# Audit d’exposition aux plateformes externes

boreal.example | Constats clés et faiblesses possibles

Période : du 16 août au 13 novembre 2026 (90 jours) | Source : journaux de courriels LastSpam | Exemple de rapport, données fictives

## 1. En un coup d’œil

**En bref :** Bien des adresses courriel de Boréal servent à s’inscrire sur des sites externes. Si l’un de ces sites est piraté, ou si quelqu’un réutilise un mot de passe, un attaquant obtient une porte d’entrée. Cette page montre l’ampleur de cette exposition.

**72 / 100**
Cote de risque LastSpam, zone ambre (100 = peu de risque, 30 derniers jours)

**318**
personnes trouvées dans des fuites de données connues

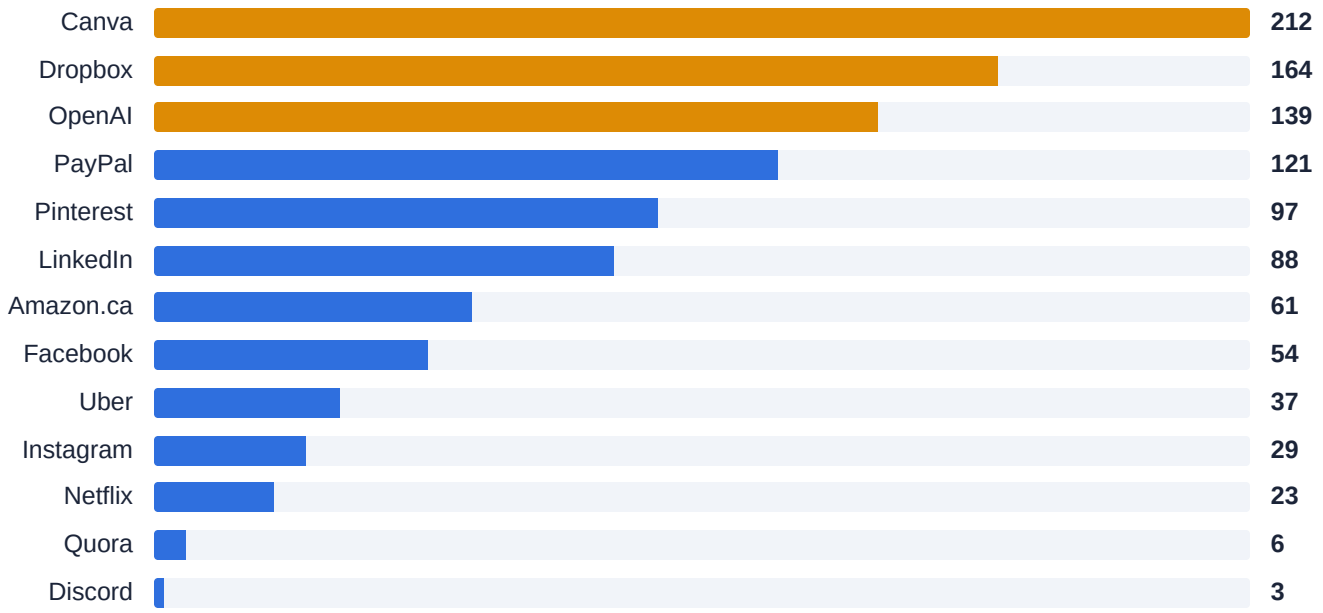
**412**
boîtes atteintes par un seul courriel suspect de mot de passe

**212**
adresses sur la plateforme externe la plus utilisée

L’audit a examiné les courriels livrés dont l’objet indique un compte sur une plateforme externe : réinitialisations de mot de passe, vérifications d’inscription, reçus et commandes. Il couvre tous les destinataires de boreal.example.

