



# ARDA

## Help colleagues defend themselves against cybercrime

Serious games • Real-life situations • Measurable results

# It's not a matter of if, but *when* you will be hacked

**Unfortunately, your organization is an attractive target for hackers.**

Even if you think there's nothing valuable to steal.

In 2023, nearly three-quarters of Dutch companies experienced a cyberattack\*.

In the first quarter of 2025, the number of cyberattacks in the Netherlands even rose by 53% compared to the same period in 2024\*\*.

The good news? Many of these incidents can be prevented — or at least, their impact can be significantly reduced.

\* **ABN AMRO Report (Increasingly Sophisticated Cyberattacks – April 2024)**

\*\* **Check Point Research Cyber Security Report 2025**

## Cybersecurity is Human Work

Even if your technical defenses are excellent, your organization's safety still depends on your people. 90% of cyberattacks start with someone clicking a fake link in a phishing email.

If your colleagues don't behave safely online, hackers will always find a way in. That's why it's critical to teach employees how to protect themselves — and your organization — from cybercriminals.

You already have enough on your plate without constantly training employees about passwords, phishing, and ransomware. How can cybersecurity become as normal as locking the door when you leave?



# Protect your organization against cybercrime

Your colleagues don't need to become cybersecurity experts. They just need to know how to protect themselves and your organization's data.

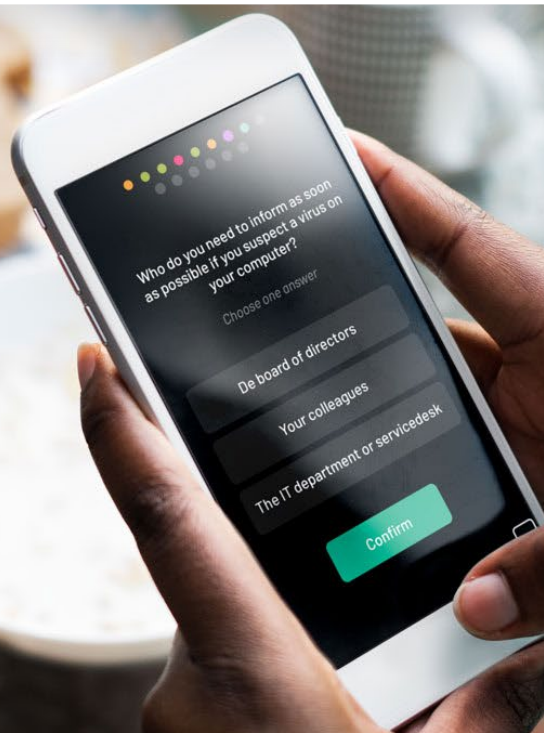
Through Arda's online training program, colleagues learn about the dangers of cybercrime through serious games, varied content, and reward systems. Learning is continuous and engaging – not boring – with recognizable examples, challenges, and milestones.

The program includes:

- E-learning modules
- Videos with integrated quizzes
- Knowledge challenges
- Expert interviews
- Phishing simulations (*optional*)
- Sector-specific modules (e.g., government, education, operations)

Your colleagues receive:

- Notifications for new modules
- Challenges to reinforce learning
- Points for completed activities
- Certificates upon achieving milestones



