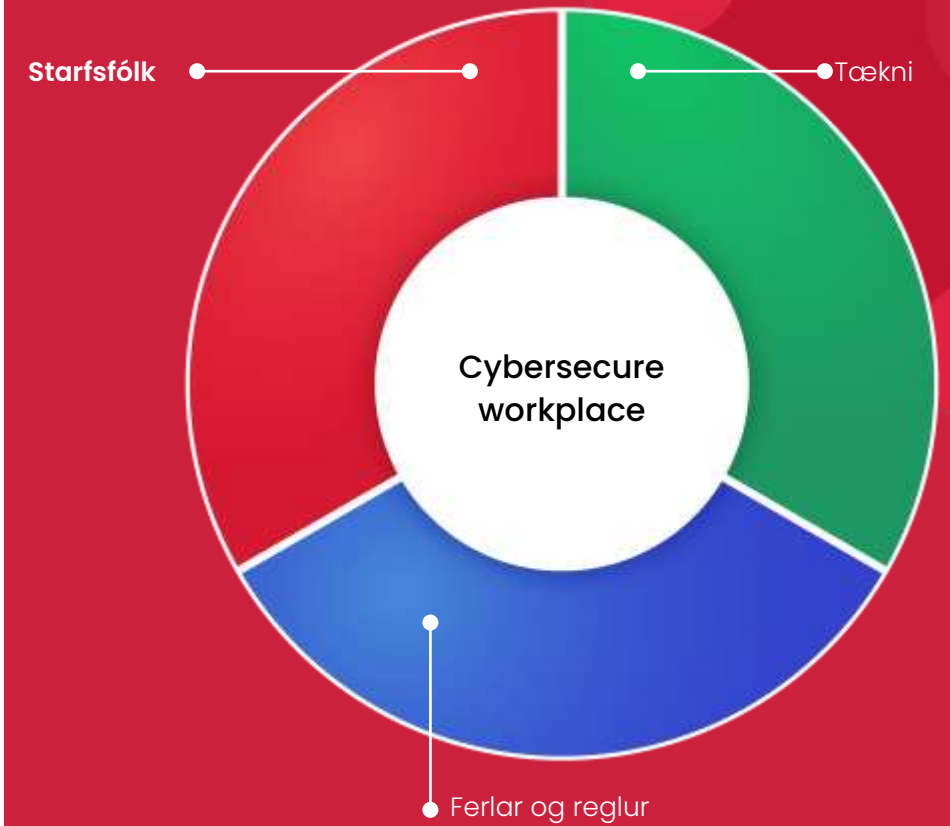


Vandamálið

Þarf að loka gatinu

- Fræðsla starfsfólks er lykilatriði
  - Þekkja “phishing” pósta
  - Gæta sín með nettengingar
  - Hugsa sig um áður en er millifært eða gögnum deilt
  - o.fl.