## 2. Où vos adresses ont des comptes

**En bref :** Chaque barre indique le nombre d’adresses différentes qui ont reçu des courriels de cette plateforme en 90 jours. Recevoir des courriels de compte veut dire qu’un compte ou un abonnement existe. Les barres ambre sont des outils pouvant contenir vos fichiers ou vos données.




Adresses recevant des courriels de chaque plateforme, du 16 août au 13 novembre 2026. Les nombres sont un maximum : ils comptent toute adresse d’expéditeur contenant le nom de la plateforme. Treize plateformes ont été vérifiées; d’autres peuvent être ajoutées.

## 3. Faiblesses possibles, par ordre d’importance

**En bref :** Voici les constats les plus susceptibles de devenir un vrai problème de sécurité. Le mot « possible » compte : chacun est un signal tiré des journaux de courriels que votre équipe TI doit vérifier, pas un incident confirmé.

| N° | Faiblesse | Preuve | Niveau |
|---|---|---|---|
| 1 | **Un courriel suspect de mot de passe a atteint 412 boîtes** | Expéditeur security@m365-account-verify.example, objet « Password protection update », du 6 au 8 octobre. Livré comme sain. Le domaine n’appartient pas à Microsoft. Soit votre propre test de sensibilisation, soit de l’hameçonnage de mots de passe. | ÉLEVÉ |
| 2 | **318 personnes figurent dans des fuites connues** | Rapport de risque LastSpam. Toute personne qui réutilise un vieux mot de passe sans authentification à deux facteurs est une porte ouverte. | ÉLEVÉ |
| 3 | **De faux avis de paiement ont été livrés** | 96 messages le 21 août provenant de domaines imitateurs (apple-receipt-info.example et semblables). Des échantillons ont été classés pourriel, mais livrés quand même. | ÉLEVÉ |
| 4 | **Des outils non gérés qui peuvent contenir vos données** | Canva (212 personnes), Dropbox (164), OpenAI (139). S’il s’agit de comptes personnels, des documents d’entreprise et des renseignements sur vos clients se trouvent hors de votre contrôle. | MOYEN |
| 5 | **Des comptes de paiement personnels sur des adresses de travail** | PayPal joint 121 adresses; des services de transport, de magasinage et de banque envoient aussi des reçus. Une boîte piratée permet de réinitialiser ces comptes, et l’inverse. | MOYEN |
| 6 | **Une boîte avec un volume anormal de réinitialisations** | scanner-3@boreal.example a reçu 143 messages de mot de passe en 90 jours. Probablement un compte partagé ou de service. | MOYEN |
| 7 | **Des comptes sociaux et grand public sur des adresses de travail** | Pinterest (97 personnes), LinkedIn (88), Facebook (54), Netflix (23). Risque direct plus faible, mais chacun est un mot de passe peut-être réutilisé. | FAIBLE |
| 8 | **Une source d’inscription non identifiée** | quickdeal-offers.example a envoyé 19 messages de vérification du 22 au 25 septembre. La plateforme n’a pas pu être identifiée. | FAIBLE |

## 4. Achats personnels liés au courriel de travail

**En bref :** Les reçus et confirmations de commande révèlent des comptes qui contiennent des données de paiement. Ce sont les comptes qu’un attaquant veut le plus, et ils devraient être liés à une adresse personnelle, pas à une adresse de travail.

| Plateforme | Messages en 90 jours | Usage probable |
|---|---|---|
| Amazon.ca | 412 | Mixte : achats personnels et d’entreprise |
| Uber | 187 | Personnel |
| PayPal | 163 | Personnel |
| Apple | 98 | Personnel |
| Microsoft Store | 71 | Probablement des achats d’entreprise |
| Un club-entrepôt | 44 | Personnel |
| Une banque | 22 | Services bancaires personnels |

L’« usage probable » est un jugement fondé sur le nom de la plateforme; les journaux ne le disent pas.

