



بيت الاستثمار
Investment House

التوعية بالاحتيال والهجمات الإلكترونية

التوعية بالاحتيال والهجمات الإلكترونية

شركة بيت الاستثمار هي شركة رائدة في إدارة الاستثمارات البديلة، وهي تشمل عدة مجالات من الأعمال، قد يحاول المجرمون، بما في ذلك المهاجمون الإلكترونيون، الاستفادة من أسم شركة بيت الاستثمار للانخراط في عمليات احتيال أو عمليات إجرامية أخرى، حيث يتم خداع الضحايا من خلال انتحال اسم أو سمعة الشركة أو موظفيها. ومن خلال هذا الانتحال، يتم إقناع الضحايا بأنهم يتعاملون مع شركة بيت الاستثمار أو موظفيها، مما يؤدي إلى تقديم معلومات شخصية حساسة أو حتى تحويل أموال إلى هؤلاء المجرمين تحت انطباع خاطئ بأن هذه الأموال يتم تقديمها إلى شركة بيت الاستثمار.

وفي الآونة الأخيرة تبين لنا ان هناك جهات احتيالية تقوم بتنفيذ عمليات احتيال فعلية عبر البريد الإلكتروني والمواقع الإلكترونية، حيث تستهدف هذه المواقع والتواصلات أفراد الجمهور والمستثمرين المحتملين (الضحايا) باستخدام هوية أعضاء الفريق التنفيذي لشركة بيت الاستثمار أو مجلس إدارتها بشكل غير قانوني، وذلك بهدف طلب استثمارات، عروض عمل مزيفة أو تعاملات أخرى، دون إذن ولغرض خبيث.

إن الرئيس التنفيذي لشركة بيت الاستثمار وأي عضو في مجلس إدارتها أو الفريق التنفيذي لم يقدموا أي عروض لشركات استثمارية، أو عروض عمل أو أي تعاملات عبر هذه القنوات، كما أن الأسماء والهوية الخاصة بهؤلاء الأفراد يتم استخدامها بشكل غير قانوني ودون موافقتهم.

تتم هذه الاحتيالات عبر العديد من الوسائل، بما في ذلك المواقع الإلكترونية، التطبيقات المحمولة، الرسائل النصية، البريد الإلكتروني، البريد العادي، المكالمات الهاتفية، وسائل التواصل الاجتماعي (بما في ذلك مقاطع الفيديو المرفوعة على وسائل التواصل الاجتماعي)، وغيرها من منصات الاتصال (مثل "واتساب"، "تيليجرام" وغيرها). وعلى الرغم من أن أساليب المجرمين تتطور باستمرار، إلا أن العديد من هذه الاحتيالات تستخدم أسلوب "التصيد الاحتيالي (Phishing)"، وهو عملية يقوم فيها المجرم الإلكتروني بمحاولة الحصول على معلوماتك الشخصية السرية (مثل اسمك، تاريخ ميلادك، عنوانك، رقم الضمان الاجتماعي أو أي وثائق رسمية أخرى، معلومات الحسابات/المالية وأسماء المستخدمين وكلمات المرور) بهدف استخدامها لأغراض غير قانونية وغير مصرح بها.

تلتزم شركة بيت الاستثمار بالحفاظ على أعلى معايير الأمن والنزاهة، وضمان حماية البيانات الشخصية وفقًا لأحكام القانون رقم 13 لسنة 2016 بشأن حماية البيانات الشخصية. وتستند سياساتنا وإجراءاتنا إلى منع الوصول غير المصرح به، وتسريب البيانات، والأنشطة الاحتيالية.

نحرص على عدم جمع أو تخزين أو معالجة البيانات الشخصية دون وجود أساس قانوني واضح أو الحصول على موافقة الفرد المعني. وفي حال حدوث اختراق أمني أو وصول غير مصرح به إلى المعلومات الشخصية، سيتم إخطار الأفراد المتضررين والجهات المختصة على الفور.

تتم معالجة تقارير الاحتيال بسرية تامة وتُحتفظ بها حصريًا لأغراض التحقيق. بالإضافة إلى ذلك، تضمن شركة بيت الاستثمار أيضًا عدم مشاركة أو نقل البيانات الشخصية خارج دولة قطر إلا عند الضرورة وبما يتوافق مع الأنظمة واللوائح المعمول بها.

أمثلة على الاحتيالات الشائعة:

1. التصيد الاحتيالي/الاحتيال الصوتي: يتضمن هذا إرسال مجرم بريداً إلكترونياً أو رسالة نصية أو أي نوع آخر من الاتصالات الإلكترونية (مثل التطبيقات المحمولة، منصات التواصل الاجتماعي أو غيرها من وسائل الاتصال مثل "واتساب"، "تيليجرام" وغيرها)، والتي تظهر وكأنها صادرة من مصدر موثوق، وتطلب منك النقر على رابط، تنزيل مرفق أو تقديم معلومات شخصية. يشمل أسلوب مشابه يُسمى "الاحتيال الصوتي (Vishing)" حيث يتصل المجرم بك ويزعم أنه يمثل شركة (بيت الاستثمار) مثلاً، ويحذرك من وجود مشكلة متعلقة بك أو بمعلوماتك قد تؤدي إلى خسارة مالية أو ضرر، ويخبرك أنه يمكنه حل المشكلة إذا قدمت له معلوماتك الشخصية.

