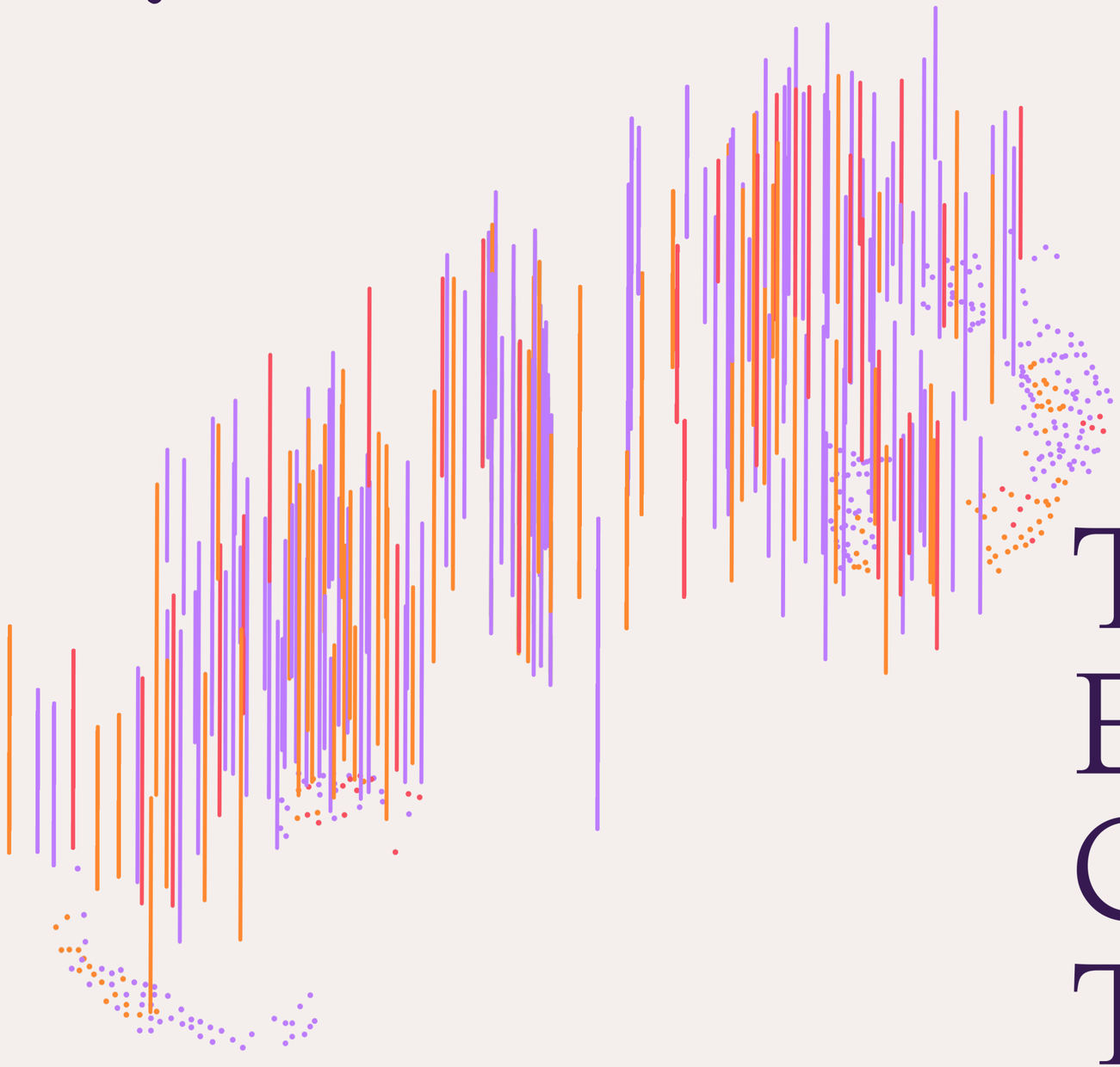
pistachio

italik



The Next Evolution in Cybersecurity Training

pistachio

italik

Empowering digital freedom of movement

People should be able to navigate the digital world with confidence, not fear. They should be able to perform their jobs and live their lives without the threat of cybercriminals getting in the way. Unfortunately, that is not the case for many today. As the cost of cybercrime continues to increase each year, and the vast majority of data breaches occur due to human error, people are justified in feeling nervous.

