Securing Postal Communications

Lars Sandbergen

Dawley Stuvel

Inaugural DNS Security Forum 2026

23 June 2026

— 01 THE THREAT LANDSCAPE

Email is the front door, and it's wide open

90%+

of all cyberattacks begin with an email.

Industry consensus

3.4bn

phishing emails hit inboxes every day, **82.6%** are now AI-generated.

StationX, Phishing Statistics 2026

21sec

median time for someone to click a phishing link.

Verizon DBIR 2025

54%

click rate for AI spear-phishing

Harvard Business Review 2024

- Postal, shipping & supply-chain is **uniquely exposed** : high transaction volumes, constant vendor communication, and tracking links that everyone is trained to click.

02 WHY POSTAL IS AN INTERESTING TARGET

Three ways attackers weaponise the post

RISK 01

The transportation risk

The transportation and logistics sector is a prime target for Business Email Compromise (BEC), suffering from some of the **highest response rates** to scam emails.

Top 3 sector for BEC

RISK 02

The delivery bait

Retail and logistics impersonation dominates global phishing traffic because attackers exploit our **reflex to click on "failed delivery" or "update address" notifications.**

#1 most-impersonated consumer category

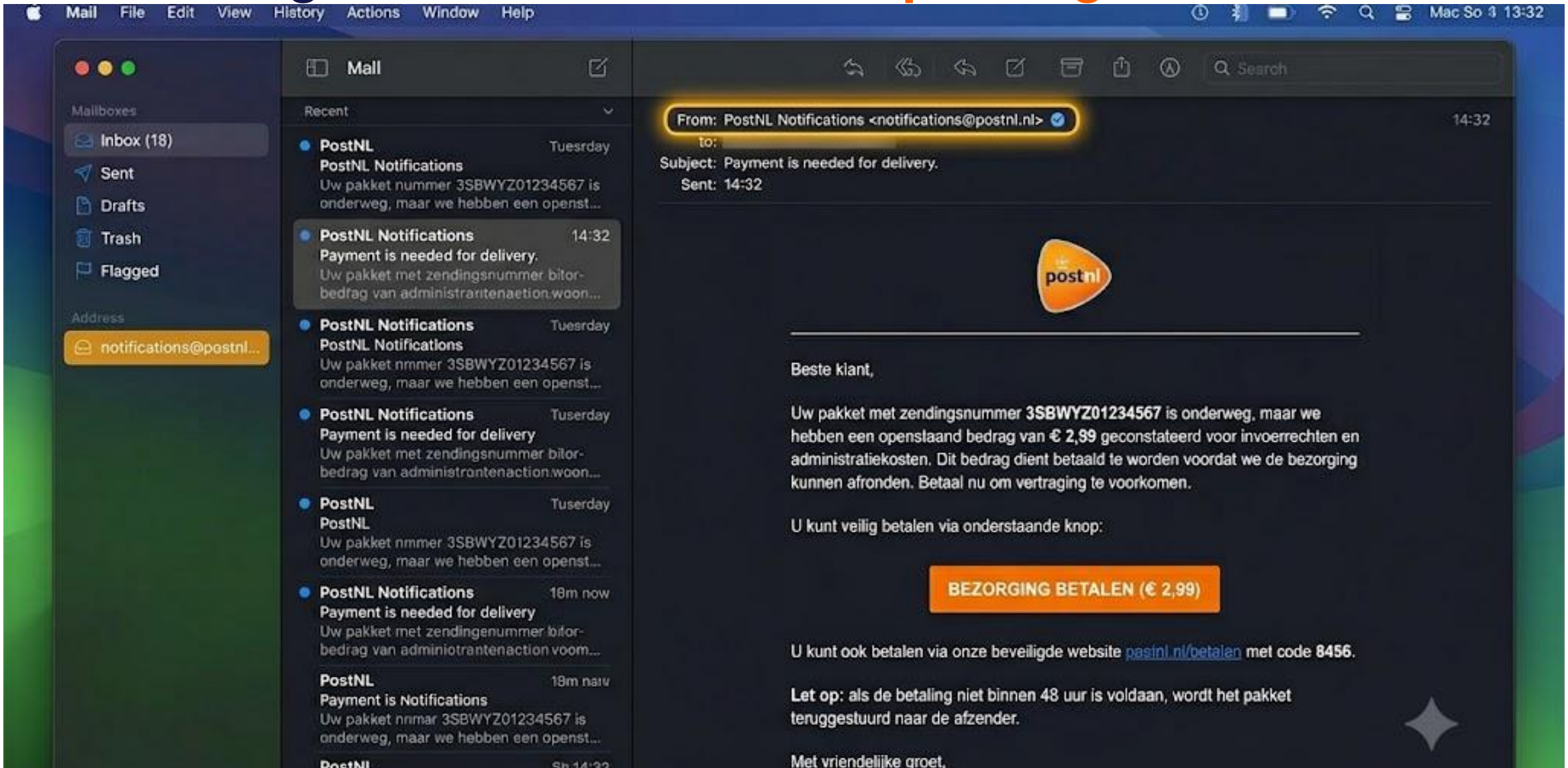
RISK 03

Vendor email compromise

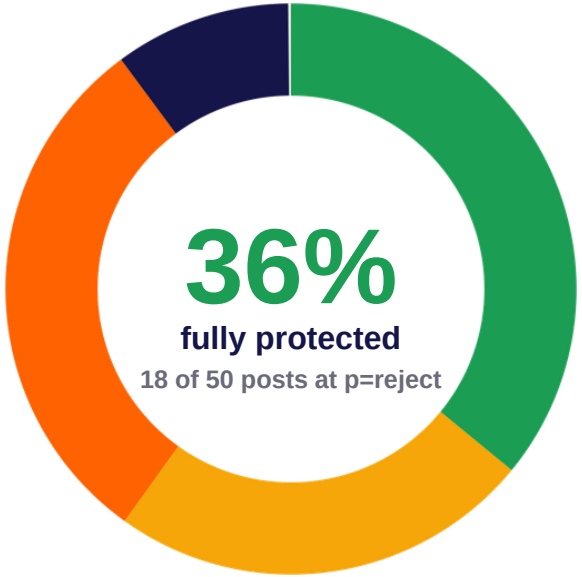
Postal networks process millions of third-party supplier invoices, making them prime targets for fake billing and invoice updates

66% of organisational phishing is pretexting & fake billing

Preventing exact-domain name spoofing



Only 18 of 50 are actually protected



p=reject	Protected	18
p=quarantine	Not fully protected	12
p=none	Not protected	15
No record	Not protected	5
TOTAL SURVEYED		50

! **32 of the 50 most-trusted postal brands can still be spoofed today. Anything below p=reject leaves the door open.**

Email is critical infrastructure

- 55 to 60 million messages each month
- Track & Trace
- Delivery Notifications
- Customer communications

A high value phishing-target

Email security is about protecting our customers trust

Email is not built for security

Built for delivery, not for authentication

- Store-and-forward protocol
- No inherent sender verification
- From header and domain spoofing

