تحذير للجمهور من الاحتيال عن طريق انتحال صفة بنك إسرائيل أو المؤسسات المصرفية

تلفت الرقابة على البنوك انتباه الجمهور إلى محاولات جهات إجراميّة للاحتيال عليهم وسحب أموال منهم من خلال انتحال شخصيّات مندوبي بنوك وشركات بطاقات ائتمان وبنك إسرائيل وشرطة إسرائيل. ويرسل أحيانًا الطرف المشبوه مستندات مزوّرة لإبراز هويته المزورة، مثل بطاقة شرطي، أو رسالة من قبل بنك إسرائيل. وتشمل محاولات الاحتيال التوجّه من قبل جهات مشبوهة لزبائن الجهاز المصرفي، من خلال قنوات اتصال متنوعة مثل المكالمات الهاتفية، وإرسال الرسائل النصية، وإرسال رسائل البريد الإلكتروني. ويتم إرسال الرسائل من عنوان يبدو وكأنه يعود للجهة التي ينتحلون هويتها مثل البنك. وخلال عملية الاحتيال، يتم استخدام عنوان أو رقم هاتف وهمي يبدو وكأنه يعود للبنك أو لبنك إسرائيل، وأحيانًا تتضمن الرسائل توجيهًا إلى موقع الكتروني مزيّف.

وبعد تواصل الطرف المشبوه مع صاحب الحساب، يطلب منه أن يرسل له أو يعطيه بيانات شخصية أو معلومات مالية تمكنه من سحب الأموال من حسابه. قد تتضمن المعلومات التي يطلبها الطرف المشبوه: التفاصيل الشخصية وتفاصيل الحساب وتفاصيل بطاقة الائتمان والرمز الذي يرسل لصاحب الحساب أو صاحب بطاقة الائتمان على الهاتف الخليوي.

وتطلب الجهات المشبوهة أحيانًا التفاصيل باستخدام التهديدات واستراتيجية التخويف والضغط، مع الادعاء بأن المعلومات المطلوبة تهدف لحماية الحساب من نشاط طرف مشبوه أو عطل مزعوم حدث على خوادم البنك أو شركة بطاقة الائتمان والذي يتطلب معالجة عاجلة تتطلب المعلومات المطلوبة. وهناك استراتيجية أخرى تستخدمها الجهات المشبوهة وهي الوعد بالحصول على المال أو الفوز باليانصيب أو الحاجة للدخول للحساب المصرفي من أجل القيام باستثمار جذاب.

ويُطلب من الجمهور زيادة يقظته والامتناع عن تقديم تفاصيل شخصية وسرية. ونود الإشارة إلى أن بنك إسرائيل والبنوك التجارية وشركات بطاقات الائتمان لا يتوجهون للمواطنين بطلب أخذ تفاصيل شخصية وسرية وتفاصيل مالية تتضمن وسائل لتحديد الهوية أرسلت للمتوجه مثل رسالة نصية تحتوي على رمز شخصي.

وإذا كان لديك أي تخوّف من وقوعك ضحية لحادثة احتيال، فننصحك بالتوجه بأسرع وقت لقسم الأمن في المؤسسة المصرفية أو مفوضيّة شكاوى الجمهور. وفي حال عدم تلقي استجابة أو أنّ الاستجابة لا ترضيك، يمكنك التوجّه للرقابة على البنوك لتقديم شكوى حول هذا الموضوع.

توصيات لحماية حساب البنك:

- **لا تدخلوا لحساب البنك من رسالة نصيّة أو رسالة بريد الكترونيّ تتلقونها.**
- **افحصوا عنوان الموقع الالكتروني الذي تدخلون اليه (تأكدوا أنّ الكتابة صحيحة)، بالذات حين تدخلون إليه بعد البحث عن العنوان عبر محرّكات البحث.**
- **أعطوا التفاصيل الشخصيّة فقط بعد إجراء مكالمة ثانية مع المؤسّسة المصرفيّة عبر رقم هاتف وجدتموه بأنفسكم في موقع البنك.**
- **لا تعطوا تفاصيل بطاقة الائتمان أو الرمز الذي يرسل إليكم عبر رسالة نصيّة أو رسالة بريد الكتروني. البنوك أو شركات الائتمان لا تطلب تفاصيل رمز سرّي بمحادثة هاتفية لم يبادر إليها الزبون.**
- **أخطأتم وتتخوّفون ما إذا كنتم قد أعطيتم تفاصيلكم لجهة مشبوهة، توجهوا على الفور للمؤسّسة المصرفيّة وأبلغوا عن ذلك.**
- **قوموا بفحص المعاملات في حسابكم بشكل دوري لاكتشاف المعاملات المشبوهة.**
- **في حال كان لديكم شك، من الأفضل عدم الرد على الرسالة أو المكالمة وعدم الضغط على أي رابط قبل التحقّق من ذلك مقابل البنك أو الشركة.**