ARDA

Leer collega's wat ze zélf kunnen doen tegen cybercrime

Spelend leren • Herkenbare situaties • Meetbare resultaten

De vraag is niet of je wordt gehackt, maar wanneer

Helaas. Iedere organisatie is interessant voor hackers. Zelfs als je denkt dat er bij jullie niets te halen valt.

In 2021 waren er gemiddeld 270 cyberaanvallen per bedrijf.* Criminelen kregen toen dus ongeoorloofde toegang tot gegevens, applicaties, diensten, netwerken of apparaten. Misschien wel die van jou. In 2022 registreerde de politie zelfs bijna drie keer zoveel gevallen van cybercriminaliteit als in 2019.**

Het goede nieuws? Je kunt deze incidenten meestal voorkomen, of op zijn minst de schade beperken.

*** Accenture, State of Cybersecurity Resilience 2021**
**** AD.nl, 18-01-23**

“Mensen denken vaak dat hacken heel technisch is. Maar voor een groot deel is hacken gewoon slim mensen om de tuin leiden en je net anders voordoen dan je bent. En daar gebruik van maken.”

— Frank Plattel Ethisch hacker

Cybersecurity is mensenwerk

Al is je beveiliging nog zo goed, of jouw systemen en data veilig blijven hangt af van je collega’s. 90 procent van de cyberaanvallen begint namelijk met het klikken op een valse link in een nepmailtje.

Zolang jouw medewerkers zich online niet veilig gedragen, vinden kwaadwillenden altijd een weg naar binnen. Daarom is het superbelangrijk om je collega’s te leren wat zij zelf kunnen doen om zichzelf en jouw organisatie te beschermen tegen cybercriminelen.

Maar jij hebt zelf wel iets anders te doen dan collega’s continu bijscholen over wachtwoorden, phishing en ransomware. Hoe wordt cybersecurity voor iedereen net zo gewoon als de deur op slot doen wanneer je weggaat?

centric

Hier wil je niet tussen staan

Datum	Waar?	Wat?	Schade?
dec 2022	MAKRO	Via een ransomwareaanval zijn in november 2022 de gegevens van werknemers gestolen. In december ervaart Makro nog steeds de gevolgen.	~ € 40 - € 70 miljoen omzet
dec 2022	Nova College	Gijzelsoftware (ransomware)	Onbekend
dec 2022	Gemeente Haarlemmermeer	Via een phishingaanval is er geld overgemaakt naar criminelen.	€ 250.000
okt2022	ID-ware	Via een ransomwareaanval zijn data van 21.000 pashouders gestolen.	Onbekend
sep 2022	Uber	Door te profiteren van MFA-moeheid zijn gegevens van 57 miljoen gebruikers gestolen.	Nog onbekend
aug 2022	Colosseum Dental	Na een ransomwareaanval moesten 120 tandartspraktijken tijdelijk de deuren sluiten.	€ 2 miljoen losgeld

Grote cyberaanval

Tandartsketen betaalt 2 miljoen euro losgeld aan criminelen na cyberaanval

Aangepast 10 augustus 2022 17:40

Zo bescherm je jouw organisatie tegen cybercrime

Je collega's hoeven geen cyberexperts te worden. Ze moeten wél goed weten wat zij zelf kunnen doen om hun eigen gegevens en die van jouw organisatie te beschermen. Met de online training van Arda ontdekken jouw medewerkers al spelend de gevaren van cybercrime en leren ze zich wapenen tegen online dreigingen.