Phishing, brand impersonation and fraud

Establishing trust with open standards

SPF → Sending infrastructure

- Authorized list of sending sources

DKIM → Message integrity

- Adds digital signature
- Domain match
- Original message

DMARC → Policy & Enforcement

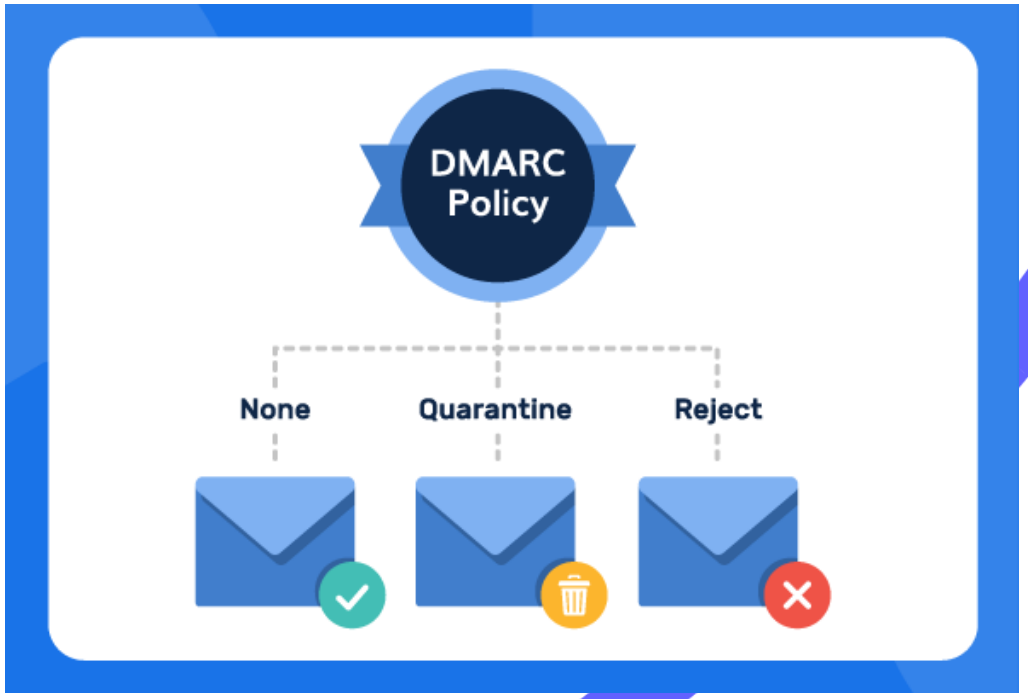
Combined control needed

15 juli 2026

The move to p=reject is not a switch but a project

PostNL DMARC Journey

- Start in 2016
- Insights in the email flows
  - Unknown senders
  - Misconfigurations
- Domains to P=quarantine
- Analysis of DMARC reports
- Over to P=reject



15 juli 2026

Complexity

- 6 months of DMARC data
- 500+ senders
  - Internal systems
  - SaaS platforms
  - Vendors
- Organizational challenges
  - Unknown senders
  - Unclear ownership
  - Misconfigurations
  - Fear of blocking

