

PRODUCT INFORMATION · MICROSOFT 365

Cybereinforce Email Security

Every email investigated, every verdict explained, every link checked twice, and PhishSecure for anything in doubt.

November 2026 · Cybereinforce Threat Enforcement, a Cybeurope product

WHY EMAIL NEEDS MORE THAN A SCORE

Today's phishing is built to look legitimate.

The link points at a real file-sharing site. The sign-in page is the real Microsoft one. The invoice comes from a domain one letter away from your supplier's. And when something is flagged, people are told a number, not a reason.

Lures behind trusted links

"A file was shared with you" on SharePoint, Drive or Dropbox, one click away from a credential page on another domain.

Device-code theft

Victims are sent to Microsoft's genuine device login with an attacker's code, handing over a full Microsoft 365 session.

Payment fraud without links

New bank details, an IBAN and urgency, sent from a look-alike of your own or a supplier's domain.

Verdicts nobody can read

A bare risk score gives users and admins no way to tell whether to trust, release or report a message.

THE PRODUCT

Intelligence-driven email protection for Microsoft 365.

Cybereinforce Email Security brings the engine that already protects browsers into the inbox. It connects through Microsoft Graph, so there is no MX change, no gateway and no agent on devices.

Investigates every email

Sender, authentication, history, every link to its final page and every attachment, checked within seconds of arrival.

Explains every verdict

Five clear bands from Clean to Critical, always with the exact reasons, shown in the email itself.

Checks links twice

On arrival and again at the moment of the click, across every redirect, because pages change after delivery.

PhishSecure

One click opens a doubtful email in an isolated cloud browser. Nothing on it reaches the user's device.

One engine, two products. Indicators, threat intelligence and your organisation's rules are shared with Cybereinforce browser protection, so a threat caught in email is blocked in browsers as well, and the other way round.

HOW IT CONNECTS

From arrival to verdict, without touching mail flow.

Microsoft 365 delivers as usual. Microsoft Graph notifies Cybereinforce the moment a message lands, and every action is taken in the mailbox itself.

Microsoft 365
Mail delivered normally by Exchange Online.

›

Graph notification
Change notification for the protected mailbox, within seconds.

›

Instant pass
"Being checked" banner and protected links while the scan runs.

›

Investigation
Sender, links, attachments and content scored in your region.

›

Verdict in the email
Checked strip, warning banner or quarantine with a notice.

Admin consent, once

A Global Administrator approves the Cybereinforce app in Microsoft Entra ID. No passwords or client secrets are exchanged.

Mailboxes join automatically

Licensed mailboxes are protected straight away; new users can be protected automatically as they join.

Works alongside Microsoft

Exchange Online Protection and Defender for Office 365 keep running; Microsoft's Report button stays in place.

THE INVESTIGATION ENGINE

Five angles on every message.

Each email is examined the way an analyst would: who sent it, where its links really go, what it carries, what it asks for, and whether it fits the history between sender and recipient.

Sender

- SPF, DKIM and DMARC, weighed by real enforcement
- Registration age of the sending domain
- Reply-To routed to free webmail
- Machine-generated domain names
- Brand name on an unrelated domain

Links

- Redirect chains followed to the end
- File-share "sign in to view" lures crawled hop by hop
- Password forms and Microsoft look-alikes on the final page
- Device-code login steering
- Link-domain age and reputation

Attachments

- File hashes against threat intelligence
- HTML attachments with a live password field
- Hashes of quarantined attachments added to intelligence

Content

- Checksum-valid IBANs
- Payment and financial-action language
- Account set-up combined with payment
- Extortion, advance-fee, crypto and prize scams

Relationship

- First-time sender to this mailbox
- "RE:" with no real prior thread
- Link domain outside the sender's usual pattern
- Known senders learned per tenant

HOW A VERDICT IS REACHED

Two tiers of evidence, one explained verdict.

Decisive signals act on their own. Weaker signals add up. Every signal that fires is written into the verdict as a reason.