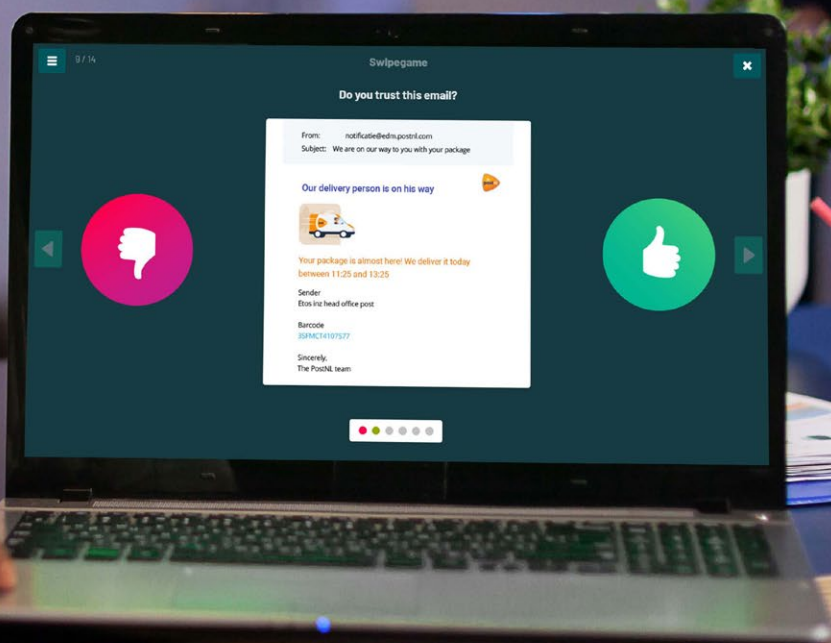
# What Arda offers your organization

Arda creates cyber-aware employees who can keep cybercriminals at bay themselves. Will this mean there will be no more incidents within your organization? Well, no – we can't promise that. But we can guarantee that your employees will be much better equipped to protect themselves – and, by extension, your organization – against cyber threats.

This significantly reduces the risk of a successful cyberattack and helps ensure that your organization can continue to operate smoothly.

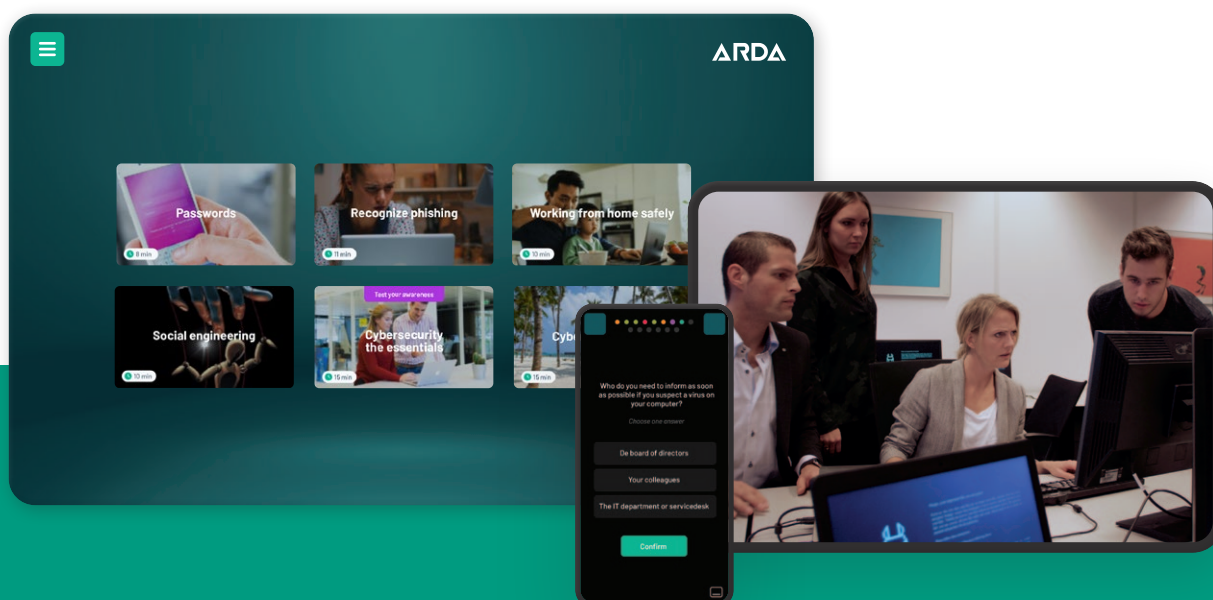
## Your benefits:

- *50% more reporting of suspicious emails.*
  - *80% adoption rate in the first year, thanks to campaign support.*
  - *Improved recognition of phishing and social engineering attempts.*
  - *Reduced stress around reputational damage and recovery costs.*
- Safer data and IT systems.*



# About the Arda Program

Making cybersecurity second nature



## Short learning moments:

Learning regularly is more effective than one-time trainings.

