Come restare informati su attualità, scienza e cultura con fonti diverse

Ricevere molte notifiche e avere una copertura equilibrata dell’attualità non sono la stessa cosa. Una sequenza continua di avvisi può riproporre più volte il medesimo evento, mentre temi scientifici complessi o fenomeni culturali meno immediati restano fuori dal campo visivo. Il problema, quindi, non è soltanto quante informazioni arrivano, ma quale funzione svolge ogni fonte e quali lacune lascia.

Quotidiani, newsletter, app e pubblicazioni specialistiche non sono strumenti intercambiabili. Un quotidiano può offrire una mappa dell’agenda pubblica; una newsletter può ordinare gli sviluppi di un argomento; un’app può rendere più rapido l’accesso a contenuti provenienti da canali diversi; una fonte specialistica può fornire metodo, documenti e terminologia. Per restare informati su attualità, scienza e cultura serve un incastro consapevole tra queste funzioni.

Tre bisogni informativi, tre profondità diverse

Il primo bisogno è sapere che cosa è accaduto. Qui conta una fonte generalista capace di dare una visione d’insieme: politica, economia, esteri, società e cronaca. La sua utilità principale non consiste nell’esaurire ogni tema, ma nel segnalare quali fatti stanno entrando nel dibattito pubblico e quali sviluppi meritano attenzione.

Il secondo bisogno è comprendere che cosa significhi una notizia scientifica. Il resoconto iniziale può segnalare una scoperta, una pubblicazione o una decisione sanitaria, ma

difficilmente può contenere tutto ciò che serve per valutarne portata e limiti. A quel punto occorrono fonti in grado di distinguere tra ricerca, divulgazione, valutazione della qualità e reperimento dei documenti.

Il terzo bisogno è collocare fatti e opere in un contesto culturale. L'annuncio di un premio, di una mostra o dell'uscita di un libro risponde alla domanda "che cosa è successo?". Una recensione argomentata, un saggio o il catalogo di un'istituzione rispondono invece a domande diverse: da quali tradizioni nasce un'opera, come è stata interpretata e perché può avere rilievo oltre il momento dell'uscita.

Confondere questi livelli produce aspettative sbagliate. Un articolo breve non deve essere trattato come una valutazione scientifica definitiva; una newsletter tematica non può sostituire da sola la copertura generale; una recensione non equivale a una cronaca neutrale dell'evento che commenta.

Il compito dei quotidiani, delle newsletter e delle app

Il quotidiano come mappa dell'agenda

La consultazione di un quotidiano generalista può essere il primo passaggio della giornata informativa. Titoli, sezioni e gerarchie editoriali aiutano a vedere insieme avvenimenti che altrimenti arriverebbero come frammenti isolati. Questa mappa, però, riflette una selezione: per i temi controversi o decisivi è utile confrontare resoconti distinti e risalire, quando possibile, ai documenti originari.

La pluralità non coincide semplicemente con il numero di pagine aperte. Se diversi canali riprendono lo stesso testo o la medesima ricostruzione, aumenta il volume, non necessariamente la varietà. Una copertura più solida combina

differenze reali: cronaca e analisi, fonte generalista e documento diretto, punto di vista nazionale e competenza settoriale.

La newsletter come filo di continuità

Una newsletter è particolarmente utile quando raccoglie e ordina gli sviluppi di un tema nel tempo. Può ridurre la dispersione perché arriva con una periodicità definita e propone una selezione delimitata. La sua attendibilità, tuttavia, dipende da chi la cura, dai criteri dichiarati e dai collegamenti ai materiali su cui si basa: il formato, da solo, non è una garanzia.

Per questo conviene assegnarle un ambito preciso. Una newsletter può seguire la ricerca scientifica, un settore culturale, la politica internazionale o un territorio, senza essere caricata del compito di rappresentare tutto ciò che accade. È più efficace come approfondimento ricorrente che come unica porta d’ingresso all’informazione.

L’app come punto di accesso

Un’app può riunire feed, notifiche, segnalibri e contenuti provenienti da varie sezioni, rendendo più semplice il passaggio dalla segnalazione alla lettura. Resta però un livello di distribuzione: per giudicare una notizia bisogna comunque identificare l’autore, la testata o l’istituzione che l’ha prodotta.

Le notifiche funzionano meglio quando sono selettive. Se ogni aggiornamento ottiene lo stesso grado di urgenza, diventa difficile distinguere un fatto appena avvenuto da un approfondimento che può essere letto più tardi. L’app può quindi servire per intercettare gli sviluppi; la valutazione richiede di aprire il contenuto, controllarne la provenienza e decidere se occorra una fonte ulteriore.

Per la scienza conta la funzione della fonte

La categoria “informazione scientifica” comprende materiali con scopi differenti. Un contributo del CNR-Ceris sull’informazione scientifica distingue, tra le altre, funzioni professionali, valutative, formative, divulgative, documentarie e di supporto alle decisioni pubbliche. Questa distinzione chiarisce perché nessun singolo canale possa soddisfare ogni esigenza: il testo che rende un tema accessibile al pubblico non svolge necessariamente lo stesso lavoro di una pubblicazione destinata ai ricercatori o di un documento istituzionale.

Quando una notizia rimanda a uno studio, è utile verificare almeno quale documento sia stato pubblicato, da chi e attraverso quale procedura. La peer review svolge una funzione di controllo della qualità da parte di altri ricercatori, ma non certifica in modo definitivo che ogni conclusione sia corretta. È un elemento della valutazione, non un timbro capace di sostituire l’esame del metodo, dei dati e delle successive verifiche.

Le fonti istituzionali assumono un ruolo specifico quando la domanda riguarda regole, autorizzazioni o informazioni comprese nelle loro competenze. In campo farmaceutico, per esempio, la pagina dell’AIFA dedicata all’informazione medico-scientifica collega l’informazione indipendente all’impiego sicuro e appropriato dei medicinali e offre un riferimento per gli aspetti regolatori e per la cultura del farmaco. Questo non significa che ogni fonte istituzionale sia automaticamente sufficiente per qualsiasi quesito scientifico: significa che, nel proprio ambito, consente di verificare la posizione e i documenti dell’ente competente.

“Istituzionale” e “specialistica” indicano dunque qualità diverse. Il primo termine identifica il ruolo del soggetto che

pubblica; il secondo riguarda la competenza e il metodo impiegati. Una fonte può essere entrambe le cose, oppure possedere soltanto una delle due caratteristiche.

Il contesto culturale richiede tempi meno compressi

Le notizie culturali hanno spesso una doppia vita. Nella prima fase prevalgono l'annuncio, l'apertura di un evento, l'uscita di un'opera o l'assegnazione di un riconoscimento. Nella seconda emergono interpretazioni, confronti e conseguenze. Limitarsi alla prima fase permette di conoscere l'agenda, ma non sempre di capire il significato di ciò che vi compare.

