FOR SMALL & MEDIUM BUSINESSES

Your inbox is *the #1 attack surface.* We protect it.

SafeToOpen Email Security analyses every email your team receives in Microsoft Outlook and Google Gmail — detecting phishing, CEO fraud, and social engineering attacks in seconds, before anyone clicks anything dangerous.

WHY THIS MATTERS

#1

most-reported cybercrime: phishing tops the FBI's complaint list, ahead of every other crime type

FBI IC3 Report 2024

$4.8M

average cost of a data breach that starts with a phishing email

IBM Cost of a Data Breach 2025

86%

of breached organisations suffered significant operational disruption

IBM Cost of a Data Breach 2025

THE COST OF ONE SUCCESSFUL ATTACK

SMBs are the #1 target

Attackers know smaller businesses have fewer defences. The financial and reputational damage from a single breach is often insurmountable.

$50K

Median loss per BEC incident for SMBs

FBI IC3 Report 2023

21 days

Average downtime after a ransomware attack

Coveware Q4 2023

1 in 5

SMBs were victims of a cyberattack in the past year

Hiscox Cyber Readiness 2024

$3.0B

Total BEC losses reported to the FBI in 2025 alone

FBI IC3 Report 2025

THE QUICK VERIFY PIN

Verify any email in seconds

A small SafeToOpen pin sits beside every email in Outlook and Gmail. The moment a message is opened, analysis pre-loads in the background — click the pin once and the full verdict appears in seconds.

< 3 sec typical verdict time

Pre-loads when you open an email so verification feels instant. Works across Outlook and Gmail — web, desktop, and mobile — same pin, same speed, no extra clicks.

HOW IT WORKS

Protection in four steps, zero effort from your team

SafeToOpen works directly inside Microsoft Outlook and Google Gmail — no new apps, no browser extensions, no training required.

STEP 01

Email arrives — pin appears

Your staff receive emails as normal. The SafeToOpen pin sits beside every message in Outlook or Gmail, ready to verify with one click.

STEP 02

Click the pin to verify

One click on the pin runs all 71 checks: sender, headers, links, attachments, domain intel, and behaviour — simultaneously, in the background.

STEP 03

Instant verdict

A clear trust score — Safe, Caution, or Dangerous — appears in seconds with plain-English explanation of any threats found.

STEP 04

Act & report

Move the email to junk or report it to your security team with one tap. Your whole team is safer, instantly.

WHAT WE DETECT

Every major email threat, covered

- **Sender spoofing & impersonation**
  Detects when attackers fake your CEO's name, your bank, or a trusted supplier. Display name tricks, look-alike domains, and header forgery are all caught.
  ALL PLANS
- **Malicious link detection**
  Every link in the email is scanned and rated before anyone clicks. Redirects, shortened URLs, and phishing pages are flagged instantly with a safe preview option.
  ALL PLANS
- **Attachment scanning**
  Attachment filenames, types, and embedded links are analysed for malware patterns — PDFs, Office docs, and executables all checked before opening.
  PLUS & EXECUTIVE
- **Domain intelligence**
  Newly registered domains (less than 30 days old), look-alike typosquatting domains, and unknown senders are flagged with full WHOIS context right in the inbox.
  ALL PLANS
- **Thread hijacking detection**
  Catches attacks where a criminal inserts themselves into an existing email thread to appear legitimate. A major BEC vector often missed by spam filters.
  PLUS & EXECUTIVE
- **Email authentication (SPF/DKIM/DMARC)**
  Full verification of sender authentication protocols. Broken or missing authentication is a strong indicator of spoofing — shown clearly in the advanced view.
  PLUS & EXECUTIVE

BEHIND THE SCENES

Up to 71 checks per email

Every "Verify" runs dozens of independent checks across the email — combined into one plain-English verdict.

71 total checks per email

Sender authentication & headers	12 checks
Domain intelligence & WHOIS	10 checks
Link & URL scanning	14 checks
Attachment analysis	8 checks
Content & language patterns	10 checks
Sender behaviour & history	7 checks
AI Deep Analysis (Executive)	10 checks

Plus runs every check except AI Deep Analysis. Executive adds full AI body analysis on top.

EXECUTIVE SHIELD

Your executives and finance team are the *most targeted people* in your organisation.

BEC attacks specifically target CEOs, CFOs, and finance staff — impersonating trusted contacts to authorise fraudulent wire transfers or share sensitive data. A single successful attack can cost tens of thousands.

TARGET HIGH-RISK ROLES

- ✓ CEO / Managing Director
- ✓ CFO / Finance team
- ✓ Legal & Compliance
- ✓ Accounts Payable
- ✓ Executive Assistants
- ✓ IT Administrators

REAL-WORLD THREATS WE STOP

The attacks hitting businesses like yours, today

CEO FRAUD / BEC

"Urgent wire transfer request from the CEO"

An email appears to come from your MD asking accounts to urgently transfer funds to a new supplier. The sender's domain is a one-character variation of yours.

SafeToOpen catches: Domain typosquatting, failed DMARC, first-time sender, urgency language, wire-transfer pattern

Statistics sources: IBM Cost of a Data Breach 2025 · FBI IC3 2023–2025 · Hiscox 2024 · Coveware Q4 2023

SUPPLIER IMPERSONATION

"Our bank details have changed — please update your records"

A criminal compromises a supplier's email and sends your accounts team updated bank details for upcoming invoices. The email looks completely legitimate.

