ما هو اختراق البيانات؟

يحدث اختراق البيانات عندما يتم سرقة أو الوصول غير المصرح به إلى المعلومات التي تحتفظ بها المؤسسة.
يمكن للمجرمين استخدام هذه المعلومات عند إنشاء رسائل احتيالية (مثل الرسائل الإلكترونية والرسائل النصية) بحيث تبدو مشروعة. تم تصميم الرسالة لتجعلك تشعر أنه يتم استهدافك بشكل فردي، عندما في الواقع يقوم المجرمون بإرسال ملايين من هذه الرسائل الاحتيالية. قد يرسل المجرمون رسائل يدعون فيها أنهم من مؤسسة تعرضت لاختراق بيانات مؤخرًا.
حتى إذا لم يتم سرقة بياناتك في اختراق البيانات، فإن المجرمين سيستغلون الاختراقات ذات الشهرة العالية (بينما لا تزال طازجة في ذهن الناس) لمحاولة خداع الناس وجعلهم ينقرون على رسائل احتيالية.

هل تعرضت فوري لاختراق بيانات؟

نعتقد أن قراصنة برامج الفدية حصلوا على جزء من أنظمة فوري المعزولة التي نستخدمها لاختبار منتجات جديدة وتغييرات على منصتنا الحية.
في ذلك الوقت، كانت تفاصيل بعض العملاء متواجدة على هذه المنصة التجريبية ، بما في ذلك معلومات مثل عناوين المنازل و البريد الإلكتروني وأرقام الهواتف وتواريخ الميلاد. نعتقد أن القراصنة قد قاموا بتنزيل بعض أو كل هذه البيانات وقد يتم أو لا يتم نشرها على الإنترنت.
وتظل فوري واثقة من أن هذه البيانات لن تؤثر على سلامة أو أمان المعاملات المالية على منصتها، ولكن يجب عليك أن تكون حذرًا وتكون في حالة تأهب لأن المجرمين قد يستخدمون هذه المعلومات عند إنشاء رسائل احتيالية عبر البريد الإلكتروني أو الرسائل النصية، التي تبدو وكأنها من مصدر شرعي.

ما هو تأثير ذلك عليك؟

لا يشكل أي من البيانات المسروقة في الهجوم السيبراني خطرًا على أمانك. بالمثلأيضًا، لم يفقد أي من عملاء فوري أي أموال. يمكنك الاستمرار في استخدام منصة فوري الحية بثقة تامة، حيث بقيت آمنة دائمًا.

ما الذي يجب عليك فعله؟

ما لم تشتبه في وجود نشاط مشبوه (راجع "كيفية الحفاظ على أمان نفسك")، فلا يلزم اتخاذ أي إجراء من قبل العملاء. إذا كان من المستحسن تحديث معلومات الأمان الخاصة بك – مثل كلمات المرور – سنتواصل معك مباشرة من خلال القنوات الرسمية.

كيفية الحفاظ على أمان نفسك.

سنقوم بالاتصال بك فقط عبر البريد الإلكتروني / الرسائل النصية / الهاتف. إذا تلقيت اتصالاً من شخص يدعي أنه من فوري عبر أي قناة أخرى، فمن المحتمل أن يكون ذلك عملٍ احتيالي.
لن نطلب منك تفاصيل حسابك أو كلمات المرور. إذا تلقيت اتصالاً من شخص يطلب منك تأكيد رقم حسابك أو كلمات المرور أو المعاملات، فمن المحتمل أن يكون ذلك عمل احتيالي.
تشمل العمليات الاحتيالية النموذجية أيضًا رسائل يزعمون فيها أنهم من مؤسسة تعرضت لاختراق بيانات مؤخرًا والتي قد تطلب منك تسجيل الدخول للتحقق من حسابك أو إعادة تعيين كلمة المرور الخاصة بك. تحتوي هذه الرسائل الاحتيالية غالبًا على روابط إلى مواقع وهمية تبدو حقيقية، ولكنها تخزن بياناتك الحقيقية بمجرد إدخالها.

إذاكنت تشتبه في وجود نشاط مشبوه.

إذا كنت تعتقد أنك تعرضت لعملية احتيال أو أن حسابك قد يكون في خطر، يرجى الاتصال بفريق دعم العملاء على الرقم16421 او زيارة الموقع الألكتروني www.fawry.com

كيف ستمنع حدوث ذلك مرة أخرى؟

نحن نعمل مع شركة جروب-آي بي وهي واحدة الشركات العالمية الرائدة في تطوير حلول الحماية الإلكترونية المخصصة للكشف عن الهجمات الإلكترونية وصدها، وتحديد عمليات الاحتيال عبر الإنترنت، والتحقيق في جرائم التكنولوجيا الفائقة وحماية الملكية الفكرية، للاستمرار في مراقبة نشطة لأنظمة فوري في المستقبل المنظور والتحقق من الحاجة إلى أي تدابير أمنية إضافية حسب الاقتضاء.
تواصل جروب-آي بي وفوري تحقيقهما في الحادث وسيعملان مع السلطات المعنية على تنفيذ أفضل الممارسات لمنع هجوم مماثل في المستقبل.
تواصل كل بالإضافة إلى ذلك، فإن فوري تجري محادثات نشطة مع مجموعة من الشركات الاستشارية العالمية لمراجعة سياسات المجموعة فيما يتعلق بالحوكمة وتقييم المخاطر لتقديم المشورة بشأن اعتماد أحدث الإطارات الدولية.
سلامة وأمان أصول عملائنا تبقى أولويتنا المطلقة، ونحن ملتزمون باتخاذ جميع الخطوات اللازمة لتجنب حدوث حوادث مماثلة في المستقبل.