CYBEREINFORCE

FOR MICROSOFT 365 IT TEAMS

Phishing protection your users can see, connected in minutes.

Cybereinforce Email Security connects to Microsoft 365 through Microsoft Graph and works alongside the filtering you already have. There is no MX record to change, no gateway to run and nothing to install on devices. Every email gets a clear verdict in its own banner, dangerous mail is quarantined, and your team decides how strict it should be.

CONNECTED IN THREE STEPS

STEP 1
Grant consent
A Global Administrator approves the Cybereinforce app once in Microsoft Entra ID. No passwords or secrets are exchanged.

STEP 2
Mailboxes join automatically
Licensed mailboxes are protected straight away, and new users can be added automatically as they join.

STEP 3
Choose your mode
Pick how strict to be, from monitor-only to Security First. Change it any time; it applies within minutes.

WHAT YOUR USERS SEE

⏳ **Cybereinforce is checking this email**
Appears within seconds of arrival, while links already route through our check.

✓ **Checked by Cybereinforce**
Safe mail gets a slim green strip with the PhishSecure button. PhishSecure

⚠ **Flagged: be careful with this email**
The reasons in plain words, with sender and per-link evidence behind "Show details".

⛔ **An email to you was quarantined**
A notice takes the place of dangerous mail, so nobody wonders where it went.

What your team controls

- ✓ **Quarantine review.** Preview, release to the inbox or delete. Quarantined copies are kept 7 days, then removed.
- ✓ **Per-mailbox protection** on or off, with new users protected automatically if you choose.
- ✓ **Recent activity** with every verdict and the reasons behind it, for any mailbox.
- ✓ **PhishSecure time** used and remaining this month, at a glance.
- ✓ **Your rules count here too.** Blocks and allow-listed domains from the Cybereinforce console apply to email.
- ✓ **Licence and renewal** handled in the same console, with reminders before anything runs out.

THREE MODES, ONE ENGINE

MODE	WHAT USERS SEE	WHAT IS QUARANTINED
Connectivity	Nothing changes in the mailbox. Every email is still checked and logged for your team.	Nothing automatically: ideal for a quiet first look at your mail.
Balanced Default	Checking banner, green strip, every link checked again when clicked, PhishSecure in every email.	Critical mail: known threats and decisive evidence.
Security First	All of Balanced, plus a warning banner with reasons on anything Elevated.	Critical and High mail.

How your data is handled

- **Your region, chosen once.** Tenant data and PhishSecure sessions stay in the region set for your organisation.
- **Email content is not kept.** Only verdicts and evidence are logged; quarantined copies go after 7 days.
- **PhishSecure is never recorded** and leaves nothing behind when it closes.
- **ISO/IEC 27001 certified** information security management.

Fits next to Microsoft 365

- ✓ **Works with Exchange Online Protection and Defender for Office 365**, adding explained verdicts on top.
- ✓ **Microsoft's own Report button stays** exactly where users expect it.
- ✓ **Shared with Cybereinforce browser protection**: a threat caught in email is blocked in browsers too.

Start with a 14-day trial on your own tenant.

Grant consent, pick a mode and watch the first verdicts arrive. Or upload a real email to the free checker first.

Try it free →