We created Pistachio because we believe that the problem is not with people, but with the awareness training they receive. Existing awareness training products share a critical flaw: they expect you to solve the problem yourself. They provide a toolbox but leave it to you to sort the users, configure settings, whitelist domains, select the training campaigns, pick out phishing emails, and review results.

Pistachio is different. We aim to fix the problem, not just hand you the tools and ask you to do it. Turn it on, and your employees will start receiving fully personalized attack simulations and training content delivered directly to their inboxes. We adjust the frequency, difficulty, and content of our attacks and training to meet the unique requirements of each user, and the system continues to run without you having to do a thing.

As for who we are, Pistachio is a cybersecurity company founded in 2019 in Oslo, Norway. The name comes from the movie The Master of Disguise, where the protagonist, Pistachio Disguisey, uses his skills of disguise for good. We felt that was fitting, as we disguise ourselves as malicious actors in order to help people learn about cybersecurity in a safe environment.

Average cost of a data breach in 2022

$4.35 million

Breaches due to human error

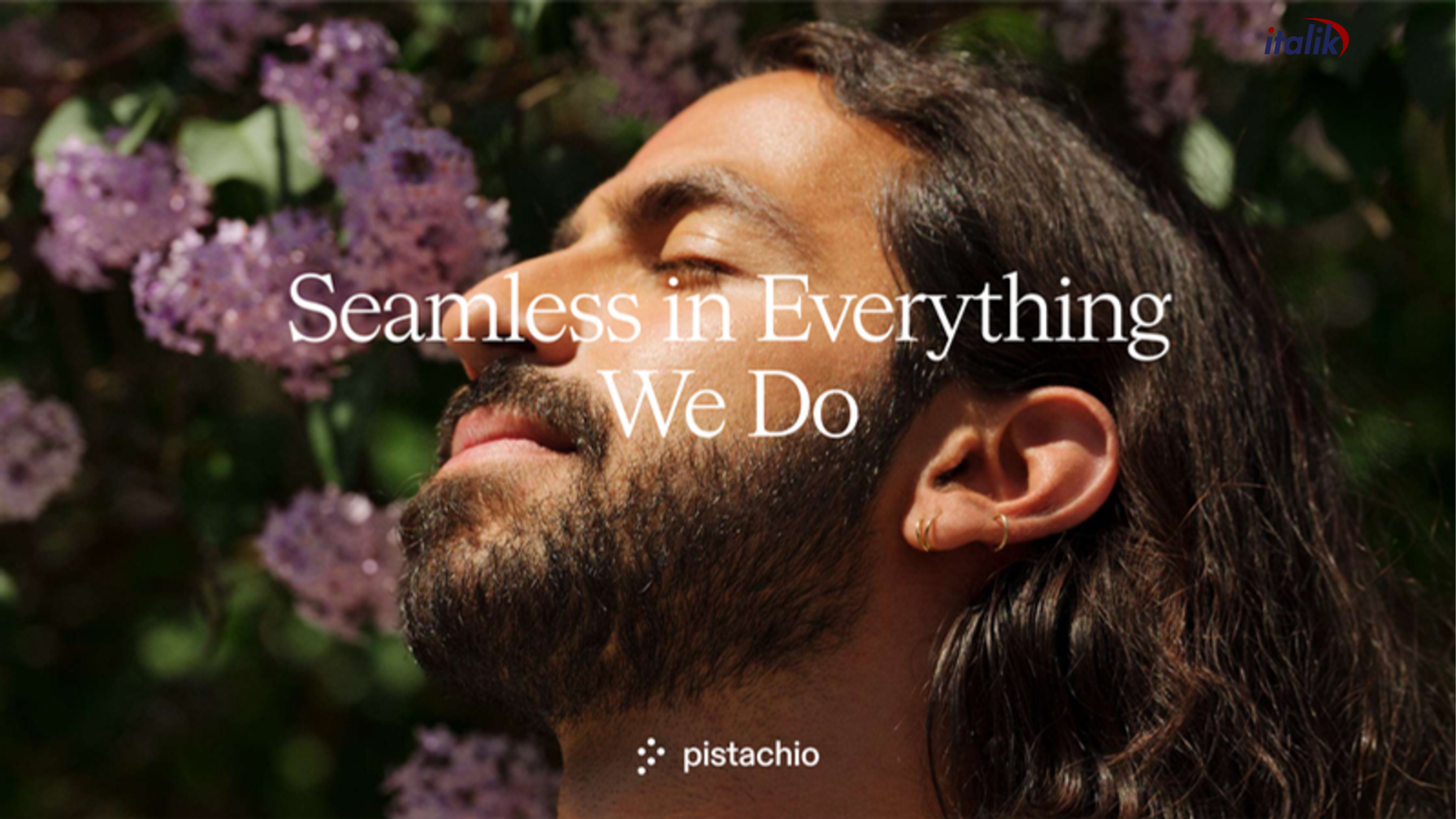
82%

Estimated global cybercrime cost by 2025

$10.5 trillion

Organizations affected by cyber attacks in 2022

83%


italik
Seamless in Everything We Do
pistachio

pistachio

italik

Online sign-up

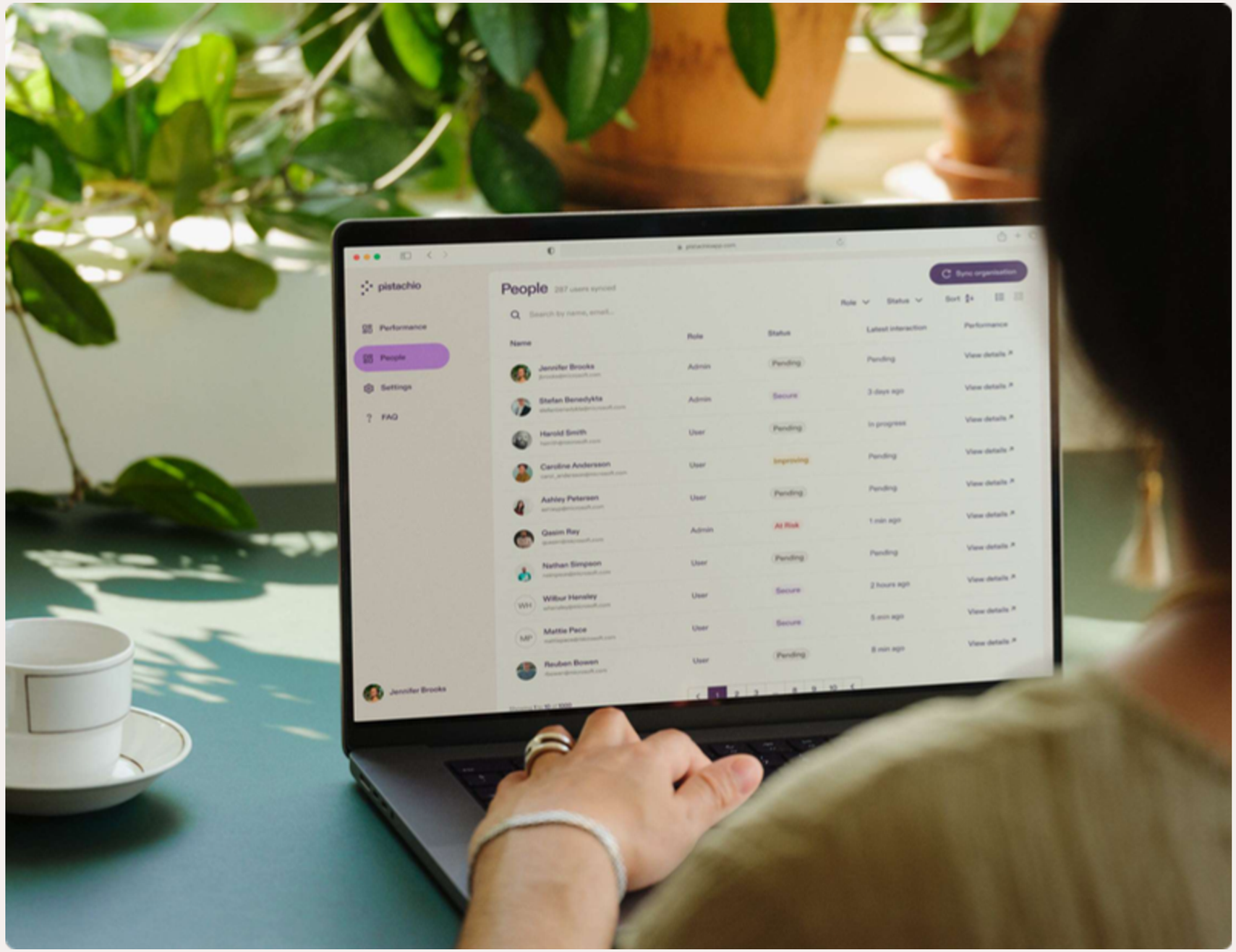
Our solution is so easy to set up that you can do it yourself directly on our website.