No longer a technnical problem

Most of the time, it’s not a technical problem, but an operational one

Emailsecurity of today

3000 domains

100% DMARC p=reject

Full enforcement

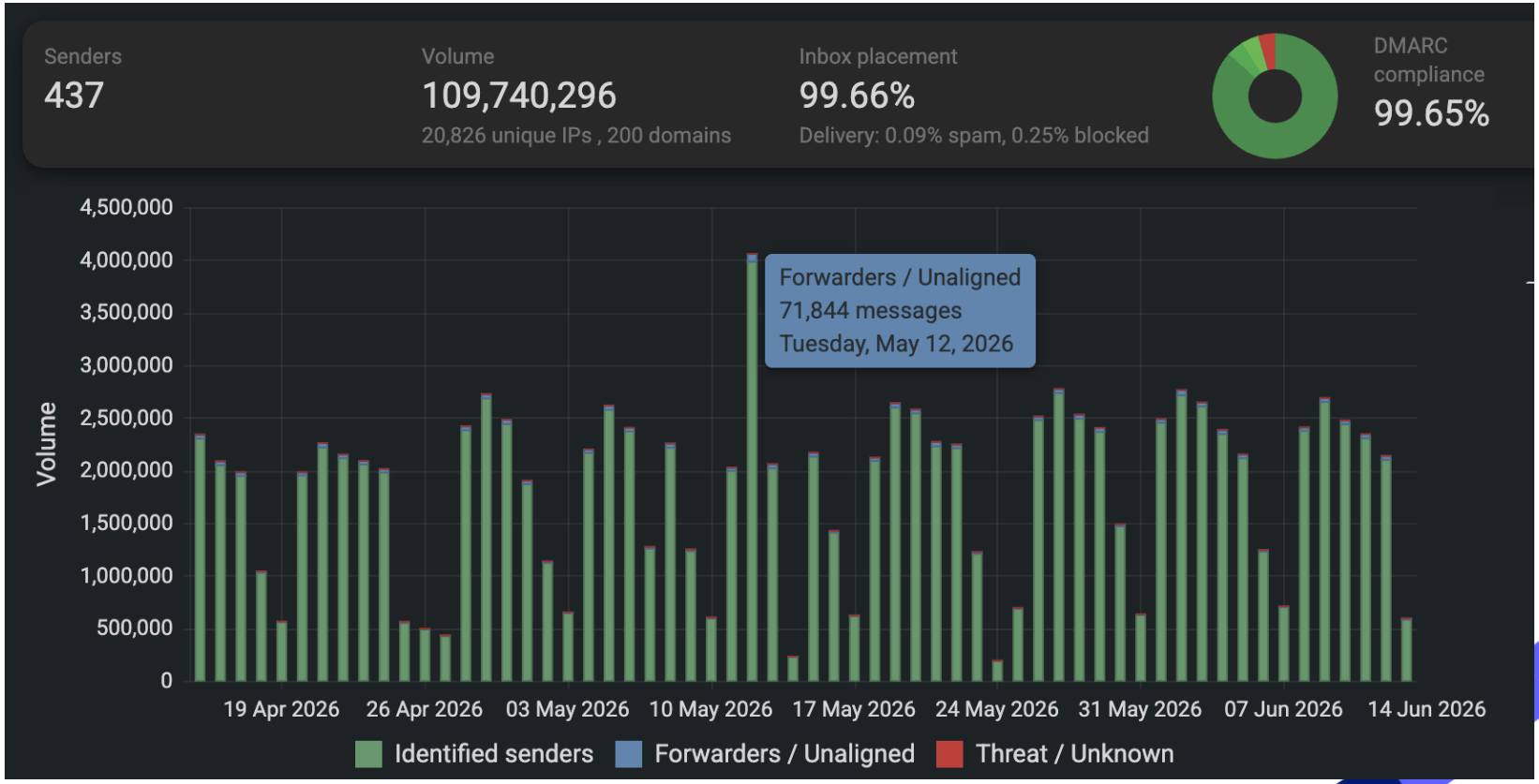
Clear outcome

Valid mail passes

Invalid mail is rejected