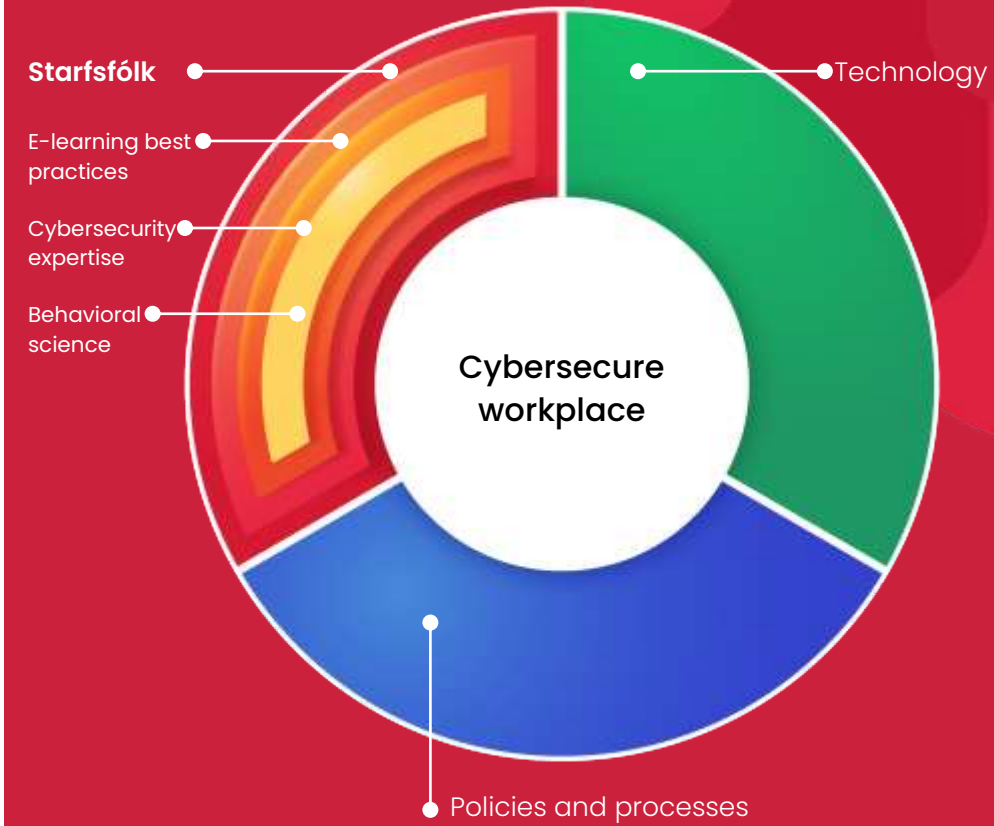
- Hegðun mikilvægari en þekking
  - Hvernig bregst það við?
  - Hvenær efast það?
  - Hvernig hagar það sér?



Þekking og hegðun starfsfólks varðandi tölvuöryggi

Nálgun AwareGO

- Nýtum þekkingu á tölvuöryggi
  - Nýjustu hættur
  - Veikleikar í kerfum
  - Aðferðafræði þrjóta
  - Breytingar á vinnustöðum
- Skilningur á mannlegri hegðun
  - Skapa tengingar
  - Vekja umhugsun
  - Breyta hegðun
- Nýta bestu stafrænu tólin
  - Meta þekkingu og hegðun
  - Þjálfa og breyta hegðun



awarego

Hefðbundin aðferðafræði

- Fyrirlestrar í sal eða á netinu
  - Allt upp í klukkutíma langir
  - Áhersla á þekkingu
  - Krefjandi að halda athygli
  - Tengir misvel við hegðun
- Kostnaðarsamt fyrir fyrirtæki
  - Tími starfsmanna
  - Ánægja starfsmanna
- Hentar illa sveigjanlegri vinnu og nýjum kynslóðum

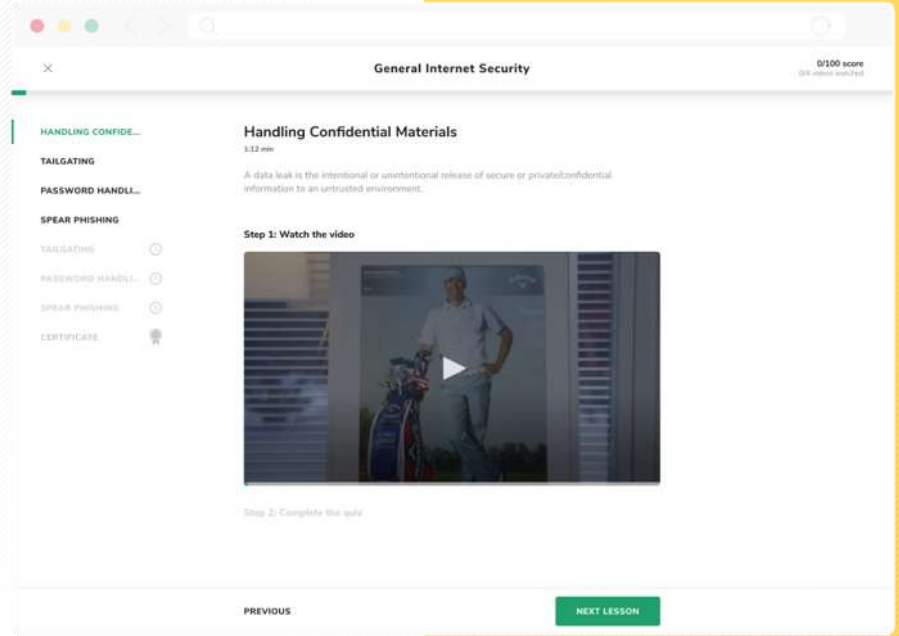
Laurentius de Voltolina – from “L*iber ethicorum des Henricus de Alemannia”*