Connects to your Microsoft AD

We understand the struggle of keeping up with multiple tools. That's why we sync with your Active Directory, saving you from extra work.

No special settings required

You won't find anything to whitelist or tools to configure here. Just follow the steps on our site and you're all set.



pistachio

italik

Turn on Pistachio and we'll do the rest

Our product is designed to make your life easier, not add more work. Just press the big "on" button and you're done.

Attacks and training delivered automatically

Leave the training logistics to us. We'll handle everything for you, ensuring your people get the absolute best without any hassle on your end.

Tailored content based on your role, software used, location, and more

We adjust the frequency, difficulty, and content of our attacks and training to meet the unique requirements of each user.

Seamless for Your Employees

pistachio

italik

No login required

Don't let sign-ups and logins get in the way of your awareness training—we've streamlined the process for you.

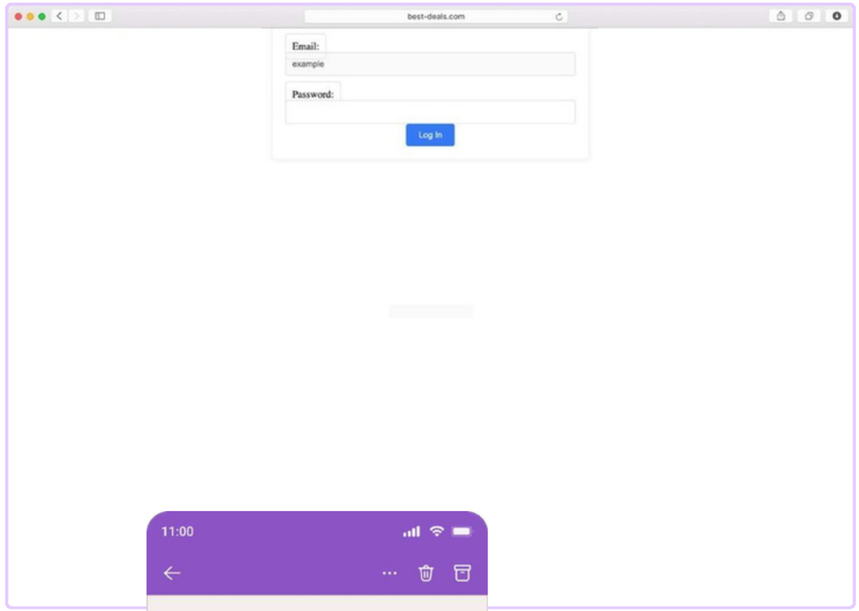
Training and attacks sent straight to each user's inbox

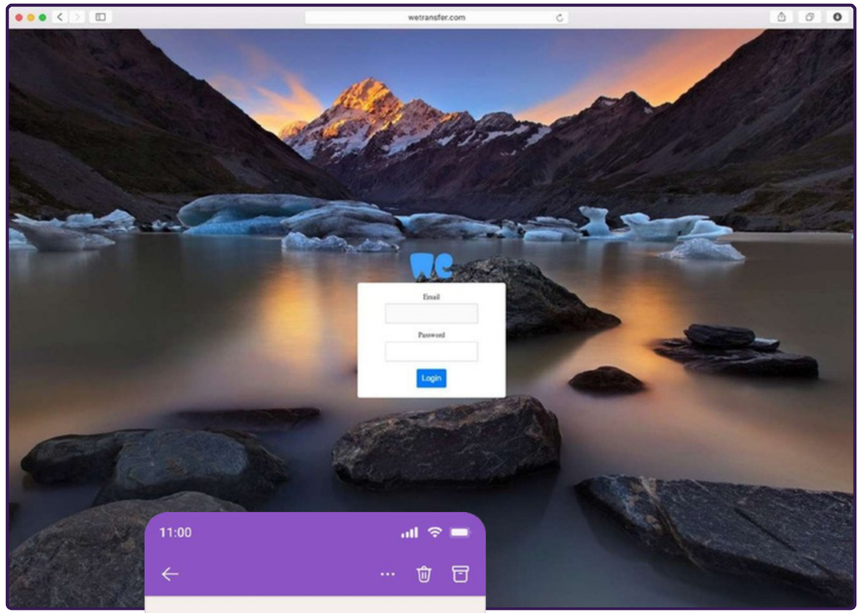
We take the content directly to your employees, saving them time and eliminating the dread.