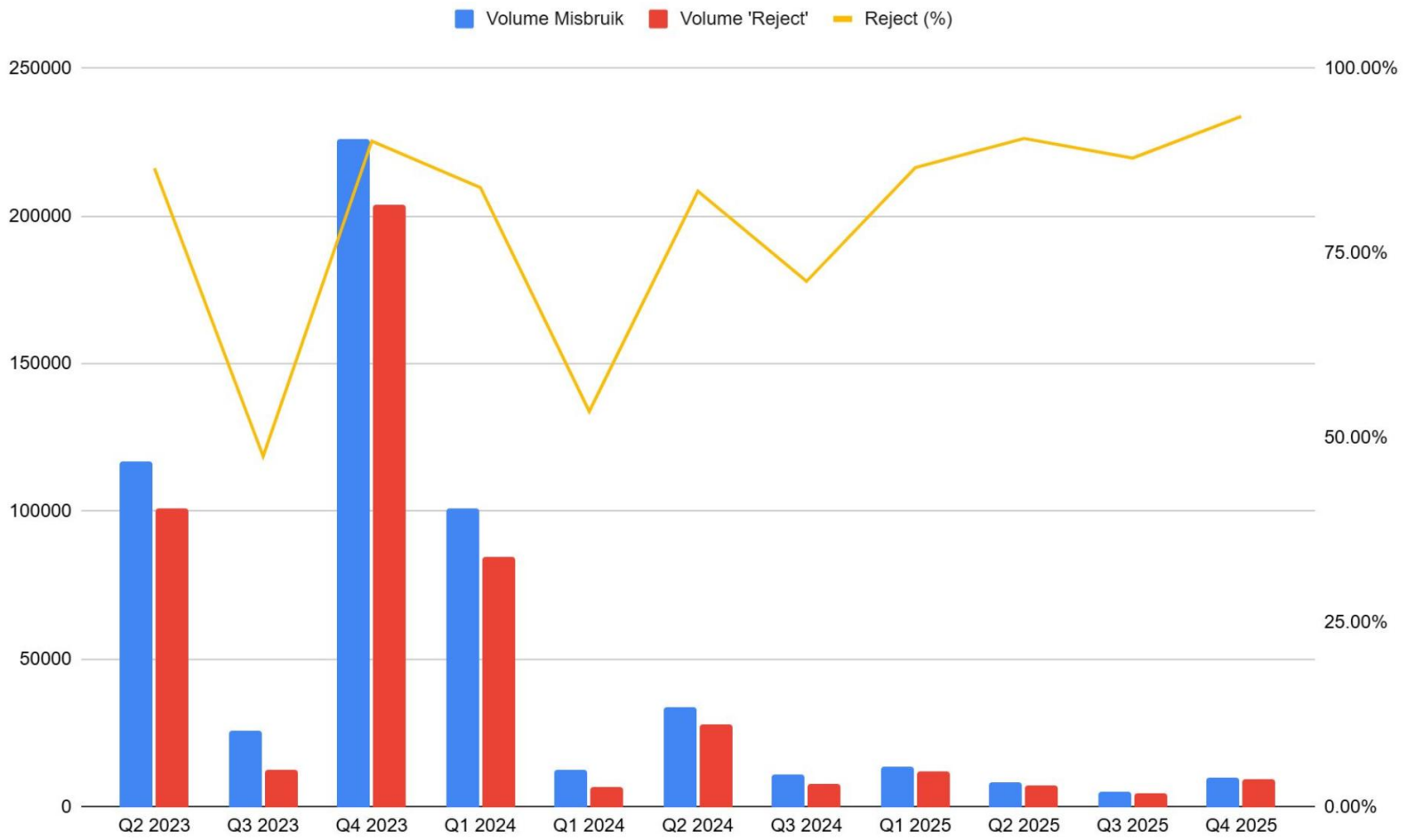
Emailsecurity of today

Clear outcome



Emailsecurity of today

Clear outcome



We have a reject percentage of 98.45%

Local override policies

What’s next?

- Relaxed Alignment (Default)
- Allows partial domain matching
  - Flexibility
  - Loopholes
- Moving to strict alignment