Per costruire contesto conviene affiancare alla cronaca almeno una fonte che lavori su una scala temporale più ampia: riviste culturali, inserti, saggi, cataloghi, archivi o lezioni pubbliche. Anche qui il compito va riconosciuto con precisione. Una recensione contiene un giudizio argomentato; un'intervista restituisce la prospettiva dell'intervistato; un catalogo documenta un progetto; un saggio può collegarlo a una storia più lunga. Leggerli come se fossero lo stesso tipo di contenuto crea confusione tra fatto, interpretazione e promozione.

Una frequenza sostenibile evita sia i vuoti sia la saturazione

Una routine efficace può cominciare con una finestra quotidiana dedicata all'aggiornamento generale. Non deve occupare l'intera giornata: serve a individuare gli eventi rilevanti e a scegliere quali meritino un secondo livello di lettura. Le notifiche possono restare riservate ai pochi temi per i quali la tempestività ha un valore concreto.

Gli approfondimenti scientifici e culturali possono seguire

una cadenza meno serrata. Una o più newsletter tematiche, consultate nei momenti stabiliti dalla loro periodicità, aiutano a recuperare sviluppi che il flusso quotidiano ha trattato in modo sommario. Le fonti specialistiche entrano invece quando una notizia solleva una domanda precisa, riguarda una decisione o richiede il controllo di termini, dati e documenti.

Il sistema cambia in base al tempo disponibile. Chi dispone di pochi minuti può mantenere una fonte generalista come base, aggiungere una selezione periodica per scienza e cultura e ricorrere alle fonti dirette solo per i temi più importanti. Chi segue un settore per lavoro avrà bisogno di consultazioni specialistiche più frequenti, senza rinunciare a una fonte generalista che mostri i legami con il resto dell'attualità.

La sostenibilità è decisiva: un sistema troppo esigente viene presto abbandonato, mentre uno dominato dagli avvisi favorisce una lettura reattiva. Stabilire in anticipo quali strumenti consultare ogni giorno, quali periodicamente e quali solo in presenza di una domanda riduce entrambe le difficoltà.

La completezza nasce dall'incastro

Restare informati non significa trovare una piattaforma capace di fare tutto. Significa sapere dove cercare la prima notizia, dove controllare un'affermazione scientifica e dove recuperare il contesto culturale che il flusso immediato non può contenere.

Il quotidiano disegna la mappa, l'app facilita l'accesso, la newsletter mantiene il filo e la fonte specialistica interviene quando servono competenza e verifica. La copertura diventa più completa quando questi strumenti si compensano a vicenda, non quando uno solo occupa tutto il tempo disponibile.

L'articolo Come restare informati su attualità, scienza e

cultura con fonti diverse proviene da Il Kim Magazine.

https://www.ilkim.it/come-restare-informati-su-attualita-scienza-e-cultura-con-fonti-diverse/

OpenAI Investigates Report Linking AI Agents to RubyGems Attack

The incident occurred in May, when RubyGems maintainers suspended new account registrations due to what appeared like malicious activity.

The post OpenAI Investigates Report Linking AI Agents to RubyGems Attack appeared first on SecurityWeek.

https://www.securityweek.com/openai-investigates-report-linking-ai-agents-to-rubygems-attack/

Climate Publisher Heatmap Turned Data Centers Into Triple-Digit Growth

Heatmap, the climate and energy outlet that launched a little over three years ago, is on pace to post triple-digit revenue growth this year as corporate and policymaker interest in […]

https://www.adweek.com/media/climate-publisher-heatmap-turned-data-centers-into-triple-digit-growth/

Enterprise email marketing shortfalls and the upmarket features to avoid them

Most email marketing teams know the basics. Authenticate your domain. Clean your list. Write a compelling subject line—test before you send.

But for enterprise and mid-market teams, doing the basics well is rarely where performance stalls. The gap shows up later — when a growing contact database starts fragmenting sender reputation, when automation workflows built for 50,000 contacts start conflicting at 500,000, when leadership asks which email campaigns actually influenced closed-won revenue, and the reporting falls silent.

Start building your audience, for free, with Marketing Hub.

Email marketing challenges at scale are not beginner problems. They are infrastructure, governance, and measurement problems — and most generic advice is not written for them.

This post is. Whether you are diagnosing declining inbox placement, trying to personalize at scale without a one-to-one content operation, or building the attribution model that finally connects email engagement to pipeline, the sections

below give you a diagnostic framework, concrete fixes, and the right tool path to make improvements that hold.

Table of Contents

- Why Email Marketing Challenges Get Worse at Enterprise Scale
- Fix email deliverability issues before they suppress growth.
- Solve low engagement with better targeting, timing, and testing.
- Reduce email production and automation challenges.
- Connect email marketing performance to pipeline and revenue.
- Use AI where it improves speed without weakening quality.
- 30-Day Action Plan for Improving Email Marketing Challenges
- Frequently Asked Questions About Email Marketing Challenges

Why Email Marketing Challenges Get Worse at Enterprise Scale

A single marketer sending a monthly newsletter to 10,000 subscribers faces a manageable set of problems. A demand generation team running multi-channel nurture sequences across 500,000 contacts — segmented by industry, lifecycle stage, product interest, and region — faces an entirely different category of challenge.

Scale multiplies both the work and the failure points.

Governance breaks down first. When multiple teams, regions, or business units share a sending domain and a contact database, the rules governing who can email whom, how often, and under what suppression conditions become critical infrastructure.

Without them, the same contact receives overlapping sequences from sales, marketing, and customer success simultaneously. Complaint rates climb. Unsubscribe rates rise. And because no single team owns the problem, no single team fixes it.

Data quality degrades over time. Enterprise contact databases grow through dozens of sources — form fills, CRM imports, event lists, third-party enrichment, and product signups. Without consistent hygiene standards and validation logic applied during ingestion, invalid addresses, duplicate records, and misclassified lifecycle stages quietly accumulate.

By the time bounce rates spike or segmentation logic starts misfiring, the underlying data problem has often been compounding for months.

Measurement models no longer scale with the program. Open rates and click-through rates are useful signals, but they do not answer the question enterprise leadership actually asks: Is email driving pipeline? Attribution at scale requires connecting email interactions to CRM contacts, open opportunities, and closed-won revenue — across touches that may span weeks or months.

Teams relying on campaign-level reporting alone cannot make that connection, which makes it difficult to justify investment or diagnose where the funnel is leaking.

These are the three critical layers where **email marketing challenges** compound at enterprise scale: governance gaps that allow over-messaging, data problems that undermine segmentation and deliverability, and measurement gaps that make email impact invisible to the business.

Fix email deliverability issues before they suppress growth.

