Secura

A BUREAU VERITAS COMPANY

CYBERSECURITY: AWARENESS EN GEDRAG VOOR HET HOOGHEEMRAADSCHAP

3 APRIL 2024

INGE WETZER

Inge Wetzer
Principal psychologist
Cybersecurity & compliance

Een psycholoog? Over cybersecurity?

WAAROM CYBERSECURITY?
IMAGOSCHADE

Mogelijk lekte alweer informatie Defensie uit

Defensie-personeel heeft mogelijk weer vertrouwelijke informatie gelekt. Een medewerker wisselde muziekbestanden uit, en stelde zo ook andere informatie op zijn computer beschikbaar.

Volgens de Telegraaf gaat het onder meer om formele correspondentie van het koninklijk huis, adressen van leden van het koningshuis en verslagen van telefoongesprekken binnen het Korps Mariniers.

Door Tim Wijkman-van Aalst

13 apr 2023 om 09:31 178 reacties

Energiebedrijf Vattenfall heeft een mogelijk datalek ontdekt in zijn systemen. De kans bestaat dat de gegevens van ongeveer 30.000 klanten zijn uitgelekt. Zij zijn per e-mail geïnformeerd.

Secura
A BUREAU VERITAS COMPANY

WAAROM CYBERSECURITY?
FINANCIËLE SCHADE & BUSINESS CONTINUITY

Ransomware kostte Universiteit Maastricht bijna twee ton: 'we moesten wel betalen'

Plotseling, eind december, zat de Universiteit Maastricht op slot. Getroffen door ransomware. Nu, ruim een maand later, vertelt de universiteit het complete verhaal. Er is betaald, en ook het bedrag mag de buitenwereld weten.

Veiligheid

© ANP

Wereldwijde hack legt bedrijven en Rotterdamse terminal plat

UPDATE | Voor de tweede keer in korte tijd hebben computercriminelen tientallen bedrijven lamgelegd met een wereldwijde ransomware-aanval. In Nederland liggen twee grote containerterminals in de Rotterdamse haven sinds gistermiddag stil. Ook farmaceut MSD, pakketbezorger TNT en de 38 vestigingen van bouwmaterialenleverancier Raab Kärcher zijn getroffen.

Secura
A BUREAU VERITAS COMPANY

WAAROM CYBERSECURITY?
PERSOONLIJKE CONSEQUENTIES

Nieuwe app Forum lek: privégegevens alle 92.000 (oud-)leden op straat

Door Daniël Verlaan
1 december 2022 15:56 • Aangepast 2 december 2022 09:22

Net binn
21:06 Sparta penalty
20:56 Pizzabe overled Emmen
20:50 Spits Be van Rec
20:42 Van Bor landstit
20:40 Succest met thu

Door een lek in de dit weekend gelanceerde ForumApp van Forum voor Democratie ligt de hele ledenadministratie op straat. Daarin staan de privégegevens van 92.901 leden en oud-leden. Het gaat onder meer om namen, woonadressen, telefoonnummers en rekeningnummers.

NOS NIEUWS • ECONOMIE • GISTEREN, 20:04

Als je bedrijf platligt door ransomware: 'Klanten stonden met knuppels op de stoep'

Lege kaasschappen in een Albert Heijn na een ransomware-aanval NOS

Secura
A BUREAU VERITAS COMPANY

SOMS DOOR HET HANDELEN VAN 1 MEDEWERKER

Pensioenfonds ABP lekt mailadressen die in verkeerde veld geplakt zijn

3 juni 2023 14:00 • Aangepast 3 juni 2023 14:00

Foto ter illustratie.

Pensioenfonds ABP heeft per ongeluk de e-mailadressen gelekt van 500 gepensioneerden. Het fonds spreekt van een 'menselijke fout'. De e-mailadressen zijn ingevuld in het verkeerde veld, zegt het ABP. In plaats van in het zogeheten BCC-veld werden ze in het CC-veld ingevoerd.

DAAROM CYBERSECURITY

Processen

Hoe ziet het beleid eruit?