Participants receive short modules throughout the year that only take about 15 minutes to complete.

## Variety

Sometimes your colleagues watch a video depicting a recognizable situation;

other times, they receive in-depth explanations or complete a refresher quiz.


They learn to recognize phishing emails, understand the importance of two-factor authentication, and discover how to use a password manager.

## Earn points & badges

To encourage learning, your colleagues earn points & badges for every module they complete. They can track their progress on the leaderboard and see who's in the lead. At the end of the annual program, every participant receives a certificate.



All e-learning modules are in native English.



*“People often think that hacking is purely technical. But for the most part, hacking is simply about deceiving people and pretending to be someone you’re not.”*

— Frank Plattel Ethical Hacker

### **Cinematic videoseries**

Participants also watch episodes from our Steinitz video series, where they see real-world examples of cybersecurity threats. They follow storylines such as a data leak or a manager falling victim to CEO fraud. During the episodes, viewers are asked questions about the events to

deepen their learning.

### **Stories from experts**

Short interviews with experts and real-life victims provide participants with valuable insights and lessons learned.

For example, one story describes how a mother became a victim of bank fraud.

### **Safe at home**

Colleagues who handle online accounts securely at home are more likely to do so at work as well. That's why the modules also cover personal cybersecurity, including tips for protecting smart speakers, home networks, and security cameras.

### **Phishing campaigns (optional)**

To test their alertness, you can let us send a simulated phishing email to your colleagues. How many people click the link and enter their credentials? How many report the email to IT? After the campaign, you can view the results in your online dashboard.



What should you do if you suspect a virus on your computer?

## Our interactive videoseries

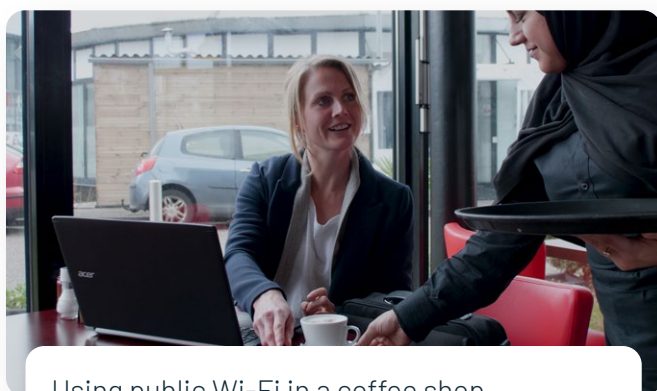
To make cybersecurity more tangible for people with little prior knowledge, we developed the four-part video series Steinitz.

In the first episode, the main character Ellis suddenly sees a black screen with a strange message while typing. She panics, and as more and more colleagues encounter the same screen, she realizes what's happening:

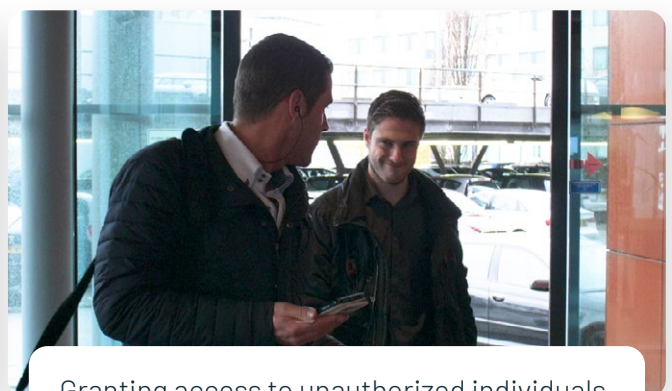
***We've been hacked, and it's my fault.***

Ellis immediately reports the incident. Shortly afterward, she has to explain what she did over the past week and where she had been.

