omnivery

RESEARCH REPORT · 2026

Email's core metrics are being overrun by bots.

Four first-party findings from Omnivery, each from a separate dataset: how bots have taken over the **open** and are now coming for the **click** in B2C email; what genuine fraud looks like on traffic screened by our Bot Detection API; and how corporate scanners and newsletter archives quietly inflate everyone's numbers.

2020–2026 **Billions** of events **Real-time** classification **Quarterly**

~50%
of B2C email opens are bots (Apple MPP)

2% → 16%
rise in B2C consumer bot click rate, 2023→2026

50%
of Bot Detection API clicks were bots by June 2026 (up from 34% in 2025)

$2M+/mo
ad fraud blocked for Beehiiv

INTRODUCTION

Email's metrics were built for humans. Machines took them over.

Opens and clicks are the two signals the entire email industry runs on. Open rates, click-through rates, send-time optimization, "most engaged" segments, and ad payouts all rely on opens and clicks. And a fast-growing share of both is no longer human. Privacy proxies, corporate security scanners, social crawlers, and fraud bots now generate a large and rising portion of recorded engagement. And because they hide inside the very numbers marketers trust, they quietly distort every decision built on them.

This report quantifies how far this has gone using real production email: billions of opens and clicks classified in real time, rather than surveys or estimates. The data spans two independent sources from 2020 to mid-2026. The first is our own **first-party B2C campaign engagement**, from messages delivered to consumer mailboxes across **126 mailbox providers in six world regions** (Gmail, Outlook, Yahoo, Apple iCloud, GMX, Seznam and beyond). The second is **third-party traffic**, the click stream that other email platforms (ESPs such as Beehiiv and Upland Adestra) route through Omnivery's Bot Detection API for real-time screening. This traffic spans **tens of thousands of individual senders and brands**, so the picture reflects a broad slice of the industry, not one company's list.

Crucially, we keep these sources apart rather than blending them; blending is what produces misleading "X% of email is bots" headlines. Consumer B2C engagement is reported separately from third-party ESP traffic, and two further recipient types - corporate inboxes behind **major security gateway vendors** (Proofpoint, Mimecast, Barracuda and others) and automated newsletter archives - which are broken out on their own so they don't contaminate the B2C picture. Every open and click is classified from network, behavioural and reputation signals, never from the user-agent strings, which are stripped by privacy proxies. What follows are four findings, each from its own dataset.

