



ARDA

Leer collega's wat ze zélf kunnen doen tegen cybercrime

Serious games • Herkenbare situaties • Meetbare resultaten

De vraag is niet of je wordt gehackt, maar wanneer

Helaas. Ook jouw organisatie is interessant voor hackers.

Zelfs als je denkt dat er bij jullie niets te halen valt, loop je risico. In 2023 kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval*. En in het eerste kwartaal van 2025 steeg het aantal cyberaanvallen in Nederland zelfs met 53% ten opzichte van dezelfde periode in 2024**.

Het goede nieuws? Veel van deze incidenten zijn te voorkomen – of de schade kan aanzienlijk worden beperkt.

* Rapport ABN AMRO (Steeds verfijndere cyberaanvallen – april 2024)

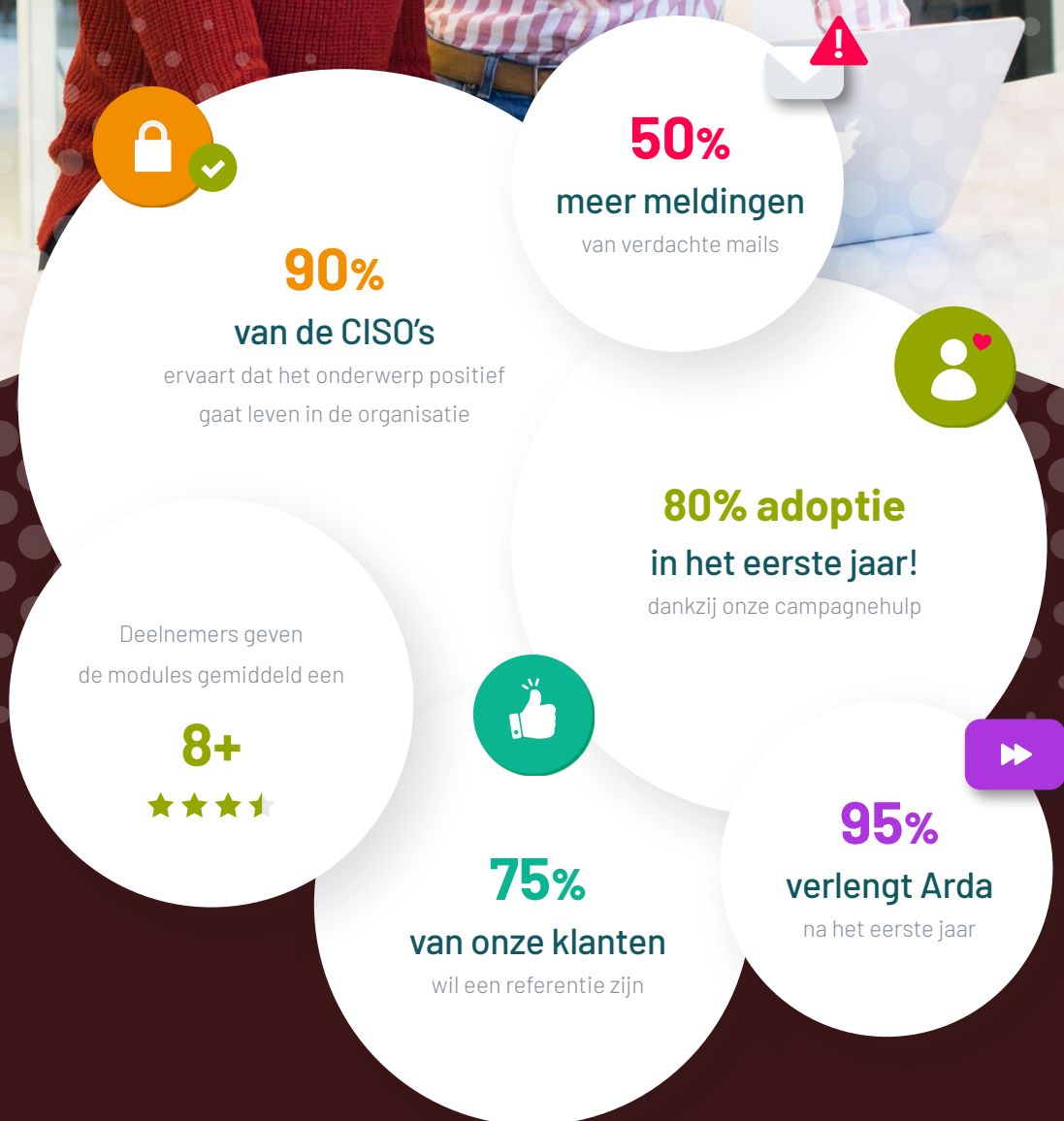
** Check Point Research Cyber Security Report 2025

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 collega's 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 bij-scholen over wachtwoorden, phishing en ransomware. Hoe wordt cybersecurity voor iedereen net zo gewoon als de deur op slot doen wanneer je weggaat?