- Exact domain match required
- No shortcuts

Relaxed alignment	
DKIM Domain	mail.vendor.**postnl.nl**
From domain	**postnl.nl**
Result	PASS

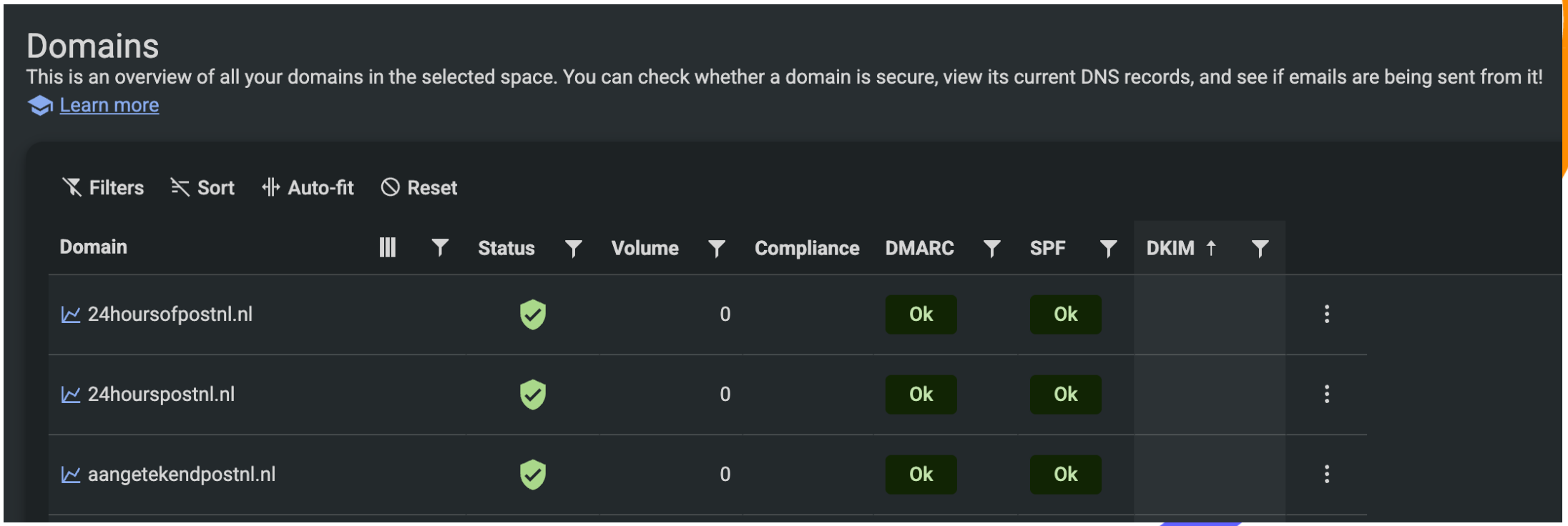
Strict Alignment	
DKIM Domain	mail.vendor.**postnl.nl**
From domain	**mail.vendor.postnl.nl**
Result	PASS