Deliverability is the precondition for everything else, and it is one of the **email marketing challenges** that compounds fastest when enterprise teams lack early visibility into what is going wrong. A campaign with precise segmentation, a well-tested subject line, and a strong offer delivers nothing if it lands in spam—and most enterprise teams lack the visibility to diagnose why until the damage compounds.

For enterprise teams, deliverability problems rarely announce themselves immediately — they surface gradually as open rates drift down and inbox placement quietly shifts toward spam folders before anyone flags it.

The diagnostic covers four interconnected factors: authentication, list quality, complaint rates, and sender reputation.

Authentication establishes trust with receiving servers, but it does not guarantee inbox placement. SPF, DKIM, and DMARC are the minimum infrastructure requirements for inbox placement, and understanding email deliverability best practices is essential before troubleshooting more complex problems. DKIM gives receiving servers a way to verify that the message content has not been tampered with between send and delivery.

DMARC defines what happens to a message that fails SPF or DKIM — whether it is quarantined, rejected, or delivered anyway. In February 2024, Google and Yahoo formalized bulk-sender requirements, making all three mandatory for volumes above certain thresholds. For enterprise teams, authentication is not an optional configuration — it is table stakes.

List hygiene directly affects the sender's reputation. A hard bounce rate above 2% signals list quality problems that will

compound over time, and re-engagement campaigns are critical to maintaining sender reputation.

The fix requires validation logic applied during ingestion, automated suppression of hard bounces after the first occurrence, and a scheduled re-engagement process for contacts who have been inactive for 90 to 180 days. HubSpot automatically suppresses hard bounces and unsubscribes, but the underlying data quality problem still requires active management.

Complaint rates are a leading indicator, not a lagging one. A spam complaint rate above 0.08% will begin to affect deliverability with Gmail. Above 0.1%, Gmail filters messages more aggressively.

Common drivers include sending to contacts who never explicitly opted in, continuing to message chronically unengaged segments, and subject lines that overpromise relative to content. Google Postmaster Tools provides domain-level complaint rate data and should be part of any enterprise sender's monitoring stack.

Sender reputation operates at both the domain and IP level. Domain reputation builds over time through consistent authentication, low bounce rates, and positive engagement signals. IP reputation is more volatile — a single large send to a low-quality list from a shared IP can affect deliverability for other senders on the same IP.

For enterprise teams sending high volumes, a dedicated IP gives one account control over its own sending reputation. HubSpot offers dedicated IPs as an add-on, with a warmup period required before sending at full volume.

HubSpot's Email Health tool surfaces these signals in one place — open rate, click-through rate, unsubscribe rate, spam reports, and hard bounce rate across your sending history, giving teams a consolidated view of where reputation risk is

accumulating.

The diagnostic question for enterprise teams is not whether deliverability problems exist—at scale, some degradation is nearly inevitable—but whether they have systematized email deliverability best practices to minimize that erosion.

The question is whether your monitoring, hygiene processes, and governance model are catching problems early enough to correct them before they suppress growth.

Solve low engagement with better targeting, timing, and testing.

Deliverability gets your email to the inbox, but email optimization through better targeting, timing, and testing determines what happens next. Engagement determines what happens next.

For enterprise teams, low engagement is rarely a creative problem — it is a targeting problem, a timing problem, or a testing problem that compounds across a large contact base and eventually feeds back into deliverability as inbox providers use engagement signals to inform placement decisions.

The diagnostic covers four areas: segmentation precision, personalization at scale, send timing, and disciplined A/B testing.

Segmentation is where most enterprise engagement problems originate. Sending the same message to your entire contact database is not a volume strategy—it is a path to declining engagement, and understanding why list segmentation matters is the first step to solving low engagement at scale.

Effective enterprise segmentation layers lifecycle stage with firmographic data (industry, company size, revenue band) and

behavioral data (pages visited, content downloaded, product usage signals) to produce segments that reflect where a contact actually is in their relationship with your business.

HubSpot’s smart lists update dynamically as contact properties change, which means a segment built on lifecycle stage, last engagement date, and product fit can serve as the foundation for effective email personalization at scale. For teams managing complex segmentation logic, the difference between a static export and a dynamic list is the difference between a snapshot and a live signal.

Personalization at scale requires a systematic approach, not one-to-one content production, and seeing how email personalization works in practice can help teams design architectures that efficiently use dynamic content. The goal is to build a personalization architecture that uses available data to make the right message feel relevant to a defined segment.

HubSpot’s personalization tokens pull contact and company data directly into email content — first name, company name, industry, lifecycle stage, and any custom property your team has defined. For more complex conditional logic, smart content rules render different content blocks based on contact properties, list membership, or lifecycle stage.

Send timing affects open rates more than most teams account for. A fixed send time ignores the reality that optimal timing varies by industry, role, time zone, and individual behavior. HubSpot’s send time optimization uses engagement data from a contact’s history to predict when each individual is most likely to open and schedules delivery accordingly — a meaningful improvement for large lists with geographic and behavioral diversity.

Subject-line strategy deserves the same rigor as any other conversion variable, and email A/B testing provides a

systematic framework for testing variables such as length, personalization, specificity versus curiosity, and social proof. Variables worth testing include length, personalization, specificity versus curiosity-gap framing, and urgency. The constraint is testing discipline — a subject line test that runs on a sample too small to reach statistical significance, or that tests two variables simultaneously, produces noise rather than insight.

A/B testing at enterprise scale requires structure to produce actionable results. HubSpot's A/B testing compares two email variations and sends the winning version to the remaining audience based on a metric you define — open rate, click-through rate, or click-to-open rate. A structured testing program isolates one variable per test, defines the success metric in advance, and maintains a test log that accumulates into institutional knowledge. Teams that test with this structure build a progressively sharper model of their contact base — which subject line framing resonates with which segment, which CTA format drives clicks from which lifecycle stage, which cadence produces the best engagement-to-unsubscribe ratio.

Reduce email production and automation challenges.

For enterprise teams, production and automation bottlenecks are **email marketing challenges** that rarely appear in generic advice — but they are where enterprise programs lose speed, consistency, and contact experience simultaneously.

And like any system running at scale, it fails in predictable places: approvals that bottleneck at a single reviewer, templates rebuilt from scratch for every campaign, QA processes that rely on individual memory rather than on documented checklists, and automation workflows that were

never designed to coexist.

The result is preventable errors in live sends, conflicting sequences that message the same contact from multiple workflows simultaneously, and suppression gaps that let disengaged or legally protected contacts slip through.

Approval workflows reduce error risk without slowing production — if they are designed correctly. A well-designed approval workflow is tiered, not linear. Routine sends using approved templates within established parameters require lighter review than net-new creative, new audience segments, or campaigns that touch legally sensitive topics such as pricing or compliance disclosures.

Explicitly defining those tiers reduces review time for low-risk sends while maintaining appropriate oversight for high-risk sends.