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 collega's al spelend de gevaren van cybercrime en leren ze zich wapenen tegen online dreigingen.

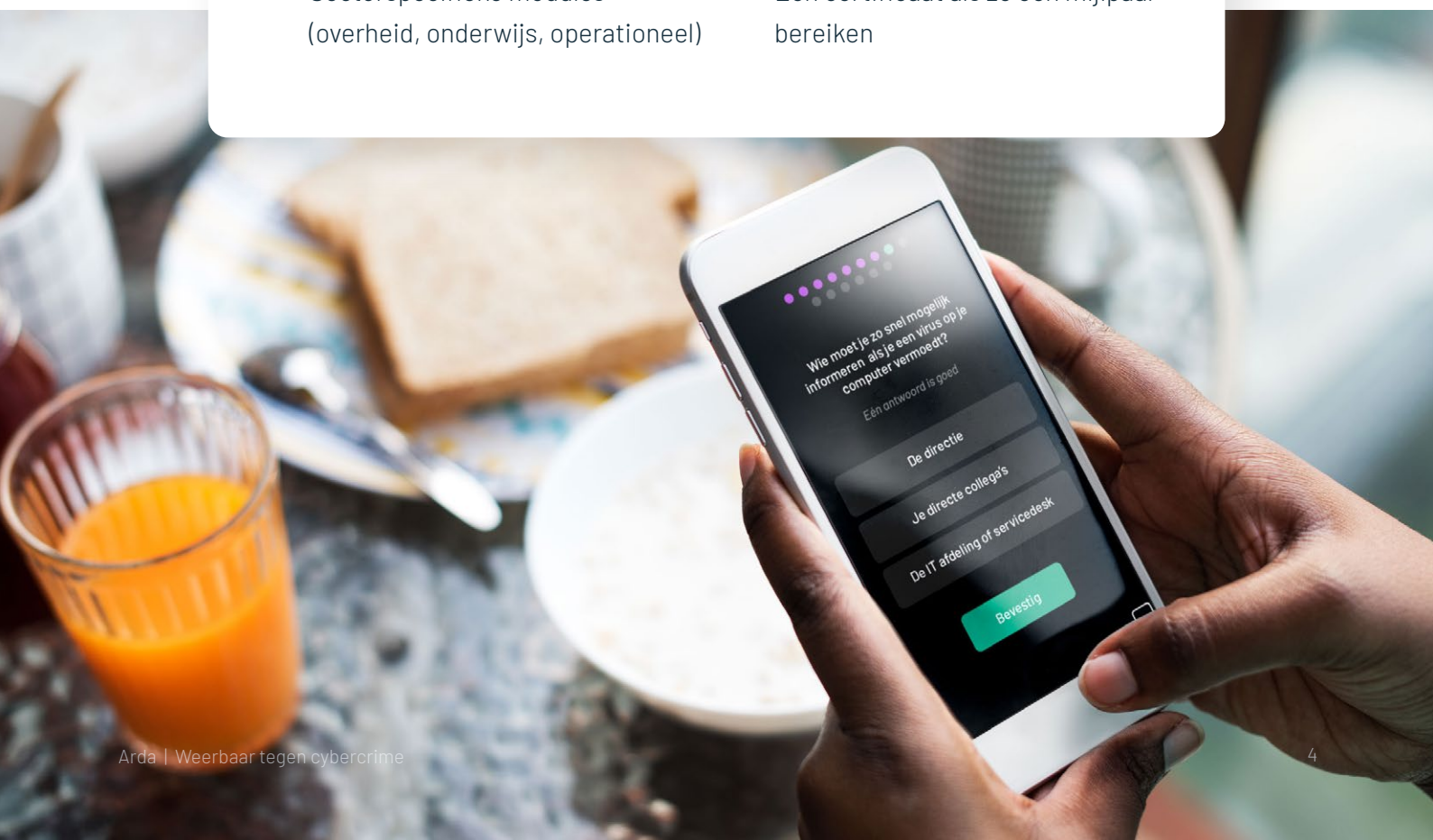
Nieuw gedrag aanleren kost tijd, dus Arda is een doorlopend meerjarenprogramma. Saai? Welnee. We houden het leuk met serious gaming, afwisselende content, herkenbare voorbeelden en beloningen.

