メール不正送信に関するお詫びとご報告

2026 年 3 月 9 日
株式会社 SaveExpats
代表取締役　岩田竜馬

平素より格別のご愛顧を賜り、誠にありがとうございます。

このたび、当社が利用する外部メール配信サービスにおいて、API キーが第三者に不正取得され、当社の意図しないメールが大量に送信されていた事実が判明いたしました。

関係者の皆様に多大なるご迷惑とご心配をおかけしましたことを、深くお詫び申し上げます。

1. 発生した事象について

2026年3月8日､外部メール配信サービス事業者より異常な送信量に関する通知を受け、当社にて調査したところ、第三者による API キーの不正利用を確認いたしました。

この不正利用により、以下の事象が発生しております。

不正送信件数：	約 140,000 件
不正送信期間：	2026 年 3 月 5 日〜3 月 7 日
送信内容：	受信者を不正なウェブサイトに誘導し、個人情報の入力等を促すフィッシング詐欺目的のメール等 ※当社はこれらのメールを一切送信しておりません。

なお、本件は当社の送信元情報を悪用したものであり、当社が保有するお客様情報が外部へ送信された事実は確認されておりません。

2. 原因について

現時点の調査では、外部メール配信サービスで利用していた API キーが外部に流出し、不正アクセスを受けた可能性が高いことが判明しております。

流出経路と不正利用の詳細については、現在も調査を継続しております。

3. 影響範囲について

本件により、第三者によるフィッシング詐欺メール等が外部の受信者へ送信され、迷惑および被害の恐れを生じさせた可能性があります。

一方で、

・当社サーバーへの侵入痕跡
・当社保有の個人情報が閲覧・取得された事実
は確認されておりません。

4. 受信者の皆様へのお願い
以下の点にご注意いただきますようお願いいたします。

・不審なメール内のリンクをクリックしない
・添付ファイルを開かない
・メールに返信しない
・「当社からの案内かどうか不明」なものは破棄する

本件に関して、当社が個人情報の入力をお願いするようなメールを送信することはございません。

5. 当社の対応および再発防止策
本件の判明後、当社では以下の対策を実施済みです。

・不正利用された API キーの 即時無効化
・外部メール配信サービスアカウントの パスワードおよび認証情報の更新
・アクセスログの精査 および不正アクセスの特定作業
・API キーの 保管方法・権限設定の見直し
・システムおよび運用面での セキュリティ強化

今後も再発防止に向けて、セキュリティ管理体制を一層強化し、類似の事象が発生しないよう努めてまいります。

6. お問い合わせ
本件に関するお問い合わせは、下記までご連絡ください。
株式会社 SaveExpats
住所：〒150-0011 東京都渋谷区東 1-1-38-404
MAIL：info@saveexpats.com

Incident Notice Regarding Unauthorized Email Sending via Compromised API Key

Date: March 9, 2026

Organization: SaveExpats Inc.

Representative: Ryuma Iwata, Chief Executive Officer

SaveExpats Inc. (“the Company”) is providing notice of a security incident involving unauthorized email activity conducted through an external email delivery service. We take the protection of our systems and data seriously and are committed to transparency regarding this matter. We sincerely apologize for any inconvenience or concern this incident may have caused.

1. What Happened

On March 8, 2026, the Company received an alert from our external email service provider regarding unusually high outbound email volume. Following an internal investigation, we confirmed that an API key used within our email delivery environment had been compromised and misused by an unauthorized third party.

The unauthorized activity occurred during the following period:

- Unauthorized email volume: Approximately 140,000 emails

- Unauthorized sending period: March 5–7, 2026

- Nature of the emails: Phishing emails intended to redirect recipients to fraudulent websites and solicit personal information.

The Company did not send or authorize these emails.

At this time, we have no indication that customer data stored by the Company was accessed or transmitted externally.

2. What Information Was Involved

Our investigation has confirmed:

- No evidence of unauthorized access to Company servers,

- No evidence that personal information held by the Company was viewed or obtained.

The incident involved only the unauthorized use of an API key to send phishing emails.

3. What We Are Doing

Upon confirming the incident, the Company immediately took the following actions:

- Revoked the compromised API key

- Updated account passwords and authentication credentials

- Conducted detailed access log reviews and forensic analysis

- Reviewed and reinforced API key storage and permission management

- Strengthened system and operational security measures, including expanded monitoring

The Company continues to investigate the cause and root method of the compromise.

4. What You Can Do

If you believe you may have received an email purporting to come from SaveExpats Inc. during the affected period, we recommend that you:

- Do not click on links in suspicious emails

- Do not open attachments

- Do not reply to the message

- Delete the email immediately

The Company does not request personal information via email.

5. For More Information

SaveExpats Inc.

1-1-38-404 Higashi, Shibuya-ku, Tokyo 150-0011

Email: info@saveexpats.com

We appreciate your understanding and sincerely apologize for the concern this incident may have caused. The Company remains committed to strengthening its security posture and preventing future incidents.