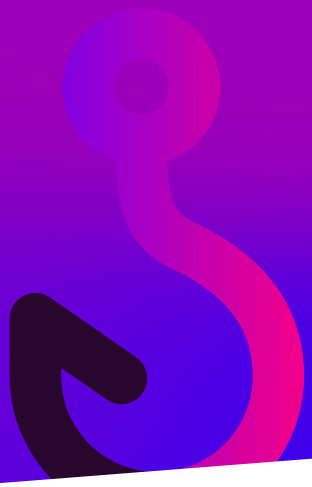
vade

Anti-Phishing Solution

AI-based phishing protection against unknown threats



WHY – Cybercriminals have developed sophisticated techniques to obfuscate the signs of phishing and bypass traditional email filters.

SOLUTION – Vade's anti-phishing technologies use artificial intelligence, including machine learning and computer vision, to detect and block malicious links and webpages.

Real-time phishing protection

Backed by proprietary, patented technologies and fed by data from more than 1 billion mailboxes, Vade's anti-phishing solution performs real-time behavioral analysis of the origin, content, and context of the email and webpage to identify phishing attacks.

Multi-faceted Anti-Phishing Analysis — Performs a real-time, multilayered behavioral analysis of the email and URL, following any redirections to determine whether the final page is fraudulent. Machine learning models analyze 47 features of the email and URL for malicious behaviors, while computer vision algorithms scan for modified logos, QR codes, and other images commonly used in phishing attacks.

Token Anonymization — Tokens within URLs are randomly replaced in order to safely explore the page content without triggering any action on behalf of the user. This capability is critical to Time-of-Click analysis, which prevents attacks that leverage dynamic links and sleeper pages.

Computer Vision — Views images as a human would, detecting images commonly used in phishing emails, including QR codes, text-based images, remotely hosted images, and brand logos. The Computer Vision Engine can detect logos from the top 60 impersonated brands, including Microsoft, PayPal, and Facebook.

Mobile Rendering — Pages are explored across more than 30 different device-browser combinations (e.g. Safari on iPhone, Chrome on Android, etc.) in order to thwart attacks designed to only display their content on mobile devices.

Regional Page Exploration — Pages are explored from four zones — North America, South America, Europe, and Asia — to combat phishing pages that display their content only when accessed from the targeted location.

Auto and One-Click Remediation* — With a real-time view of global threats, Vade's AI engine is continuously learning and automatically removes any threats from user inboxes. Admins can also remediate phishing emails with one click.

*Available in Vade For M365

Additional capabilities

- **Automatic Site Closure** — Vade shares information with organizations that are unknowingly involved in phishing attacks, rapidly blocking URLs and automatically closing malicious websites.
- **Brand Alerts** — Brands and domains that have been usurped by hackers are alerted by Vade so that they can warn their customers as quickly as possible.
- **IsItPhishing** — Vade's IsItPhishing.AI allows users to enter a URL in a search bar and automatically identify whether a suspicious link is a phishing URL.

880 million
phishing emails
detected / year

1 billion
mailboxes
feeding AI engine

100 billion
emails
analyzed per day

Vade's patented anti-phishing technologies are embedded in its:

- **Native, API-based product for Microsoft 365**
- **Cloud-based product for Exchange, Google Workspace etc.**
- **Gateway solution**

About Vade
- 1 billion mailboxes protected
- 100 billion emails analyzed / day
- 1,400+ partners
- 95% renewal rate
- 15 active international patents

Learn more
www.vadesecure.com

@vadesecure

Contact
Sales

sales@vadesecure.com