Het programma bestaat uit:

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

Jouw collega's 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

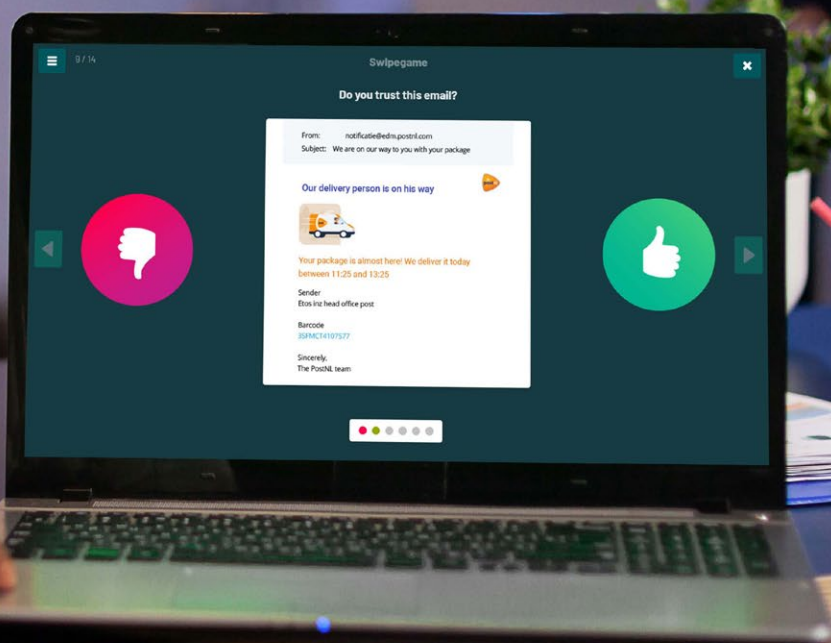


Dit levert Arda jou op

Arda zorgt voor bewuste collega's 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 collega's 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.

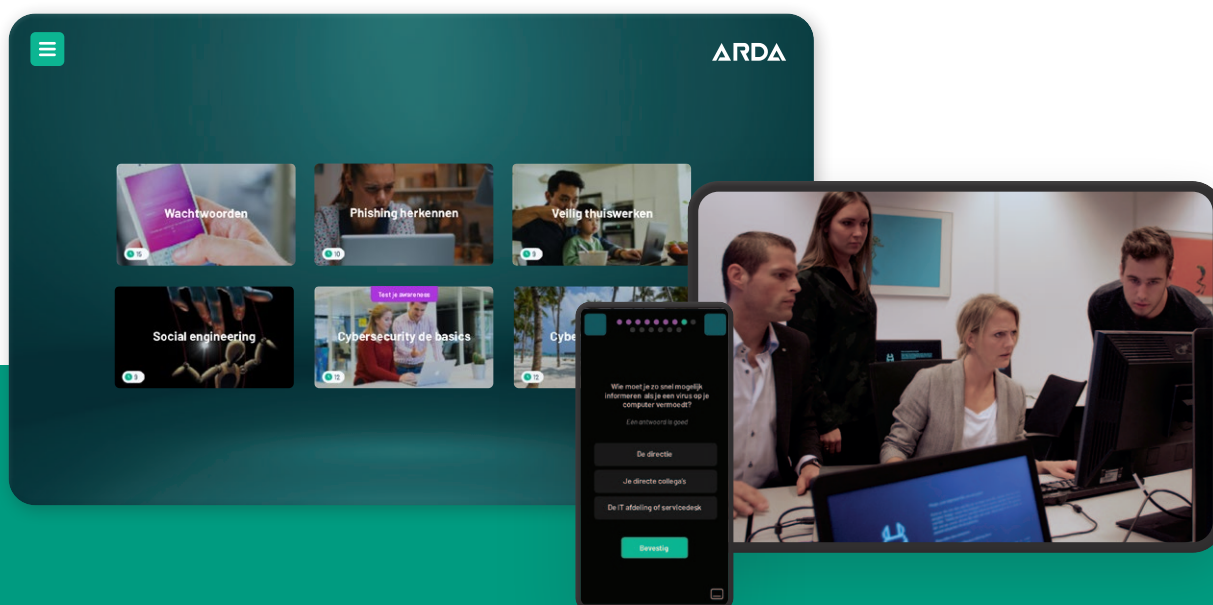
Jouw winst:

- 50% meer meldingen van verdachte e-mails
- 80% adoptie in het eerste jaar, dankzij onze campagnehulp
- Collega's herkennen phishing en social engineering beter
- 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 collega's 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 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.