Techniek

Wat is technisch mogelijk?

Mens

Wat wordt van de medewerkers verwacht?

WETEN WAT JE VERWACHT VAN MEDEWERKERS

Vaak wordt mensen verteld wat we van ze willen zien

Ze worden geïnformeerd en geïnstrueerd

Conclusie: mensen zijn de zwakste schakel in cybersecurity

Maar… weten wat je verwacht van medewerkers is niet hetzelfde als in staat zijn dit gedrag te beïnvloeden!

Kijk eens naar het dagelijks leven…

Na jaar verbod

Fietsers negeren verbod en appen er nog volop op los

02 juli 2020 16:02
Aangepast: 02 juli 2020 20:42

Archieffoto.

Het is al een jaar verboden, maar toch wordt er nog steeds veel gebeld en geappt op de fiets. En dat is de politie en de Tweede Kamer een doorn in het oog. "Het is voor iedereen de gewoonste zaak van de wereld. En het is heel erg lastig om dat om te draaien", zegt Egbert-Jan van Hasselt, de hoogste verkeersagent tegen RTL Nieuws.

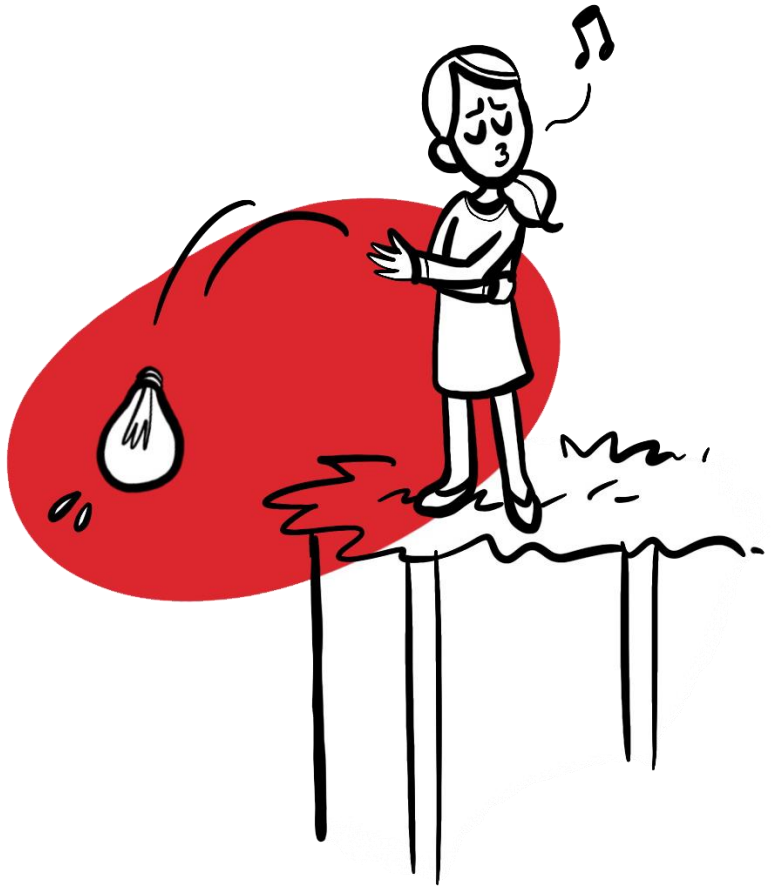
Alsof het een normale zomerdag was op het strand van Noordwijk: ‘Wat moeten we anders doen?’