Billions of events · 2020–H1 2026 **126** mailbox-provider families · 6 regions

First-party + third-party · ESP screening **Real-time** human/bot classification

HOW DETECTION WORKS

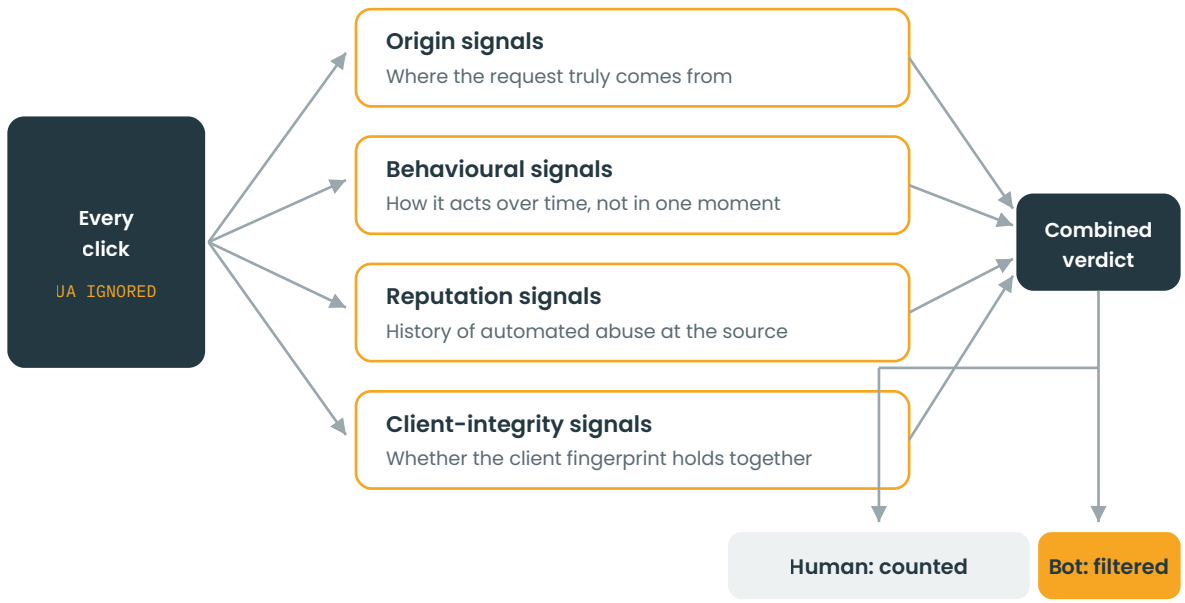
How the bots are caught

A bot's user-agent - the label that says "I'm Chrome on a Mac" - is trivially forged, and privacy proxies strip it out entirely. So Omnivery's detection never trusts what a click *claims* to be.

Instead it scores every click against several independent signals that a bot can't easily control all at once: where the request truly originates, how it behaves over time, whether its source has a history of automated abuse, and whether the client's technical fingerprint holds together. The verdict comes from the combination of several detection layers, so no single check is decisive. That layering is the point: defeating one signal doesn't get a bot through. That is how detection has kept pace as fraud networks grow more sophisticated.

How a click gets judged

BOT DETECTION API · LAYERED DETECTION MODEL



A click is judged on independent signals, not on what it claims to be. Defeating one detection layer doesn't get a bot through.

FINDING 1 · B2C CAMPAIGNS

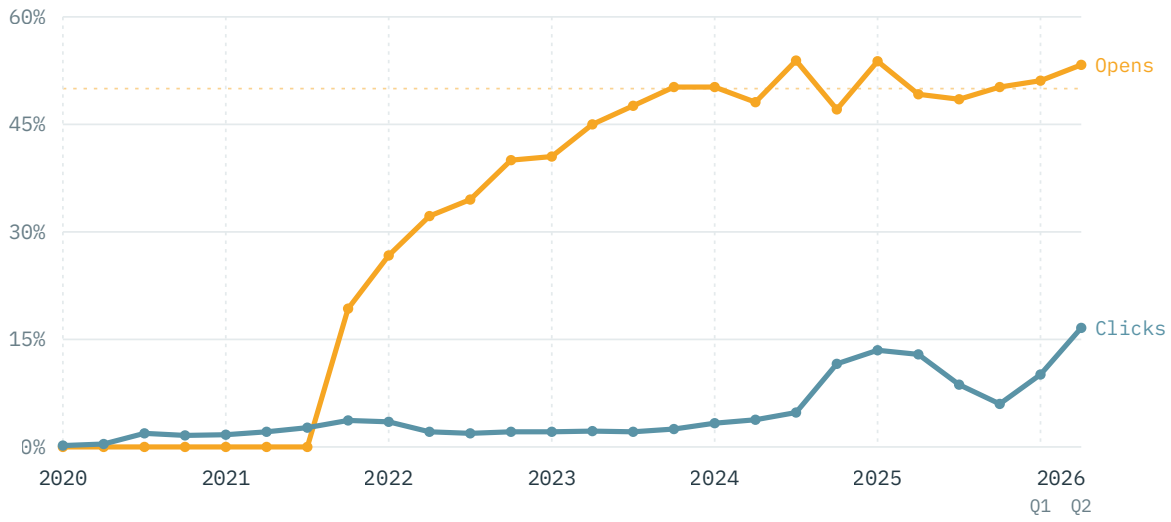
The open is already lost. The click is turning.

For B2C email, Apple Mail Privacy Protection reset the open rate. Non-human opens went from under 1% in 2020 to roughly half by 2023, and have held near 50% since. The most-quoted number in email marketing now measures machines as often as people.

The click held out far longer. Through 2023, B2C clicks were overwhelmingly human; only about **2% were bots**. But from 2024 the click-bot rate began climbing, reaching roughly **16% by 2026**. The click is following the open, just a few years behind.

