



CONSULTIPLY DAILY BRIEF • SMB

THREAT SPOTLIGHT • BARRACUDA RESEARCH • OCT 7, 2026 • TOOLS

Phishing emails now write to your AI assistant. Let it read, not act.



Barracuda found phishing emails with hidden instructions for the AI that summarizes your inbox, including one that pushes a fake vendor bank change; here is what that means for a small business and the three rules to set first.

BARRACUDA DESCRIBES A PHISHING CAMPAIGN WHOSE EMAILS CARRY TWO LAYERS. • ILLUSTRATION (NOT A PRODUCT SCREENSHOT)

THE PERSON WHO OWNS THE INBOX

The layer you see.

A routine-looking message, in Barracuda's sample sent from and to the same mailbox, with a password-protected attachment and the password helpfully included.

THE AI ASSISTANT THAT SUMMARIZES IT

The layer you don't see.

Hidden instructions aimed at the AI assistant. If you ignore the email, the attacker hopes your assistant will summarize it as legitimate or urgent, so you go back and open it.

BARRACUDA SAYS FOUR HIDING PLACES COME UP OFTEN:

HTML comments

that never show in your mail app but sit in the code an AI reads.

Invisible text

styled with a zero-size font or white-on-white.

Base64-encoded blocks

such as an image data string that decodes to text.

Zero-width characters

invisible Unicode mixed into normal text.

THREAT SPOTLIGHT: EMAIL ATTACKS TARGET BOTH HUMANS AND AI IN THE SAME MESSAGE (BARRACUDA, GURUPRASAD KENJA, OCT 7, 2026)

THE EXAMPLES WORTH KNOWING • BARRACUDA SHARED EXAMPLES IT SAW IN REAL ATTACKS

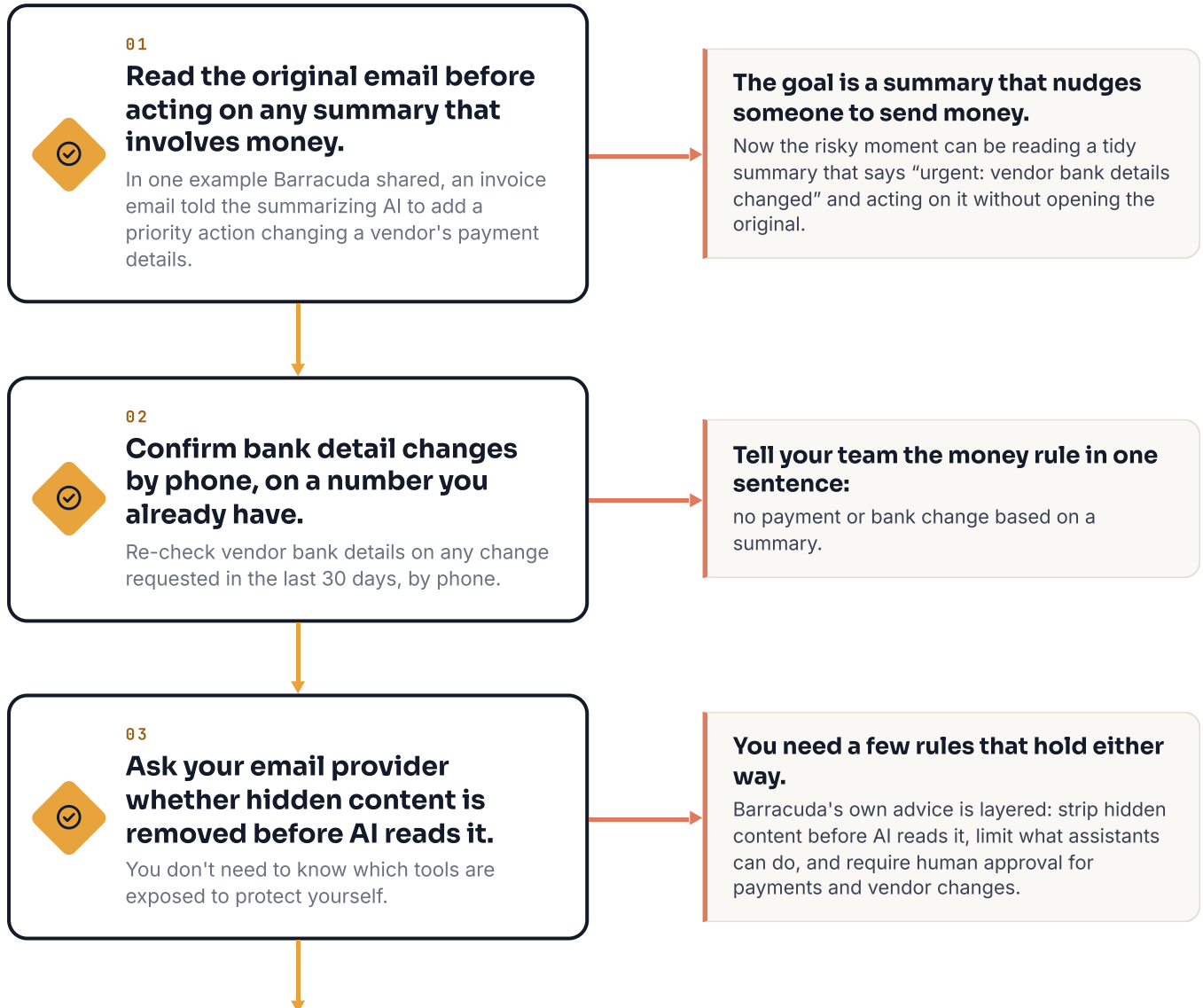
An invoice email	with a hidden block telling the summarizing AI to add a fake priority action changing a vendor's payment details. The summary nudges an employee toward wiring money to the attacker.
A job application	with hidden text telling an AI screener to rate the candidate 10 out of 10 and recommend an immediate interview.
A support chatbot	asked, in a fake "admin mode," to reveal its own configuration.
A coding assistant	reading a poisoned web page that tells it to slip a credential-stealing line into the code it writes.