HubSpot Marketing Hub's approval workflow functionality allows teams to require approvals before emails go live, with configurable routing based on campaign type or team structure. For organizations with multiple regional teams or business units sharing a sending domain, this governance layer prevents one team's send from affecting another team's sender reputation.

Reusable components cut production time and enforce brand consistency simultaneously. Every rebuild of a standard header, footer, or CTA button introduces a new opportunity for inconsistency. HubSpot's drag-and-drop email editor supports saved modules — reusable content blocks that can be locked to prevent unauthorized edits or left flexible for campaign-specific customization.

The practical application is a modular template library: approved, brand-compliant building blocks that production teams assemble rather than build from scratch.

QA processes need to be systematic, not individual, and a documented pre-send checklist should cover at a minimum rendering tests, link validation, and compliance verification. A documented pre-send checklist should cover, at minimum: rendering tests across major email clients and mobile devices, personalization token fallback values for contacts with missing data, link validation, UTM parameter consistency, plain-text version accuracy, unsubscribe link functionality, and sender name verification.

HubSpot's pre-send checklist surfaces several of these checks automatically. However, the team-level process — who runs it, who signs off, and what happens when something fails — still requires explicit documentation.

Rendering deserves particular attention. A layout that renders correctly in Apple Mail may break in Outlook, which still uses Microsoft Word's rendering engine rather than a modern HTML engine. Tools like Litmus or Email on Acid integrate with HubSpot and provide rendering previews across dozens of client and device combinations before a send goes live.

Suppression rules are the governance layer that prevents over-messaging. A contact enrolled in a product onboarding sequence, a competitive win-back campaign, and a monthly newsletter simultaneously is not receiving a coordinated experience — it is evidence of a governance gap.

The fix requires two things: a contact-level frequency cap that limits total sends per rolling time window, regardless of which workflow triggers them, and a regular workflow audit that identifies overlap, redundancy, and conflicting messaging.

HubSpot allows teams to set communication limits at the account level, capping marketing emails within a defined period.

Combined with suppression lists — segments excluded based on

lifecycle stage, recent purchase, active deal status, or opt-out preference — frequency caps provide enterprise teams with a systematic mechanism for protecting the contact experience without requiring manual coordination across every active campaign.

Connect email marketing performance to pipeline and revenue.

Click rates and open rates answer one question: Did contacts engage with this email? They do not answer the question that matters most to enterprise leadership: Did email contribute to revenue? For demand generation and marketing operations teams, the gap between those two questions is where email's business case is either made or lost.

Bridging that gap requires three things: a measurement model that connects email interactions to CRM records, an attribution framework that assigns credit across multi-touch buying journeys, and a reporting infrastructure that surfaces email-influenced pipeline and revenue in a format leadership can act on.

The measurement model starts with contact-level data, not campaign-level aggregates. Campaign-level reporting tells you how a send performed in aggregate. It does not tell you which contacts moved lifecycle stages as a result of email engagement, which open opportunities have email touches in their history, or which closed-won deals were influenced by a nurture sequence that ran six weeks before the sales conversation started.

When email interactions are recorded at the contact and deal levels in HubSpot, revenue operations teams can query which contacts with open opportunities engaged with email in the last 30 days and which nurture sequences correlate with faster

progression through lifecycle stages — a materially different level of insight than campaign open rate.

Attribution connects email touches to the pipeline across multi-touch journeys. B2B buying journeys rarely convert on a single touch. Multi-touch attribution distributes credit across all interactions in the journey, giving enterprise teams a defensible view of which channels and content types are contributing at different stages.

HubSpot Marketing Hub Enterprise supports multi-touch revenue attribution, connecting marketing interactions — including email clicks, form submissions, and content downloads — to contacts, associated deals, and closed-won revenue.

Influenced pipeline is a more honest near-term metric than attributed revenue. Influenced pipeline — the total value of open or closed deals where an associated contact had a qualifying email interaction within a defined window — is more transparent and easier to defend in a leadership conversation than a model-based attribution number.

Use click-based interactions rather than email opens as the qualifying signal, since Apple Mail Privacy Protection prefetches tracking pixels regardless of whether the recipient actually engaged, systematically inflating open rates from Apple Mail users.

Revenue attribution reporting needs to be built for the audience that reads it. HubSpot's custom report builder allows teams to create role-specific views — granular, contact-level engagement reports for MOps teams and influenced pipeline and revenue contribution summaries for leadership.

For enterprise teams on Marketing Hub Enterprise, revenue attribution reporting connects closed-won revenue to the marketing interactions that preceded it, giving demand generation leaders a data foundation for investment decisions that goes beyond campaign open rate.

The attribution conversation is ultimately a credibility conversation. Enterprise marketing teams that can connect email to pipeline — with contact-level data, a defined attribution model, and CRM-connected reporting — earn the organizational credibility to invest in better tools, larger lists, and more sophisticated programs.

Use AI where it improves speed without weakening quality.

AI adoption in email marketing tends to polarize into two failure modes. The first is avoidance — treating AI-generated content as inherently lower quality. The second is overreliance — using AI output as final copy without the review and refinement process that separates serviceable content from content that actually performs.

For enterprise teams, the practical question is not whether to use AI in email production — it is where AI creates real leverage in the workflow and where human judgment remains the non-negotiable quality-control layer.

Drafting is where AI creates the most immediate value. The most time-consuming part of email production is not the strategic brief or the final review — it is the blank page.

Getting from a campaign objective to a working draft involves significant low-leverage writing work: structuring the narrative, generating subject line options, drafting body copy, writing preview text, and producing CTA variations to test.

HubSpot's AI tools can generate and refine marketing emails, including subject lines, body copy, preview text, and CTAs, using context from the campaign brief and contact data available in HubSpot. For production teams running multiple campaigns simultaneously, compressing that work from hours to

minutes frees reviewer capacity for higher-value tasks.

Iteration is where AI accelerates testing programs. A disciplined A/B testing program requires a steady supply of variations — not minor word swaps, but meaningfully different approaches to subject line framing, CTA structure, or email length.

Producing those variations manually is one reason enterprise testing programs stall. Breeze generates multiple subject lines and copy variations from a single brief, giving testing programs a larger set of options without proportionally increasing production time. Each variation still requires human review for brand voice consistency, factual accuracy, and compliance with messaging guidelines before entering a test.

Optimization support extends AI's value beyond the draft stage. Beyond drafting and iteration, AI can support the analysis layer — identifying patterns in engagement data, flagging subject line characteristics that correlate with higher open rates in a specific segment, or surfacing contacts whose engagement behavior suggests readiness for a different message type or cadence.

For enterprise teams managing complex segmentation logic and large active contact bases, AI-assisted pattern recognition can surface insights that would take a MOps analyst significant time to produce manually.

