FOR SMALL & MEDIUM BUSINESSES

# Protect your business where phishing *actually succeeds.*

SafeToOpen protects your team in **the inbox and the browser** — before phishing becomes business loss — for a few dollars per person each month.

- ✓ Set up in under 30 minutes
- ✓ Works with Microsoft 365 & Google Workspace
- ✓ Keeps your existing antivirus & email filtering
- ✓ Cloud-native SaaS — nothing to host or maintain

**1 in 5**

small businesses suffered a cyberattack in the past 12 months

*Hiscox Cyber Readiness Report*

> *Modern phishing doesn't beat your firewall. It convinces your team.* ***SafeToOpen protects that moment.***

THE RISK

## Phishing reaches your team — with or without email filtering.

Phishing arrives through email, SMS, QR codes, search ads, social media, and AI tools. Whatever the source, the attack succeeds in one of two places: **the inbox**, when someone trusts a fraudulent message — or **the browser**, when someone enters credentials or payment information. SafeToOpen protects both — whether or not you already have email security.

| WHAT YOU LIKELY HAVE TODAY | COVERED? |
|---|---|
| Microsoft 365 / Google Workspace · antivirus | ✓ |
| **Browser & inbox protection — SafeToOpen** | ★ |

NO SECURITY TEAM REQUIRED

The expensive part of security isn't the software — it's the people required to act on what the software finds. Detection tools tell you something happened; a human still has to work out what it means.

Prevention doesn't create that work. When a fake sign-in page is blocked before the password is entered, there are no credentials to reset, no sessions to revoke, no mailbox rules to audit, and no customers to notify.

*The notification is a receipt for something that didn't happen — not a ticket someone has to work.*

WHAT YOU GET

## Choose Browser, Email, or both.

PRODUCT 1 — $5 /user/mo

### Browser Protection

*Stops phishing, fake websites and credential theft inside the browser.*

PROTECTS YOUR TEAM WHEN THEY

- ✓ Click malicious links
- ✓ Visit zero-day phishing sites
- ✓ Paste and upload sensitive information
- ✓ Download malicious files

**For:** staff who use Microsoft 365, web apps, or handle sensitive information.

- **Also protects**
  Pasted PII and payment card data, plus links inside webmail, search results, and GenAI chats.
- **Any link source, one browser protection layer**
  Email, text message, social media, search, or ad — if it opens in the browser, it's protected.

WHY BUSINESSES BUY SAFETOOPEN

- ✓ Reduce the risk of invoice fraud & credential theft
- ✓ Protect staff without extra security training
- ✓ Add protection beyond Microsoft 365 & antivirus
- ✓ Deploy without changing email or network setup
- ✓ No minimum seat counts — pay for the people you have

PRODUCT 2 — $4 /user/mo

### Email Protection

*Scores every email as Safe, Caution or Dangerous — and explains why — before your team replies, clicks or pays.*

HELPS YOUR TEAM VERIFY

- ✓ Suspicious senders
- ✓ Business Email Compromise (BEC)
- ✓ Unexpected payment requests
- ✓ QR codes in email bodies & attachments

**Ideal for:** staff who handle payments, customer data, supplier communication, or sensitive requests.

BUNDLE & SAVE

**Browser + Email = $7** /user/mo

Protection across the two places phishing succeeds — the inbox and the browser.

- ✓ One platform · One monthly invoice
- ✓ Cancel anytime — no lock-in contracts

WHAT IT COSTS YOUR TEAM

| | |
|---|---|
| Team of 10 — both products | **$70 / month** |
| Team of 25 — both products | **$175 / month** |

*A single prevented fraudulent payment can cover years of protection.*



Statistics sources: Hiscox · Interisle 2024 · FBI IC3

BROWSER PROTECTION

## Why it catches what filters miss

- **Sees what your team sees**
  VisionAI analyzes page visuals, brand signals, and content — catching phishing before anyone reports it.
- **Spots what attackers hide**
  X-Ray uncovers hidden redirects, lookalike web addresses, and forms that send passwords somewhere else.
- **Always up to date**
  Threat intelligence from trusted security feeds and SafeToOpen detection — updated every minute.