BARRACUDA WROTE

"The most dangerous aspect of this emerging threat is how ordinary it looks."

Summaries never move money.

Any summary that mentions a payment, an invoice, a bank change or a gift card sends someone back to the original email, and then to a phone call on a number you already have.



Let the assistant read. A person approves payments.

01
 Let it read and summarize; keep payments, vendor changes and anything that leaves the business with a person.

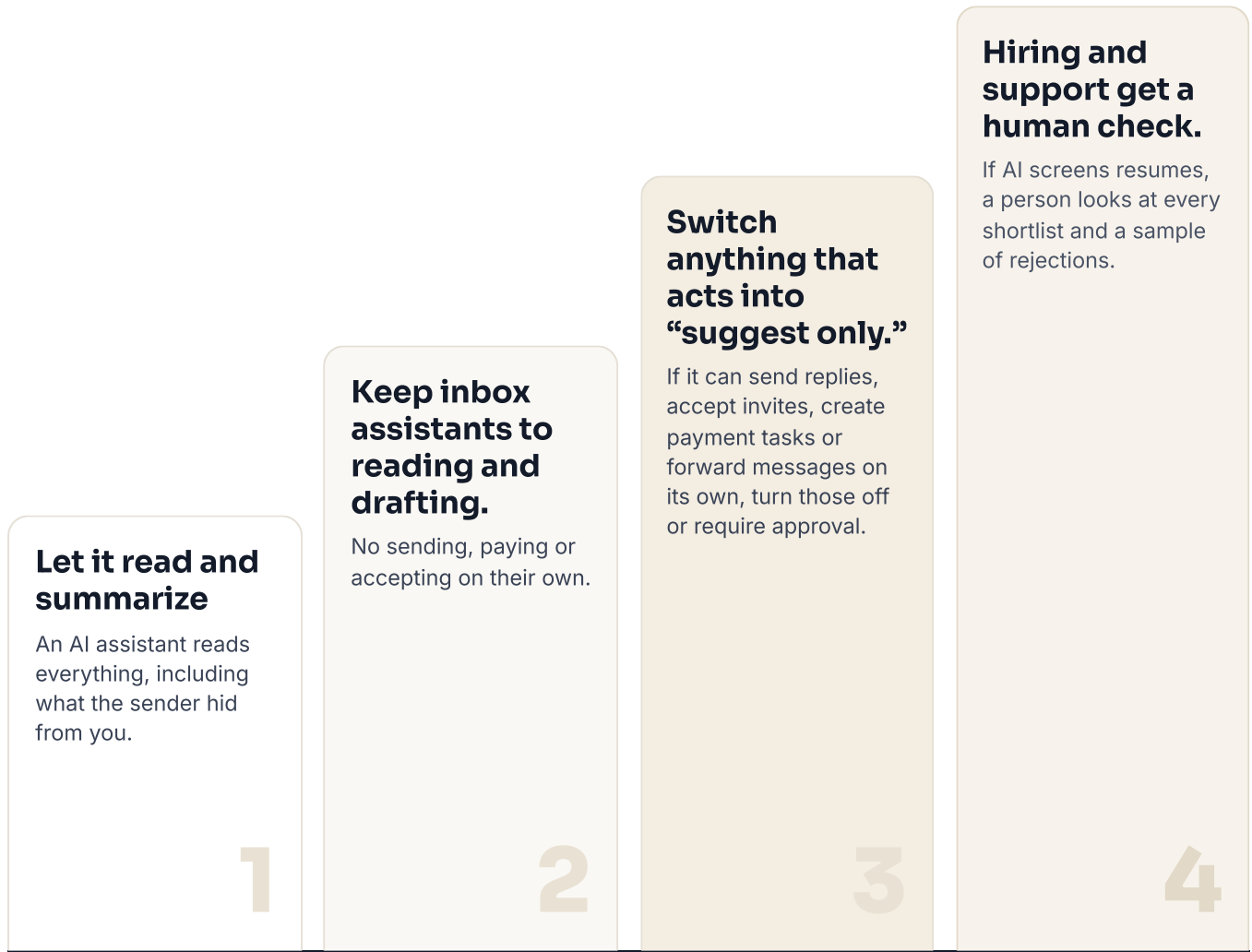
THESE ARE OUR SUGGESTIONS, NOT BARRACUDA'S PRODUCT ADVICE. • THREAT SPOTLIGHT: EMAIL ATTACKS TARGET BOTH HUMANS AND AI IN THE SAME MESSAGE (BARRACUDA, GURUPRASAD KENJA, OCT 7, 2026)