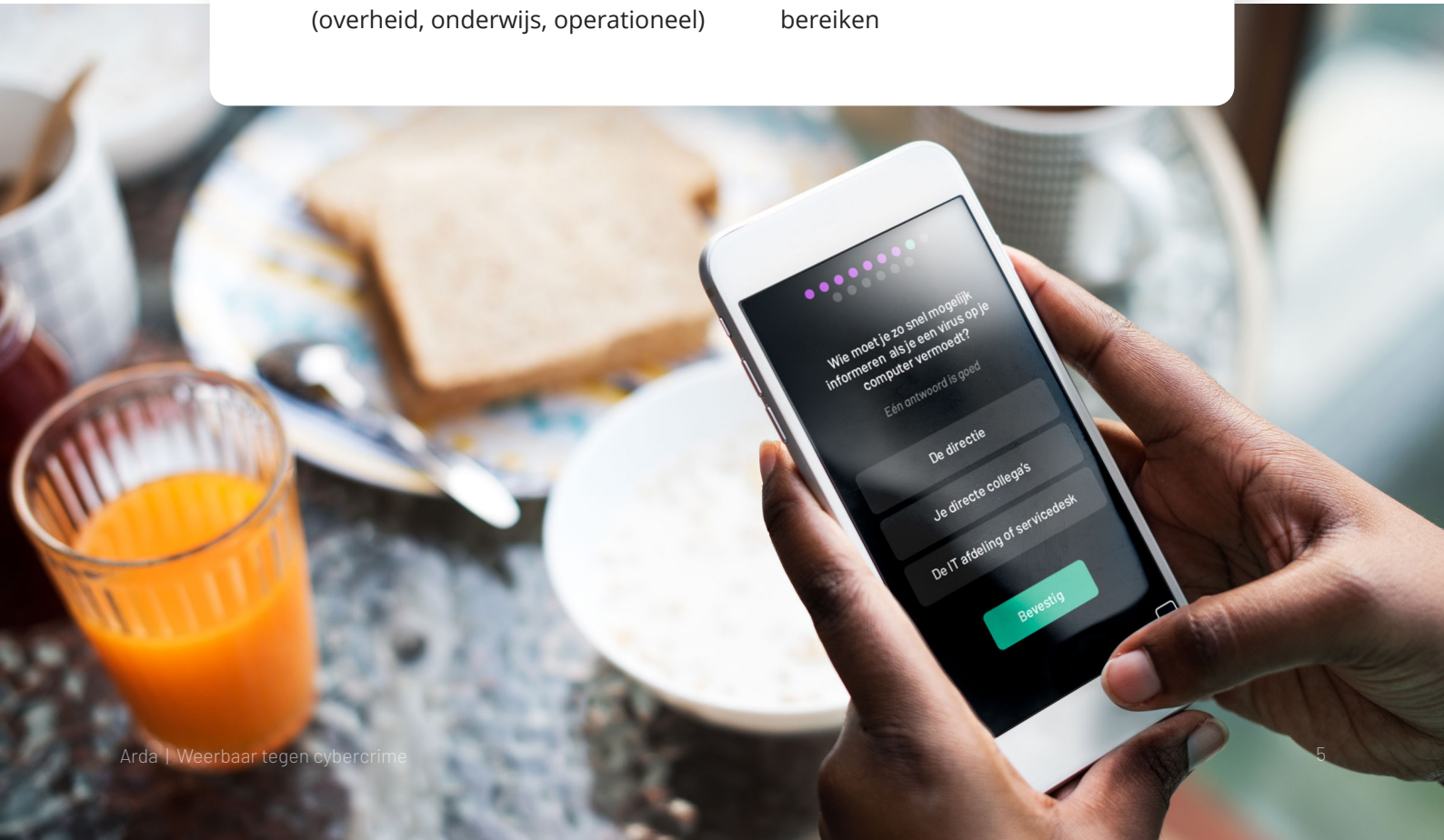
Nieuw gedrag aanleren kost tijd, dus Arda is een doorlopend meerjarenprogramma. Saai? Welnee. We houden het leuk met serious gaming, afwisselende content, herkenbare voorbeelden en beloningen.