B2C consumer email: non-human share of opens vs. clicks

B2C CAMPAIGNS · CONSUMER MAILBOXES · 2020–Q2 2026



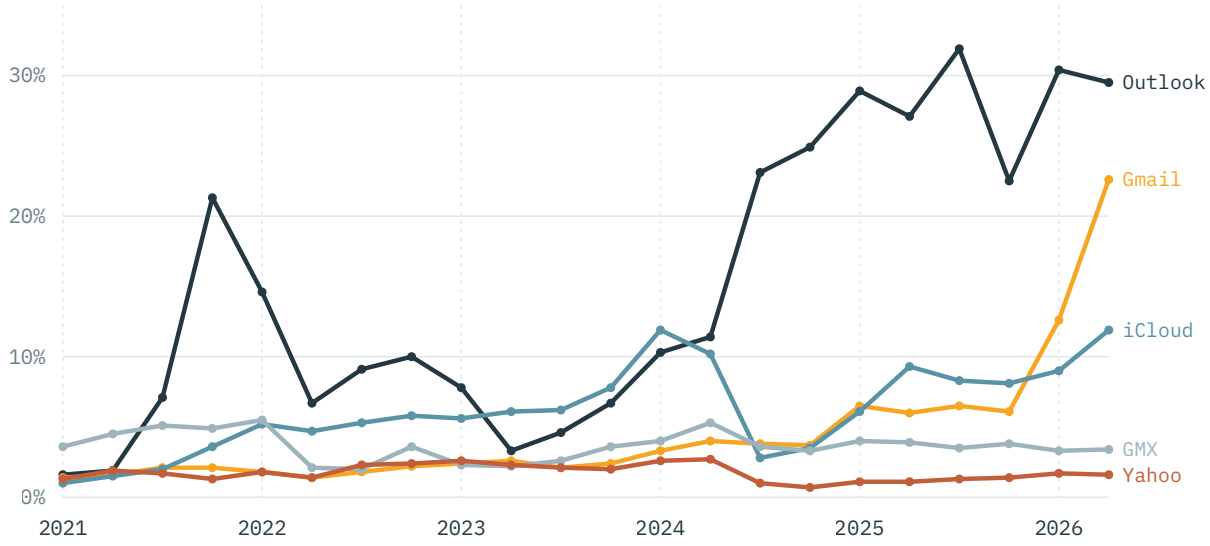
NHI opens crossed 50% with Apple MPP (late 2021); NHI clicks stayed ~2% until 2024, now climbing.

By provider: same metric, very different reliability

The click picture varies sharply by mailbox provider. Microsoft's Outlook/Hotmail is the most bot-contaminated of the major mailbox providers - around **30%**, reflecting Defender/SmartScreen link scanning - while **Gmail surged from ~2% to over 20%** through 2026, and Apple iCloud climbed to ~12%. Yahoo and GMX have held low, at ~2–4%. The same inbox metric carries very different reliability depending on where your recipients read their mail. Smaller consumer providers tend to be steady rather than volatile: Italy's Libero has stayed under 1% bot every year since 2022, and Germany's web.de holds at ~3–4%. The consistently high-bot inboxes are business and security-filtered mail, not consumer webmail.

Bot-click share by consumer email provider

B2C CAMPAIGNS · 2021–Q2 2026



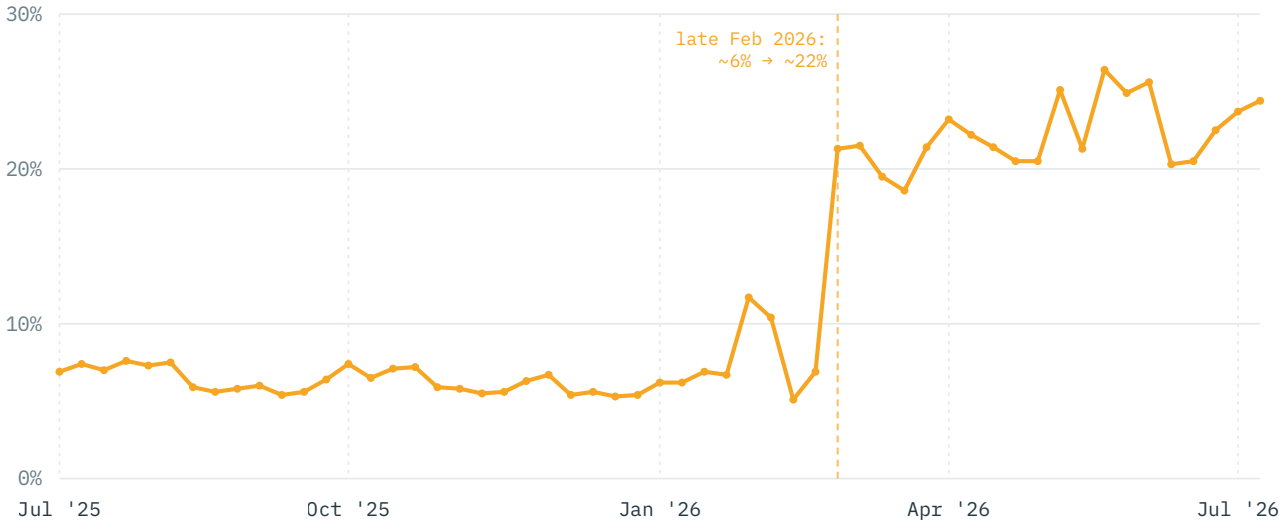
Microsoft's Outlook leads (~30%, Defender/SmartScreen); Gmail surged past 20% in 2026; Yahoo and GMX stay low.