Brand control requires explicit governance, not assumed restraint. The risk of AI in enterprise email production is not that it generates bad content — it is that it generates content that is technically competent but misaligned with brand voice, messaging hierarchy, or compliance requirements in ways that are easy to miss under production pressure.

The governance response requires a documented brand voice guide that AI prompts reference directly, a review checklist

that evaluates AI-generated content against brand and compliance standards, and a clear policy on which content types are eligible for AI-assisted drafting. Legal disclaimers, pricing statements, regulated-industry claims, and crisis communications are content types in which compliance risk outweighs the production efficiency gains.

AI earns its place in enterprise email by accelerating the work that slows teams down rather than replacing the expertise that makes the work effective. Breeze compresses the time from brief to working draft and expands the set of variations available for testing.

What it does not replace is the strategic judgment about which segments to target, the brand expertise that distinguishes on-voice copy from technically acceptable copy, and the measurement discipline that determines whether a test result is actionable.

30-Day Action Plan for Improving Email Marketing Challenges

Diagnosing enterprise email problems is straightforward compared to fixing them across an organization where multiple teams share a sending domain, a contact database, and a reporting stack. The risk of a comprehensive diagnostic framework is that it produces a long backlog of improvements with no clear starting point.

The plan below is deliberately constrained. One deliverability fix. One segmentation cleanup. One test. One governance improvement. One measurement improvement. Each phase builds on the previous one, and the total scope is achievable within 30 days without requiring a full platform migration or a cross-functional project team.

Week 1: Deliverability Foundation

Audit your authentication configuration and baseline complaint rate.

Action items for week one:

- Verify SPF, DKIM, and DMARC records are correctly configured for your sending domain. If DMARC is set to p=none, assess whether the data collected is sufficient to move to p=quarantine, which actively protects your domain from unauthorized use.
- Set up Google Postmaster Tools if not already active. Establish your complaint rate baseline. If your complaint rate exceeds 0.08%, identify the segments or campaigns driving it before sending additional volume.
- Pull your hard bounce rate from the last 90 days in HubSpot's Email Health dashboard. If it exceeds 2%, flag the contact sources contributing most to invalid addresses and pause sends to those segments until hygiene is addressed.
- Build a suppression list of contacts who have not opened or clicked in the last 180 days. Run a re-engagement sequence before removing them from your active database.

The deliverable at the end of week one is a clear picture of your authentication status, complaint rate, and bounce rate — and a suppression list that removes your highest-risk contacts from active sends while hygiene work continues.

Week 2: Segmentation Cleanup

Rebuild your primary active segment on behavioral and firmographic criteria.

Action items for week two:

- Define an engaged contact threshold for your program. A reasonable starting definition is a contact who has

opened or clicked at least one email in the last 90 days, or visited a tracked page in the last 30 days. Adjust the window based on your typical sales cycle length.

- Build a dynamic smart list in HubSpot that combines lifecycle stage, engagement recency, and at least one firmographic property relevant to your ICP— such as industry, company size, or revenue band. This becomes your primary active segment for the week three test.
- Audit existing active lists for contacts appearing in multiple overlapping segments. Flag contacts enrolled in more than two active automation workflows and assess whether the overlap is intentional or a governance gap requiring a suppression rule.
- Document the segmentation logic so the criteria are repeatable and do not depend on the individual who built the list.

The deliverable at the end of week two is a rebuilt primary active segment with documented criteria, a clear engaged contact threshold, and a flagged list of contacts enrolled in conflicting workflows.

Week 3: One Structured Test

Run a single, properly structured A/B test on your highest-volume send.

Action items for week three:

- Select one variable to test. Subject line framing is the highest-leverage starting point for most enterprise programs. Choose two meaningfully different approaches — specificity versus curiosity gap, personalized versus non-personalized, question format versus declarative statement — rather than minor word variations unlikely to produce a detectable difference.
- Define your success metric before the test runs. Open

rate is the appropriate metric for a subject line test. Use a minimum of 1,000 contacts per variation as a sample size floor.
- Use HubSpot’s A/B testing functionality to split your rebuilt active segment, define the winning metric, and automatically deploy the winning version to the remaining audience.
- Document the hypothesis, variable, success metric, sample size, and result in a test log. This becomes the foundation of your testing program’s institutional knowledge.

The deliverable at the end of week three is one completed, documented test result and a test log template that the team commits to using for all future experiments.

Week 4: Governance and Measurement

Implement one suppression rule and build one email-influenced pipeline report.

Governance action items:

- Set a contact-level communication frequency cap in HubSpot, limiting marketing email sends to a defined maximum per rolling seven-day window. Three to four emails per week is a reasonable starting ceiling for most enterprise programs.
- Define at least one suppression list based on CRM status: contacts with an open opportunity in a defined late stage, contacts who purchased in the last 30 days, and contacts who filed a support ticket in the last 14 days are common exclusions that prevent marketing sends from conflicting with active sales or customer success conversations.
- Document both the frequency cap and suppression criteria so new campaign managers can apply them without reverse-engineering existing workflow settings.

Measurement action items:

- Build a basic email-influenced pipeline report in HubSpot that shows open opportunities where the associated contact clicked an email link in the last 90 days. Use click-based engagement rather than opens as the qualifying interaction.
- Share the report with one stakeholder outside the marketing team — a revenue operations lead or demand generation director — and gather feedback on whether the metric definition answers the questions they actually ask about email's contribution to the pipeline.
- Identify the gap between what the report currently shows and what a full multi-touch attribution model would show. That gap becomes the roadmap for the next phase of measurement investment.

The deliverable at the end of week four is an active frequency cap, at least one documented suppression list, and a shared email-influenced pipeline report incorporating stakeholder feedback.

What 30 Days Buys You

At the end of this plan, you will have a stable authentication foundation, a cleaner active segment, one documented test result, and a governance layer that collectively establishes the conditions for sustained email performance improvement. More importantly, you will have established the operational discipline — documented criteria, repeatable processes, shared reporting — that makes every subsequent improvement compound.

Solving **email marketing challenges** at enterprise scale requires successive iterations of the same disciplined cycle: diagnose, fix, test, measure, repeat. Thirty days is enough to complete one full cycle. That is where sustained improvement begins.

Frequently Asked Questions About Email Marketing Challenges

What is the fastest way to diagnose deliverability problems?

Start with three data sources: HubSpot’s Email Health dashboard, Google Postmaster Tools, and your authentication record configuration. Email Health surfaces hard bounce rate, unsubscribe rate, and spam complaints in one view. Postmaster Tools shows domain-level reputation and complaint rate data directly from Gmail’s infrastructure. MXToolbox confirms whether SPF, DKIM, and DMARC are correctly configured.

If all three check out and deliverability problems persist, the issue is likely engagement-based filtering. Suppress unengaged contacts, rebuild sends to your highest-engagement segment, and gradually scale volume back up.