2. احتيالات التوظيف: قد يستهدف المجرمون الباحثين عن وظائف من خلال انتحال صفة تمثيل إحدى المنظمات وتقديم عروض توظيف عبر مواقع أو حسابات غير مصرح بها على وسائل التواصل الاجتماعي أو من خلال رسائل بريد إلكتروني غير موثوقة. يرجى ملاحظة أن جميع الوظائف المتاحة في شركة بيت الاستثمار يمكن العثور عليها هنا.

3. احتمالات التطبيقات المحمولة: قد يسعى المجرمون لسرقة المعلومات الشخصية من خلال إنشاء تطبيقات محمولة تدعي أنها تطبيق رسمي للشركة. يرجى العلم بأن لا يوجد تطبيق محمول حالياً مقدم من شركة بيت الاستثمار.
4. احتمالات التحويل البنكي: قد يتصل بك المجرمون عبر الهاتف أو البريد الإلكتروني (أو أحياناً عبر وسائل أخرى)، ويعرضون قصة مزعومة وعاجلة ويطلبون منك تحويل الأموال إلى أو من حسابك البنكي أو حساب طرف آخر.
5. احتمالات الاستثمار: قد يتصل بك المجرمون وهم يعرضون استثمارات مزيفة أو غير موجودة أو عوائد استثنائية على منتجات يُزعم أنها تحت إدارة شركة بيت الإستثمار، أو قد يروجون لهذه الاستثمارات عبر موقع ويب أو تطبيق محمول أو قناة تواصل اجتماعي، بهدف إقناعك بتحويل الأموال إليهم بشكل غير قانوني.

كيفية الإبلاغ عن عمليات الاحتيال

ندعوكم إلى التواصل فوراً مع fraud-detection@inveshouse.com في حال حدوث أي من الحالات التالية:

1. إذا كنت قد تلقيت أي مراسلات غير مؤثوق بها أو نصائح استثمارية أو تم الاتصال بك بخصوص عملية احتيال (سواء عبر الهاتف أو البريد الإلكتروني أو البريد العادي) من مصادر تنتحل صفة أعضاء مجلس إدارة شركة بيت الاستثمار أو أي من أعضاء الفريق التنفيذي.
2. إذا تلقيت إشعاراً من أي شخص خارج شركة بيت الاستثمار يفيد بأنهم قد تم الاتصال بهم من قبل أي مصادر تنتحل صفة أعضاء مجلس إدارة شركة بيت الاستثمار أو أي من أعضاء الفريق التنفيذي أو الموظفين.
3. إذا تلقيت أي تواصل يشير إلى أسماء أعضاء مجلس إدارة شركة بيت الاستثمار وتشعر بأن تلك الرسائل مشبوهة أو لست متأكداً من كيفية الرد عليها.
4. إذا كانت لديك أي شكوك بشأن مصداقية أي موقع إلكتروني يدعي أنه تابع لشركة بيت الاستثمار أو يشير إلى أسماء وهويات أعضاء مجلس إدارة الشركة أو أي من أعضاء الفريق التنفيذي دون إذن.

5. إذا كانت لديك أي أسئلة حول ما ورد أعلاه أو إذا كنت تشك في أن موقعًا إلكترونيًا أو تطبيقًا محمولًا أو بريدًا إلكترونيًا أو أي تواصل آخر (بما في ذلك عبر وسائل التواصل الاجتماعي) يدعي أنه صادر عن شركة بيت الاستثمار أو يرتبط بها قد يكون احتياليًا، يرجى الاتصال بنا عبر البريد الإلكتروني fraud-detection@inveshouse.com

أحي نفسك :

نوصي بعدم الدخول في معادنة مع المحتالين أو الكشف عن أي معلومات شخصية أو تعريفية، ولكن يجب عليك محاولة تسجيل الاسم المفترض للشخص والمنظمة وأي معلومات أخرى يقدمها (مثل رقم الهاتف أو العنوان) ثم إرسال جميع هذه المعلومات إلى fraud-detection@inveshouse.com

ولاستثمار الأموال بالمحافظ والصناديق الإستثمارية التي تديرها أو تمثل الشركة وكيلا عليها يجب عليك التالي :
مقابلة المسؤولين أو الفريق القائم على خدمة العملاء بداخل الشركة حيث ان الشركة لا تقدم منتجاتها وخدماتها الإستثمارية عبر الإنترنت او عن بعد او الحصول على مشورة قانونية ومالية واستشارية مستقلة قبل تسليم أي أموال أو الدخول في أي اتفاقيات متعلقة بهذه الدعوات.

نوصي بعدم الرد أو فتح أي مرفقات أو روابط مرتبطة برسائل بريد إلكتروني مشبوهة.