Decisive tier: straight to Critical

Any one of these is enough on its own:

- **Known indicator** in your rules or Cybereinforce threat intelligence
- **Device-code phishing** or a Microsoft sign-in form off Microsoft
- **A look-alike of your own domain**, as sender or link
- **Link or sender domain under two years old**
- **HTML attachment** with a live password field
- **Blocked by independent security DNS**, or a link domain that no longer resolves
- **Confirmed phishing-hosting patterns** and extortion templates

Additive tier: weight builds the band

First-time sender, a fake reply, a valid IBAN, a brand name on an unrelated domain, an elevated-risk extension, generic cloud hosting, a suspicious listing in threat intelligence: each adds weight, and the total sets the band.

- **Soft signals alone stay a warning.** Mail with only weak evidence is capped at Elevated and never quarantined on that alone.
- **Real evidence escalates.** An unusual link from a regular sender counts only alongside other evidence.

Clean	Low	Elevated	High	Critical
Checked strip	Checked strip	Warning with reasons	Warning or quarantine	Quarantined

EXPLAINED, IN THE EMAIL ITSELF

Your people see the reason, not a number.

⏳ **Cybereinforce is checking this email**

Appears within seconds of arrival. Links already route through Cybereinforce while the scan finishes.

✓ **Checked by Cybereinforce**

A slim green strip on safe mail, so users learn what "normal" looks like.

PhishSecure

⚠ **Flagged: be careful with this email**

"Sender's domain was registered 12 days ago." "Link domain doesn't match this sender's historical pattern."

PhishSecure Show details

⛔ **An email to you was quarantined**

A notice takes the place of dangerous mail, with the sender and the reason, so nobody goes looking for it.

Show details

One click opens the full evidence, signed and self-contained, with nothing stored:

- **Sender:** address, domain, first contact or known, domain age, authentication result
- **Every link:** its verdict and the evidence behind it
- **Defanged names** such as `example[.]com` so nothing in the banner is clickable by accident

The same reasons appear in the admin console and the quarantine review, so users, IT and analysts all read one explanation.

CLICK-TIME PROTECTION

Every link is checked again when it is clicked.

A page can be harmless at delivery and weaponised an hour later. Every link in a protected email is rewritten to pass through Cybereinforce first, so the decision is made with what the page is now.

User clicks
Any link, in any protected email, at any time after delivery.

›

Signed link check
Tamper-proof link; your rules and threat intelligence checked first.

›

Every hop followed
Redirects and file-share lures followed to the final page.

›

Final page judged
Domain age, device-code steering, brand look-alikes, password forms.

›

Go, warn or block
Safe pages open directly; dangerous ones are stopped with the reason.

Independent of the delivery scan. The click check runs fresh every time, so a domain that turned malicious after delivery is still caught, even in an email that was marked clean.

PHISHSECURE

Unsure about an email? Open it where it can't touch you.

PhishSecure opens the email and its links in a fresh browser running in the Cybereinforce cloud. Your user sees and uses a live picture of the page, while everything on it runs far away from their device and your network.

1 · One click

The PhishSecure button sits in the banner of every checked email, and in Outlook through the add-in.

›

2 · Isolated browser

A new remote browser loads the email in seconds, in a region matched to your tenant.

›

3 · Every page checked

Each page is checked by Cybereinforce threat intelligence; malicious pages are blocked with the reason.

›

4 · Gone on close

Destroyed when the window closes, or after 3 minutes at the latest. No cookies carry over.

Nothing reaches the device

Scripts, redirects and credential pages run remotely. File downloads are blocked inside the session.

Same rules as the browser

Pages are judged by the browser product's rules, newly registered domains included, before the user sees them.

Visible to security

Every page opened or blocked in a session is logged as a security event for your tenant.

PHISHSECURE

Private by design, with time included in every plan.

Privacy and safety controls

- **Never recorded.** Session recording and logging at the browser provider are switched off.
- **Email content is not stored.** The message is loaded into the session and nowhere else.
- **Your mailbox only.** Each PhishSecure link is signed and opens only that message, in that mailbox.
- **Your region.** Sessions run in a region matched to your organisation's data region.
- **Short-lived.** A hard 3-minute limit, and the session is released the moment the window closes.