SafeToOpen catches: Thread hijacking detection, request anomaly (bank-detail change), sender history anomaly

PHISHING LINK

"Your Microsoft 365 account will be suspended — verify now"

A convincing Microsoft-branded email with a link to a fake login page — designed to steal credentials that give attackers full access to your business email.

SafeToOpen catches: Malicious URL flagged, domain registered 4 days ago, authentication failed, urgency language

SIMPLE, TRANSPARENT PRICING

Protection for every role in your organisation

FOR EVERYONE

Plus

Full protection for your whole team

Comprehensive email security for every staff member — from reception to management.

- ✓ Trust score & instant verdict
- ✓ Full header analysis (SPF/DKIM/DMARC)
- ✓ Link scanning with safe preview
- ✓ Attachment scanning
- ✓ Sender history & first-contact alert
- ✓ Domain intelligence & WHOIS
- ✓ Thread hijacking detection
- ✓ Forwarding-rule monitoring
- ✓ Move to Junk & Report actions

RECOMMENDED FOR EXECUTIVES

Executive

AI-powered BEC protection

Everything in Plus, plus unlimited AI Deep Analysis for your highest-risk team members.

- ✓ Everything in Plus
- ✓ Unlimited AI Deep Analysis
- ✓ BEC & social-engineering scoring
- ✓ Urgency & authority manipulation detection
- ✓ Content vs subject mismatch analysis
- ✓ Recommended action per threat
- ✓ AI confidence score & re-analysis

ORGANISATIONS

Business

Team management at scale

Centralised control for IT admins — provision the whole team from one portal with Azure AD or Google Workspace directory.

- ✓ Mix Plus & Executive seats
- ✓ Team management portal
- ✓ Azure AD or Google directory sync
- ✓ Automatic member provisioning
- ✓ Custom report email routing
- ✓ Centralised billing
- ✓ Add-in settings per organisation

YOUR FIRST WEEK

From signup to fully protected, in days

SafeToOpen takes minutes to deploy and starts protecting your team immediately. Here's what to expect.

STEP **Day 1**

Sign up & install

Start your free trial at safetoopen.com — no credit card required. Your IT admin pushes the add-in via the Microsoft 365 Admin Centre or Google Workspace Marketplace in about 5 minutes. No mail-flow changes.

STEP **Day 2**

Your team is protected

The SafeToOpen pin appears in everyone's Outlook or Gmail beside every email. Staff click it to verify anything suspicious — verdicts return in seconds.

STEP **Week 1+**

You see threats blocked

Review the threat dashboard to see what was caught. Common first-week catches: spoofed domains, supplier impersonation attempts, and malicious links.

COMMON QUESTIONS

What businesses ask us

How do you keep our email private?

Email content is never stored. Deep Analysis happens in transit and is discarded. All scan metadata is anonymised. Full privacy details at safetoopen.com/privacy.

Do you support Gmail / Google Workspace?

Yes — fully. SafeToOpen ships as both a Microsoft 365 Outlook add-in and a Google Workspace Gmail add-on. Same pin, same 71 checks, same Executive AI Deep Analysis whichever inbox your team uses.

Does it replace our existing spam filter?

No — it complements it. Your existing filter (Microsoft Defender, Google's native filters, Mimecast, etc.) catches obvious spam. SafeToOpen catches the sophisticated attacks that look legitimate and slip through.

Do we need IT to deploy it?

No. Any Microsoft 365 admin can install via the M365 Admin Centre, and any Google Workspace admin can install via the Workspace Marketplace — both take under 5 minutes. No mail-flow changes, no infrastructure.

What if we want to cancel?

Cancel any time, no contract lock-in. Pause or remove seats from the admin portal. We'll keep your service running through the end of your billing period.

ABOUT SAFETOOPEN

Built for the modern threat landscape

SafeToOpen Email Security is an add-in for Microsoft Outlook and Google Gmail, built specifically for the inbox. Where gateway filters look at message metadata, we look at what users actually see and click — display names, link destinations, content patterns, and behavioural anomalies — applying real-time analysis to every email a user opens.

COMPLIANCE & TRUST

- ✓ GDPR compliant — EU data residency available
- ✓ ISO 27001 information security framework
- ✓ Microsoft 365 certified add-in
- ✓ Google Workspace Marketplace listed
- ✓ Email content never stored — analysed in transit
- ✓ 99.9% uptime SLA with 24/7 monitoring
- ✓ Annual third-party penetration testing

BUILT FOR THESE BUSINESSES

Industries we protect

SafeToOpen is used across SMBs that handle sensitive client data, regulated information, or high-value transactions:

- ✓ **Professional services** — Legal firms, accounting practices, consultancies
- ✓ **Financial services** — Advisors, brokers, wealth managers, accountants
- ✓ **Healthcare practices** — GPs, dentists, specialist clinics, allied health
- ✓ **Real estate & property** — Agencies, conveyancers, property management
- ✓ **Construction & trades** — Builders, contractors, trade-based businesses
- ✓ **Retail & manufacturing** — Online stores, distributors, B2B operations

GET STARTED

Start protecting your team *today*.

Free trial, no card required. Takes 5 minutes to deploy. Works instantly in Outlook and Gmail — web, desktop, and mobile. Cancel any time.

Email **contact@safetoopen.com**
Web **safetoopen.com**

AT A GLANCE

Works with	**Microsoft 365 & Google Workspace**
Deployment time	**Under 5 minutes**
Mail-flow changes	**None — works inside your inbox**
Free trial	**Yes, no card required**
Plans available	**Plus, Executive, Business**
Email storage	**None (analysed in transit)**
Compliance	**GDPR, ISO 27001 certified**
Cancel any time	**Yes — no contract lock-in**