مكالمات نظام الرد الصوتي التفاعلي... حيل قد تجردك من كافة أموالك احذرها

مع تقدم التكنولوجيا، أصبح المحتالون أيضًا أكثر تعقيدًا، فهم يبتكرون طرقًا جديدة لخداع الأشخاص، وسرقة أموالهم التي كسبوها بشق الأنفس، مما يجعل من الضروري البقاء على دراية.

فعملية الاحتيال التي تتم باستخدام نظام الرد الصوتي التفاعلي "IVR" والتي أخذت تنتشر بشكل كبير مؤخراً، قد تتسبب في أضرار أكبر مما قد يتصوره المرء.

نظام الرد الصوتي التفاعلي

ونظام الرد الصوتي التفاعلي IVR هو نظام هاتف آلي تستخدمه البنوك، ومقدمو خدمات الاتصالات، وخطوط المساعدة، لخدمة العملاء.

ويسمح للمتصلين بالتنقل بين الخدمات باستخدام الأوامر الصوتية أو عبر لوحة المفاتيح مثل الضغط على "1" للغة الإنجليزية أو "2" للاستعلام عن الرصيد وما إلى ذلك.

والآن، وجد المحتالون طريقة لاستغلال هذه التكنولوجيا لاستهداف الضحايا.

طريقة الاستهداف

يقوم المحتالون بإعداد أنظمة استجابة صوتية تفاعلية وهمية تبدو تمامًا مثل الأنظمة الحقيقية، ويخدعون الأشخاص لإدخال معلومات حساسة مثل تفاصيل الخدمات المصرفية، أو كلمات المرور لمرة واحدة، أو أرقام البطاقات.

وتبدأ عملية الاحتيال عادةً بمكالمة تتظاهر بأنها من أحد البنوك، وتقول إن هناك مشكلة في الحساب المصرفي أو معاملة عاجلة تحتاج إلى التحقق.

و إذا وقعت في الفخ وأدخلت تفاصيلك، سيتمكن المحتالون من الوصول إلى أموالك.

ومع العلم أن مكالمة الاحتيال تأتي من رقم يبدو شرعيًا، وأحيانًا يتطابق حتى مع الرقم الرسمي للمؤسسة المالية أو الوكالة الحكومية، وتستخدم صوتاً يحاكي الصوت الآلي لأنظمة الاستجابة الصوتية التفاعلية الحقيقية، مما يجعلها تبدو موثوقة.

وفي الآونة الأخيرة، خسر الكثير من الأشخاص أموالهم بعد أن ردوا على مكالمة هاتفية آلية تحاكي نظام الرد الصوتي التفاعلي الخاص ببنكهم، حيث تم إخبارهم أن أموالًا يتم تحويلها من حسابهم، وإذا أرادوا الاعتراض على هذه المعاملة يجب أن يضغطوا على أزرار محددة في لوحة المفاتيح.

وبالطبع قام الضحية بتتبع التعليمات دون تردد، وعند انتهاء المكالمة، تلقّى الضحية رسالة تخبره بأن المبلغ قد تم خصمه من حسابه.

التعرّف على المكالمات المزيفة

إن التعرّف على مكالمات IVR المزيفة بسيط إلى حد ما. فأنظمة IVR المشروعة لا تطلب أبدًا كلمات مرور لمرة واحدة أو رموز البطاقات البنكية.

وإذا طلب النظام ذلك، فهذه عملية احتيال، أما إذا اتبعت تعليمات مكالمات IVR المزيفة للوصول إلى

نقطة، حيث يتحدث إليك محتال متنكراً في هيئة ممثل خدمة عملاء مزيف، فتذكر دائماً أن المحتالين يستعجلونك للتصرف على الفور على عكس ممثلي خدمة العملاء الحقيقيين.

وفي حالة الشك، أغلق الهاتف، واتصل بالرقم الرسمي للبنك أو للخدمة التي تواصلوا معك عبرها.

وهنا لا بد من الإشارة إلى أنه:"لا يجب إدخال بيانات حساسة أبداً، بينما يجب تمكين تنبيهات الرسائل القصيرة والبريد الإلكتروني للتحقق من المعاملات".

وإذا انقطعت المكالمة فجأة بعد إدخال التفاصيل، فاتصل بالبنك أو بالخدمة المعنية على الفور لحظر بطاقتك أو تجميد المعاملات.