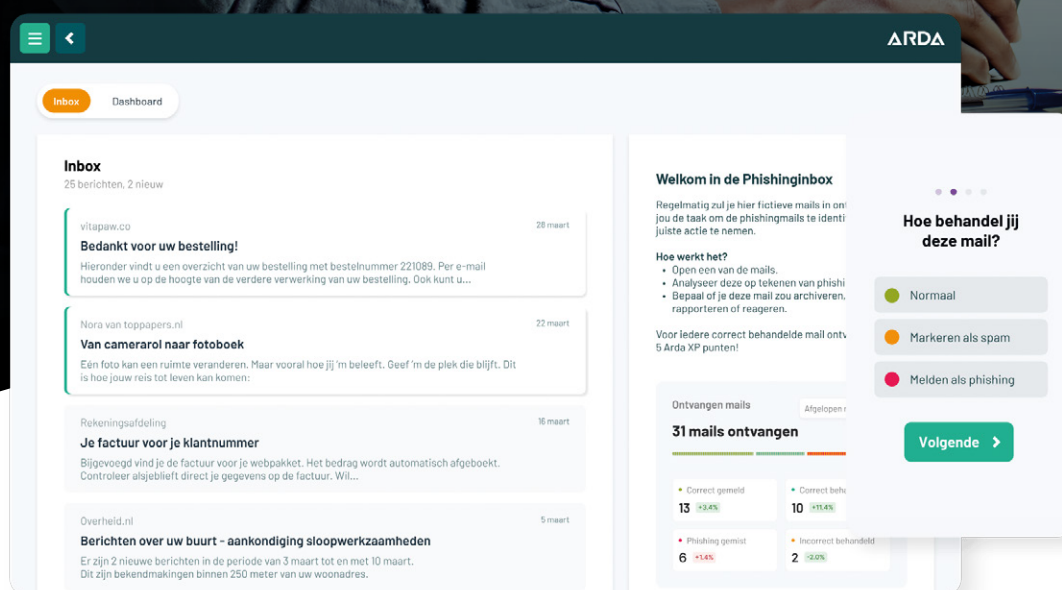


ARDA

Phishinginbox

Phishing herkennen leer je door te oefenen,
niet door betrappt te worden.



Traditionele phishingsimulaties meten vooral wie er klikt. Medewerkers weten niet dat ze getest worden en krijgen pas achteraf te horen dat ze erin zijn getrappt. Dat kan leiden tot irritatie, onzekerheid en wantrouwen. Bovendien zegt een klik nog weinig over wat iemand daadwerkelijk heeft gezien, overwogen of geleerd.

**De Phishinginbox draait de traditionele aanpak om.
Wij communiceren naar mensen, net als bij een brandoefening.**

Medewerkers oefenen in een realistische mailomgeving binnen het Arda-platform. Ze krijgen regelmatig een kleine batch e-mails voorgeschoteld: phishing, social engineering, spam én gewone legitieme e-mail. Ze weten dat ze oefenen, maar niet welke mails veilig of onveilig zijn. Er worden géén nepmails door de echte mailomgeving van de organisatie gestuurd.

Van testen naar trainen

Zo werkt het

- 1. Bekijk de mail**
 De medewerker controleert afzender, inhoud, links en eventuele bijlagen, net zoals in een echte mailbox.
- 2. Maak een keuze**
 Kiest de medewerker voor normaal behandelen, markeren als spam of melden als phishing?
- 3. Leg uit waarom**
 Welke signalen bepaalden de keuze?
 De afzender, inhoud, link of bijlage?
 Zo meet je niet alleen **wat** iemand doet, maar ook **waarom**.
- 4. Leer direct**
 Na iedere mail volgt meteen feedback: wat ging goed, wat niet en welke signalen waren belangrijk?