YOUR PLAN	PHISHSECURE TIME INCLUDED
Up to 500 mailboxes	1 hour per month
501 – 750 mailboxes	90 minutes per month
751 – 1,000 mailboxes	2 hours per month
Above 1,000	30 more minutes for every 250 mailboxes
Trial	10 minutes in total

Paid time renews on the 1st of every month. Only the time a session actually runs is counted, and a new session starts whenever at least 3 minutes remain. Time used and remaining is shown in the admin console.

SECURITY MODES

Choose how strict to be. Change it any time.

The same investigation runs in every mode. The mode decides what users see and what is quarantined, and a change applies across your tenant within minutes.

Connectivity

For a quiet first look at your mail.

- Nothing changes in the mailbox
- Every email still checked, scored and logged
- Nothing quarantined automatically

Balanced Default

Visible protection with the fewest interruptions.

- Checking banner and green strip
- Every link checked again at click time
- PhishSecure in every checked email
- **Critical** mail quarantined

Security First

For teams that want every doubt surfaced.

- Everything in Balanced
- Warning banner with reasons on Elevated mail
- **Critical and High** mail quarantined

SHARED INTELLIGENCE

A threat caught once is blocked everywhere.

Email Security and Cybereinforce browser protection run on one engine. What one learns, the other enforces.

Email quarantined
The indicator that triggered it is identified precisely.

›

Threat intelligence
Added to Cybereinforce intelligence and your tenant's rules; attachment hashes too.

›

Analyst review
Automatic findings are reviewed by Cybereinforce analysts.

›

Browsers protected
The same domain or URL is blocked in every protected browser.

Browser rules in email

Curated threat intelligence, suspicious listings, learned impersonation patterns and machine-generated hosts all apply to links in email.

Your allow-list wins

Domains your organisation has allow-listed in Cybereinforce are respected in email exactly as in the browser.

Your rules apply

Blocks your team adds in the Cybereinforce console take effect for email links and PhishSecure sessions too.

FOR ADMINISTRATORS

One console for mail, mailboxes and licence.

The Email Security console sits inside the Cybereinforce admin portal your team already uses for browser protection.

Quarantine review

Preview quarantined mail safely, see every reason, then release it to the inbox or delete it. Copies are kept 7 days, then removed.

Recent activity

Every verdict for every protected mailbox, with the band, the reasons and the action taken.

Mode and mailboxes

Switch modes, turn protection on or off per mailbox, and protect new users automatically.

PhishSecure time

Minutes used and remaining this month, at a glance.

Connection health

See how many mailboxes are connected and reconnect them in one click if anything is missing.

Licence and renewal

Buy or renew in the console, with reminders before a trial or licence ends.

DATA PROTECTION AND TRUST

Built to see as little as it needs, and keep less.

What is processed

- **Message metadata and content** are read through Microsoft Graph to reach a verdict.
- **Verdicts, reasons and indicators** are logged for your tenant; the email body is not.
- **Sender history** (who writes to whom, and their usual link domains) is kept to spot the unusual.
- **Quarantined copies** are held 7 days for review and release, then deleted.

How it is protected

- **Data residency.** Your organisation's region is set once and tenant data stays there.
- **Microsoft consent model.** Access is granted by your administrator in Entra ID and can be revoked there at any time.
- **Signed links.** Rewritten links, PhishSecure links and detail links are signed and cannot be forged.
- **ISO/IEC 27001 certified** information security management.

Defanged by default. Domains shown in banners and notices are written as `name[.]com`, so warnings never become a clickable path to the threat they describe.

GETTING STARTED

One package. Every feature. Minutes to connect.

Every customer gets every detection, banners, quarantine, click-time link checks and PhishSecure. Price scales with the number of protected mailboxes, with the per-mailbox price falling as you grow.

14 days
free trial on your own Microsoft 365 tenant

3 steps
consent, mailboxes, mode, and protection is live

0
MX changes, gateways or device agents

1 engine
shared with Cybereinforce browser protection

Try it on a real email today.
Upload a suspicious email to the free checker at cybereinforce.com/Email_Security, or start a trial with your tenant.

info@cybereinforce.com