Step by step, viewers see how a hacker used Ellis's account to ultimately infect her employer's system with a virus.



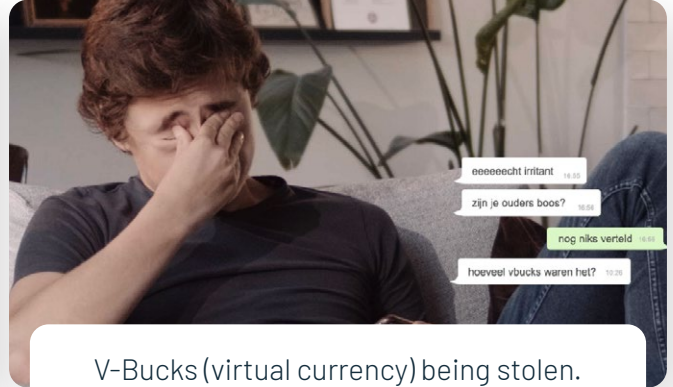
Using public Wi-Fi in a coffee shop.



Granting access to unauthorized individuals.



A rental company copying your passport.



V-Bucks (virtual currency) being stolen.

### Questions during the episodes

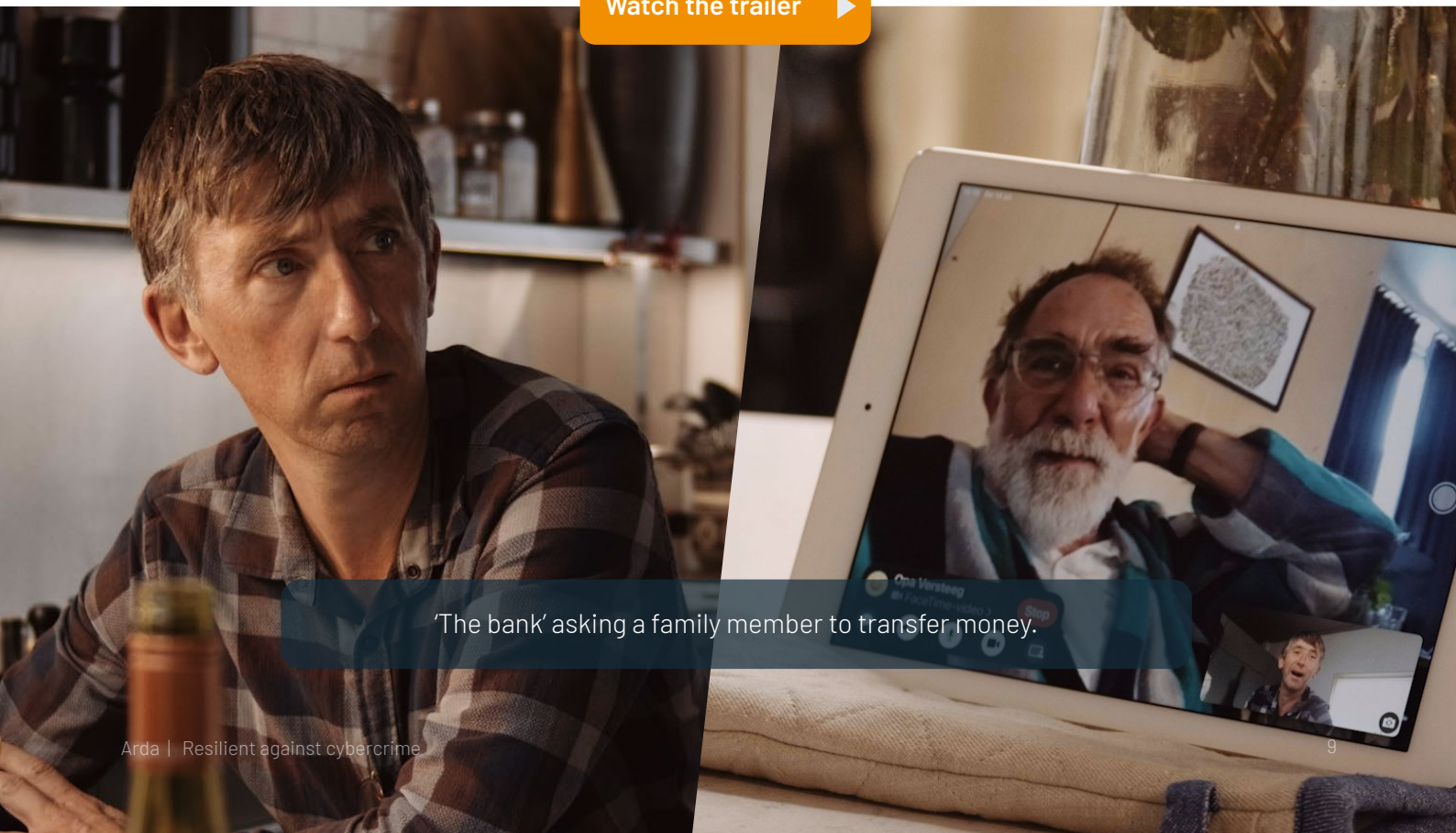
During each Steinitz episode, viewers are asked several questions about the scenes or other related topics they should be aware of. This way, they learn even more from the real-life scenarios shown in the videos.