Het programma bestaat uit:

- E-learningmodules
- Video's met vragen tussendoor
- Quizzes
- Interviews met experts
- Phishingcampagnes
- Sectorspecifieke modules (overheid, onderwijs, operationeel)

Jouw medewerkers krijgen:

- Een mailtje wanneer er een nieuwe module klaarstaat
- Herhaalchallenges om hun kennis te oefenen
- Punten voor ieder onderdeel
- Een certificaat als ze een mijlpaal bereiken

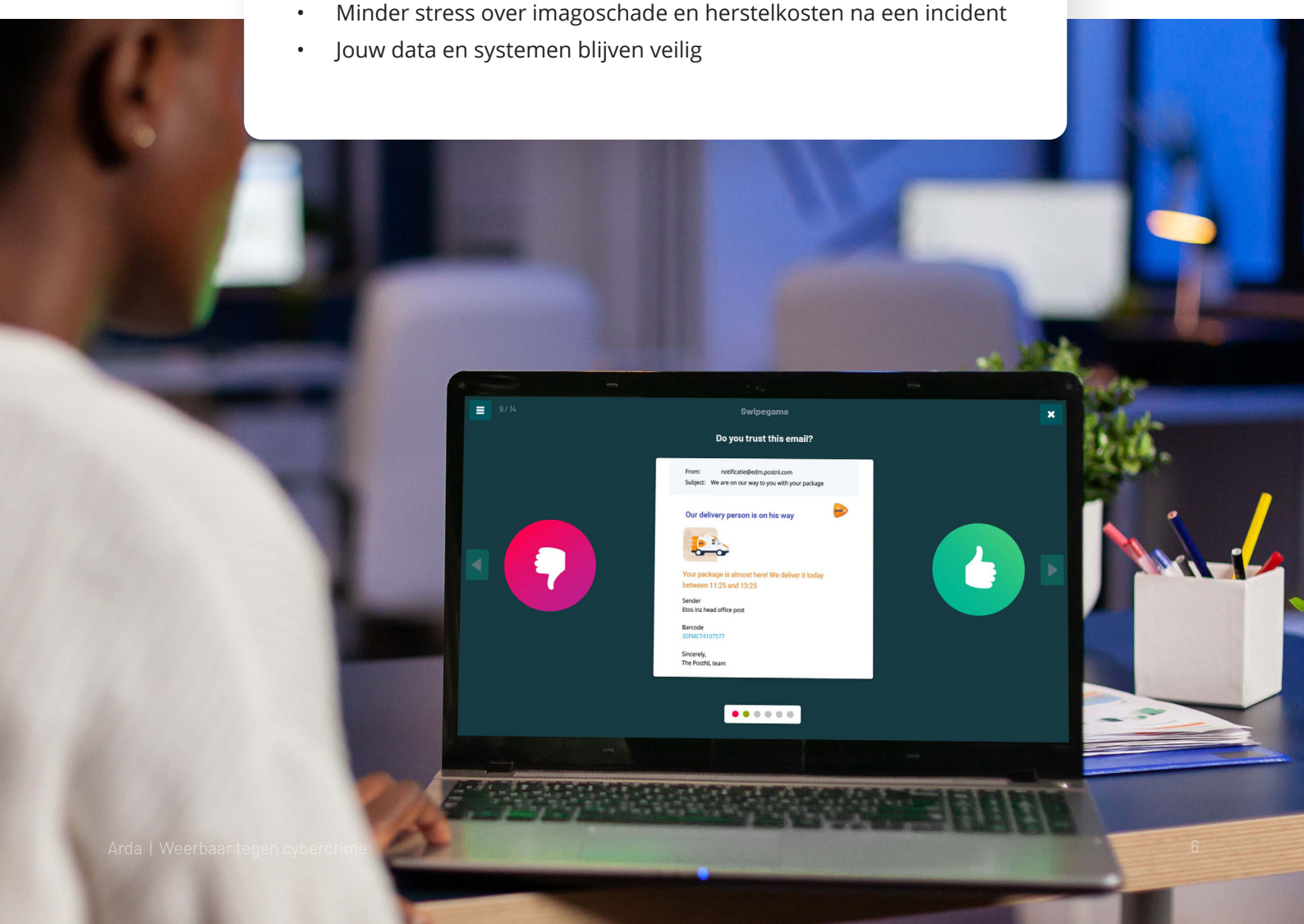


Dit levert Arda jou op

Arda zorgt voor bewuste medewerkers die cybercriminelen zelf buiten de deur houden. Zijn er dan straks helemaal geen incidenten meer in jouw organisatie? Nou nee, dat kunnen we niet beloven. Maar we garanderen wel dat jouw medewerkers een stuk beter weten hoe ze zichzelf, en dus ook het bedrijf, kunnen beschermen tegen cybercriminaliteit. Daarmee wordt de kans op een geslaagde cyberaanval veel kleiner en kan jouw organisatie gewoon door blijven draaien.