VIDEO **Op een stralende Hemelvaartsdag besloot Nederland massaal naar het strand te gaan. Op sommige plekken was het zó druk, dat gemeenten de toegangswegen afsloten. Ook het strand van Noordwijk werd overspoeld door zonaanbidders.**

Tijdens Hemelvaartsdag trokken mensen in groten getale naar het strand, ondanks de dreiging van besmetting met het coronavirus. © Marco Okhuizen

WETEN WAT JE MOET DOEN

BETEKENT NIET DAT JE HET OOK DOET



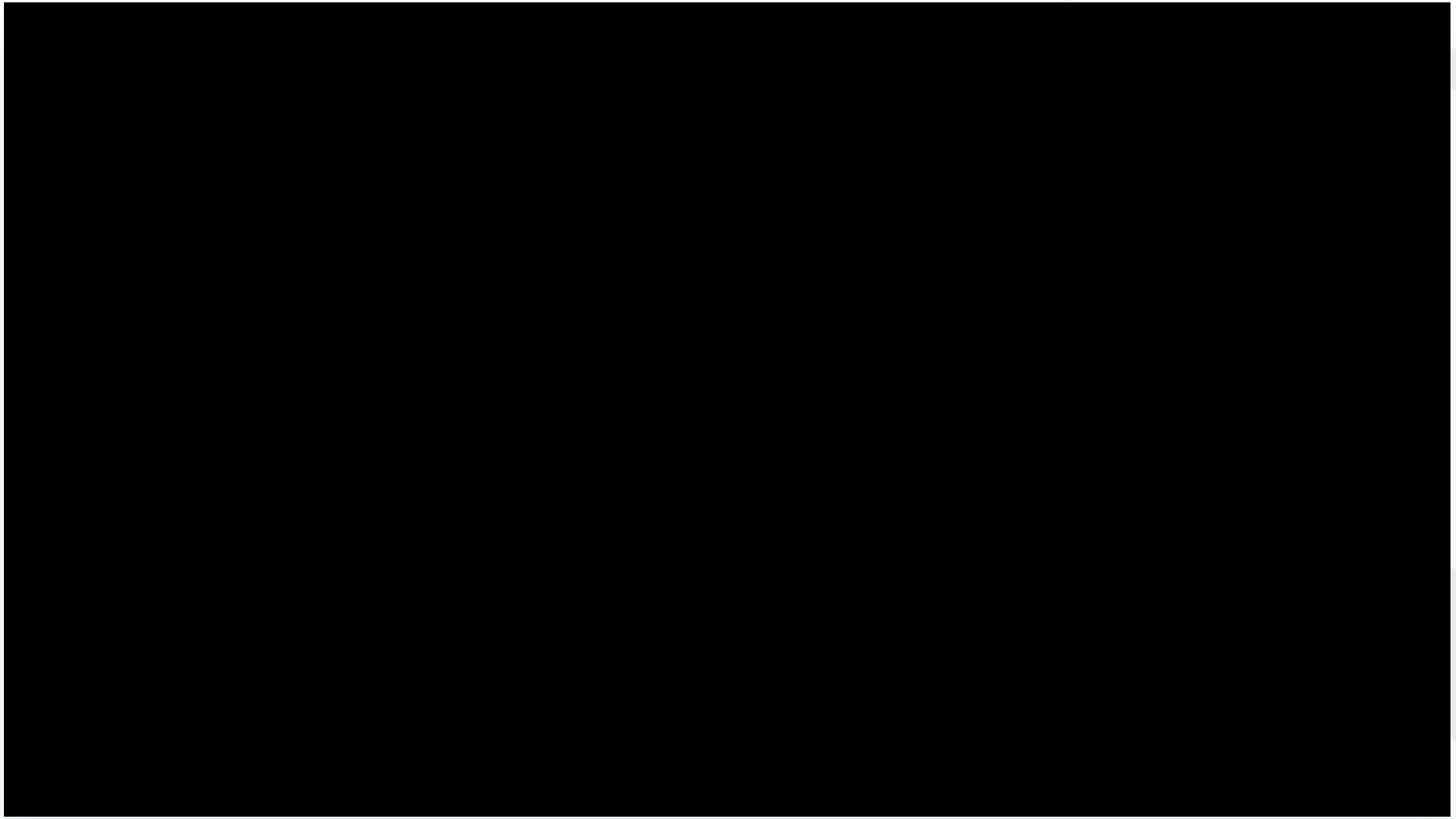
AWARENESS EN GEDRAG IN CYBERSECURITY

Awareness: je mag je wachtwoord niet geven via de telefoon

Strak protocol

- ‘gewoon’ vragen

FILMPJE



AWARENESS EN GEDRAG IN CYBERSECURITY

Toch twijfel?