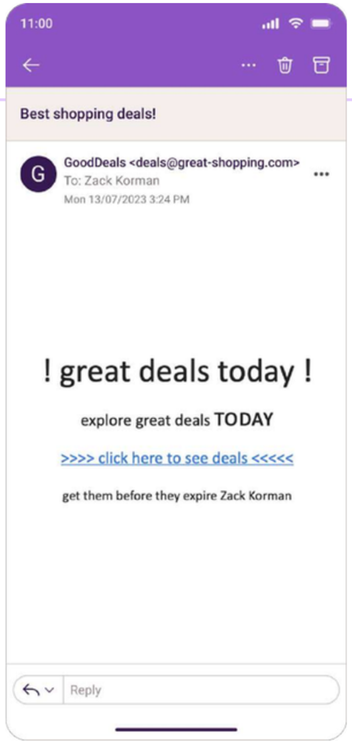
pistachio

italik

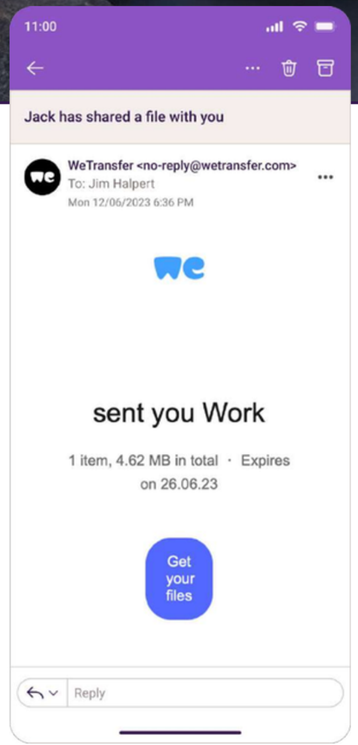
Attacks







Easy

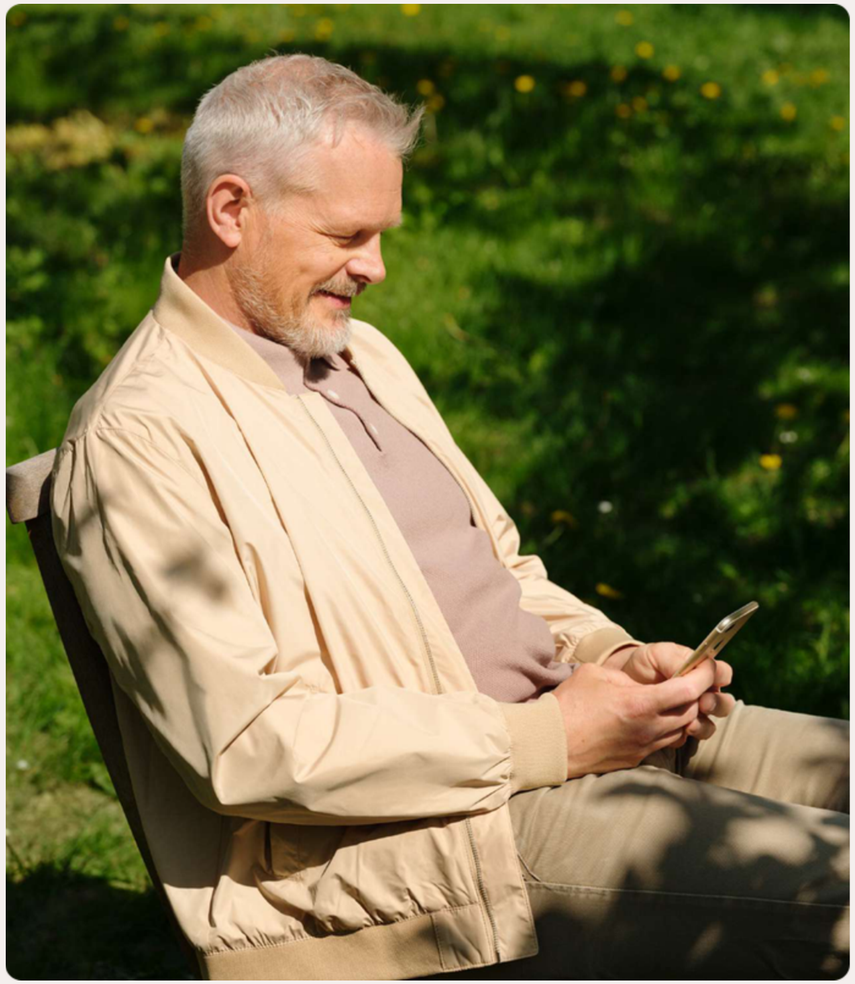


Hard

- Our library contains hundreds of attacks covering different software services, locations, departments, roles, and more.
- We employ email spoofing as part of our tactics, enabling us to replicate any email address, such as support@netflix.com.
- Testing link clicks alone won't reveal your full exposure. Our attacks go beyond that, checking if users leak their credentials too.
- C-suite impersonation is a tactic frequently used by attackers, and we do the same in our attacks.