AwareGO

Öryggisþjálfun í smáskömmtum

- **Skilvirk** 60 sekúndna myndbönd
- **Hnitmiðaðar** spurningar til eftirfylgni
- Leikin atriði eru **eftirminnileg** og hafa áhrif
- **Grípa athygli** með sögu og húmor
- Yfir **70 viðfangsefni** í tölvuöryggi
- Fyrir alþjóðlegan markað: **18 tungumál**

- Auðveld stjórn á hver fær hvaða þjálfun
- Dreift gegnum: email, Slack, Teams, o.fl.



awareGO

Öryggisþjálfun í smáskömmtum

Viðbrögð starfsmanna. Elska þetta!

Is training meeting your expectations?	91%	9%	0%
Do you like the content?	86%	14%	0%
Is the information actionable?	85%	15%	0%
Would you recommend it to colleagues?	100%	0%	0%

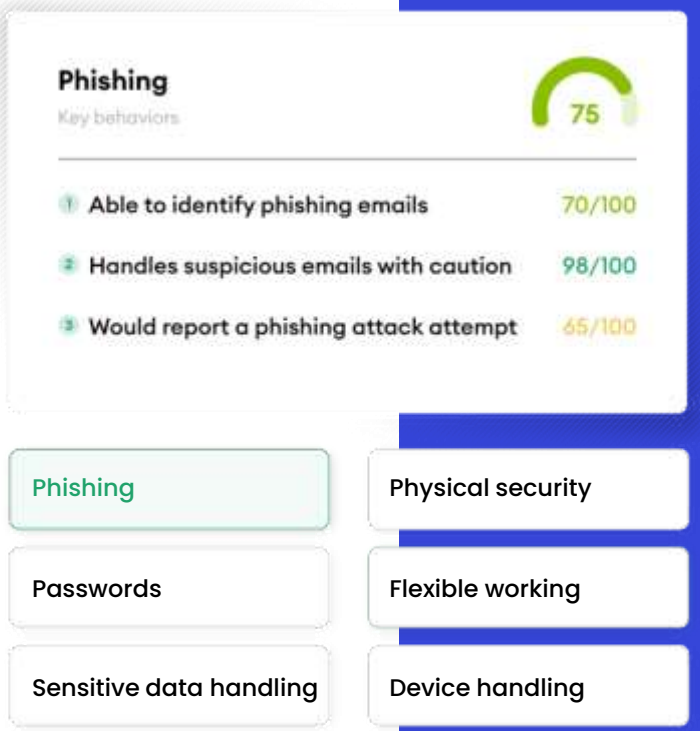
CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

awarego

Þjálfun er ekki nóg

Þarf að meta mannlega áhættuþáttinn

- Meta þarf alla áhættuþætti í tölvuöryggi **ekki bara „phishing“**
- Nauðsynlegt að greina milli **þekkingar og hegðunar**
- Skilningur á ólíkum starfsmönnum **sparar tíma og orku** – hver þarf þjálfun í hverju!
- Meta áhrif þjálfunar og bregðast hratt við nýjum hættum