Plan b

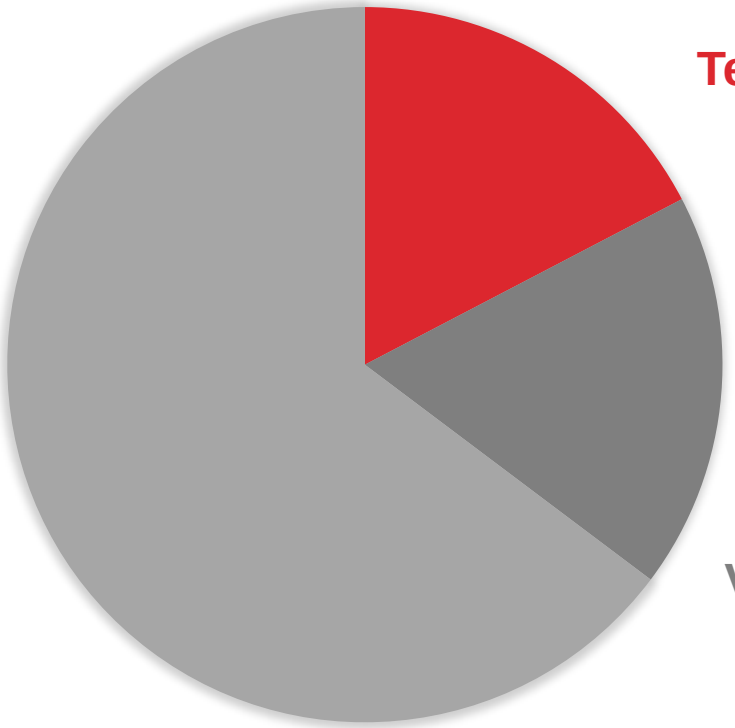
- Via website

We hebben jouw account gecontroleerd

- Onverwachte activiteit geregistreerd op account
  Accountcontrole uitvoeren
- Antivirus geverifieerd
- Instellingen geverifieerd

Voer accountcontrole uit

CIJFERS



35%
deelde
wachtwoord

Secura
A BUREAU VERITAS COMPANY

GEDRAG IS MEER DAN KENNIS

gedrag	=	capaciteit	×	motivatie	×	gelegenheid
						
interventie	=	leren	×	motiveren	×	faciliteren

STERKE WACHTWOORDEN

HOE KRAAKT EEN HACKER?

Woordenboekwoorden! + Films, nieuws… etc… (Secura's database bevat er 5,1 miljard…)

- Hoofdletter vooraan
- Cijfers aan het eind… Jaartallen…
- Evt gevolgd door !?
- Een bestaand woord/naam
- Evt a vervangen door @, e door 3, o door 0 etc…

= 1 triljoen opties

NIET IN DE DICTIONARY ATTACK?

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

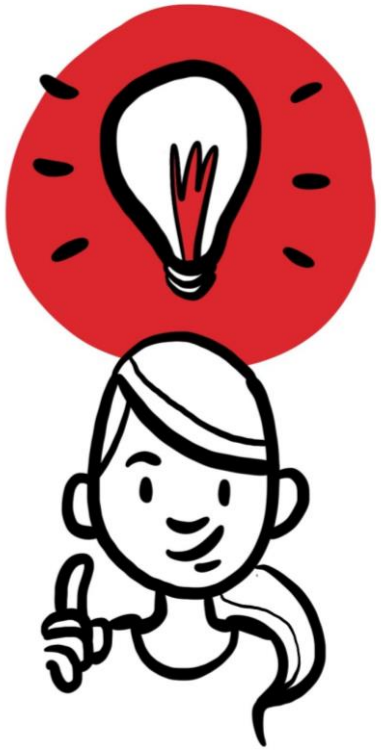
› Learn how we made this table at hivesystems.io/password

WAT VOOR WACHTWOORD DUS?

