

إشعار إلى المسافرين بشأن حادثة أمنية متعلقة بالبيانات

حددت شركة ترافلبورت (Travelport) مؤخراً أن بيانات تخص بعض المسافرين والمحفوطة في نظام «فيو تريب» (ViewTrip) قد تعرضت لوصول غير مصرح به.

وفور علمنا بالحادثة، نفذنا تدابير الاحتواء، وعملنا بالتعاون مع مستشارين متخصصين، واتخذنا الخطوات المناسبة لحماية عملائنا وأنظمتنا. كما تواصلنا مع عملاء ترافلبورت المتأثرين من وكالات السفر ومزودي خدمات السفر.

وعلى الرغم من عدم وجود أي دليل على نشر البيانات الشخصية للمسافرين أو بيعها أو استخدامها لأغراض التصيد الاحتيالي أو انتحال الهوية، فإننا ننشر هذا الإشعار لإحاطة المسافرين علماً بالحادثة وبالإجراءات التي يمكنهم اتخاذها لحماية أنفسهم. وإذا لم تكن متأكداً مما إذا كان هذا الإشعار ينطبق عليك، فيرجى التواصل مع وكالة السفر الخاصة بك.

أولاً: تفاصيل الحادثة

علمت ترافلبورت بوجود نشاط غير معتاد على منصة «فيو تريب» بتاريخ ٦ أغسطس ٢٠٢٦. وعلى إثر ذلك، بادرت ترافلبورت إلى تنفيذ تدابير الاحتواء، وطُبقت معالجة فنية بتاريخ ٧ أغسطس ٢٠٢٦.

ومنذ ذلك الحين، أعيدت منصة «فيو تريب» إلى الخدمة بصورة آمنة، وذلك عقب تطبيق تدابير أمنية معززة.

وأكد التحقيق الجنائي الرقمي الذي أجرته ترافلبورت أن مجموعة محدودة من سجلات المسافرين المحفوظة على منصة «فيو تريب» قد تعرضت لوصول غير مصرح به، بما في ذلك بيانات أفراد عالجتها ترافلبورت عبر المنصة من خلال شركائها من وكالات السفر. وقد تمكن طرف ثالث غير مصرح له من الوصول إلى بعض المعلومات المتعلقة بالحجوزات، وربما الحصول عليها.

وقد اقتصرَت الحادثة على منصة «فيو تريب»، التي تُستخدم حصراً كأداة لعرض مسارات السفر، ولم تنطو على أي اختراق لأي من أنظمة ترافلبورت أو شبكتها أو بيئاتها الأخرى. كما لا تعلم ترافلبورت بحدوث أي تعديل غير مصرح به على أي من خطط السفر.

ثانياً: البيانات التي قد تكون تأثرت

ترد أدناه عناصر البيانات المتأثرة. ومع ذلك، نود الإشارة إلى أن نطاق البيانات المتأثرة يختلف بحسب المعلومات التي تم تحميلها على منصة «فيو تريب»، ومن ثم فليس بالضرورة أن تكون جميع عناصر البيانات المبينة أدناه قد تأثرت بالنسبة إلى كل فرد:

1. أسماء المسافرين كما تظهر في الحجوزات؛
2. تفاصيل مرجع الحجز وسجل اسم المسافر (PNR) ؛
3. الأرقام المرجعية الخاصة بمزودي خدمات السفر؛
4. بيانات الاتصال، مثل عناوين البريد الإلكتروني أو أرقام الهواتف (وفي كثير من الحالات، تخص هذه البيانات وكالات السفر بدلاً من المسافرين الأفراد)؛
5. معلومات مسارات رحلات الطيران والإقامة الفندقية وتأجير السيارات والسفر بالقطارات؛
6. رموز طلبات الخدمات الخاصة (مثل متطلبات إمكانية الوصول أو التفضيلات الغذائية)؛
7. أرقام بطاقات برامج الولاء.

يرجى ملاحظة أن أرقام الهوية أو أرقام جوازات السفر لم تتأثر، كما أن أرقام بطاقات الدفع لم تكن مخزنة أو مكشوفة بنص واضح.

ويتعلق جزء كبير من البيانات المتأثرة برحلات سابقة، وليس برحلات مرتقبة. ولا يوجد أي دليل على نشر البيانات الشخصية للمسافرين أو بيعها أو استخدامها لأغراض التصيد الاحتيالي أو انتحال الهوية.