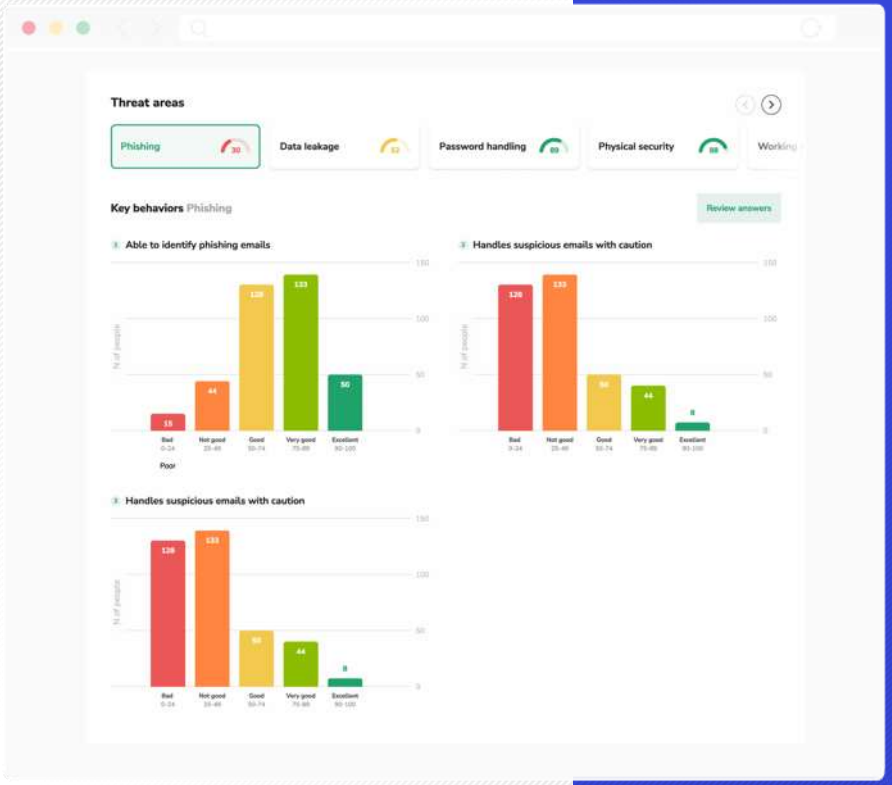


awarego

AwareGO

Fá skýra mynd af áhættu

- Bera kennsl á **hvar áhættan er** (eftir deildum, hlutverkum,...)
- Hafa **skýra mynd af áhættu** í fyrirtækjum – fyrir stjórnendur og fyrir stjórn
- Stýra þjálfun og fræðslu í eftir þörf frekar en tilfinningu - **gagnadrifin þjálfun**
- Yfirsýn yfir þróun áhættuþátta, þ.m.t. fyrir nýjar hættur



awarego

AwareGO

Heildarlausn fyrir mannlega þáttinn í tölvuöryggi

Human Risk Assessment

Meta mannlega áhættuþáttinn með tilliti til fjölda ólíkra áhættuþátta í tölvuöryggi

Security Awareness Training

Bæta meðvitund starfsmanna og breyta hegðun til að auka tölvuöryggi verulega

- Nýtist til að taka ákvarðanir um þjálfun o.fl.
- Skýr mynd af áhættuþáttum í fyrirtækjum, deildum og hlutverkum
- **Áhrifaríkt:** Heur raunveruleg áhrif á hegðun starfsfólks
- **Skilvirkt:** Stutt og hnitmiðað – kennir bara það sem þarf

- Keyrir í skýinu
- Auðvelt að tengja við önnur kerfi
- Uppfyllir kröfur fyrir vottanir
- Vinnur með öðrum hugbúnaði

