

Anti-Phishing Solution

AI-based phishing protection against unknown threats



Cybercriminals have developed sophisticated techniques to obfuscate the signs of phishing and bypass traditional email filters. Vade Secure's anti-phishing technologies use artificial intelligence, including machine learning and computer vision, to detect and block malicious links and webpages.

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

REAL-TIME PHISHING PROTECTION



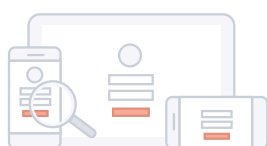
Multi-faceted Anti-Phishing Analysis: Performs a real-time, multilayered behavioral analysis of the email and URL, following any redirections to determine whether the final page is fraudulent. Machine learning models analyze 47 features of the email and URL for malicious behaviors, while computer vision 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, and brand logos. The Computer Vision Engine can detect logos from the top 30 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 Secure for Microsoft 365*

ADDITIONAL CAPABILITIES

-  **Automatic Site Closure:** Vade Secure 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 Secure so that they can warn their customers as quickly as possible.
-  **IsItPhishing:** Vade Secure'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 in the last year



1 billion

mailboxes feeding AI engine



10 billion

emails analyzed per day

Vade's anti-phishing technologies are embedded in all of its products, including its native, API-based solution for Microsoft 365; its cloud-based solution for Exchange, GSuite, and other environments; and its Content Filter SDK for ISPs and telcos.

About Vade Secure

- ✓ 1 billion mailboxes protected
- ✓ 1,400 partners
- ✓ 95 percent renewal rate
- ✓ 11 active international patents
- ✓ 2 billion messages filtered last year

Contact

Vade Secure Sales
US/EMEA

sales@vadesecure.com