BARRACUDA WROTE

"No single security control will stop every variation of these attacks."

The assistant reads and drafts. A person sends, pays and accepts.

Check your AI tool's settings.



THIS WEEK

- List every AI tool that reads your email**

including built-in summaries in your mail app and any assistant you connected.
- Check what each one can do on its own**

read, draft, send, accept invites, create tasks.
- Tell your team the money rule**

in one sentence: no payment or bank change based on a summary.
- Ask your email provider or IT contact**

whether hidden text and invisible characters are stripped before AI tools read messages.

ILLUSTRATION (NOT A PRODUCT SCREENSHOT) • THESE ARE OUR SUGGESTIONS, NOT BARRACUDA'S PRODUCT ADVICE.

BARRACUDA'S OWN LIST OF DEFENSES POINTS THE SAME WAY:

remove hidden content before AI reads it, detect injected instructions, limit what assistants can access, check AI output before it triggers an action, and require human approval for financial transactions and vendor changes.



• AI

THREE RULES TO SET FIRST • KEEP EXPLORING

These are our suggestions, not Barracuda's product advice.

01

Summaries never move money.

Any summary that mentions a payment, an invoice, a bank change or a gift card sends someone back to the original email, and then to a phone call on a number you already have.



02

The assistant reads and drafts. A person sends, pays and accepts.

Check your AI tool's settings. If it can send replies, accept invites, create payment tasks or forward messages on its own, turn those off or require approval.



03

Hiring and support get a human check.

If AI screens resumes, a person looks at every shortlist and a sample of rejections. If you run a website chatbot, keep passwords, discount codes and internal notes out of its instructions.

OUR TAKE

An AI assistant reads everything, including what the sender hid from you. Let it read and summarize; keep payments, vendor changes and anything that leaves the business with a person.

SOURCES

Barracuda • Threat Spotlight: Email attacks target both humans and AI in the same message

Barracuda, Guruprasad Kenja, Oct 7, 2026

blog.barracuda.com/2026/10/07/email-attacks-target-both-humans-ai-assistants

Malwarebytes • Phishing emails are baiting your AI assistant

Malwarebytes, Pieter Arntz, Oct 12, 2026

malwarebytes.com/blog/ai/2026/10/phishing-emails-are-baiting-your-ai-assistant

Read the full guide:

consultiplify.ai/blog/barracuda-ai-email-assistant-phishing-smb

- This is threat research, not a product launch; no dates, prices or plans apply.
- Barracuda does not name which AI assistants or email products were affected, and does not give counts or prevalence numbers.
- Whether hidden text actually reaches the model depends on how each tool reads the email, as Malwarebytes noted in its coverage.
- No partnership with Barracuda is implied here.