## 5. Plateformes ayant subi des fuites connues

**En bref :** LastSpam compare les expéditeurs qui vous écrivent à une liste de plateformes ayant subi une fuite. Une correspondance ne veut pas dire que vous avez été piraté. Elle veut dire que votre personnel utilise un service dont les données d’utilisateurs ont fui à un moment donné, ou correspond avec lui.

| Plateforme | Dernière fuite | Gravité | Personnes jointes chez vous | Comment le lire |
|---|---|---|---|---|
| Un fournisseur de courriel Web | 2012 | Critique | 148 | Surtout des clients et des contacts qui écrivent à partir de ce fournisseur |
| Les boîtes d’un fournisseur de télécommunications | 2017 | Critique | 19 | Même chose : un fournisseur de boîtes courriel |
| Un réseau professionnel | 2021 | Critique | 88 en 90 jours | De vrais comptes détenus par votre personnel |
| Une plateforme de design | 2019 | Critique | 212 en 90 jours | De vrais comptes détenus par votre personnel |
| Une application d’animation | 2024 | Élevée | 2 | La fuite la plus récente de la liste |

Dans cet exemple, les noms des plateformes sont remplacés par des descriptions; votre propre rapport les nomme. Aucun avis de fuite adressé à vos titulaires de compte n’a été trouvé pendant la période.

## 6. Actions recommandées

**En bref :** Classées par urgence. Les trois premières visent des constats peut-être déjà actifs; les autres réduisent l’exposition avec le temps.

| N° | Action | Quand |
|---|---|---|
| 1 | Demandez à votre équipe TI si le courriel de mot de passe de m365-account-verify.example était sa propre campagne de sensibilisation. Sinon : bloquez le domaine, trouvez qui a cliqué, réinitialisez ces mots de passe. | Maintenant |
| 2 | Bloquez les expéditeurs imitateurs apple-receipt-info et vérifiez pourquoi des courriels classés pourriel ont été livrés. | Maintenant |
| 3 | Confirmez que l’authentification à deux facteurs est imposée aux 318 personnes figurant dans des fuites connues; forcez un changement de mot de passe pour celles qui ne l’ont pas. | Cette semaine |
| 4 | Examinez scanner-3@boreal.example et ses 143 messages de mot de passe. | Cette semaine |
| 5 | Décidez pour Canva, Dropbox et OpenAI : des comptes gérés par l’entreprise avec authentification unique, ou une règle claire interdisant de mettre des données de l’entreprise dans des comptes personnels. | Ce mois-ci |
| 6 | Publiez une courte règle d’usage acceptable : les adresses de travail ne servent pas au magasinage, aux services bancaires, aux médias sociaux ni au divertissement. | Ce mois-ci |
| 7 | Identifiez quickdeal-offers.example et les personnes qui ont reçu ses messages de vérification. | Ce mois-ci |

## 7. Ce que cet audit peut et ne peut pas montrer

**En bref :** Les journaux prouvent que des comptes existent. Ils ne peuvent pas prouver que des mots de passe sont réutilisés ni qu’un compte a été compromis.

- **Visible :** l’expéditeur, le destinataire, l’objet, le verdict et le résultat. Pas le contenu des messages.
- **Un audit de tendances, pas un inventaire :** chaque classement retourne les 15 à 25 premières entrées, donc les petites plateformes échappent à l’audit.
- **Portée :** tous les destinataires. Aucune personne n’est nommée dans ce rapport.
- **Les chiffres du rapport de risque** (cote, plateformes ayant subi une fuite, personnes dans des fuites) couvrent les 30 derniers jours; tous les autres couvrent 90 jours.
- **Prochains audits possibles :** les rôles sensibles (TI, finances, RH, direction), une liste de plateformes plus large et les objets en français.

**Comment ce rapport a été produit.** Une seule question, tapée ou dictée, à un assistant IA (Grok, ChatGPT ou Claude) branché à LastSpam. L’assistant a fait les recherches, compté et rédigé le rapport. Personne n’a ouvert un menu.