External platform exposure audit

boreal.example | Key findings and possible weaknesses

Period: August 16 to November 13, 2026 (90 days) | Source: LastSpam mail logs | Sample report, invented data

1. At a glance

In short: Many Boréal email addresses are used to sign up on outside websites. If one of those sites is breached, or someone reuses a password, an attacker gets a way in. This page shows how big that exposure is.

72 / 100
LastSpam risk score, amber band (100 = little risk, last 30 days)

318
people found in known data breaches

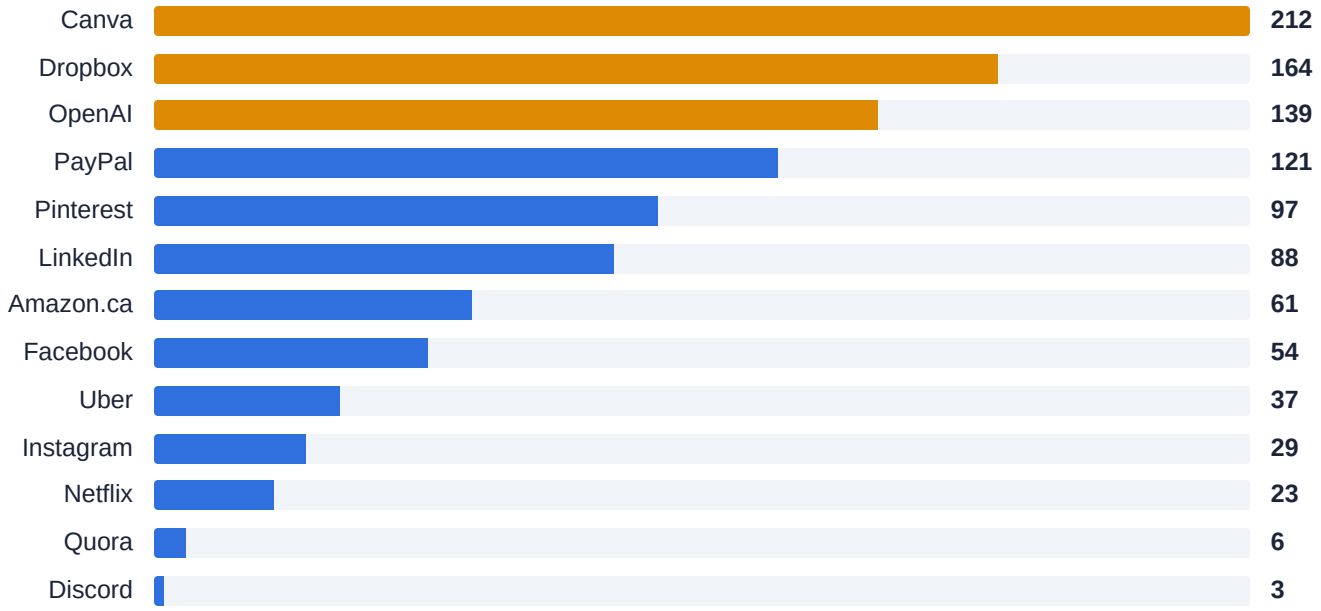
412
mailboxes reached by one suspicious password email

212
addresses on the single most-used outside platform

The audit looked at delivered mail whose subject signals an account on an outside platform: password resets, sign-up verifications, receipts and orders. It covers every boreal.example recipient.

2. Where your addresses have accounts

In short: Each bar is the number of different addresses that received mail from that platform in 90 days. Receiving account mail means an account or subscription exists. Amber bars are tools that can store your files or data.



Addresses receiving mail from each platform, August 16 to November 13, 2026. Counts are an upper bound: they match any sender address containing the platform name. Thirteen platforms were checked; others can be added.

3. Possible real weaknesses, ranked

In short: These are the findings most likely to turn into a real security problem. “Possible” matters: each one is a signal from the mail logs that your IT team needs to check, not a confirmed incident.

