# تقارير عن تعرّض بيانات 851 ألف حساب في جامعة هارفارد



أفاد موقع BleepingComputer بأن خرقاً في جامعة هارفارد كشف معلومات مرتبطة بـ 851 ألف حساب. لم يكن نص المقال مقروءاً في نسختنا، لذا لم نتمكن من تأكيد بقية التفاصيل.

- يشير عنوان BleepingComputer إلى أن خرقاً في جامعة هارفارد كشف معلومات تخص 851 ألف حساب.
- كان نص المصدر غير مقروء، ولذلك لا يمكن تأكيد السبب أو التاريخ أو أنواع البيانات أو الفئات المتأثرة.
- تُعد حوادث كشف الحسابات واسعة النطاق في المؤسسات التعليمية فرصة لمراجعة ضوابط الهوية وحماية البيانات.
- ينبغي للجهات في المملكة الرجوع إلى التقرير الأصلي والإشعارات الرسمية قبل استخلاص أي استنتاج.

## ما الذي ورد في التقرير

نشر موقع BleepingComputer تقريراً بعنوان «Harvard University data breach exposed info of 851,000 accounts». ويفيد العنوان بأن خرقاً في الجامعة كشف معلومات مرتبطة بعدد كبير من الحسابات.

لم يكن نص المقال مقروءاً في النسخة التي وصلتنا. ولذلك لا يمكننا تأكيد كيفية وقوع الحادثة، أو وقت اكتشافها، أو فئات المعلومات المعنية، أو الجهات المتأثرة. وقد تركنا هذه النقاط عمداً بدلًا من التخمين.

## لماذا يهم ذلك الجهات في المملكة

حتى مع محدودية التفاصيل، يذكّر الحجم المعلن بأن بيانات الحسابات لدى الجامعات والمؤسسات الكبرى قد تنكشف بأعداد كبيرة. وتحتفظ الجهات المنظمة في المملكة بأعداد مماثلة من حسابات العملاء والموظفين والطلبة، وتنطبق الأسئلة نفسها: ما الذي يُخزَّن، ومن يستطيع الوصول إليه، وما سرعة اكتشاف أي انكشاف.

وإذا تضمنت حادثة مشابهة في جهة سعودية بيانات شخصية، فستترتب التزامات بموجب **نظام حماية البيانات الشخصية (PDPL)** والضوابط القطاعية، ومنها تقييم الأثر والإبلاغ للجهات المختصة عند اللزوم.

## الخطوة المقترحة

يُنصح بالاطلاع على مقال BleepingComputer الأصلي وعلى أي بيان صادر عن هارفارد مباشرة، واعتبار هذا الخبر إشارة أولية لا سرداً كاملًا. ويمكن استثمار الوقت للتأكد من أن جرد الحسابات وضوابط الوصول وإجراءات الإبلاغ عن الحوادث لديكم محدّثة ومجرّبة.

## ما يجب فعله الآن

1. الاطلاع على تقرير BleepingComputer الأصلي وأي بيان رسمي من هارفارد قبل الاعتماد على هذا الملخص.
2. مراجعة جرد بيانات حسابات العملاء والموظفين والطلبة والتأكد من أماكن تخزينها.
3. التحقق من تفعيل المصادقة متعددة العوامل ومراقبة عمليات الدخول غير المعتادة على الحسابات التي تحوي بيانات شخصية.
4. اختبار خطة الاستجابة للحوادث وإجراءات الإبلاغ عن الخروقات وفق PDPL عبر تمرين مكتبي.