

مكالمات هاتفية خطيرة قد تعرض بياناتك للسرقة.. احذر هذه الحيل



هل تلقيت يوماً مكالمة هاتفية دولية وتساءلت عن هوية المتحدث؟ عليك أن تحترس، لأن هذه المكالمات قد تخترق هاتفك وتسرق بياناتك، فإذا تلقيت مكالمات من رقم يبدأ بثلاثة أرقام دولية محددة، فقد تكون عملية احتيال إلكتروني. أو حتى إذا تلقيت مكالمات من رقم محلي غير محفوظ في جهات اتصالك، يقدم لك عروضاً مغرية أو يطلب منك بيانات، فاحذر لأنه ربما يكون فخاً للاحتيال عليك وهو ما حذر منه خبراء الأمن السيبراني.

كيف تعمل المكالمات الاحتيالية على سرقة بياناتك؟

تلقيت مكالمات هاتفية من رقم غير محفوظ وكنت قلقاً من أن يكون ذلك عملية احتيال، دليلك في الأرقام الثلاثة الأولى،

حيث إن القراصنة يستخدمون بشكل غير متناسب رموز المناطق من أربع ولايات أمريكية وأكثر المناطق شيوعاً للمحتالين العام الماضي كانت تبدأ بأكواد 720(كولورادو)، و272 (بنسلفانيا) و959 (كونيتيكت) و346 (تكساس). يستخدم المحتال برامج الاتصال التلقائية للاتصال بأرقام الهواتف بشكل عشوائي، بعد أول رنة يقطع المحتالون الاتصال آملين أن يرى الضحايا المحتملون الرقم المتصل في سجل المكالمات الفائتة وأن يكون لديهم الفضول الكافي لإعادة الاتصال.

فور اتصال الضحية بالرقم المبيّن سيكون متصلاً بخط ساخن دولي باهظ الثمن. أحياناً يتم الرد على المكالمات برسالة مسجلة تطالب الضحايا بانتظار رد الموظف، الأمر الذي يدفع الضحايا إلى الاستمرار في المكالمات لمدة أطول. يتبع المحتالون طرقاً أخرى ومنها الاتصال من رقم دولي ليتحدث مع المتلقي عن عدة أمور مغرية مثل فوزه بجائزه ويرسل عبر المكالمات روابط تستطيع اختراق الهاتف والحصول على بياناته. قد ينتحل المتصل شخصية مؤسسات موثوقة، مثل البنوك أو الوكالات الحكومية، لكيسب ثقتك، لكن قبل الكشف عن أي معلومات، من الضروري التأكد من هوية المتصل

طرق الحماية من المكالمات المشبوهة وحماية خصوصيتك .

كيفية تجنب عمليات الاحتيال عبر الهاتف؟ بسيطة ولكن تتطلب ألا تنخدع بالمغريات حتى لا تقع في الفخ وهناك بعض النصائح التي يمكنك اتباعها.

1- كن حذراً:

لا تثق في أي اتصالات غير مرغوب فيها تطلب معلومات شخصية أو مالية.

ابق دائماً متشككاً، بغض النظر عن مدى إحساسك بمعرفة هوية المتصل.

لا تفتح أي روابط أو مرفقات إذا لم تكن متأكداً منها.

تابع الأخبار الخاصة بأحدث عمليات الاحتيال ووسائله.

2- حافظ على أمان معلوماتك:

لا تشارك كلمة السر أو رقم التعريف الشخصي أو بياناتك المصرفية أو المعلومات الشخصية مع أي شخص.

قم بتغيير كلمات السر لديك كل بضعة أشهر.

3- احرص على زيادة الحماية الخاصة بك:

على الرغم من أنه لا يمكنك دائماً تجنب تلقي المكالمات ورسائل البريد الإلكتروني، إلا أنه يمكنك إبقاء هاتفك محدثاً عن طريق تثبيت برامج الحماية ومكافحة الفيروسات. حافظ على تحديث المتصفح والبرامج لديك.

4- أبلغ الشرطة:

إذا كنت تشك أنك تتعرض للاحتيال، فأبلغ عنه على الفور.

5- حذر وتجاهل

إذا تلقيت مكالمات احتيالية، قم بحظر الرقم وتجاهل أي محاولات أخرى للاتصال، يمنع الحظر المتصل من الوصول إليك

مرة أخرى، مما يقلل من مخاطر حدوث المزيد من عمليات الاحتيال

أشهر أساليب الاحتيال عبر الهاتف وكيف تتجنبها .

يرسل المحتالون رسالة نصية قصيرة مزيفة يتظاهرون بأنهم من شركة شهيرة ويطلبون منك الرد ببياناتك الشخصية أو تفاصيل حسابك حتى يتمكنوا من سرقة الأموال منك. تشجعك هذه الرسائل على اتخاذ إجراء عاجل من خلال النقر على رابط أو الاتصال تليفونياً. ستكون من أرقام غير معروفة وتبدو أصلية. كما يتصل بك المحتالون الذين يدعون أنهم من شركة أو هيئة تعرفها وتثق بها، مثل البنك أو مزود الهاتف لديك وقد تجدهم يعرفون بعض التفاصيل الشخصية الخاصة عنك، التي ربما حصلوا عليها من صفحاتك على مواقع التواصل الاجتماعي. ثم يطلبون منك بعد ذلك مشاركة بعض بياناتك الشخصية أو المالية، حيث يتم اختراق حسابك بعدها.

ماذا تفعل إذا تلقيت مكالمة مشبوهة تطلب معلوماتك الشخصية؟ .

إذا واجهت مكالمة احتيال عبر الهاتف، الأمر بسيط فقط أغلق الخط فوراً ويمكن للمحتال تشغيل نغمة اتصال مزيفة وإبقاء الخط مفتوحاً بحيث تظل تتحدث معه حتى بعد طلب رقم آخر، كما أنه يمكن استخدام تقنيات الذكاء الاصطناعي في التواصل مع الضحايا. إذا تلقيت مكالمة أو رسالة من رقم دولي غير معروف على «واتساب»، تخبرك بعرض وظيفي أو أنك فزت بجائزة، فتابع بحذر، حيث يستخدم المحتالون أرقاماً غير مألوفة لإخفاء هويتهم. احترس من المتصلين الذين يستخدمون أساليب للضغط عليك لاتخاذ إجراء فوري، قد يزعمون أنك فزت بجائزة أو أن حسابك في خطر، ولكن من المهم أن تظل هادئاً وتتحقق من جهة رسمية. احذر من المتصلين الذين يرسلون لك روابط أثناء مكالمة على «واتساب»، قد تؤدي هذه الروابط إلى مواقع ويب متخصصة في الاحتيال أو تحميل برامج ضارة وتذكر لا تفتح أي رابط