Stronger control over who can send on your behalf

PostNL approach

- Governance
  - Digital Security & Trust Services
    - Enterprise Firewall
    - Certificate Services
    - Public DNS
    - Secure Emailing
- Ownership
  - Every domain & sender
  - Requested through the webshop
- Onboarding
  - SPF, DKIM, DMARC
- Lock the domain down

PostNL approach



Governance makes e-mailsecurity scalable

Phishing... A problem of the past?

Unfortunately, only PostNL owned domains are protected

- DMARC only protects your own domains
- Lookalike domains still bypass protection
  - p0stnl.nl
  - postnl-tracktrace.net
- Phishing remains a real threat
- Takedown processes are required
  - Cybersecurity Office
- Continuous improvement with DMARC partner

Security is an ongoing process

15 juli 2026

BIMI, what about it?

Next to security, also interesting from marketing perspective

- Brand Indicators for Message Identification
- Displays your verified brand logo in the inbox
- Builds brand recognition & user trust

- Survey by Entrust:
  - 21% increase in open rates
  - 18% increase in brand recall
  - 34% increase in purchase likelihood

BIMI, the reality

- Not a security control
- Requires p=quarantine
- Requires registered trademark + SVG logo
- Requires VMC certificate

Emailsecurity requires a combination of controls

Extra layers of security

Securing the full outbound communication chain

Domain Security

– DNSSEC

Sender Authentication

- SPF
- DKIM
- DMARC

Transport Security

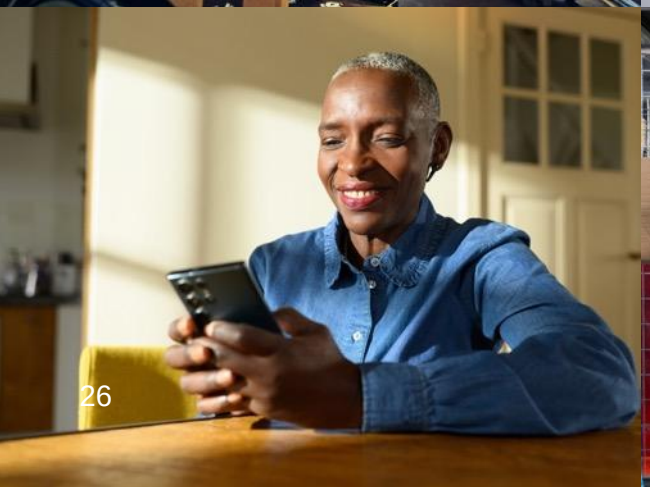
- STARTTLS
- MTA-STS
- DANE (In progress)

Brand & Visibility

- BIMI
- Anti Phishing Code

A layered approach to securing email




Key Takeaways

- DMARC is the foundation
- Enforcement (p=reject) is critical
- Control is knowing your senders & domains
- Governance makes it scalable
- Attackers move on. Don’t be the next target

Call to action

Postal operators are high value targets.

Reduce your attack surface by protecting your domains

Start:

DMARC Journey

Move to enforcement

Take control of your domains

Trust in postal services must extend to digital communication