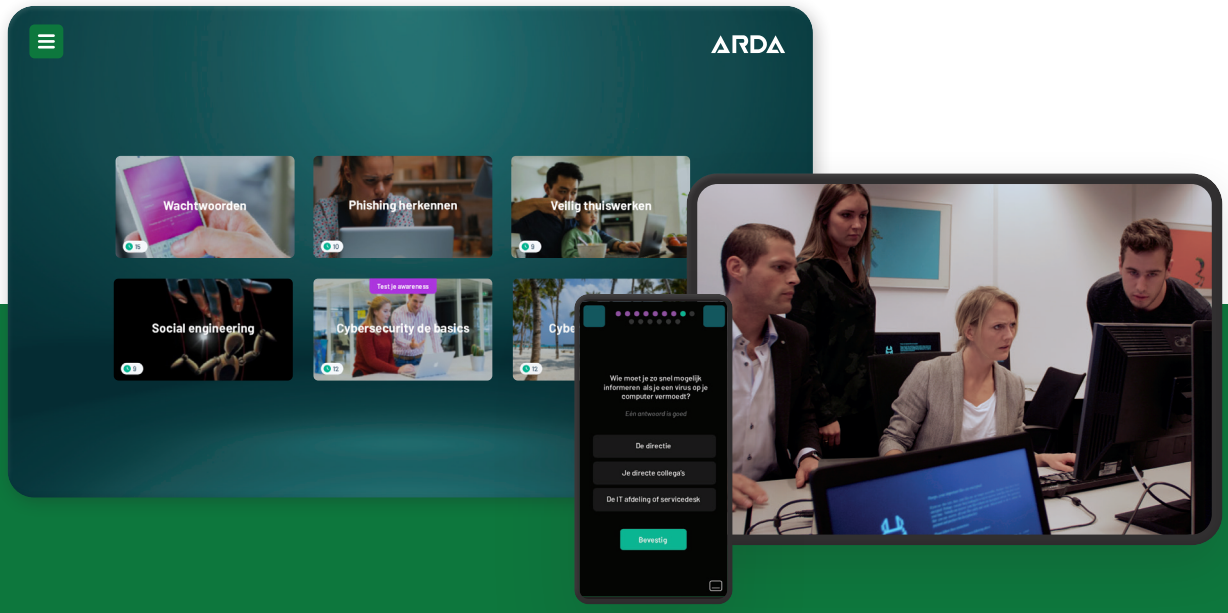
Jouw winst:

- Medewerkers herkennen en melden sneller mogelijke aanvallen
- Minder stress over imagoschade en herstelkosten na een incident
- Jouw data en systemen blijven veilig



