خدعة الرسوم المدفوعة مقدما

ما هي خدعة الرسوم المدفوعة مقدما؟

خدعةالرسوم المدفوعة مقدماالمعروفة أيضاً باسم حيلة الرسوم المقدمة هي عملية تحايل يستخدمها المحتالون لاختلاس أموال من الضحايا عن طريق تحصيل رسوم معاملة معينة مقابل فرصة للمشاركة في صفقة مالية خاصة أو وعد بمنح حصة في صندوق ميراث. وقد توجد أشكال أخرى من هذه عمليات الغش لكن الأسلوب الشائع أنهم يطلبون من الضحية دفعة مقدمة من الرسوم مقابلوعد بصفقة "خيالية".

ما هي طريقة تنفيذ هذا التحايل؟

يتصل المحتال بالضحايا مدعياً أنه موظف أو مسؤول تنفيذي في أحد البنوك أو محامي ذو صلةبصندوق ميراث حيث يزعم بأن العميل قد توفى وليس له أقارب على قيد الحياة، ويتم هذا الاتصال من خلال البريد الإلكتروني، أو سكايب، أو لينكد إن، أو واتس آب أو أي قناة أخرى من قنوات التواصل الاجتماعي. وتحدث معظم عمليات الاحتيال هذه في منصات التواصل الاجتماعي المختلفة من خلال البريد الإلكتروني أو حلقات/غرف المحادثة، حيث يزعم المحتال أنه مسؤول مصرفي كبير ويفعل ذلك من خلال إنشاء صفحة على مواقع التواصل الاجتماعي تماثل صفحة مسؤول مصرفي حقيقي باستخدام الصور المتاحة على شبكة الانترنت وينشئ عنوان بريد إلكتروني واسم مستخدم مماثل ليخدع الضحايا.

يدعي المحتال بأن اسم عائلة المتوفي يتطابق مع اسم الضحية ويعرض حصة نسبتها 50% من الإرث. وإذا وافقت الضحية، يقدم المحتال وثائق مالية مزيفة يدعي أنها صادرة من البنك وتتضمن في معظم الحالات محتال آخر يدعي أنه المحامي أو المسؤول القانوني الذي سيساعد في إتمام المعاملة.

ولكي يكسب المحتالون الثقة ويتجنبون الإبلاغ عنهم، يطلبون من ضحاياهم المستهدفون كذباً بأنه يجب عليهم أن يحافظوا على سرية المحادثة مدعين أنها قد تنبه السلطات الأمر الذي قد يؤدي إلى إلغاء "العرض". كما يسعون للحصول على تفاصيل الضحايا المستهدفين بما في ذلك بيانات الحسابات المصرفية ووثائق الإثبات الشخصية، التي قد يتم استخدامها لارتكاب جرائم سرقة الهوية.

في نهاية المطاف، يطلب المحتالون من الضحية تسديد "دفعة مقدمة" مقابل الضرائبوالرسوم القانونية ورسوم البنك ورسوم التوثيق وما إلى ذلك، وبالتالي يتمكنون من إختلاس أموال من الضحية.

ما الذي يمكن عمله لتجنب الوقوع ضحية لحيل الرسوم المدفوعة مقدما؟

من المهم التذكير أن البنوك لا ترسل مثل هذه الرسائل الإلكترونية على الإطلاق من خلال وسائل التواصل الاجتماعي مع العملاء. فيما يلي بضع نصائح للحماية من هذه الحيل:

- تكون المراسلات المصرفية أو الوثائق المالية التي يقدمها المحتالون مكتوبة بلغة رديئة وبها بعض الأخطاء الإملائية الواضحة أو مكتوبة بصيغة ركيكة نحوياً.
- غالباً ما يزعم المحتالون أن الشخص المتوفي كان ضحية حادث تم نشر أخباره في الإعلام، مثل حادث تحطم طائرة، أو تسونامي وما إلى ذلك. ولإضفاء المصداقية، قد يستخدمون هوية شخص لقي حتفه بالفعل في الحادث.
- تجنب فتح رسائل البريد الإلكتروني الواردة من مرسلين مجهولين، يتم من خلالها إضافة أشخاص مجهولين إلى المحادثات ومنصات التواصل الاجتماعي وما إلى ذلك.
- لا تعطي بياناتك المصرفية أو أي وثائق إلى المحتالين، وإذا كنت قد فعلت ذلك، أرسل تحذيراً إلى مصرفك في الحال.
- تذكر أن "الشيء الأروع من أن يكون حقيقيا" نادراً ما يكون حقيقياً.

إذا إتصل بك شخص ما باسم مؤسسة، أرسل كل التفاصيل المتاحة إلى عنوان البريد الإلكتروني المعلن على الموقع الإلكتروني الفعلي للمؤسسة نفسها. وبصفة عامة، تكون بيانات الاتصال هذه متاحة على الموقع الإلكتروني للمؤسسات تحت عنوان "اتصل بنا" و "أبلغ عن احتيال" وما شابه. وإذا وقع شخص ما ضحية لعملية احتيال فعليك:

- إنهاء كل الاتصالات المستقبلية وعدم التواصل معهم
- ابلاغ السلطات المختصة.
- إذا كنت قد دفعت أي أموال إلى المحتالين، أبلغ مصرفك بالتفاصيل بخطاب مكتوب وقدم نسخة من البلاغ المقدم إلى الشرطة.

يمكن بعدئذ إرسال رسالة استرداد أموال إلى البنك المستفيد من طرف البنك المحول وإذا كانت الأموال متوفرة في حساب المستفيد، من المحتمل استردادها.

تنويه: أصدر اتحاد مصارف الإمارات هذه الوثيقة للعلم والمعرفة وتحقيقا للصالح العام، ولا يتحمل أي مسؤولية إذا وقع أي شخص ضحية للاحتيال حتى بعد اتباع الخطوات الوقائية أعلاه.