# Cleverbridge تؤكد سرقة بيانات بطاقات الدفع المخزنة بما فيها رموز CVV



أعلنت منصة التجارة الإلكترونية Cleverbridge أن جهة خارجية نسخت بيانات بطاقات دفع مخزنة، منها رموز CVV، بعد رصد نشاط غير مصرح به في 4 نوفمبر 2026. بدأ الإشعار في 20 نوفمبر والتحقيق متواصل.

- رصدت Cleverbridge نشاطاً غير مصرح به في 4 نوفمبر 2026 واحتوته، وعادت الأنظمة للعمل في اليوم نفسه.
- شملت البيانات المنسوخة أرقام البطاقات وتواريخ الانتهاء ورموز CVV/CVC، ولم تُسرق الأسماء ولا بيانات الاتصال أو الفوترة بحسب الرسالة.
- تقول الشركة إن الحادثة ليست فدية ولم يُشفَّر أي نظام، ولم تفصح عن طريقة الدخول ولا عدد حاملي البطاقات.
- بدأ إرسال الإشعارات في 20 نوفمبر عبر Cyberscout التابعة لـ TransUnion.

- أبلغت CorvusPay الكرواتية بشكل منفصل عن خرق كشف بريداً إلكترونياً وأرقام IBAN، والتصيد هو الخطر الرئيسي.

## ما حدث

أكدت Cleverbridge، وهي منصة تتولى المشتريات والمدفوعات والاشتراكات لحساب شركات أخرى، أن جهة خارجية نسخت بيانات بطاقات دفع مخزنة على منصتها. رصدت الشركة نشاطاً غير مصرح به في 4 نوفمبر 2026 وبادرت إلى احتوائه، وأُوقفت الأنظمة المتأثرة لفترة قصيرة ثم أُعيد تشغيلها جميعاً في اليوم نفسه.

وبحسب إشعار الخرق الذي اطلع عليه موقع BleepingComputer، تشمل البيانات أرقام البطاقات وتواريخ الانتهاء ورموز الأمان CVV/CVC، بينما تؤكد الرسالة أن الأسماء وبيانات الاتصال والفوترة لم تُنسخ. وتقول الشركة إن الحادثة ليست هجوم فدية وإنه لم يُشفَّر أي نظام. ولم تذكر كيف دخل المهاجمون ولا عدد حاملي البطاقات المتأثرين ولا العملاء المعنيين من شركاتها، إن وُجدوا. ويورد موقعها عملاء مثل Red Hat وSony وSUSE وVeeam وTenable وJamf.

## الإشعار وحادثة مرتبطة

بدأ الإشعار في 20 نوفمبر، وتُرسل الرسائل عبر Cyberscout التابعة لـ TransUnion نيابة عن Cleverbridge. يُنصح المتلقون بمراجعة كشوف بطاقاتهم، والإبلاغ عن أي عملية غير مألوفة لدى جهة الإصدار، والاستفسار عن الحاجة إلى بطاقة بديلة. وتشدد الشركة على أنها لن تطلب بيانات البطاقة أو كلمات المرور أو رموز الأمان عبر البريد أو الهاتف أو الرسائل النصية.

وفي واقعة منفصلة، رصدت CorvusPay الكرواتية في 17 نوفمبر وصولًا غير مصرح به إلى جزء من النظام الخاص بخدمة CorvusPayByIBAN. سُرقت عناوين البريد وأرقام IBAN وبعض تفاصيل المعاملات، دون أرقام البطاقات أو بيانات اعتماد الدفع. وتحذر الشركة من رسائل تصيد لاحقة مقنعة تذكر مشتريات حقيقية.

## لماذا يهم ذلك

تتعلق الحادثتان بمعالجي دفع من أطراف ثالثة، حيث يقع التعرض خارج بيئة التاجر نفسه. وينبغي للمؤسسات التحقق مما إذا كانت بطاقاتها أو عملاؤها أو مورّدوها يعتمدون على مزودين من هذا النوع.

## ما يجب فعله الآن

1. تحقق مما إذا كان أي مورّد أو اشتراك أو مسار دفع للعملاء يستخدم Cleverbridge أو منصات دفع مماثلة من أطراف ثالثة.
2. اطلب كتابياً من المزودين المعنيين حالة الحادثة ونطاق البيانات وهل تشمل بطاقاتكم أو عملاءكم.
3. راجع البطاقات المؤسسية المستخدمة في اشتراكات البرمجيات، وراقب الكشوف، واستفسر من جهة الإصدار عن الاستبدال عند وصول إشعار.
4. نبّه الموظفين والعملاء إلى رسائل تصيد تذكر مشتريات حقيقية، وإلى التحقق من طلبات الدفع عبر وسائل اتصال معروفة.
5. تأكد من أن عقود الأطراف الثالثة تُلزم بالإبلاغ السريع عن الخروقات، وقيّم التزامات الإشعار بموجب

PDPL إذا شملت الحادثة بيانات شخصية.