ثالثاً: الإجراءات التي اتخذتها ترافلبورت

عند اكتشاف الحادثة، تحركت ترافلبورت على وجه السرعة واتخذت الإجراءات التالية:

1. فعلنا على الفور إجراءات الاستجابة للحوادث، ونفذنا تدابير تقنية، وأجرينا تحقيقاً مفصلاً.
2. طبقنا تدابير الاحتواء اللازمة. كما أوقفنا موقع «فيو تريب» مؤقتاً لإتاحة تنفيذ تدابير أمنية إضافية والتحقق من فعاليتها.
3. تواصلنا مع عملاء ترافلبورت المتأثرين من وكالات السفر ومزودي خدمات السفر.
4. استعنا بمتخصصين خارجيين في الأمن السيبراني ومستشارين قانونيين لدعم جهودنا في التحقيق والمعالجة.
5. طبقنا حلاً دائماً وضمائم إضافية قبل إعادة الخدمة إلى العمل.
6. عطلنا سجلات أسماء المسافرين المتأثرة (PNR) على منصة «فيو تريب» كإجراء احترازي.
7. أبلغنا عدداً من سلطات حماية البيانات بالحادثة.
8. واصلنا مراقبة شبكة الإنترنت المظلمة.

رابعاً: ما الذي يمكنك القيام به؟

لا تعلم ترافلبورت بوقوع أي حالات نُشرت فيها البيانات أو بيعت، أو استُخدمت فيها لأغراض التصيد الاحتيالي أو انتحال الهوية فيما يتصل بهذه الحادثة. ومع ذلك، لا يمكننا استبعاد احتمال استخدام بعض بيانات الاتصال، مثل عناوين البريد الإلكتروني أو أرقام الهواتف، لأغراض التصيد الاحتيالي.

ونؤكد مجدداً أننا لسنا على علم بوقوع أي محاولات تصيد احتيالي من هذا القبيل، وأن البيانات المتأثرة لم تشمل بيانات الدخول إلى الحسابات المالية، أو أسئلة الأمان وإجاباتها، أو غيرها من بيانات المصادقة التي من شأنها تسهيل محاولات تصيد احتيالي شديدة الاستهداف أو مقنعة بدرجة كبيرة.

ومع تزايد شيوع الهجمات من هذا النوع، أصبح من المهم أكثر من أي وقت مضى توخي اليقظة تجاه أي نشاط مشبوه، حمايةً لك عند استخدام الإنترنت والحد من مخاطر التعرض لهجمات التصيد الاحتيالي. وكما هو الحال دائماً، نشجع المسافرين على مواصلة اتباع التوصيات الأمنية المعتادة، بما في ذلك ما يلي:

1. توخي الحذر عند النقر على الروابط الواردة في المراسلات الصادرة عن مصادر مجهولة أو غير موثوق بها؛
2. توخي اليقظة إزاء المكالمات الهاتفية أو الرسائل المشبوهة التي تشير إلى ترتيبات سفر، أو تطلب منك التحقق من بياناتك الشخصية أو إجراء مدفوعات؛
3. عدم تقديم أي معلومات شخصية أو مالية استجابةً لطلبات غير متوقعة، حتى وإن بدت صادرة عن مزود خدمات سفر معروف؛
4. مراقبة حساباتك في برامج الولاء لرصد أي نشاط غير معتاد؛
5. التحقق بصورة مستقلة من صحة أي مراسلة يُزعم أنها صادرة عن مزود خدمات سفر، وذلك بالتواصل معه عبر موقعه الإلكتروني الرسمي أو باستخدام بيانات الاتصال المنشورة الخاصة به.

يرجى ملاحظة أن ترافلبورت لن تتواصل معك لطلب كلمات المرور أو أرقام التعريف الشخصية (PIN) أو بياناتك المصرفية فيما يتصل بهذا الإشعار. وإذا تلقيت طلباً من هذا القبيل، فنوصيك بعدم الاستجابة له.

معلومات التواصل

للاستفسارات المتعلقة بحجزك، يرجى التواصل مع وكالة السفر الخاصة بك.

أما بالنسبة إلى أي استفسارات أخرى، فيمكنكم التواصل مع فريق الخصوصية العالمي في ترافلبورت عبر عنوان البريد الإلكتروني التالي:

ViewtripPrivacy@travelport.com