*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.*

— Frank Plattel Ethisch hacker

Phishingcampagnes

Om hun alertheid te testen sturen we je collega's 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.

Veiligheid thuis

Collega's 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.

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.

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?

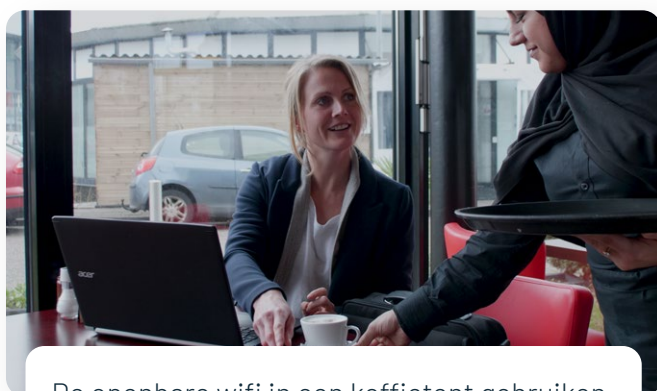
Een voorbeeld uit onze videoserie

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

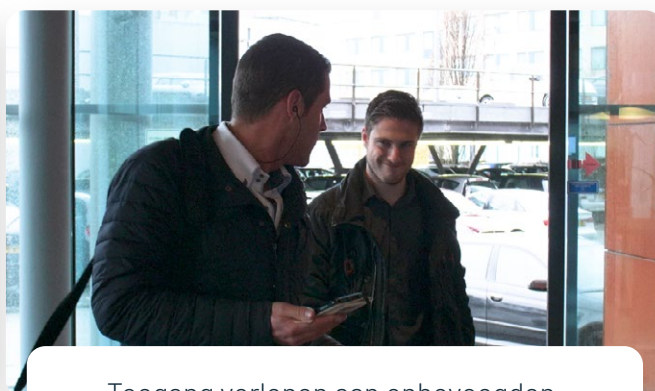
In aflevering één krijgt hoofdpersonage Ellis tijdens het typen ineens een zwart scherm met een vreemde tekst voor haar neus. Ze schrikt en wanneer steeds meer collega's hetzelfde scherm krijgen, begrijpt ze wat er aan de hand is.

We zijn gehackt, en het is mijn schuld.

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



De openbare wifi in een koffietent gebruiken.



Toegang verlenen aan onbevoegden.



Een verhuurbedrijf kopieert je paspoort.



V-Bucks die worden buitgemaakt.

