الولايات المتحدة تعلن أكبر حملة على الاحتيال وتضبط نحو 17 مليار دولار من الأموال غير المشروعة



أعلنت وزارة العدل الأمريكية حملة طالت أكثر من 800 محتال مزعوم، وضبط مكتب التحقيقات الفيدرالي نحو 17 مليار دولار وتفكيك أكثر من 29 مجمعاً احتيالياً خارج البلاد.

- تقول وزارة العدل إن الحملة شملت أكثر من 400 قضية في 85 دائرة قضائية اتحادية وأكثر من 800 محتال مزعوم، مع تسليم 30 متهماً إلى الولايات المتحدة.
- في إطار عملية Blackout ضبط مكتب التحقيقات الفيدرالي نحو 17 مليار دولار، وفكك أكثر من 29 مجمعاً احتيالياً، وساعد في إعادة أكثر من 2,200 عامل من ضحايا الاتجار.
- ساعدت وزارة الخارجية في تجميد أكثر من مليار دولار من العملات المشفرة المسروقة وإزالة أكثر من 1.4 مليون موقع وحساب احتيالي.
- شملت القضايا وسيطاً باع بيانات شخصية لكبار السن إلى محتالين، وسجناء استخدموا هواتف مهرّبة في مكالمات احتيال.

- وافقت لجنة الاتصالات الفيدرالية في 19 نوفمبر على قاعدة تتيح للسجون استخدام تقنيات التشويش ضد الهواتف المهرّبة.

أعلنت وزارة العدل الأمريكية ما وصفته بأكبر حملة في تاريخها ضد عمليات الاحتيال التي تستهدف الأمريكيين. وتشمل الحملة أكثر من 400 قضية في 85 دائرة قضائية اتحادية، بين اتهامات جديدة وأحكام إدانة وعقوبات، مع تسليم 30 متهماً. وعمل العملاء الأمريكيون مع شرطة أكثر من 10 دول لمداهمة مراكز اتصال ومجمعات احتيالية خارج البلاد.

ما الذي أُعلن

في إطار عملية Blackout، ضبط مكتب التحقيقات الفيدرالي نحو 17 مليار دولار من الأموال غير المشروعة، وفكك أكثر من 29 مجمعاً احتيالياً، وساعد في إعادة أكثر من 2,200 عامل من ضحايا الاتجار. وساعدت وزارة الخارجية في تجميد أكثر من مليار دولار من العملات المشفرة المسروقة وإزالة أكثر من 1.4 مليون موقع وحساب احتيالي.

وتضمنت عدة قضايا الاتجار بالبيانات الشخصية. فقد باع وسيط في المكسيك، بحسب الاتهام، أسماء وبيانات تواصل كبار السن الأمريكيين إلى عشرات المحتالين. وفي قضية أخرى استخدم سجناء في ولاية جورجيا هواتف مهرّبة لانتحال صفة جهات قضائية وطلب مبالغ مالية، ما دفع لجنة الاتصالات الفيدرالية إلى إقرار قاعدة تتيح التشويش على الهواتف المهرّبة في السجون.

الأهمية للمؤسسات في المملكة

يشير المصدر إلى امتداد عمليات الاحتيال من جنوب شرق آسيا إلى مناطق أخرى منها الشرق الأوسط. والأساليب الواردة فيه، كانتحال صفة الجهات الرسمية واستخدام بيانات شخصية مشتراة وتحريك الأموال عبر العملات المشفرة، ليست خاصة بالولايات المتحدة. ولا يذكر المصدر أي قضايا في المملكة.

والدرس العملي للمؤسسات المنظمة أن الاحتيال يعتمد على انكشاف البيانات وضعف التحقق من العملاء، ومراجعة هذين الجانبين استجابة معقولة لهذا الخبر.

ما يجب فعله الآن

1. مراجعة إجراءات التحقق من العملاء والاتصال العكسي، ليتمكن الموظفون والعملاء من التمييز بين التواصل الحقيقي وانتحال صفة الجهات الرسمية أو المؤسسة.
2. التحقق من كيفية مشاركة بيانات العملاء الشخصية مع أطراف ثالثة ووسطاء، والتأكد من تطبيق العقود والتزامات نظام حماية البيانات الشخصية.
3. إطلاق رسائل توعوية للعملاء، وبخاصة كبار السن، حول طلبات الدفع عبر الهاتف تحت التهديد بالتوقيف أو الغرامات.
4. التأكد من أن مراقبة الاحتيال تغطي التحويلات إلى وجهات مرتبطة بالعملات المشفرة، واختبار مسارات التصعيد إلى الجهات الأمنية.
5. إطلاع فرق مكافحة الاحتيال ومركز العمليات الأمنية على الأنماط المذكورة وإدراجها في تمارين السيناريوهات.