CYBEREINFORCE

EMAIL SECURITY · MICROSOFT 365

Every email checked. Every verdict explained.

Cybereinforce Email Security checks every message in your Microsoft 365 mailboxes with the same threat intelligence that already protects browsers, follows each link to where it really leads, and tells your people in plain words why an email is safe, suspicious or gone. When someone is unsure, PhishSecure opens the email in an isolated browser in the cloud, so nothing on it ever reaches their device.

Seconds	**2 checks**	**1 engine**	**0 agents**
from arrival to the "being checked" banner and protected links	for every link: when the email arrives and again when it is clicked	shared with Cybereinforce browser protection, learning in both directions	no MX change, no gateway, no software on devices

HOW AN EMAIL IS HANDLED

STEP 1
Arrives
Microsoft 365 tells us the moment mail lands. A "being checked" banner and protected links appear within seconds.

STEP 2
Investigated
Sender, authentication, history, every link and every attachment are checked, redirect chains followed to the end.

STEP 3
Scored
Signals combine into Clean, Low, Elevated, High or Critical, with the reasons written out every time.

STEP 4
Acted on
Safe mail gets a green "Checked" strip. Dangerous mail is quarantined and a notice left in its place.

PhishSecure: open it where it can't touch you

One button in every checked email. The message opens in a fresh browser running in our cloud, and your user sees a live picture of it.

- **Nothing reaches the device.** Scripts, redirects and sign-in pages run remotely; downloads are blocked.
- **Every page is checked** by Cybereinforce threat intelligence, and malicious pages are blocked with the reason.
- **Gone when it closes**, or after 3 minutes at the latest. No cookies or profile carry over.
- **Private by design.** Never recorded, email content never stored, run in your tenant's region.

Two tiers of evidence

- ✓ **Decisive signals act alone.** A known indicator, device-code phishing, a look-alike of your own domain, a link domain under two years old or a password form in an HTML attachment go straight to Critical.
- ✓ **Weaker signals add up.** A first-time sender, a fake "RE:", a valid IBAN, a brand name on an unrelated domain: each adds weight, and together they raise the band.
- ✓ **Weak alone stays a warning.** Mail with only soft signals is never quarantined on those alone.
- ✓ **Your known senders are learned**, so the first unusual link from a regular contact stands out.

WHAT IT CATCHES

LURES
"Shared file, sign in to view"
Links through SharePoint, Drive or Dropbox are followed hop by hop to the credential page they lead to.

ACCOUNTS
Device-code phishing
Pages steering victims to the real Microsoft device login with an attacker's code are recognised and stopped.

PAYMENTS
Invoice and IBAN fraud
Checksum-valid IBANs, payment requests and look-alikes of your own domain, even in emails without links.

MAILBOXES	PER MAILBOX / MONTH	ONE PACKAGE, EVERY FEATURE
50 – 100	$1.88	Every detection, banners, quarantine, click-time link checks and PhishSecure. Billed annually.
101 – 500	$1.60	
501 – 1,000	$1.37	
1,001 – 10,000+	$1.14 → $0.95	PhishSecure: 1 hour a month up to 500 mailboxes, 30 more minutes for every 250 above.

See what your inbox is letting through.

Upload a real email to the free checker, or connect Microsoft 365 for a 14-day trial. Prices in USD, plus VAT where it applies.

Try it free →