Over het Arda-programma

Afwisselend, herkenbaar en nog leuk ook



Korte leermomenten

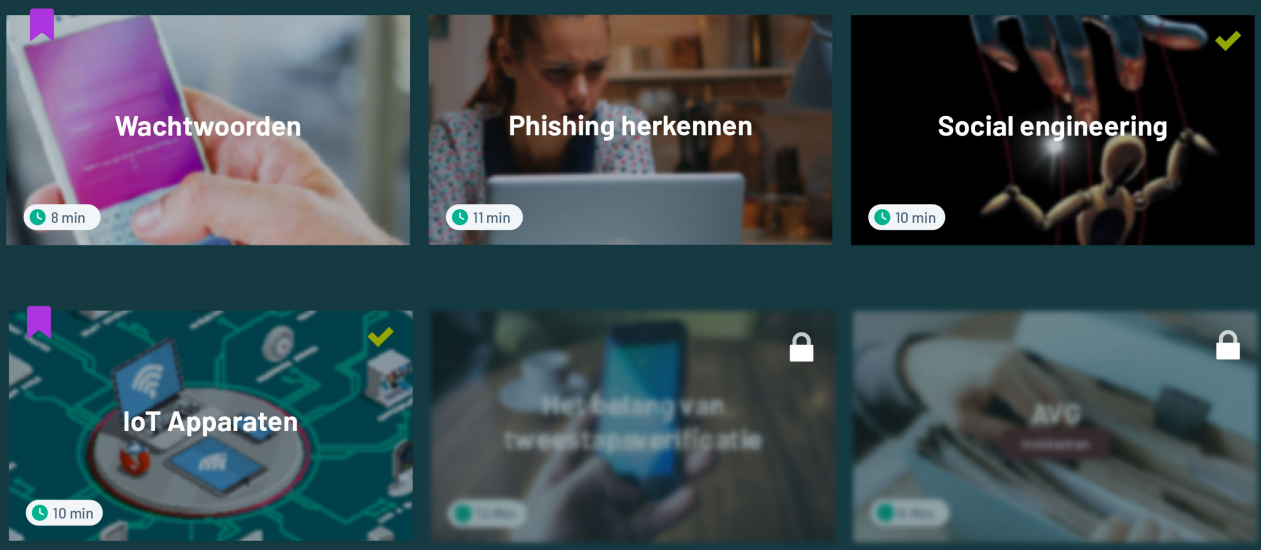
Regelmatig iets leren werkt beter dan in één keer een hele training volgen. Daarom krijgen Arda-deelnemers een jaar lang steeds korte onderdelen aangeboden. Met een kwartiertje kan iemand weer verder met z'n werk.

Afwisseling

De ene keer bekijken je medewerkers een video van een herkenbare situatie, de andere keer krijgen ze inhoudelijke uitleg of doen ze een opfrisquiz. Ze leren onder andere nepmails herkennen, het belang van tweestapsverificatie en hoe ze een wachtwoordmanager gebruiken.

Punten verdienen

Om het leren te stimuleren verdienen je collega's verdienen punten met ieder onderdeel dat ze afronden. Op het scorebord kunnen ze zien wie er bovenaan staat. Na afronding van het jaarprogramma krijgt elke deelnemer een certificaat.



Verhalen van ervaringsdeskundigen
Korte interviews met experts en ervaringsdeskundigen geven deelnemers meer inzicht in wijze lessen uit de praktijk. Zo vertelt iemand hoe zijn moeder slachtoffer werd van bankfraude.

Veiligheid thuis
Medewerkers die thuis op een veilige manier met online accounts omgaan, doen dat waarschijnlijk op kantoor ook. Daarom gaat het in de modules ook over privésituaties en de veiligheid van bijvoorbeeld smart speakers of beveiligingscamera's.

Phishingcampagnes
Om hun alertheid te testen sturen we je medewerkers vier keer per jaar een nepmail. Hoeveel mensen klikken er op de link en laten hun gegevens achter? Hoeveel collega's melden de mail bij IT? Na zo'n campagne zie jij de cijfers in een rapportage.

Filmische videoserie
Deelnemers krijgen ook afleveringen te zien van onze videoserie Steinitz. Daarin zien ze bijvoorbeeld dat iemand gevoelige data lekt en hoe een manager slachtoffer wordt van CEO-fraude. Tijdens de afleveringen krijgt de kijker vragen over de gebeurtenissen.

Wat moet je doen als je een virus op je computer vermoedt?

Een voorbeeld uit onze videoserie

Om cybersecurity extra tastbaar te maken voor mensen die er weinig van weten, ontwikkelden we de vierdelige videoserie Steinitz.

In aflevering één krijgt hoofdpersonage Ellis tijdens het typen ineens een zwart scherm met een vreemde tekst voor haar neus. Ze schrikt en wanneer steeds meer collega's hetzelfde scherm krijgen, begrijpt ze wat er aan de hand is.

We zijn gehackt, en het is mijn schuld.