The Gmail step change, week by week

Gmail's rise wasn't gradual - it was a switch. After holding around 6% through 2025 and early 2026, Gmail's share of bot clicks share jumped to ~22% in **late February 2026** and has held there every week since. The shape - a clean ~3.5× step, sustained and network-wide rather than tied to any single campaign - points to a change by Gmail (most likely more aggressive link prefetching/scanning), not a botnet.

Gmail bot-click share, weekly

B2C CAMPAIGNS · CONSUMER GMAIL · 2025 H2–Q2 2026



A step change, not a burst: ~6% → ~22% in late February 2026, holding for 20+ weeks.

FINDING 2 · OMNIVERY BOT DETECTION API

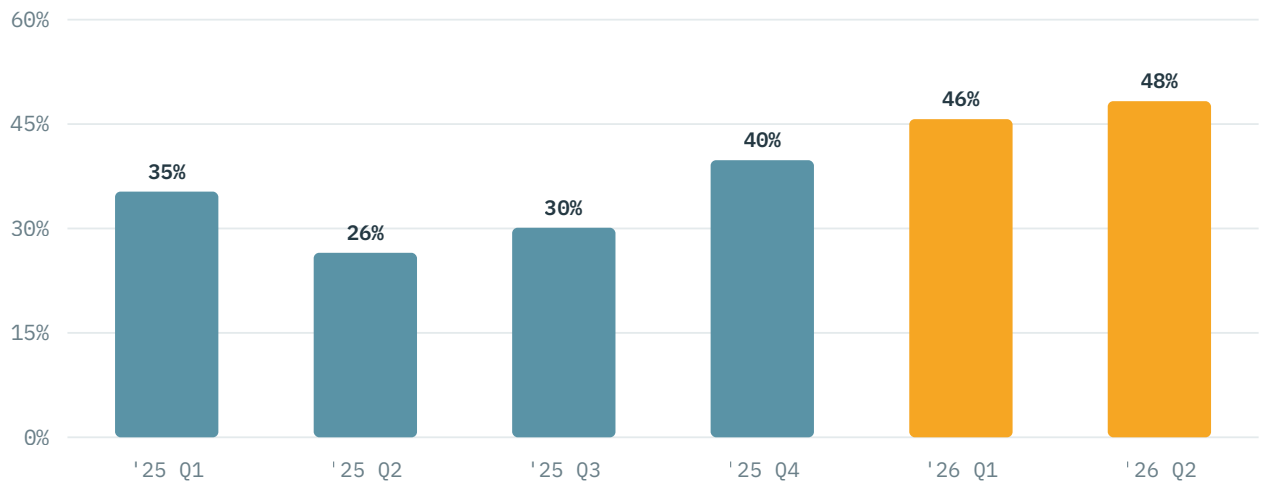
On Bot Detection API traffic, most clicks are now bots

Third-party ESP traffic - the click data that email service providers (ESPs) such as Beehiiv and Upland Adestra run through the Omnivery Bot Detection API to classify in real time - is distinct from the the first-party traffic covered in Finding 1, and it behaves very differently.

Across Bot Detection API traffic, bot clicks rose from 33.8% in 2025 to around 48% across the first half of 2026. In June 2026, the latest complete month, they **crossed 50% for the first time**. For this traffic, the majority of clicks are now bots. This is the sharp end of the click problem, where automated networks click for money.

Bot share of clicks screened by the Bot Detection API

BOT DETECTION API TRAFFIC (ESP CUSTOMERS) · 2025–Q2 2026



Bot Detection API traffic from ESP customers reached half of all clicks by mid-2026.