pistachio

italik



We want our attack simulations to be a tool for learning, not a source of anxiety. Making mistakes won't get you in trouble.

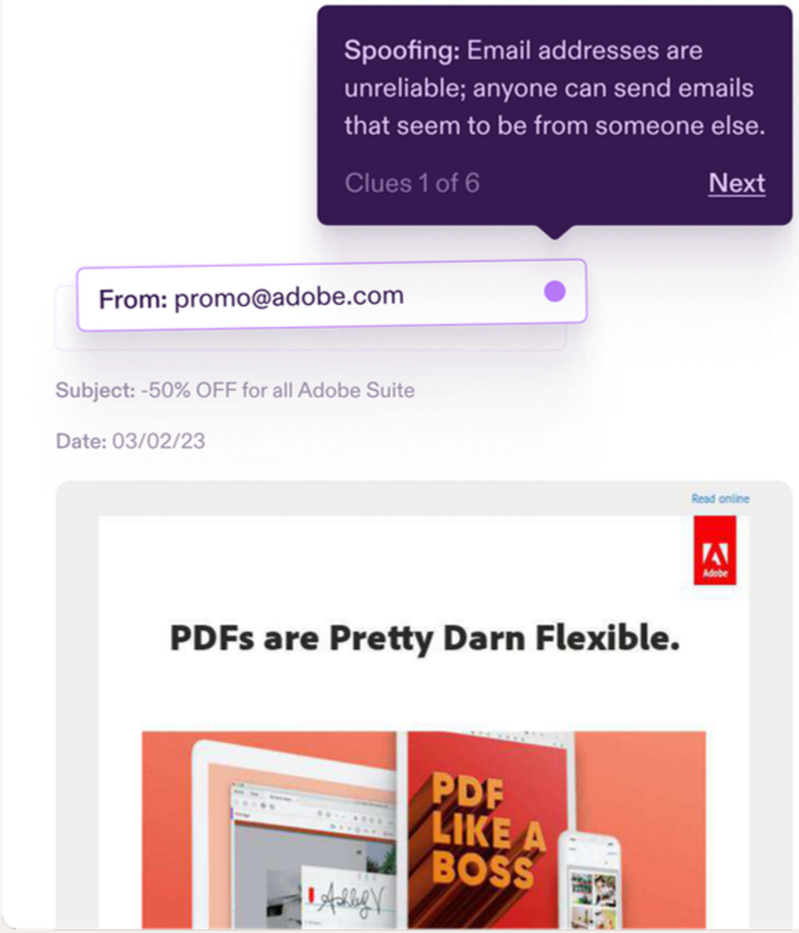
After falling for an attack simulation, we'll show you what gave it away as a phishing attack.

Uh-oh! You just gave your info to potential scammers!

During our cybersecurity training, you shared some info you shouldn't have. Don't panic! It's just a test, but a reminder to be more careful next time.

What clues did I miss?

