PRODUCT

Carmen extension, Carmen Email and the Carmen app.

Three doors a scam can arrive through. The same four things happen to it at each one: something arrives, it is read on the device, personal details are scrubbed, a verdict comes back with reasons.

BROWSER

Carmen extension

Watches: the page you open: sign in pages, checkouts, links from mail. And the sites you choose (Gmail, Outlook, WhatsApp Web, LinkedIn and others), checking suspicious messages on its own.

Magic Mouse: point at anything on a page and Carmen reads it; hold still and it checks it.

How it alerts: a card in the side panel with the risk level, the reasons and one action, before you type.

Never reads: what you type. Personal details are removed on the device first.

Setup: a Chrome extension. Sign in once.

INBOX

Carmen Email

Watches: mail as it arrives in the connected mailbox.

How it alerts: an alert email with the verdict, the reasons and the action. In a company, the same alert can go to an address the admin chooses. Everything flagged appears in the activity log.

Keeps: the verdict and the reasons. The email itself for 30 days, then deleted.

Setup: approved once by your admin through Google Workspace or Microsoft 365, then each person connects in one click. On a Personal plan you connect it yourself.

PHONE

Carmen app

Watches: texts from numbers not in your contacts.

How it alerts: High risk texts with hard evidence go to the junk folder with the reason. Anything Carmen is unsure about stays, with a note. A notification when something needs a look.

Never reads: texts from your contacts. Those never leave the phone.

Also: connect your inbox in the app for alerts on your phone. Calls: coming soon.

Setup: the app on iPhone or Android, one switch in Settings.

SAME ANSWER EVERYWHERE

Wherever it arrives, the answer comes back the same.

Low, Medium or High risk. The reasons. One thing to do. The phone, the inbox and the browser, watched by one brain.

The privacy model

QUESTION	ANSWER
What leaves the device	The scrubbed text or link, over an encrypted connection. Names, numbers and IDs are removed first.
What is kept	The verdict, the reasons, which account it was for, and when.
What is not kept	Screened texts. Screened emails are kept 30 days for the case record.
Who sees it	Software. A person only if you ask for expert help.
Your contacts	Never screened. Texts from people you know do not go anywhere.
Turning parts off	Mail, browsing and phone screening are each a switch, per person.

What is included

All three products come with every paid plan. Screening on all three is included and not counted, within fair use. Credits are only used for checks a person chooses to run.

Where to get them

Chrome	The Carmen extension from the Chrome Web Store.
Mailbox	Approved once by your admin, then one click for you. On a Personal plan, connect it yourself.
Phone	The Carmen app, on the App Store and Google Play as Carmen Guardian.

Three things that happen

A page that copies your bank

A sign in page on acme-banking-login.com. The Carmen extension sees the address is four days old and already listed as a phishing site. High risk, before you type.

An invoice with new bank details

A real thread with a real supplier, except the account number changed. Carmen Email sees the change mid thread and a sending address nine days old. High risk, with the action: confirm by phone on a number you already hold.

A parcel held at the depot

A text asking for a $2.99 release fee. The Carmen app sees the link is four days old and that no carrier charges a fee by text. Junk, with the reason.

Rollout in a company

1. Admin invites people by email from the admin page.
2. Admin approves Carmen Email once; each person connects their mailbox in one click.
3. Each person installs the extension and the app. About ten minutes, once.

Fair use

A seat is a person, not a device. It covers that person's own mailboxes, browsing and phone at normal human volume. Shared inboxes and anything a script sends belong on the API plans.