Hoe maak je dan wèl een sterk wachtwoord dat

1. niet te raden is, en
2. je ook nog kunt onthouden?

Twee opties!



HOE MAAK JE ZO'N WACHTWOORD?

Gebruik de eerste letters van een goed te onthouden zin

Mijn kinderen heten Jip en Janneke en zijn 6 en 8 jaar oud

MkhJ&J&z6&8jo

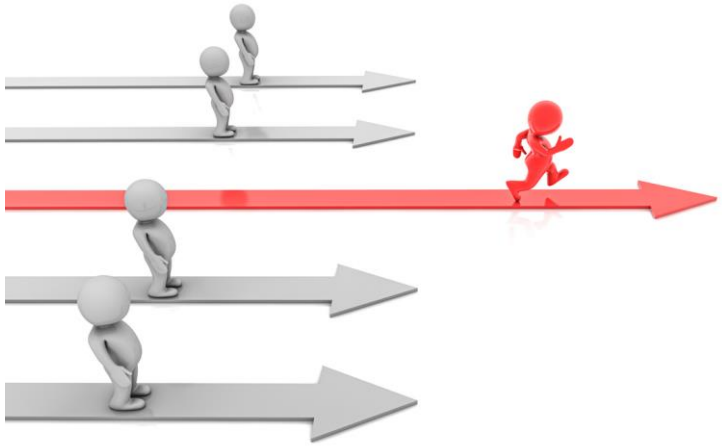
Plak drie random woorden aan elkaar waarvan 1 nonwoord

PannekoekTenerifeWappewaaier

(of, nog liever: Pannekoek,Tenerife&Wappewaaier)

gedrag	=	capaciteit	×	motivatie	×	gelegenheid
						
Interventie	=	leren	×	motiveren	×	faciliteren

MOTIVATIE



Rol van management en bestuur

- Voorbeeldgedrag
- Aanspreken
- Aandacht geven
- Vragen stellen

Risicoperceptie

gedrag	=	capaciteit	×	motivatie	×	gelegenheid
						
Interventie	=	leren	×	motiveren	×	faciliteren

CULTUUR

Een veilige cultuur begint bovenin

Durft men iedereen aan te spreken?

Top down & bottom up!

HOE STAAT RIJNLAND ERVOOR EN WAT GAAN WE DOEN?

Kroon juwelen en High risk objecten/ assets van HHR en HHSK

De high risk assets en de kroonjuwelen zijn als volgt binnen HHR en HHSK geïdentificeerd door de eigenaren en het VST team en opgenomen in het onderstaande overzicht Daarbij is ook rekenschap gehouden met de uitkomsten vanuit de risico analyses en het BIA proces. De legenda geeft de inschattingen van de vertrouwelijkheids-, integriteits- en beschikbaarheid niveaus weer conform de geldende BIV & BNN criteria.

Kroon juwelen # & High risk objecten/assets							
Data	**B**	**I**	**V**	**System/Platform/Application**	**B**	**I**	**V**
Vertrouwelijke informatie				Endpoints			
Vertrouwelijke client information				**Business applications (I&D)**			
Persoonlijke data van cliënten				SharePoint			
Interne Informatie				Email			
Persoonlijke data van medewerkers & inhuur				Corsa			
Intellectual property				Topdesk / Ultimo			
Financiële data				SAAS			
Gebouwen	**B**	**I**	**V**	Teams			
				# Active Directory (toegang -en rechtenbeheer HHR en HHSK			
Kantoor locaties				***- HR Systems (I&D)***			
Installaties; waterzuivering, waterkeringen				H@RM *employees			
datacenter				Payroll			
				contractors			
				- Financial systems			
				CSF			
				Business applications			
				# 800XA Watersysteem – en zuiveringsbeheersproces HHSK			
				# BOSBO Watersysteembeheerproces HHR			
				# AVEVA Zuiveringsbeheerproces HHR			
				# LCMS Crisisbeheersingsproces van HHR en HHSK			