Ellis meldt het incident meteen. Niet veel later start het onderzoek over wat ze de afgelopen week heeft gedaan en waar ze is geweest. Zo zie je stap voor stap hoe een hacker via het account van Ellis het virus uiteindelijk in het systeem van haar werkgever kreeg.

Bekijk de trailer

Vragen tussendoor
Tijdens elke Steinitz-aflevering krijgen kijkers meerdere vragen over de scènes of over andere onderwerpen waar ze zich bewust van moeten zijn. Zo steken ze meer op van het voorbeeld in de video.

Samenvatting achteraf
Na een Steinitz-aflevering volgt altijd een korte samenvatting van wat iemand net heeft gezien. In deze recapvideo worden de cruciale fouten en lessen nog even extra toegelicht.

Situaties in de video's

Een verhuurbedrijf maakt een kopie van je paspoort.

De openbare wifi in een koffietent gebruiken.

V-Bucks die worden buitgemaakt.

Toegangsdeuren die openstaan voor onbevoegden.

‘De bank’ vraagt een familielid om geld over te maken.

centric

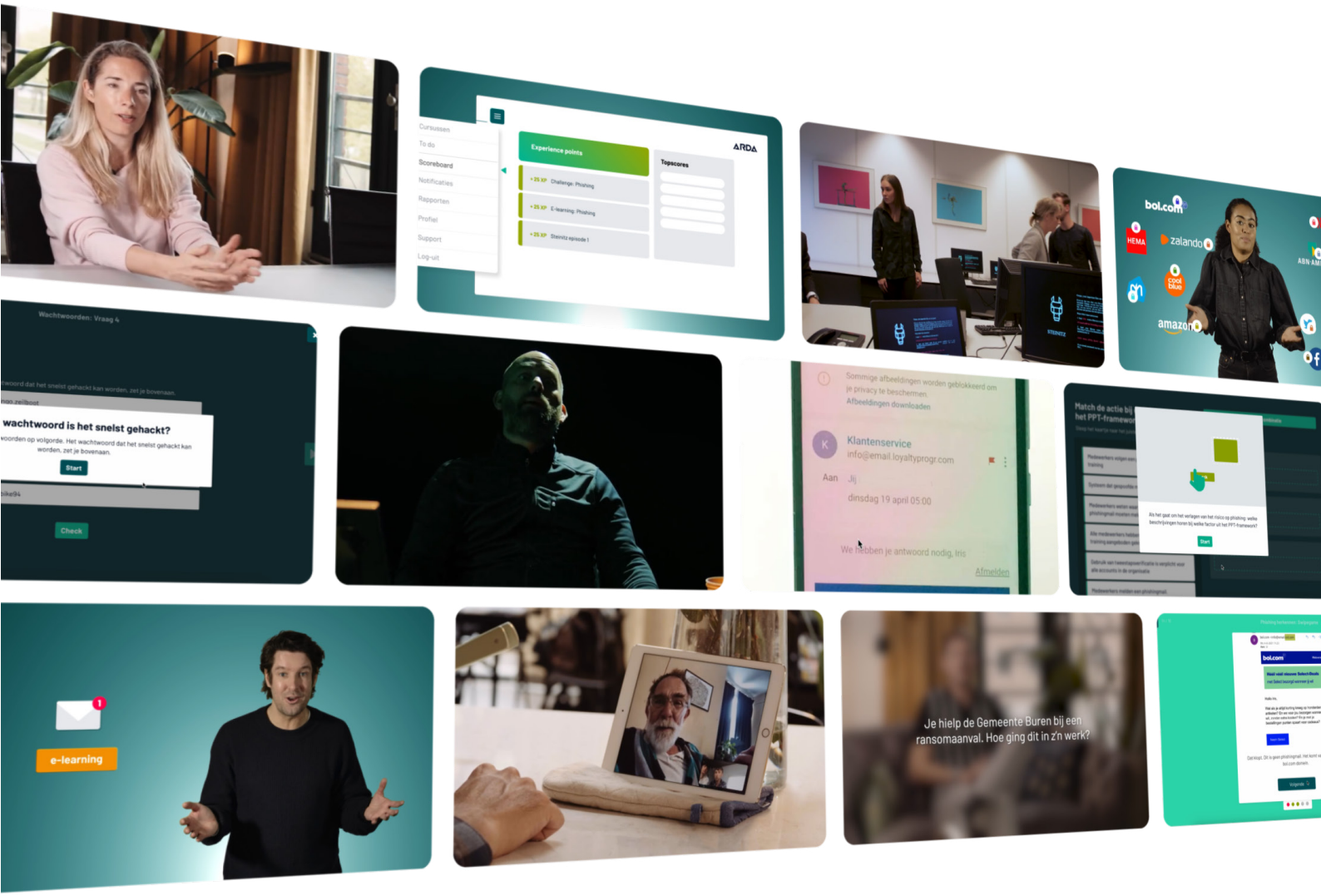
Opbouw van het programma

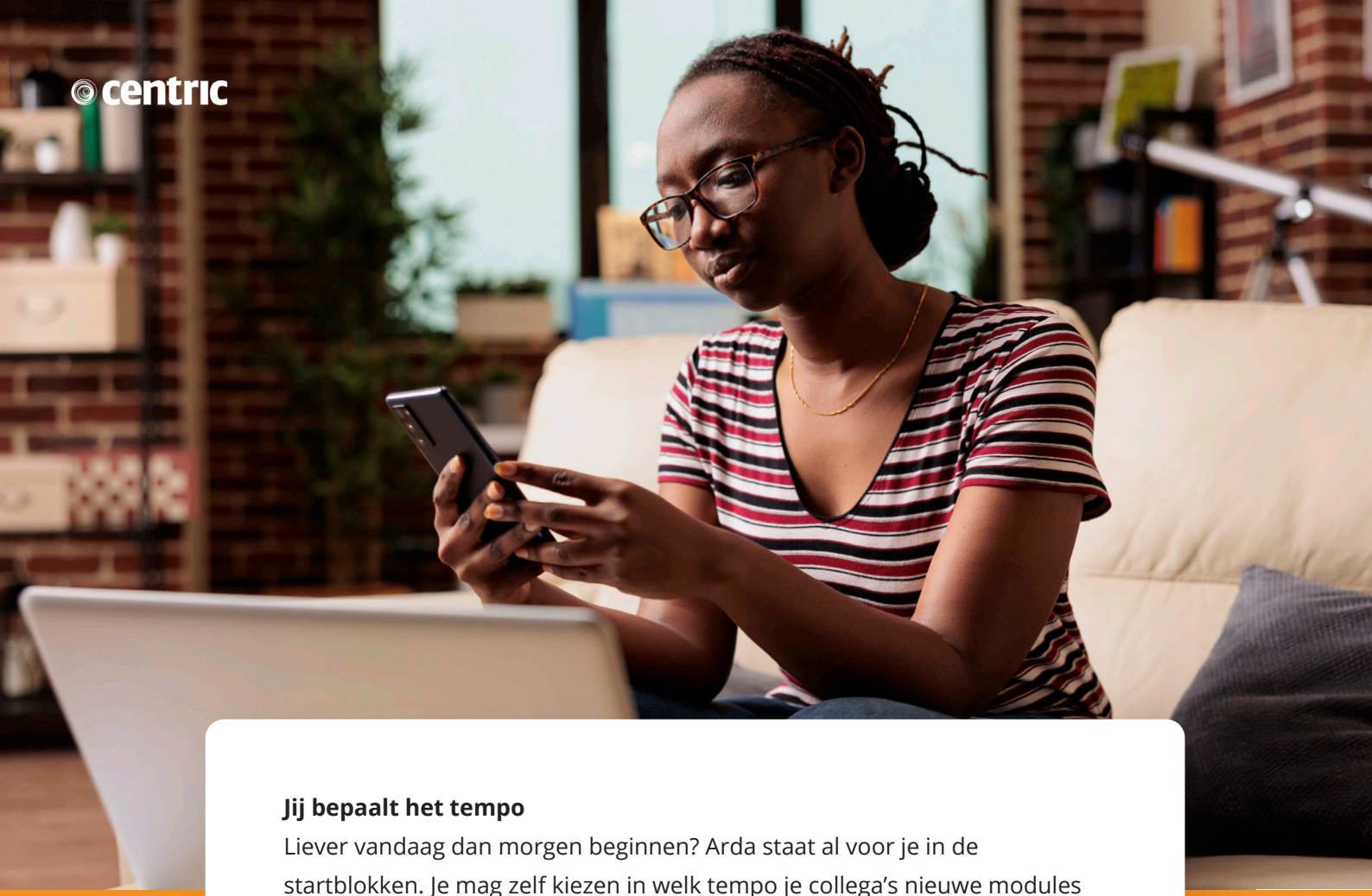
Er gebeurt heel veel in cybersecurityland, dus we houden de modules up-to-date en er komen vaak nieuwe onderwerpen bij. Hieronder zie je een voorbeeld van de opbouw.