How often should you email without hurting engagement?

Track unsubscribe rate by send frequency — that is the most direct signal your audience gives you about cadence tolerance. For most enterprise B2B programs, one to three marketing emails per week is a reasonable operating range. Still, frequency should be calibrated by segment rather than applied uniformly across your entire contact base.

The governance mechanism that makes this manageable at scale is a contact-level frequency cap in HubSpot that limits sends per rolling seven-day window, regardless of how many workflows a contact is enrolled in. Let engagement data set the ceiling, and treat a rising unsubscribe rate as a signal that the ceiling has already been exceeded.

What’s the best way to quickly fix low email open rates?

Diagnose before you intervene. Low open rates have three primary causes: deliverability problems, routing mail to spam folders, and sending to disengaged contacts who are unlikely to open, regardless of creative quality. Check inbox placement first, then segment quality, then subject line performance — in that order.

If deliverability and segment quality are sound, use HubSpot’s A/B testing to test one subject line variable at a time — length, personalization, or framing approach. The fastest sustainable open rate improvement combines clean deliverability, a well-segmented active list, and a subject line testing program that compounds over time.

How should enterprise teams test email changes effectively?

Effective testing requires four commitments: single-variable isolation, pre-defined success metrics, statistically valid sample sizes, and documented test logs. Test one element at a time, agree on the success metric before the test runs, use a minimum sample size of 1,000 contacts per variation, and record every result in a shared log that accumulates into institutional knowledge.

HubSpot’s A/B testing handles the mechanical split and automatic deployment of the winning version. The four structural commitments above determine whether the output is noise or insight.

How do you prove email drives pipeline and revenue?

Start with the influenced pipeline — the total value of open

or closed deals where an associated contact clicked an email within a defined window. Use clicks rather than opens as the qualifying signal, since Apple Mail Privacy Protection inflates open rates by prefetching tracking pixels regardless of whether the recipient actually engaged.

HubSpot Marketing Hub Enterprise supports multi-touch revenue attribution, connecting email interactions to associated deals and closed-won revenue. Build role-specific reports — granular engagement data for MOps teams, pipeline and revenue contribution summaries for leadership — and share them with revenue operations stakeholders early to refine the metric definition before the first full measurement period closes.

Source

Mattel Partners With Bluey as It Shifts From Toy Maker to Building Fandom

The multi-year licensing partnership with BBC Studios brings Bluey to Barbie, Hot Wheels, Fisher-Price, Polly Pocket, and UNO.
https://www.adweek.com/brand-marketing/mattel-partners-with-bluey-as-it-shifts-from-toy-maker-to-building-fandom/

240,000 Hit by Data Breach at Japan’s Digital Agency

Hackers exploited a vulnerability in a VPN product to steal the personal information of roughly 240,000 people.

The post 240,000 Hit by Data Breach at Japan’s Digital Agency appeared first on SecurityWeek.

https://www.securityweek.com/240000-hit-by-data-breach-at-japans-digital-agency/

LA28 Looks to Bring Golden Opportunity to Brands With New Offerings, Massive Viewership

Each day of the Olympics will be like staging seven Super Bowls, according to Janet Evans, chief athlete officer for LA28.
https://www.adweek.com/brand-marketing/la28-brands-new-offerings-massive-viewership/

Richieste dell’autorità contraffatte: il caso Revolut e la verifica delle istanze

Un soggetto non autorizzato ha scritto dal dominio autentico di un’agenzia governativa e si è fatto consegnare documenti d’identità, immagini di verifica facciale e cronologie complete di transazioni. Nessun sistema è stato violato: è stato aggirato il processo con cui un istituto valuta la legittimità di una richiesta dell’autorità. Dal 18 agosto 2026 il regolamento e-Evidence ha standardizzato quel processo per i prestatori di servizi digitali. Le banche, però, restano fuori dal suo perimetro.

La dinamica: dominio autentico, controllo aggirato, dati consegnati

Il 12 settembre 2026 Revolut ha confermato a TechCrunch di avere comunicato dati di clienti a un soggetto non autorizzato. Le richieste arrivavano da un indirizzo di posta attivo sul dominio legittimo di un’agenzia governativa e superavano i controlli tecnici di autenticazione.

La società ha parlato di una sofisticata truffa di impersonificazione esterna. Ha dichiarato di avere bloccato l’indirizzo non appena rilevata la frode e di avere allertato l’agenzia interessata, le forze dell’ordine, le autorità per la protezione dei dati e i regolatori finanziari. Ha aggiunto che i propri sistemi e i fondi dei clienti non risultano compromessi. Sono dichiarazioni dell’azienda, non accertamenti di terzi.

Le categorie di dati emergono dalla notifica inviata ai clienti. TechCrunch, che ne ha visionato il testo, elenca

nome, data di nascita, indirizzo postale, indirizzo di posta elettronica, numero di telefono e copia del documento d’identità. La notifica indica come possibilmente coinvolti anche il selfie di verifica, gli estratti conto e la cronologia delle transazioni. The Register aggiunge professione, IBAN e cronologia completa delle operazioni, comprese quelle in bitcoin.

Revolut non ha detto quanti clienti siano coinvolti, limitandosi a definirli un gruppo molto limitato, e non ha identificato né l’agenzia né i mercati toccati. Le cifre che circolano su alcuni siti di aggregazione non hanno fonte.

Su tre punti serve cautela, perché ciascuno si regge su una fonte sola.

Il primo riguarda il profilo delle vittime. Il ricercatore indipendente ZachXBT, che ha reso pubblica la notifica con un messaggio su Telegram fra la sera dell’11 e il 12 settembre, scrive che l’incidente sembra mirato a clienti ad alto patrimonio. È la valutazione di un singolo ricercatore.

Il secondo riguarda l’estorsione. The Register riferisce che alcuni soggetti si sono attribuiti l’attacco su più gruppi Telegram e chiedono un riscatto di diecimila bitcoin. La testata scrive di avere visto frammenti di dati riferibili a dirigenti, sportivi e artisti. Revolut non ha commentato.

Il terzo riguarda la scoperta. Le notifiche ai clienti risultano inviate l’11 settembre, la conferma aziendale è del 12. Revolut non ha spiegato come abbia rilevato la frode, né quanto tempo sia passato fra la prima risposta e il blocco dell’indirizzo.

Un fenomeno già segnalato

La tecnica ha un nome nella letteratura investigativa di lingua inglese: fraudulent emergency data request, cioè la

falsa richiesta di dati presentata come urgente. Il 4 novembre 2024 l’FBI le ha dedicato una Private Industry Notification.

