فيفا تؤكد وصول مخترقين إلى مجموعة محدودة من البيانات الشخصية وبيانات الأعمال



أكدت فيفا وصولًا غير مصرّح به إلى مجموعة محدودة من البيانات الشخصية وبيانات الأعمال. وتزعم مجموعة HBHC سرقة أكثر من 12 غيغابايت ونشرها، فيما تتعاون فيفا مع جهات إنفاذ القانون.

- أكدت فيفا أن مخترقين حصلوا على وصول غير مصرّح به إلى مجموعة محدودة من البيانات الشخصية وبيانات الأعمال.
- تزعم مجموعة HBHC (Handsome Boy Hacking Club) سرقة أكثر من 12 غيغابايت وفشلها في ابتزاز فيفا، ثم نشرت البيانات في منتدى إجرامي.
- تدّعي المجموعة وصولها إلى بيئة Microsoft لدى فيفا، وتشمل البيانات المزعومة وثائق هوية وهجرة ومستندات مالية وقانونية.
- تقول فيفا إنها تعمل مع الجهات المختصة ومنها جهات إنفاذ القانون، ولم تجب عن أسئلة بشأن طبيعة الحادث.

- يأتي الحادث بعد هجمات حديثة على جهات كروية أوروبية، منها LaLiga وأندية إسبانية.

أكدت فيفا، الهيئة الدولية المنظِّمة لكرة القدم ومقرها زيورخ، أن مخترقين اخترقوا أنظمتها وحصلوا على وصول غير مصرّح به إلى ما وصفته بمجموعة محدودة من البيانات الشخصية وبيانات الأعمال. وقال متحدث باسمها إن المنظمة تعمل مع الجهات المختصة ومنها جهات إنفاذ القانون، وأدان الحصول غير المشروع على البيانات الشخصية ونشرها. ولم تجب فيفا عن أسئلة لاحقة بشأن طبيعة الحادث.

ما الذي يُزعم

تقول مجموعة Handsome Boy Hacking Club (HBHC)، وهي مجموعة ظهرت الأسبوع الماضي ولا يُعرف عنها الكثير، إنها سرقت أكثر من 12 غيغابايت من البيانات وحاولت ابتزاز فيفا دون نجاح. ثم نشرت البيانات في منتدى إجرامي وادّعت وصولها إلى بيئة Microsoft لدى فيفا. وتشمل المحتويات المزعومة وثائق هوية وهجرة وسجلات مالية ومستندات قانونية ومعلومات حوكمة. وهذه ادعاءات المجموعة، بينما اكتفت فيفا بتأكيد وصول محدود إلى بيانات شخصية وبيانات أعمال.

السياق الأوسع

يأتي الحادث بعد هجمات أخرى على كرة القدم الأوروبية. فقد أعلنت LaLiga أن مخترقين سرقوا بيانات شخصية لمشجعين في هجوم طال خدماتها الرقمية وخدمات عدة أندية إسبانية، وأوقفت الشرطة الهولندية في مايو مشتبهاً به في اختراق أنظمة نادي أياكس، كما أعلن الاتحاد الفرنسي لكرة القدم عن هجوم في 2025.

وبالنسبة للمؤسسات السعودية، خصوصاً المتعاملة مع الهيئات الرياضية ومنظمي الفعاليات والشركاء الدوليين، تذكّر الحادثة بأهمية مراجعة التعرّض عبر الأطراف الثالثة والبيئات السحابية، والاستعداد لتقييم ادعاءات تسريب البيانات بسرعة وهدوء.

ما يجب فعله الآن

1. راجع البيانات الشخصية وبيانات الأعمال التي تشاركها مؤسستك مع الهيئات الرياضية ومنظمي الفعاليات والشركاء الدوليين، وحدّد ما قد ينكشف عبر أنظمتهم.
2. تحقق من أمن بيئة Microsoft السحابية: الصلاحيات الإدارية، والمصادقة متعددة العوامل، وسجلات الدخول والتنبيهات.
3. تابع المصادر الموثوقة لرصد ذكر مؤسستك أو موظفيك في بيانات مسرّبة، وتحقق من الادعاءات قبل التفاعل معها.
4. تأكد من أن خطة الاستجابة للحوادث تغطي محاولات الابتزاز ونشر البيانات، بما في ذلك التزامات الإشعار بموجب PDPL.
5. نبّه الموظفين، خصوصاً من تُشارَك وثائق هويتهم أو سفرهم مع شركاء، إلى احتمال رسائل التصيد الموجّهة.