

The phishing email that looks exactly right. Caught anyway.

Netarx Identity Key (NIK) · Advanced AI email model

Content filters ask what a message says. The new NIK Advanced AI email model asks whether the message fits the sender's real relationships and communication patterns, drawn from the NIK social graph. A familiar name from an unfamiliar device, a request that breaks a long-established pattern, a "colleague" with no history at all: that is how it catches impersonation and business email compromise that content scanning misses.

NOTHING TO RIP OUT. NOTHING TO LEARN.

It runs alongside your current anti-phishing stack. Nothing to replace, no changes to mail flow, and no impact on the tools you already trust.

No rollout project and no retraining. Your team keeps every tool it already trusts, employees read a color instead of learning another dashboard, and the trust verdict is useful the day it is switched on.

One answer on every email. No second-guessing.

Green

Verified sender. Fits the relationship, the device, and the pattern. Act on it.

Yellow

New or partially verified sender, or one anomalous signal. Proceed with care.

Red

Likely impersonation, BEC, or fraud. Stop, and the reason is shown.

Nothing to replace

Keep your secure email gateway, Defender, or API-based filter exactly as it is.

No mail-flow changes

No MX or routing changes. NIK reads signals; it never sits in the delivery path.

No user retraining

Employees already know what a traffic light means. That is the whole interface.

Feeds your stack

Verdicts and signal context flow to SOC, SIEM, and SOAR tools you already run.

What the relationship graph catches that content filters cannot

Scenario	Content-based filter	NIK Advanced AI email model
CEO look-alike domain asks finance for an urgent wire	Passes. New, clean domain and nothing malicious in the text.	Red. The real CEO has a verified key, a known device, and has never requested a wire by email.
Compromised vendor mailbox sends new bank details	Passes. SPF, DKIM, and DMARC are all valid because the mailbox is real.	Red. Same address, but device, route, timing, and request pattern break from history.

Every suspicious email costs time. Here is how much.

Awareness training taught employees to stop and inspect. That hesitation, and the reports it generates, is a cost that shows up every day and never appears on an invoice. NIK removes it with one light on every message: green means act, red means stop.

7 hrs

lost per employee, per year, to phishing

Ponemon Institute, 2021

23.2 min

of analyst time per reported email

Osterman Research, 2026

80-85%

of employee reports are benign

Hoxhunt, 2025

36.5%

of security team hours go to phishing

Osterman Research, 2026

PER 100 EMPLOYEES, EVERY YEAR

About 1,160 hours and \$67,500 spent deciding whether email is real

Employee hesitation

700 hrs

≈ \$34,500

Analyst triage of reports

464 hrs

≈ \$33,000

Total

1,164 hrs

≈ \$67,500, or 29 working weeks

Employee hours: 7 per employee per year (Ponemon Institute, Cost of Phishing 2021) at \$49.32 per hour total compensation (U.S. Bureau of Labor Statistics, March 2026). Analyst time: one report per employee per month at 23.2 minutes and \$27.51 each (Osterman Research for IRONSCALES, June 2026). Report volume is an assumption; substitute your own.

1/10th

NIK costs about a tenth of what this hesitation costs you.

The productivity it returns is roughly ten times its price, before a single blocked attack is counted.

For employees

Green mail gets acted on. Red mail arrives with the reason attached. The inspecting, hovering, and forwarding to IT stops.

For the security team

Fewer benign reports reach the queue. Those that do carry NIK's verdict and signal context into the SIEM, so the 23 minutes go to messages that earned them.

At 1,000 employees the same math is roughly \$675,000 a year, before a single successful attack.

No passwords. Provable history. Ready for post-quantum.

Every verdict on this sheet rests on one thing: knowing, cryptographically, who is on the other end. The Netarx Identity Key is an advanced passkey bound to each device. There is no password to type, phish, reuse, or reset. Identity and verification events are anchored to a blockchain ledger, so the relationship history the AI reasons over is tamper-evident and independently verifiable, not just a database entry.



Simple

Nothing to remember, nothing to type. The key travels silently with every message and call. Employees see a color, not a prompt.



Secure

No shared secret exists, so there is no credential to steal or replay. Forging history means rewriting a ledger, not editing a record.



Upgradable

Crypto-agile by design. Signature schemes rotate to NIST post-quantum standards (FIPS 203, 204, 205) without re-enrolling users.

THE REST OF THE PLATFORM 03

One identity key, every channel



Video and voice deepfake detection

Teams, Meet, Zoom, and WebEx participants analyzed live for diffusion, GAN, faceswap, and avatar generators; organic versus synthetic speech on calls.



Mobile calls and text

Android and iOS. Device ID, calling and called party, and out-of-band verification when a message does not fit.



Call center

SIPREC compatible on most PBXs. Voice participant analysis flags synthetic speech before an agent resets a password or approves a change.



Images and social media

Upload, screen capture, or scan directories. EXIF and image forensics for diffusion, GAN, and faceswap content.



Voting ensemble of dozens of AI models

Hundreds of digital signals, multimodal and multisensory, resolved into one continuously updated answer.



SOC, SIEM, and SOAR ready

Verdicts and signal context flow to the tools your team already runs, cutting triage time and mean time to respond.



Azure cloud or federated on-prem

Deploy in Azure or federate validation on-premises. FedRAMP Moderate alignment work under way.



Audit trail by default

A verifiable record for every conversation supports regulatory obligations and strengthens cyber-insurance posture.



Restore trust in every conversation

sales@netarx.com

www.netarx.com