#	Weakness	Evidence	Level
1	**Suspicious password email reached 412 mailboxes**	Sender security@m365-account-verify.example, subject “Password protection update”, October 6 to 8. Delivered as clean. The domain is not a Microsoft one. Either your own awareness test or credential phishing.	HIGH
2	**318 people appear in known breaches**	LastSpam risk report. Any of them reusing an old password without multi-factor sign-in is an open door.	HIGH
3	**Fake payment notices were delivered**	96 messages on August 21 from look-alike domains (apple-receipt-info.example and similar). Samples were rated spam but still delivered.	HIGH
4	**Unmanaged tools that may hold your data**	Canva (212 people), Dropbox (164), OpenAI (139). If these are personal accounts, company documents and client information sit outside your control.	MEDIUM
5	**Personal payment accounts on work addresses**	PayPal reaches 121 addresses; ride, shopping and banking services also send receipts. A hijacked mailbox can reset these accounts, and the reverse.	MEDIUM
6	**One mailbox with abnormal reset volume**	scanner-3@boreal.example received 143 password messages in 90 days. Likely a shared or service account.	MEDIUM
7	**Social and consumer accounts on work addresses**	Pinterest (97 people), LinkedIn (88), Facebook (54), Netflix (23). Lower direct risk, but each is a password that may be reused.	LOW
8	**Unidentified sign-up source**	quickdeal-offers.example sent 19 verification messages from September 22 to 25. Not a platform that could be identified.	LOW

4. Personal purchases tied to work email

In short: Receipts and order confirmations show accounts that hold payment details. These are the accounts an attacker wants most, and they belong on a personal email address, not a work one.

Platform	Messages in 90 days	Likely use
Amazon.ca	412	Mixed: personal and company purchasing
Uber	187	Personal
PayPal	163	Personal
Apple	98	Personal
Microsoft Store	71	Likely company purchasing
A wholesale club	44	Personal
A bank	22	Personal banking

“Likely use” is a judgment from the platform name, not something the logs state.

5. Platforms with known breaches

In short: LastSpam compares who emails you against a list of platforms that have been breached. A match does not mean you were breached. It means your people use, or correspond with, a service whose user data leaked at some point.

Platform	Latest breach	Severity	Your people receiving	How to read it
A webmail provider	2012	Critical	148	Mostly clients and contacts writing from that provider
A telecom provider’s mailboxes	2017	Critical	19	Same: a mailbox provider
A professional network	2021	Critical	88 over 90 days	Real accounts held by your people
A design platform	2019	Critical	212 over 90 days	Real accounts held by your people
An animation app	2024	High	2	Most recent breach on the list

Platform names are replaced by descriptions in this sample; your own report names them. No breach notice addressed to your account holders was found in the period.

6. Recommended actions

In short: Ordered by urgency. The first three address findings that could already be active; the rest reduce the exposure over time.

#	Action	When
1	Ask your IT team whether the m365-account-verify.example password email was their own awareness campaign. If not: block the domain, find who clicked, reset those passwords.	Now
2	Block the apple-receipt-info look-alike senders and check why spam-rated mail was delivered.	Now
3	Confirm multi-factor sign-in is enforced for the 318 people in known breaches; force a password change for anyone without it.	This week
4	Investigate scanner-3@boreal.example and its 143 password messages.	This week
5	Decide on Canva, Dropbox and OpenAI: company-managed accounts with single sign-on, or a clear rule against putting company data in personal accounts.	This month
6	Publish a short acceptable-use rule: work addresses are not for shopping, banking, social media or streaming.	This month
7	Identify quickdeal-offers.example and who received its verification messages.	This month

7. What this audit can and cannot show

In short: The logs prove that accounts exist. They cannot prove that passwords are reused or that any account was taken over.

- **Visible:** sender, recipient, subject, verdict and outcome. Message bodies are not.
- **Pattern audit, not an inventory:** each ranking returns the top 15 to 25 entries, so smaller platforms are missed.
- **Scope:** all recipients. No individual is named in this report.
- **Risk report figures** (score, breached platforms, people in breaches) cover the last 30 days; all other figures cover 90 days.
- **Possible next audits:** high-value roles (IT, finance, HR, management), a wider platform list, and French subject patterns.

How this report was made. One question, typed or spoken, to an AI assistant (Grok, ChatGPT or Claude) connected to LastSpam. The assistant ran the searches, counted and wrote the report. Nobody opened a menu.