### Summary afterwards

Each Steinitz episode concludes with a short summary video.

This recap highlights the critical mistakes and key lessons learned, helping to reinforce the viewer's understanding.

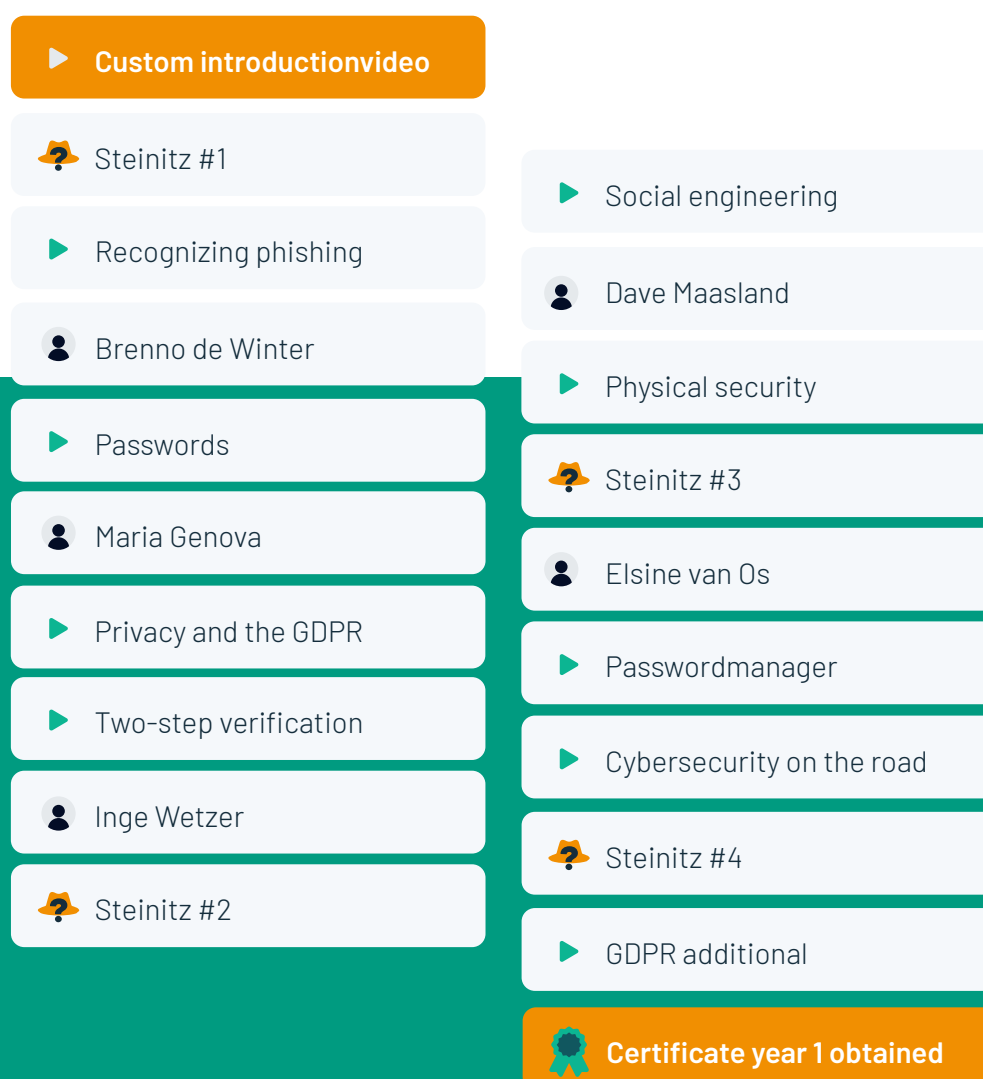
Watch the trailer ▶



'The bank' asking a family member to transfer money.