**< 24 hrs**

typical phishing site lifespan — why SafeToOpen judges the live page, not just its reputation

*Interisle Phishing Landscape 2024*

*For your IT provider: VisionAI visual & content analysis · X-Ray behavior analysis (scripts, domain age & popularity) · threat intelligence feeds.*

WHAT YOUR TEAM GETS

- ✓ A clear verdict on every page, explained simply
- ✓ Credential theft blocked at the moment of entry
- ✓ Download protection & Paste Guard
- ✓ They learn the warning signs of unsafe sites
- ✓ No security training required

EMAIL PROTECTION

## Four questions, answered on every email

- **Is the sender genuine?**
  Every sender's identity is verified automatically — impersonators and lookalike addresses are called out before anyone replies.
- **Is the message unusual?**
  First-contact alerts and unusual patterns from the mailbox's own history — new senders don't slip by unnoticed.
- **Are links, QR codes & attachments safe?**
  Every URL checked with redirect following, QR codes decoded and verified, attachments scanned before they're opened.
- **Signs of payment fraud?**
  AI analysis spots BEC patterns, urgency manipulation, and unexpected payment requests before money moves.

*For your IT provider: SPF / DKIM / DMARC sender authentication · AI content analysis · link & attachment inspection.*

WHAT YOUR TEAM GETS

- ✓ A verdict on every email they open
- ✓ Fraud flags before they reply or pay
- ✓ Silent auto-forward (compromise) detection
- ✓ Works in Outlook and Gmail

SIMPLE BY DESIGN

## Live in under 30 minutes

- **1 · Choose your products**
  Browser Protection, Email Protection, or both.
- **2 · Roll out to your team**
  Your IT admin pushes it to everyone at once via Microsoft 365 or Google Workspace — or each person installs it in a minute.
- **3 · Your team is protected**
  No mail-flow changes, no network changes, nothing to maintain.

SUPPORTED PLATFORMS

**Browsers:** Chrome · Edge · Firefox · Safari (Mac, iPhone, iPad) · Edge & Firefox on Android

**Email:** Outlook · Microsoft 365 · Gmail

COMMON QUESTIONS

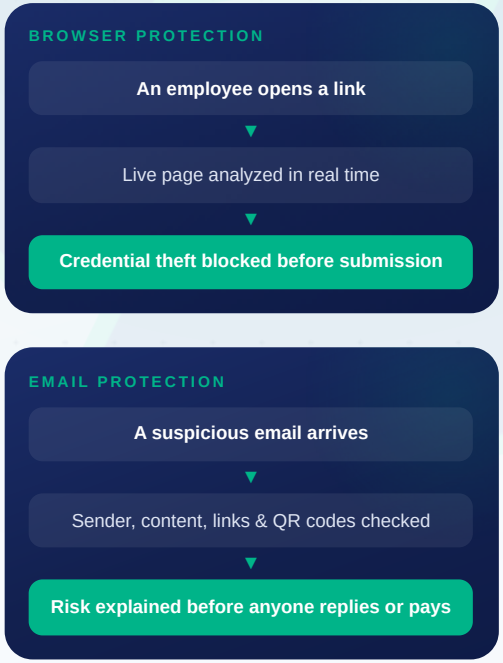
**Does it replace our antivirus or Microsoft's filters?** No — it adds the missing user layer alongside them.

**Will it slow down browsing?** No. Trusted sites are cleared instantly.

**Do we need training?** No. Every warning is explained in plain English.

HOW IT PROTECTS

## Two moments of protection




TRUST & PRIVACY

- ✓ ISO/IEC 27001:2022 certified · GDPR compliant
- ✓ Content analyzed in transit — never stored
- ✓ No browsing history collected · 99.9% uptime

GET PROTECTED

### Book a 20-minute business security review.

- ✓ Browser, Email, or both
- ✓ Setup supported by SafeToOpen
- ✓ No infrastructure changes

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