Il documento descrive un mercato maturo. Nell’agosto 2024 un soggetto vendeva caselle governative offrendosi di accompagnare l’acquirente nella compilazione della richiesta e di fornire atti giudiziari realmente sottratti. Nel marzo 2024 un altro dichiarava di controllarne in oltre venticinque paesi. Nello stesso mese un terzo pubblicava le immagini di una richiesta presentata a PayPal sotto forma di atto di assistenza giudiziaria internazionale, completa di numero di procedimento: la società l’ha respinta.

Le raccomandazioni dell’FBI sono concrete. Applicare pensiero critico alle richieste d’emergenza, perché chi attacca sfrutta l’urgenza per accorciare l’analisi. Esaminare firme e loghi alla ricerca di manipolazioni. Controllare che i riferimenti normativi appartengano davvero all’ordinamento dell’autorità che scrive. E, in caso di dubbio, contattare sia il mittente sia l’autorità di provenienza.

Gli intermediari più esposti sono quelli che detengono identità verificate e storia finanziaria: banche, istituti di pagamento, piattaforme di scambio di cripto-attività. Per adempiere agli obblighi antiriciclaggio un istituto conserva documenti d’identità e le immagini del volto raccolte in fase di verifica. Quel fascicolo può uscire per intero con una sola risposta sbagliata.

Il quadro europeo, e ciò che ne resta fuori

Dal 18 agosto 2026 si applica il regolamento (UE) 2023/1543 sugli ordini europei di produzione e di conservazione di prove elettroniche. L’autorità di uno Stato membro può rivolgersi direttamente allo stabilimento designato o al rappresentante legale del prestatore di servizi in un altro Stato, senza

passare per la cooperazione giudiziaria. La richiesta viaggia su un certificato standardizzato, l’EPOC.

Le garanzie sono graduate secondo la sensibilità dei dati. Per i dati relativi agli abbonati l’ordine può essere emesso anche da un pubblico ministero. Per i dati sul traffico e per i contenuti servono un giudice, un organo giurisdizionale o un magistrato inquirente, e su queste categorie interviene anche l’autorità di esecuzione dello Stato in cui si trova il destinatario. Il termine di risposta è di dieci giorni, che scendono a otto ore nei casi di emergenza. Chi non ottempera rischia sanzioni fino al due per cento del fatturato mondiale annuo.

Conta soprattutto la forma. Quando il regolamento richiede una firma o un sigillo, questi devono essere qualificati ai sensi del regolamento eIDAS. Le comunicazioni passano di norma per un sistema informatico decentrato fondato sui punti di accesso e-CODEX, le cui specifiche tecniche sono fissate dal regolamento di esecuzione (UE) 2025/1550. L’obbligo di usarlo è pienamente operativo dal luglio 2026. L’autenticità dell’ordine, in altre parole, non dipende dal dominio del mittente.

In Italia l’adeguamento è arrivato con il decreto legislativo 30 dicembre 2025, n. 215 e con il decreto legislativo n. 216 della stessa data, che attua la direttiva (UE) 2023/1544. Entrambi sono in vigore dal 30 gennaio 2026. I prestatori già attivi nell’Unione dovevano designare lo stabilimento o nominare il rappresentante legale entro il 18 agosto 2026, con sanzioni fino a un milione e mezzo di euro applicate dal Ministero dell’interno. La testata ne ha già analizzato l’impatto in un approfondimento dedicato.

Un passaggio di quel decreto merita attenzione. L’articolo 5 stabilisce che prestatore, stabilimento designato e rappresentante legale rispondono in solido, e che non possono giustificarsi adducendo la mancanza o l’inadeguatezza delle

procedure interne. La regola traspone la direttiva europea. Il legislatore ha già stabilito che la procedura interna è responsabilità dell'impresa, non un'attenuante.

Qui si apre il punto che il dibattito ha finora trascurato. Il regolamento definisce il prestatore di servizi escludendo espressamente i servizi finanziari. L'esclusione è agganciata al tipo di servizio, non alla natura del soggetto, ma i servizi bancari, di pagamento e di investimento vi ricadono per intero. Per un istituto come Revolut il risultato è netto: nessun certificato EPOC, nessun canale autenticato, nessun modulo standardizzato.

L'asimmetria si vede meglio guardando che cosa il modulo EPOC consente di chiedere. Fra i dati relativi agli abbonati figurano gli strumenti di verifica dell'identità usati alla registrazione, le copie dei documenti forniti dal cliente e le informazioni sulla carta di pagamento. Sono, in larga parte, le stesse categorie consegnate da Revolut. Il legislatore europeo le ha giudicate abbastanza delicate da circondarle di un certificato firmato e di un'infrastruttura autenticata. Quando le detiene una banca, invece, la richiesta continua ad arrivare per posta elettronica.

I profili di protezione dei dati

La prima domanda non è se la richiesta fosse credibile, ma su quale base giuridica il titolare abbia comunicato i dati.

Il Comitato europeo per la protezione dei dati lo ha chiarito nelle Linee guida 02/2024, adottate in versione definitiva il 4 giugno 2025. La richiesta di un'autorità straniera non è di per sé né una base giuridica per il trattamento né un presupposto per il trasferimento. Servono entrambe le cose, e vanno cercate separatamente: la prima nell'articolo 6 del RGPD, la seconda nel capo V. L'articolo 48 non fornisce né l'una né l'altra: dice soltanto che sentenze e decisioni di paesi terzi non valgono nell'Unione senza un accordo

internazionale.

Il Comitato aggiunge due indicazioni pratiche. Se l'accordo internazionale disciplina la cooperazione fra autorità pubbliche, come fa un trattato di mutua assistenza, l'impresa europea deve rinviare il richiedente all'autorità nazionale competente invece di rispondere. E se non è chiaro quale accordo si applichi, il destinatario può interpellare il ministero della Giustizia, il ministero degli Esteri o l'autorità di vigilanza di settore. È una legittimazione formale a fermarsi e verificare.

Il regime cambia dunque secondo la provenienza della richiesta. Da un paese terzo si entra nel perimetro dell'articolo 48. Da uno Stato membro si applicano le regole processuali penali nazionali. Poiché l'agenzia non è stata identificata, nel caso Revolut non è possibile stabilire quale dei due regimi fosse in gioco.

Nel diritto italiano la gradazione è netta. L'articolo 132 del Codice privacy subordina l'acquisizione dei dati di traffico all'autorizzazione del giudice, in presenza di indizi di reati puniti con almeno tre anni di reclusione nel massimo. Ai dati relativi agli abbonati, invece, provvede il pubblico ministero o la polizia giudiziaria. Un'anagrafica cliente e una cronologia di transazioni non appartengono alla stessa categoria, e una procedura che le tratti allo stesso modo è sbagliata in partenza.

C'è poi una norma che contiene il principio assente nel caso Revolut. L'articolo 132-bis del Codice impone ai fornitori di comunicazione elettronica di istituire procedure interne per rispondere alle richieste di accesso ai dati degli utenti, e di riferire al Garante quante ne ricevono, su quali basi legali e con quali esiti. Alle banche non si applica. La domanda che il caso solleva è se debba restare così.