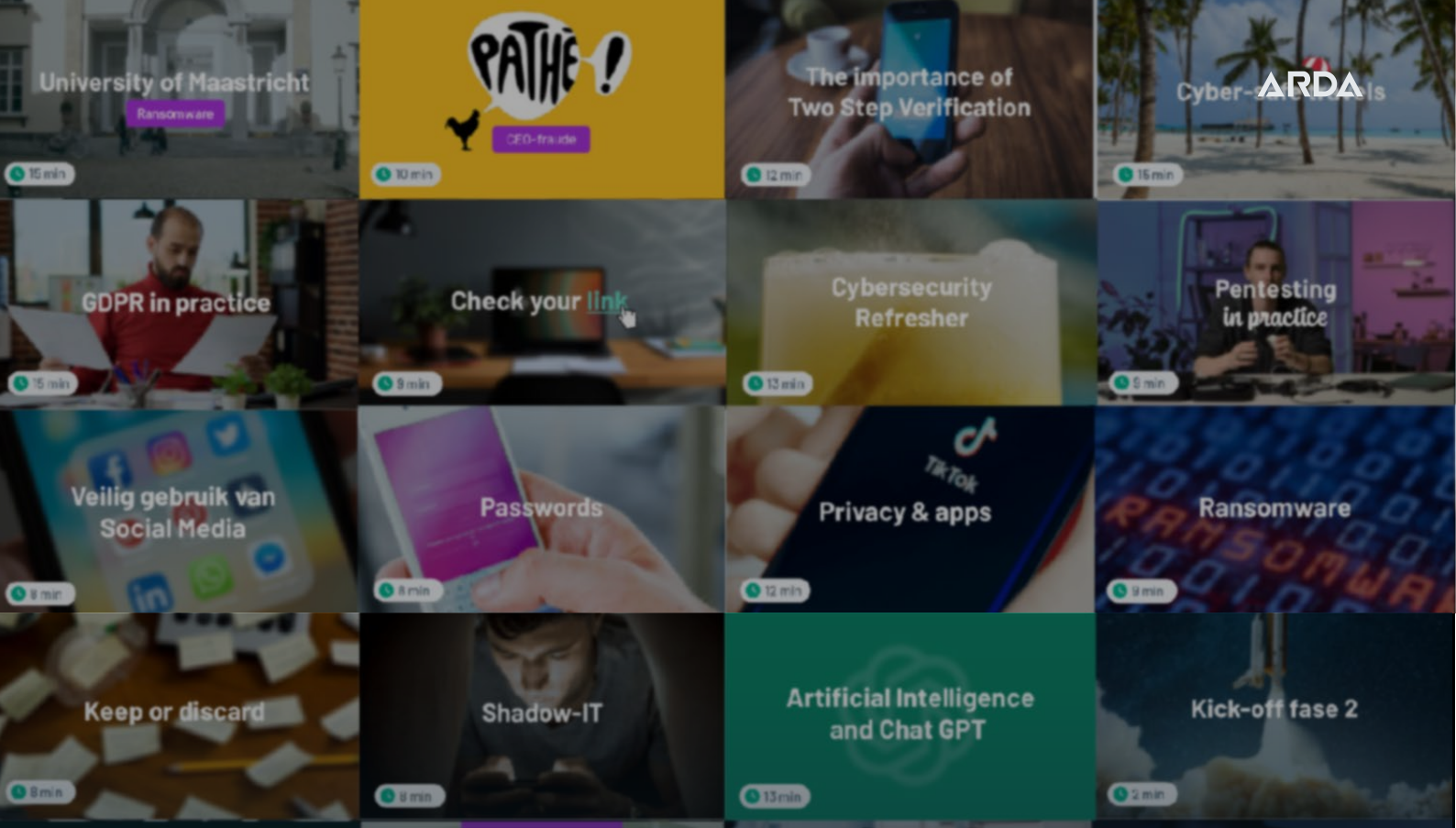
# Program structure

A lot is happening in the world of cybersecurity, so we keep our modules constantly up to date and frequently add new topics. Below is an example of how the program is structured. You can adjust the structure and frequency yourself.



Want your own custom quiz or module? We're happy to brainstorm with you to design a tailored program that raises even more cybersecurity awareness within your organization.





### **You set the pace**

Want to get started today rather than tomorrow? Arda is ready to go. You decide the pace at which your colleagues receive new modules. And if needed, you can pause the program during busy periods or holidays.

### **Custom content for each department**

About 80% of Arda's lessons are relevant for all employees. However, if you want to focus specifically on the cybersecurity awareness of certain roles or departments, we offer dedicated learning tracks. You can assign specific content to specific teams based on your needs.

### **Clear insight into results**

To ensure cybersecurity awareness is truly improving within your organization, you can set minimum score requirements for participants.

As an administrator, you have full visibility into who has started or completed which modules. Generating detailed reports is quick and easy.

# Technical details

## Licenses

To use Arda, you purchase a license for each employee. Each license is valid for one year from the start date you choose. After a year, you can adjust the number of licenses or decide to end your subscription.

Adding or removing users requires no technical expertise. If an employee leaves the organization, their license can simply be transferred to a new colleague, allowing them to immediately begin their cybersecurity training.

## Device and browser compatibility

The Learning Management System (LMS) that hosts Arda works seamlessly across all modern devices and browsers. (Note: We recommend avoiding Internet Explorer 11 and older versions.)

If something goes wrong, our support team is ready to help.  
Mail [support@arda.nl](mailto:support@arda.nl) or call 085 401 84 87.