WHAT THAT COSTS, IN THE REAL WORLD

Beehiiv: $2M+/month in ad fraud, blocked

For a platform that monetizes engagement, an undetected bot click is a direct payout to fraud. Newsletter platform Beehiiv uses Omnivery's detection to block more than $2M per month in ad fraud. This is the real-world impact of this dataset.

`Beehiiv - $2M+/month ad fraud blocked via Omnivery detection`

B2B · CORPORATE SECURITY SCANNERS

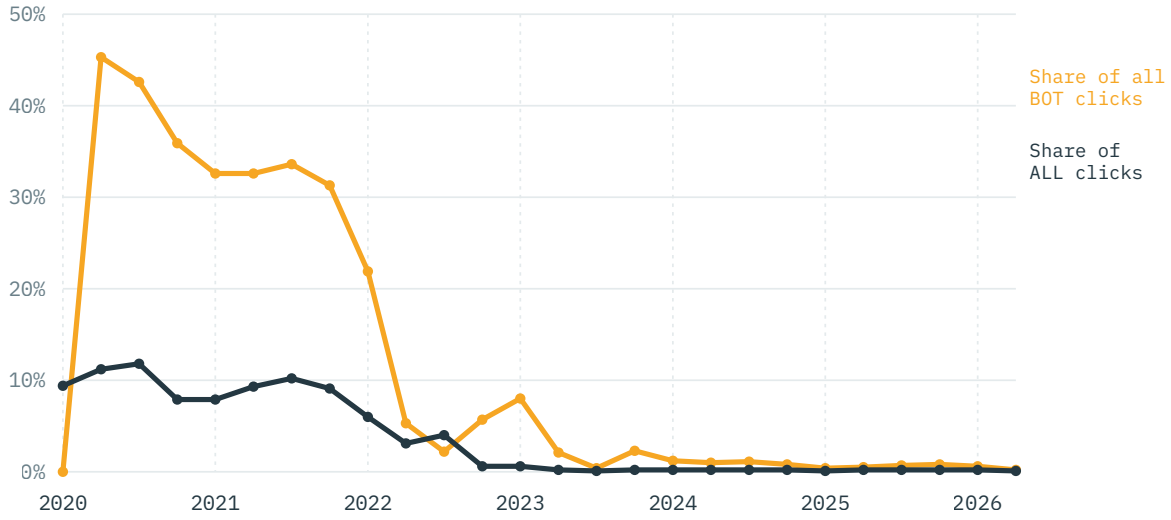
The oldest bots: corporate link scanners

Corporate and institutional inboxes sit behind email security gateways that open and click every link to sandbox it. In our data these recipient domains - Ericsson, Allianz, Pfizer, Roche, Siemens, Mastercard, the European Commission - click **80–95% of links**, and have since 2020. Where the gateway resolves, the signature is stark: Trend Micro-protected corporate mail runs ~99% bot, whereas consumer ISP security (Proofpoint/iCloud, Cisco) barely clicks.

These were the *original* email bots - in 2020–21 they were nearly half of all bot clicks. But as B2C and fraud traffic exploded, they were quickly drowned out. Corporate scanning was still ~80% bot, but its footprint shrunk drastically compared to this new bot click channel.

Corporate scanner domains: share of all clicks vs. share of all bot clicks

CORPORATE/B2B RECIPIENTS · 2020–Q2 2026



Persistent ~80–95% bot intensity, but a collapsing share of the (much larger) total.