Sul piano della violazione, consegnare dati personali a un

soggetto non legittimato è una violazione di riservatezza anche senza intrusione. Scattano la notifica all'autorità di controllo entro settantadue ore e, quando il rischio è elevato, la comunicazione agli interessati. Copia del passaporto e immagine del volto collocano l'episodio nella fascia alta. Quanto alla responsabilità, il titolare deve dimostrare di avere adottato misure adeguate al rischio, e l'articolo 82 lo esonera dal risarcimento solo se prova che l'evento non gli è in alcun modo imputabile. È una soglia alta.

Un elemento di contesto, da maneggiare con prudenza perché non si sa quale entità del gruppo abbia ricevuto le richieste. Revolut Bank UAB, la banca del gruppo per lo Spazio economico europeo, è autorizzata in Lituania e vigilata dalla banca centrale nazionale e dalla BCE, come indicano le informazioni precontrattuali della società. Nel 2022 l'autorità lituana per la protezione dei dati aveva già avviato un'istruttoria su una violazione riconducibile a ingegneria sociale. Era un episodio diverso: la ricorrenza riguarda il vettore umano, non la stessa vulnerabilità.

Una procedura di verifica riutilizzabile

Quanto segue è una traccia operativa, costruita sulle raccomandazioni dell'FBI, sulle linee guida del Comitato europeo e sull'impianto del regolamento e-Evidence. Va adattata al proprio ordinamento e al proprio modello di servizio.

- **Registro unico delle richieste.** Data e ora di ricezione, mittente dichiarato, canale, categorie di dati e periodo richiesti, esito e motivazione scritta della decisione. Senza registro non esiste responsabilizzazione dimostrabile.
- **Qualificazione preliminare.** Stabilire da quale

ordinamento arriva la richiesta e con quale strumento, prima di entrare nel merito. Se non è chiaro quale accordo internazionale si applichi, interpellare le autorità nazionali competenti invece di decidere da soli.

- **Verifica su canale indipendente.** Ricontattare l'autorità a un recapito pubblicato sul sito ufficiale, mai a quello indicato nella richiesta. La verifica deve accertare l'esistenza del procedimento e la legittimazione di chi firma, non la sola autenticità del dominio.
- **Controllo formale dell'atto.** Riferimenti normativi coerenti con l'ordinamento di provenienza, numero di procedimento, congruenza fra reato indicato e dati richiesti. Dove c'è una firma o un sigillo elettronico, verificarne la validità con strumenti propri.
- **La riservatezza non è un allarme.** Nel modello europeo è l'autorità, non il destinatario, a informare la persona interessata. Chiedere di non avvisare il cliente è quindi normale in un ordine legittimo, e non deve né insospettire né scoraggiare la verifica.
- **Minimizzazione della risposta.** Consegnare solo le categorie indicate e solo il periodo specificato. Una richiesta generica va rimandata al mittente per precisazione, non interpretata estensivamente.
- **Doppia approvazione sui dati ad alto impatto.** Documenti d'identità, immagini del volto e cronologie complete di transazioni richiedono l'assenso congiunto di funzione legale e responsabile della protezione dei dati, con un secondo approvatore estraneo all'istruttoria.
- **Urgenza presidiata.** L'urgenza dichiarata comprime i termini, non il livello di verifica. Serve un percorso rapido con reperibilità definita, invece di lasciare il singolo operatore a decidere sotto pressione.
- **Formazione e rendicontazione.** Il personale esposto è quello legale, di conformità e antifrode che evade materialmente le richieste. Un quadro periodico di

quante ne arrivano e di come sono state trattate è la misura di controllo più semplice da mettere in piedi.

Il rischio speculare: una richiesta legittima su un canale compromesso

C’è un secondo scenario, meno discusso e altrettanto serio. La richiesta è autentica, l’autorità è legittimata, il procedimento esiste. Ma la casella da cui parte, o quella verso cui la risposta viene indirizzata, è sotto il controllo di un terzo.

È la situazione descritta dall’FBI, dove il vettore iniziale è proprio la compromissione di caselle governative. Chi risponde correttamente a una richiesta formalmente valida consegna comunque i dati all’attaccante. Verificare l’atto non basta: va verificato anche il recapito di consegna.

Il canale europeo affronta il problema alla radice. Il regolamento di esecuzione impone autenticazione reciproca tramite certificati digitali, non ripudio dell’origine e della ricezione, impronte crittografiche sui file trasmessi e cifratura del contenuto con un certificato fornito dall’autorità richiedente. Dall’altra parte c’è un messaggio di posta la cui unica garanzia è che il dominio del mittente supera i controlli tecnici, cioè esattamente ciò che è accaduto a Revolut.

Fuori da quel perimetro, dove le banche si collocano, la contromisura resta organizzativa. Consegnare solo a recapiti istituzionali verificati in modo indipendente, cifrare il trasferimento, limitare la validità dei collegamenti di scarico, comunicare l’impronta crittografica di quanto consegnato, notificare l’avvenuta consegna su un canale diverso da quello della richiesta.

Vale anche il rovescio. Un’agenzia la cui casella viene

abusata subisce un incidente proprio, con obblighi di sicurezza e di notifica autonomi. Nel caso Revolut l’agenzia non identificata è tanto lo strumento dell’attacco quanto, con ogni probabilità, una vittima.

Che cosa resta da decidere

Il caso non si chiude con il numero dei clienti coinvolti, che forse non conosceremo mai. Si chiude con una domanda che ogni titolare del trattamento dovrebbe saper documentare: chi, in azienda, è autorizzato a rilasciare un fascicolo identificativo completo a un’autorità, sulla base di quale verifica e con quale prova scritta di averla fatta.

Il regolamento e-Evidence ha risposto a quella domanda per una parte del mercato. Per il resto, la risposta è ancora interamente nelle mani delle singole organizzazioni.

https://www.ictsecuritymagazine.com/notizie/richieste-dati-contraffatte-autorita-caso-revolut/

Apple Patches 200 Vulnerabilities With New iOS 27, macOS Golden Gate 27 Releases

The updates resolve kernel vulnerabilities that could lead to memory corruption, privilege escalation, system termination, and information leaks.

The post Apple Patches 200 Vulnerabilities With New iOS 27,

macOS Golden Gate 27 Releases appeared first on SecurityWeek.

https://www.securityweek.com/apple-patches-200-vulnerabilities-with-new-ios-27-macos-golden-gate-27-releases/

Retail Giant Simon Bets on Real-World Connection to Ignite Mall Culture

Simon, the largest shopping mall owner in the U.S., wants to reinforce malls as gathering places. https://www.adweek.com/creativity/retail-giant-simon-bets-on-real-world-connection-to-revive-mall-culture/