[support@rabobank.nl](mailto:support@rabobank.nl) ✓

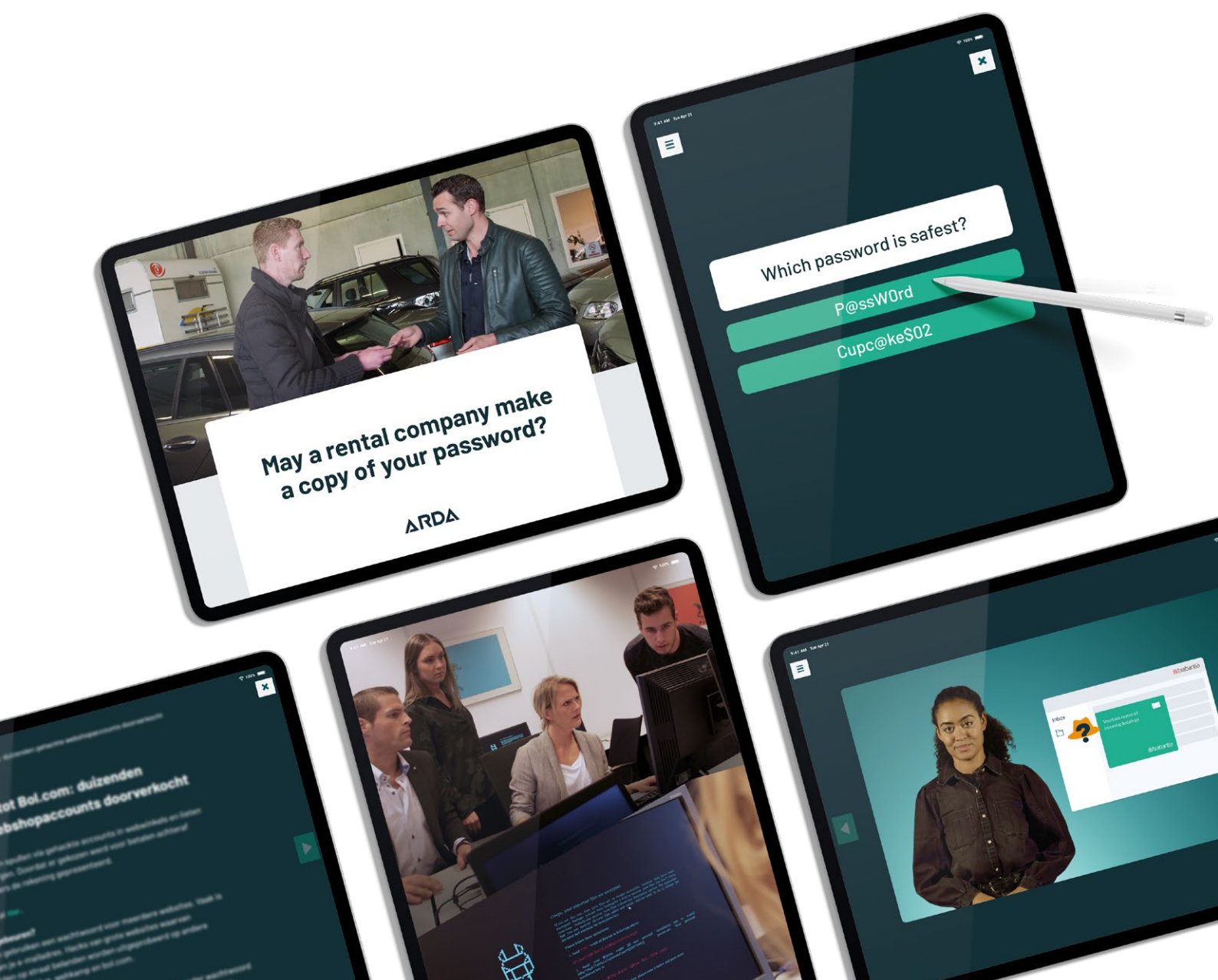
[support@rabobank-service.nl](mailto:support@rabobank-service.nl) ✗





## Get a free demo

Curious about our program? Sweet! Check out [arda.nl](https://arda.nl) for more and to book a free 30-minute demo. Afterwards you'll have all the information for the next step: a safer organization.



✉ [info@arda.nl](mailto:info@arda.nl)

☎ 085 401 84 87

📍 Röntgenlaan 25C  
2719 DX Zoetermeer