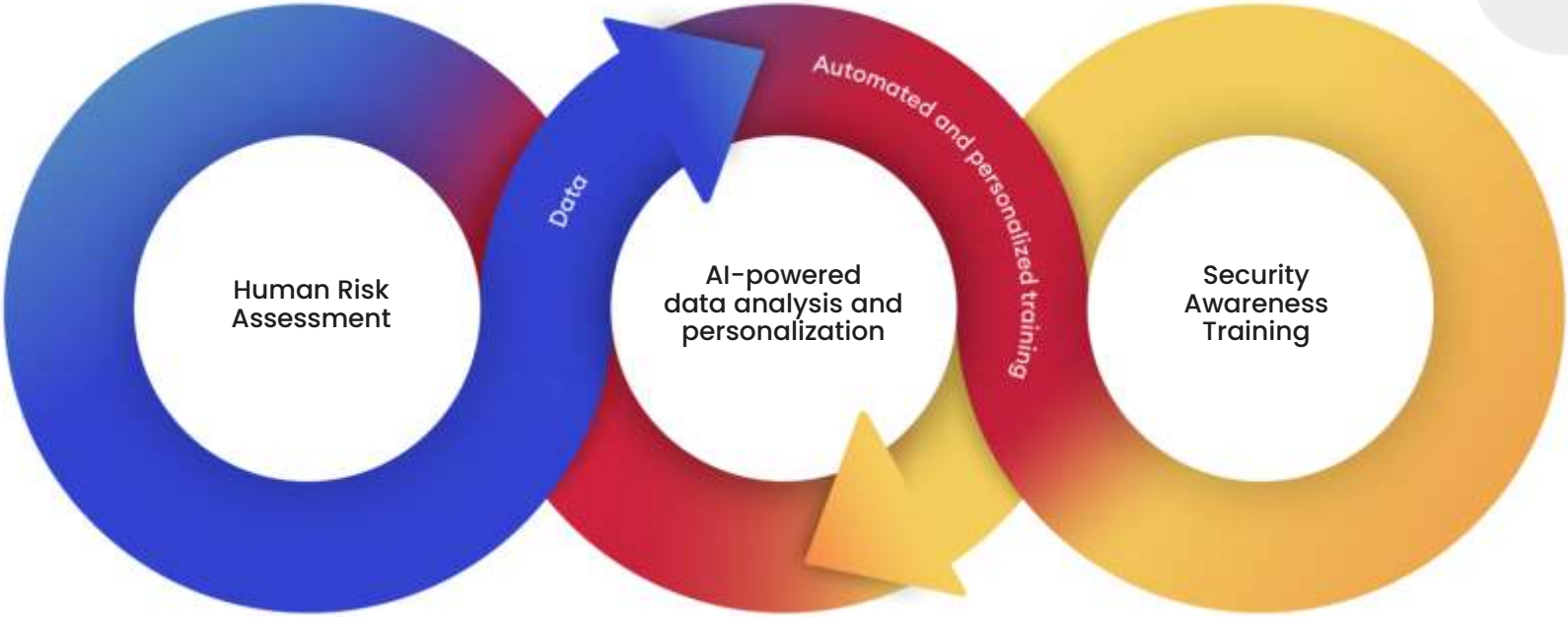
awarego

Hagnýta gögn frá mati, þjálfun og öðrum hugbúnaði

- Fræðslan í dag er handstýrð
  - Ákveða hver fær hvaða þjálfun
  - Ákveða hvenær þarf endurþjálfun
  - Yfirleitt gert fyrir stóra hópa í einu
- Það er hægt að gera betur
  - Gögn til um hvern og einn einstakling
  - Virkni í fræðslu og frammistaða í mati
  - Önnur kerfi geta líka lagt til gögn
- Hagnýta gögnin með gervigreind
  - Læra hverjir læra hvað hvernig
  - Læra hversu hratt fólk gleymir
  - Læra hversu hratt fólk lærir
  - Læra hverjir þurfa að kunna hvað
- Markmið: Einstaklingsmiðuð fræðsla
  - Kenna það sem þarf þegar það þarf

Framtíðarsýn

Gervigreindarstýrð fræðsla



“Nú er kominn tími til að minna Jón á að vara sig á svikapóstum.”

Takk fyrir!

Ari Kristinn Jónsson
CEO – ari@awarego.com

awarego