WATCH-OUT · NEWSLETTER ARCHIVES

How a handful of archive tools inflate everyone's numbers

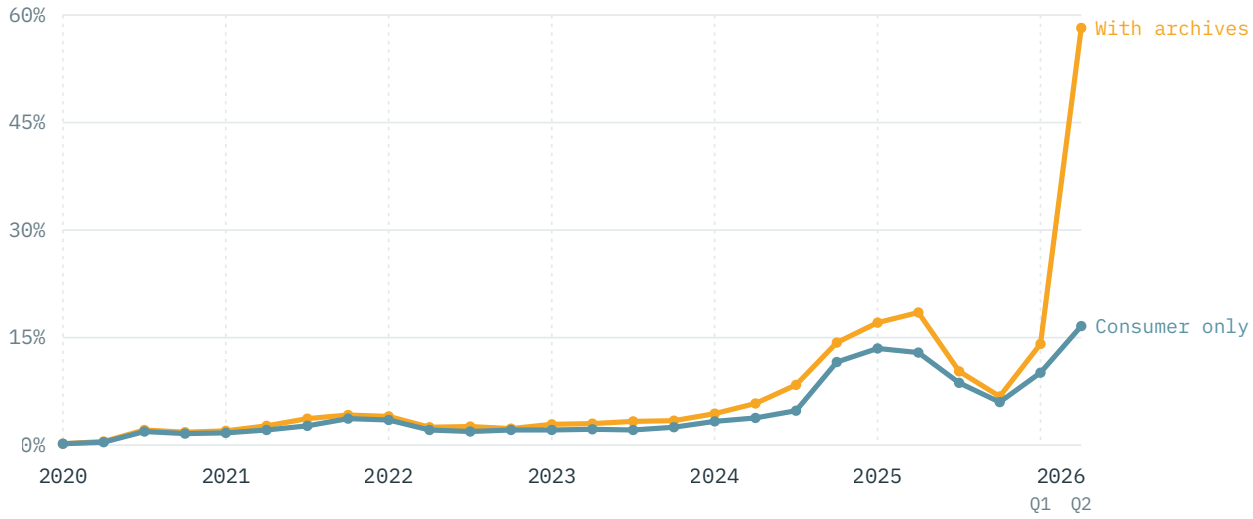
A small set of automated newsletter archive services - milledmail.com (Amazon-hosted) and a handful of peers - subscribe to consumer newsletters, then have their links mechanically fetched by crawlers. They register ~90% bot, and their click volume **spiked roughly 19× in 2026**.

What drove that spike is a single, nameable source: Meta. Meta's link crawler accounts for the large majority of archive clicks (roughly **84%**) and essentially the entire 2026 surge, concentrated on milledmail.com and nuslet.cz. When a newsletter's links surface on Meta's platforms, its crawler fetches every one, and each fetch registers as a click. It is benign in intent - a social crawler, not fraud or a scanner - but it is the single biggest distorter of raw click metrics in the data.

Left in the data, these archives badly distort the B2C click rate. In Q2 2026, real consumer clicks were **16.6% bot** - but blend the archives back in and the same metric reads **58%**. The "majority of clicks are bots" headline you may have seen is largely a few archive domains being crawled by Meta, rather than a broad consumer shift. It is also episodic - the spike receded the following quarter. It is exactly the kind of skew that makes raw engagement numbers untrustworthy.

B2C bot-click rate: consumer only vs. with archives blended in

B2C CAMPAIGNS · 2020–Q2 2026



The two track together until 2026, when a few archive domains double the apparent rate.

WHY IT MATTERS

The metrics didn’t just get noisy. They started lying.

1. Open-based metrics measure machines

With half of B2C opens non-human, open rate, “most engaged” segments, and re-engagement triggers based on opens are substantially measuring privacy proxies. Send-time optimization trained on open timestamps optimizes for machines, rather than people.

2. The click is no longer a safe proxy

The click was the last trustworthy signal in B2C. It is turning slowly on consumer mail (2%→16%), sharply on Bot Detection API traffic (over half by mid-2026), and it is the metric where money changes hands.

3. A few domains can rewrite your dashboard

As the archives show, a handful of recipient domains can double a reported rate. Aggregate engagement numbers are only as honest as the classification behind them.

WHAT TO DO ABOUT IT

Measure humans, not machines

- **Report human-only open and click rates.** Raw rates now bundle proxies, scanners, archives, and fraud.
- **Segment by recipient type.** Consumer, corporate, and archive traffic behave completely differently, and blending them hides and inflates the truth.
- **Protect the click.** It is the last human signal and the one fraud monetizes. Detect bot clicks before they hit attribution or ad payouts.
- **Filter before automation.** Send-time optimization, lead scoring, and re-engagement should run on human-classified events only.
- **Classify at the source.** Detection is most accurate when raw engagement data is available - IP, timing and behavior - not via user-agent strings, which can be stripped by proxies.

Omnivery's Bot Detection API separates humans from machines on every open and click - the same system Beehiiv uses to block $2M+/month in ad fraud.

See how it works →

omnivery

The State of Email Bots 2026: a research report by Omnivery. B2C campaign figures from consumer mailbox recipients (2020–H1 2026); Bot Detection API figures from ESP customers (2025–H1 2026); corporate scanner and newsletter archive analysis reported separately. All figures event level, classified in real time.

Cite as: Omnivery, "The State of Email Bots 2026," omnivery.com. · Media & data enquiries: hello@omnivery.com