User



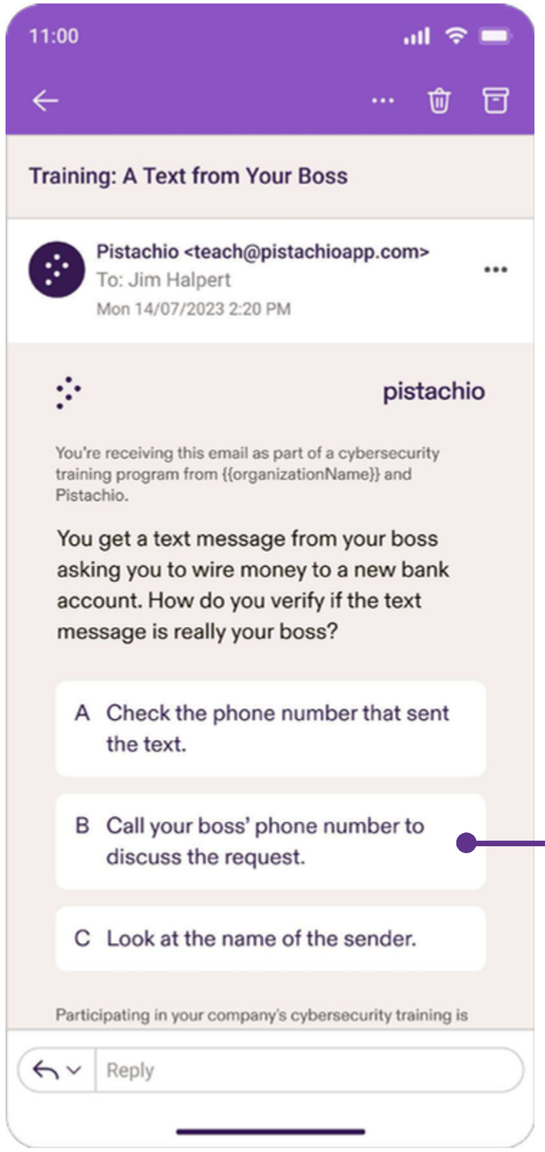
Getting instant feedback in a practical context is the best way to teach people to spot phishing attacks.

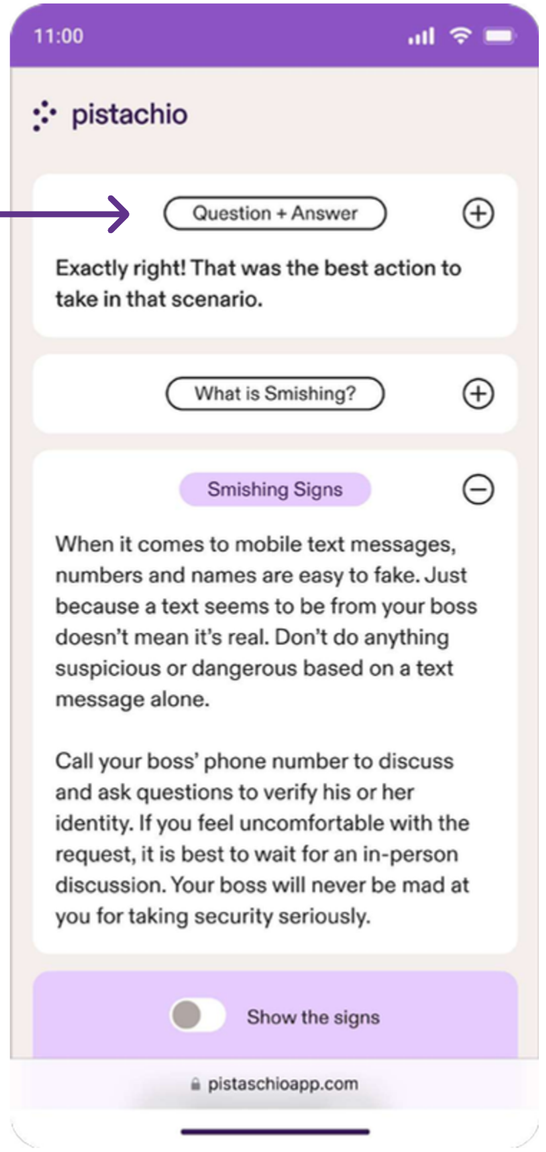
pistachio

italik

Training

- Animated videos and games can be fun, but the initial thrill wears off quickly, and people start losing interest.
- Simplified and efficient: We send emails with the security-related questions directly to employees' inboxes.
- With this approach, we have the ability to produce new content and address new threats instantly.
- Users receive simulated attacks that correspond to the subjects they have learned to verify their comprehension.