hoog middel laag

Secura
A BUREAU VERITAS COMPANY

OPTIMALISATIE ACTIES

Activiteit	
Realisatie primaire IB security Beleidsdocumenten	Strategisch, zonering, monitoring ICT incl. communicatie
Verklaring van toepasselijkheid kroonjuwelen	
Verbreden en integreren samenwerking IB en privacy	
Actualisatie BCM plannen voor HHR & HHSK	Integratie cybersecurity incidenten en wachtdienst I&A
Inrichten MS compliance center voor monitoring	Secure en compliant
Voorbereidingen NIS2	Focus op artikel 20 lid 2
Raamovereenkomsten security diensten leveranciers	
Optimalisatie en structuur IB&P Rapportages directie en MO	
Audit kalender	Voor CISO 2LoD en support 1LoD

INGEZETTE SECURITY OPTIMALISATIE ACTIES

Optimalisatie	
Project Fysiek beveiliging	ID badge, elektronische sleutels objecten
Implementatie laatste fase IAM project	
Implementeren SOC activiteiten	
Implementatie nieuwe datacenter	Lifegang, zonering en applicatie refresh
planmatige implementatie informatieveiligheid door systeem/proces eigenaren	
Alle applicaties en devices onder security controle I&A	
vergroten van awareness omtrent informatieveiligheid en digitale vaardigheden	
Implementeren Integraal Beveiliging en veiligheidsbeleid	HHR & HHSK
versterken beheer en monitoring Supply Chain	
Optimaliseren en inrichten ISMS	Met support dienstverleners
Driejarig awareness programma	Met support dienstverlener

Resultaten Effectmeting	Ambities van Rijnland	Interventies Secura
Gedrag nog niet op gewenste niveau	Kloof overbruggen tussen awareness (bewustwording) en gedrag	SAFE-programma: veilig gedrag is het einddoel
Basiskennis IB niet op gewenste niveau	Ontwikkeling van een organisatiebreed "basisniveau" training (bv e-learning, interne opleiding) incl voortgangsrapportage aan leidingegevende	Aangeboden online e-learnings voor verschillende onderwerpen (storytelling) en fysieke bijeenkomsten zoals trainingen en roadshows
Belang van IB wordt onvoldoende gedeeld	Aansluiting vinden bij belang dat wordt gehecht aan fysieke veiligheid: verplicht 'Digitaal paspoort'	Ambassadeurschap (ambassadeurs die helpen het onderwerp levend te maken) + ontwikkelen van 'Awareness toolbox' (bijvoorbeeld onderwerp bespreekbaar maken tijdens teamoverleggen met handvatten uit de toolbox)
Inzicht nodig in de belemmeringen op doelgroepen die laag scoren.	Ambitie om passend programma voor specifiekere doelgroepen te starten	Advies om te onderzoeken wat de specifieke barrières (d.m.v. interviews) zijn van de doelgroepen en deze weg te nemen door gerichte interventies
Minder alert op phishingmails	Phishing next step: 'Meld rare berichten'	Phishingactie toegespitst op de medewerkers van Rijnland (next step: smishing en vishing)
Bedrijfsinformatie wordt gedeeld via privéaccount	Alles delen via werkaccounts (geen privéaccounts)	Ontwikkelen 'Awareness toolbox' (een van de onderwerpen) toespitsen op doelgroepen
Mensen spreken elkaar niet aan op onveilig gedrag	Aanspreken medewerkers op onveilig gedrag	Handvatten en tips in de 'Awareness toolbox'

PLAN VOOR 2024-2026

Op basis van de roadmap Security Awareness hebben wij samen een plan gemaakt, dat bestaat uit verschillende onderdelen:

- Maatwerkprogramma voor 6 specifieke doelgroepen binnen HHR & HHSK
- Introductietraining Informatiebeveiliging & privacy in de Aquademie
- Roadshows
- Mystery Guest bezoeken bij HHSK & HHR
- Phishing simulaties
- Bestuurlijke informatiesessies
- Toolkit voor teamleiders en afdelingshoofden

WWW.SECURA.COM