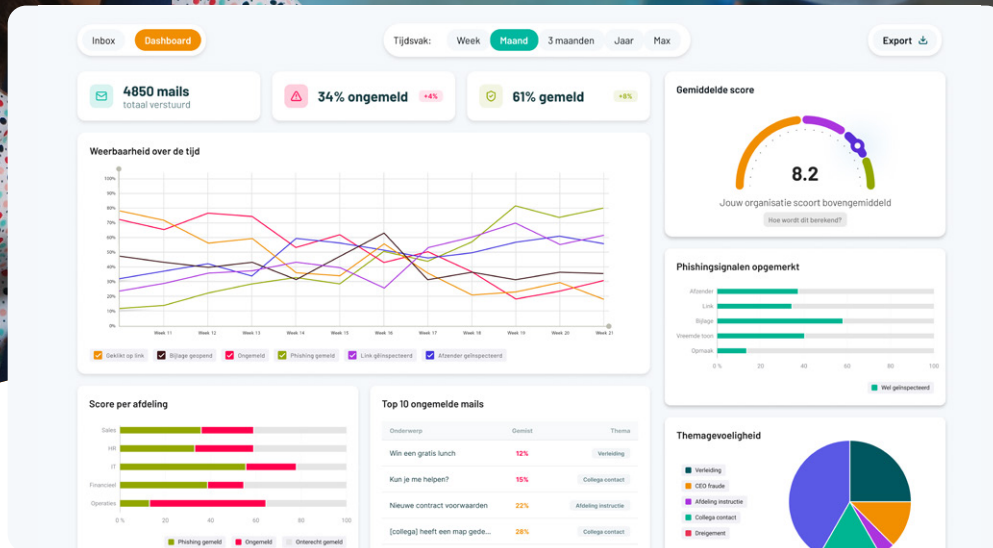
Niet betrappen, maar trainen. Niet alleen kliks meten, maar daadwerkelijk gedrag veranderen.

Weet wat je meet

De Phishinginbox kijkt verder dan het bekende klikpercentage. Het systeem legt vast hoe medewerkers daadwerkelijk met e-mail omgaan: controleren ze de afzender, bekijken ze links, openen ze een bijlage, welke keuze maken ze en waarom?

Ook goed gedrag telt mee.

Een legitieme mail correct behandelen is net zo relevant als het herkennen van phishing. Zo ontstaat een veel completer beeld van de digitale weerbaarheid van medewerkers en teams.



In het dashboard zie je onder andere hoeveel mails zijn behandeld, welk percentage correct is afgehandeld, waar signalen worden gemist en hoe resultaten zich over meerdere periodes ontwikkelen.

Resultaten zijn te filteren op bijvoorbeeld periode en afdeling en kunnen worden geëxporteerd voor rapportage en audits.

KLASSIEKE PHISHINGSIMULATIE

- ✗ Losse campagne
- ✗ Vooral klikgedrag
- ✗ Alleen phishing
- ✗ Medewerker wordt getest
- ✗ Technische inrichting nodig
- ✗ Momentopname

DE PHISHINGINBOX

- ✓ Doorlopend oefenen
- ✓ Volledig beslisgedrag
- ✓ Phishing, social engineering, spam én echte mail
- ✓ Medewerker weet dat er geoefend wordt
- ✓ Direct binnen Arda inzetbaar
- ✓ Ontwikkeling over tijd

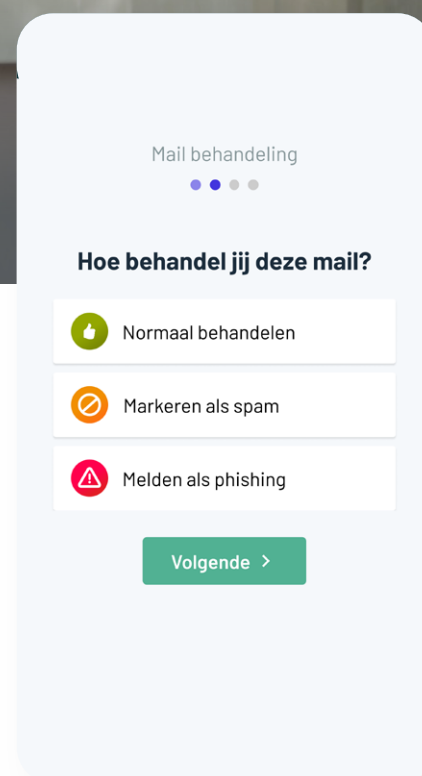
Phishing is meer dan een klik

De Phishinginbox laat zien hoe medewerkers écht omgaan met e-mail.

Direct inzetbaar

De Phishinginbox is onderdeel van het Arda-platform. Er is dus geen apart technisch implementatietraject nodig: geen allowlisting, aanpassingen aan filters of gateways en geen uitzonderingen op de eigen beveiliging.

De organisatie bepaalt zelf de frequentie en kan scenario's afstemmen op sector, software en functiegroepen.



Direct inzetbaar · Doorlopend · Meetbaar gedrag · Ethisch uitlegbaar

Benieuwd hoe de Phishinginbox eruitziet binnen jullie organisatie?
Vraag vandaag nog een demonstratie aan.

✉ info@arda.nl

☎ 085 401 84 87

📍 Röntgenlaan 25C
2719 DX Zoetermeer