- **Eigen introductievideo**
- Phishingmail #1
- Steinitz #1
- Phishing herkennen
- Brenno de Winter
- Wachtwoorden
- Maria Genova
- Privacy & de AVG
- Phishingmail #2
- Tweestapsverificatie
- Inge Wetzer
- Steinitz #2
- Social engineering
- Phishingmail #3
- Dave Maasland
- Fysieke veiligheid
- Steinitz #3
- Elsine van Os
- Wachtwoordmanager
- Phishingmail #4
- Cyberveilig onderweg
- Steinitz #4
- AVG extra
- **Certificaat jaar 1 behaald**

Maatwerk is ook mogelijk

Je kunt het programma nog aantrekkelijker maken door er bekende gezichten uit de organisatie in te verwerken. Laat bijvoorbeeld een introductievideo met de directeur maken of een film over jullie eigen pand en collega's. Opnemen kan in onze studio of op locatie. En wat dacht je van je eigen quiz of module? We denken graag met je mee over een passend programma voor nog meer veiligheidsbewustzijn in jouw organisatie.





Jij bepaalt het tempo
Liever vandaag dan morgen beginnen? Arda staat al voor je in de startblokken. Je mag zelf kiezen in welk tempo je collega's nieuwe modules krijgen aangeboden. En Arda even pauzeren tijdens drukke periodes of vakanties kan natuurlijk ook.

Iedere afdeling z'n eigen content
Arda bestaat voor 80% uit lessen die voor iedere medewerker relevant zijn. Wil jij toch extra focus op het veiligheidsbewustzijn van een specifieke functie of afdeling binnen jouw organisatie? Daarvoor bieden we je speciale leerlijnen. Jij kiest vervolgens welke afdelingen welke content moeten volgen.

Inzicht in de resultaten
Om zeker te weten dat het veiligheidsbewustzijn binnen de organisatie verbetert, kun je een minimale score eisen van jouw medewerkers. Als administrator heb je altijd inzicht in hoeveel deelnemers welke onderdelen volgen of hebben gevolgd. Rapportages uitdraaien is ook zo gepiept.

De technische details

Licenties
Om Arda te kunnen gebruiken koop je voor iedere medewerker een licentie. Zo'n licentie is een jaar geldig vanaf de startdatum die je zelf kiest. Na een jaar kun je het aantal lienties bijstellen of stoppen met Arda.

Gebruikers toevoegen of verwijderen? Daar heb je geen technische kennis voor nodig. De licenties van medewerkers die uit dienst gaan zijn trouwens overdraagbaar aan nieuwe collega's, zodat zij meteen met hun online gedrag aan de slag kunnen.

Alle apparaten en browsers
Het Learning Management System waar Arda op draait, werkt op alle soorten apparaten en moderne browsers (Internet Explorer 11 en lager raden we af).

Gaat er iets niet goed? Onze supportafdeling staat voor je klaar via support@arda.nl of telefoonnummer 085 401 84 87.

centric

ARDA

Meer informatie nodig?

Neem dan contact op met Derek Hillenaar

derek.hillenaar@centric.eu | **+31 6 105 90 189**