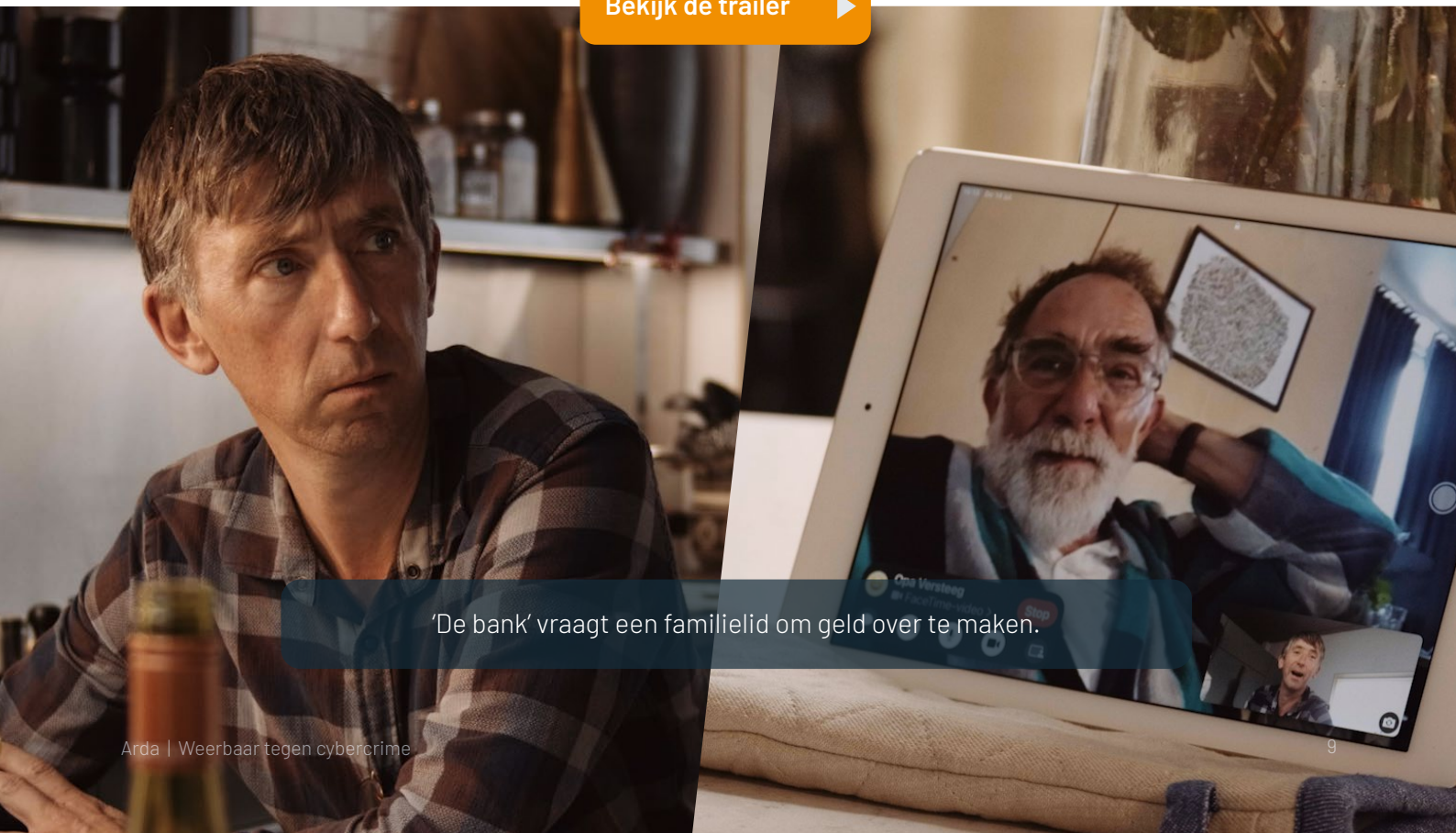
Vragen tussendoor

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.

Bekijk de trailer ▶



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.



The collage consists of 12 individual images arranged in a grid-like fashion. The images are as follows:

- Top Left:** A woman with blonde hair, wearing a pink sweater, sitting at a desk and speaking.
- Top Center:** A screenshot of a dashboard titled 'Expertise gains' with a sidebar menu and a 'Top scores' section.
- Top Right:** A woman in a dark jacket standing in a meeting room with other people and computers.
- Middle Right:** A woman in a dark jacket standing in front of a screen displaying various logos including bol.com, HEMA, zalando, and amazon.
- Middle Left:** A screenshot of a login screen with the text 'Wachtwoord is het snelst gehackt?' and a 'Start' button.
- Middle Center:** A man in a dark setting, looking upwards.
- Middle Right (Below Logos):** A smartphone screen displaying a 'Klantenservice' notification from info@email.loyaltyprogr.com.
- Middle Far Right:** A screenshot of a website with a map of the Netherlands and a 'Plan' button.
- Bottom Left:** A man in a dark sweater standing against a teal background, gesturing with his hands.
- Bottom Center:** A hand holding a tablet that shows a video call with an older man with a beard.
- Bottom Right (Center):** A blurred image of a person in a meeting room with the text 'Je helpt de Gemeente Buren bij een ransomaanval. Hoe ging dit in z'n werk?'.
- Bottom Far Right:** A screenshot of a website with a 'bol.com' logo and a 'Plan' button.

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 collega's. 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 licenties bijstellen of stoppen met Arda.

Gebruikers toevoegen of verwijderen? Daar heb je geen technische kennis voor nodig. De licenties van collega's 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 bel met 085 401 84 87.

support@rabobank.nl ✓

support@rabobank-service.nl ✗





Krijg een gratis demo

Benieuwd geworden naar ons programma? Leuk! Check arda.nl en boek daar een gratis demo van 30 minuten. Daarna heb je alle informatie voor de volgende stap: een veiligere organisatie.