pistachio

italik

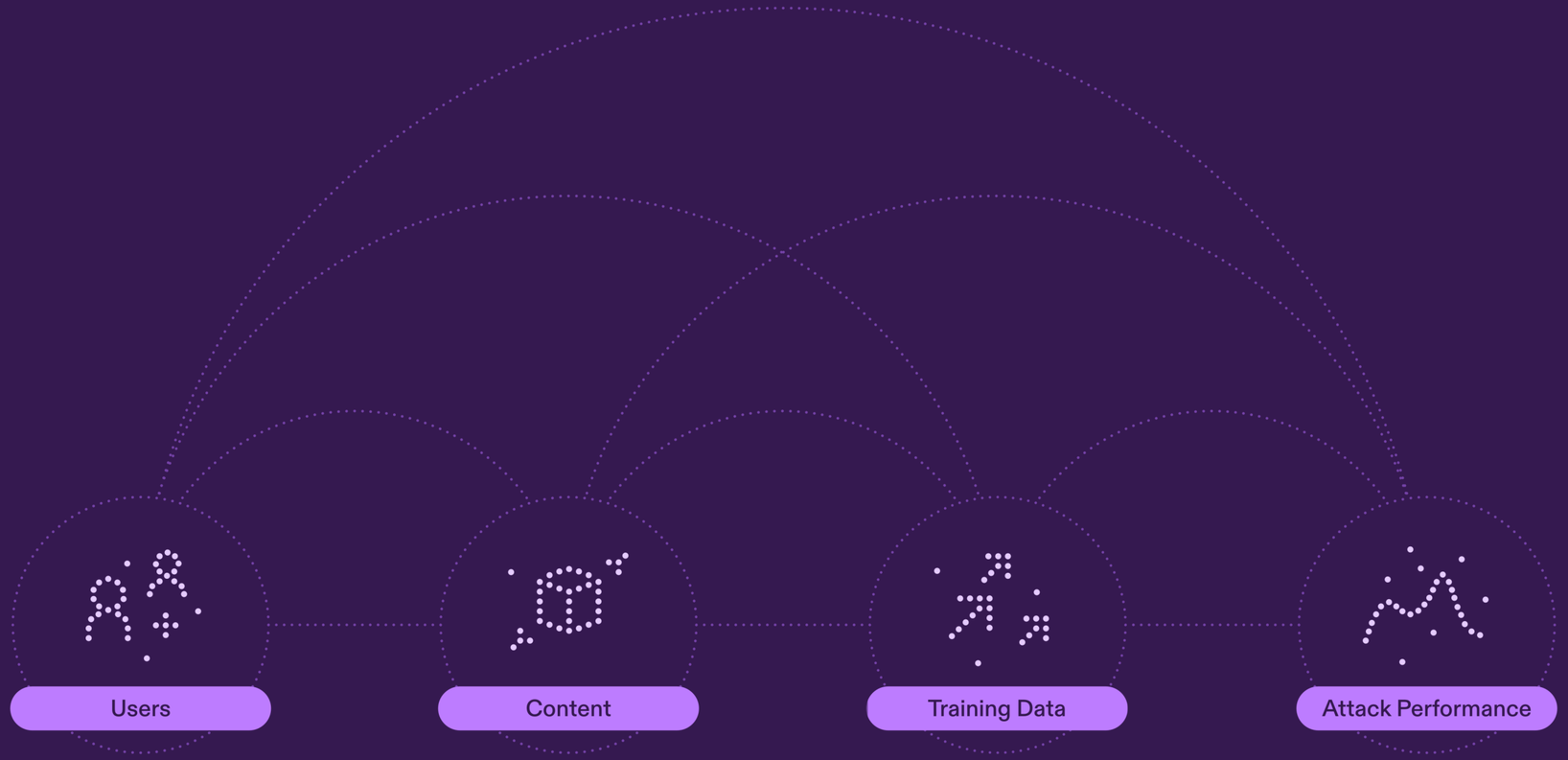
With the help of GPT4, we transform the data from your Microsoft Active Directory into a structured format, giving us valuable info about your job, location, software usage, and more.

pistachio

italik

Our system continuously evaluates each user to determine whether to deliver training materials or launch an attack. It does this by taking everything we know about the user and our content, and feeding that data into a series of algorithmic scorers.

We never send a user more than two emails in a single week.



- Time Randomizer: Based on the user's training and attack history, we make a probability-based decision on whether to send something or not.
- Sequencer: Pistachio sometimes carries out attacks in a specific order, like sending password reset reminders after the user already reset their password. These attacks get a higher score because they follow up on something the user has already received.
- Relevance Matcher: We give preference to content that matches your attributes like software, job title, department, and location.
- Difficulty Adjuster: If a user ignores attacks, we prioritize attacks that are slightly more difficult over those that are much more difficult or easier. We follow the opposite approach if the user fails attacks.
- Shuffler: We add a tiny bit of noise to the score, just to keep things interesting.
- Language Matcher: We score content higher if it is available in the user's preferred language.
- Categorizer: If we send an email training you on a given topic, we'll intentionally send more challenging attacks relating to that topic to evaluate your understanding and application of the material.