صعب الخداع - باختصار

قد يكون من الصعب اكتشاف المحتالين المهرة الذين يحاولون خداعك. فيما يلي ثلاث نصائح لتقليل خطر حدوث ذلك.

1. **قم بإنهاء المكالمة إذا شعرت بعدم الراحة أو التوتر أو وجود شيء غريب.**
2. **لا تقوم بتسجيل الدخول بواسطة جهاز الأمان säkerhetsdosa أو المعرف الإلكتروني (مثل BankID) بناءً على طلب شخص آخر.**
   لا تعطِ كلمة المرور أو أية رموز لأي شخص.
3. **أن البنك لا يتصلّ بك ليطلب منك تسجيل الدخول أو إعطاءه بياناتك الشخصية.**

← **هل وقعت ضحية للاحتيال؟** أتصل بمصرفك فوراً!
← **قُم دائماً بتقديم بلاغ للشرطة** عن محاولات الاحتيال. اتصل بالشرطة على رقم 114 14

لا تتردد في كتابة رقم هواتف مصرفك وأحد أقاربك المقربين:

يتعرض المزيد من الأشخاص للاحتيال وهناك حاجة كبيرة لنشر المعلومات عن هذا الموضوع على نطاق واسع في المجتمع.

تقف المصارف السويدية وجمعية البنوك السويدية وراء مبادرة صعب الخداع Svårlurad! وتهدف المبادرة إلى إعطاء نصائح ملموسة ومعلومات عن كيفية حماية نفسك وأقاربك المقربين من التعرّض للاحتيال!

لا تترددّ في الاتصال بمصرفك للاستفسار عن الأمان.
اقرأ المزيد من المعلومات في svårlurad.se.

SVÅR-
LURAD!
ETT INITIATIV AV
SVERIGES BANKER

هكذا يحاول المحتالون خداعك

تزداد محاولات الاحتيالوتتغير الأساليب طوال الوقت. وكلما زادت معرفتك بكيفية حدوث ذلك أصبح من الأسهل تجنب التعرض للخداع. لقد أصبح من الشائع في السنوات الأخيرة أن يتظاهر المحتالون بأنهم يتصلون من البنك الذي تتعامل معه أو الشرطة أو الشركة أو السلطة أو يزعمون أنهم من الأقارب. هذا ويمكن للمحتالين التلاعب بأرقام الهواتف بحيث يبدو على سبيل المثال أن البنك هو الذي يتصل.

ويمكن أن يحاول المحتالون الضغط عليك مثلاً من خلال الادعاء بأنك تتعرّض إلى ظرفٍ يستوجب التعامل معه ومعالجته بشكل فوري. وغالباً ما يتظاهر المحتالون بأن الأمر ملّح وعاجل للغاية.

في الخطوة التالية يستطيع الشخص المحتال أن يعرض عليك معالجة وحلّ المشكلة المزيفة وتصحيح الوضع. يمكن أن يطلب المحتال منك إعطاءه رموز الإجابة في جهاز الأمان säkerhetsdosan، أو استخدام المعرف الإلكتروني (مثل BankID) أو التوقيع على دفع مبلغ بواسطة خدمة الدفع سويش Swish.

كن يقظاً وعى أهبة الاستعداد في حالات الاتصالات العفوية! لأن محاولات الاحتيال لا تحدث فقط عن طريق الهاتف. إذ يمكن للأشخاص المحتالين خداعك بواسطة خدمة الرسائل القصيرة sms أو وسائل التواصل الاجتماعي أو البريد الإلكتروني. كما يمكن أن يتّم ذلك بواسطة الطَرق على باب بيتك أو شقتك. فكر دائمًا فيما إذا كان ما يطلبه الشخص منك معقولاً - لا تشارك المعلومات الشخصية أو كلمات المرور والرموز أبدًا. لا تقم بتسجيل الدخول إذا شعرت بأقل قدرٍ من عدم اليقين.

يمكن للمحتالين أن يدعوّا:

- بأنهم سيوقفون عملية احتيال تجري في حسابك أو بطاقتك البنكية
- بأنهم سيقدمون لك مساعدة في **استرداد الفائض الضريبي skatteåterbäringen**
- بأنهم سيساعدوك في **خدمات لها علاقة بكورونا، مثل التلقيح**
- أن باستطاعتهم **أن يُعيدوا لك نقوداً تعرضت أنت فيها للاحتيال**
- أنك **ربحت نقوداً**
- أن أحد الأقارب تعرّض لظروف حرجة و **يحتاج إلى مساعدتك**
- أن **جهاز الحاسوب (الكومبيوتر) الخاص بك تعرّض لفيروس أو أية مشاكل أخرى يقولون بأنهم قادرين على مساعدتك فيها**
- بأنك ستقوم بتنزيل **برمجيات كومبيوتر لمنع هجوم فيروسي تتعرض له الآن**

هكذا تصبح من الأشخاص الذين يصعب خداعهم

من السهل أن تكون من الأشخاص الذين يصعب خداعهم - ويمكن للجميع أن يصبحوا كذلك. يمكنك دائماً إنهاء المكالمة الهاتفية التي تشعر بأنها تحتوي على بعض الغرابة. أطلب منهم أن يتصلوا فيما بعد وأقطع المكالمة. ثم اتصل بالمصرف الذي تتعامل معه أو بأحد أقاربك وأخبرهم بما حدث - اطلب مساعدة ودعم من شخص تثق به. فيما يلي بعض العلامات التحذيرية الشائعة ومعلومات مهمة:

← **فكّر في** أن المحتال يمكن أن يدعي بأنه يتصل من المصرف (البنك) أو من الشرطة أو من شركة أو مؤسسة أو سلطة رسمية أو يدعّي بأنه أحد أقاربك المقربين.

← **هل تنتظر مكالمة من المصرف أو من هذه الشركة؟** أذا كان الجواب لا، فينبغي أن تأخذ جانب الحذر فيما يتعلق بالمعلومات التي تعطيها. أطلب إعادة الاتصال بك إذا لم تكن متأكداً من الشخص الذي يتصّل بك.

← **قم بإنهاء المكالمة إذا شعرت بأن المكالمة غير مريحة أو تسبب لك التوتر أو وجود شيء غريب.**

← **لا تقم أبداً بتسجيل الدخول بناء على طلبٍ من أي شخص آخر. وعند استخدامك المعرف الإلكتروني** (مثلاً BankID) اقرأ بعناية الخدمة التي تقوم بالتعريف بهويتك لها وما الذي توقع عليه.

← **عند استخدامك جهاز الأمان säkerhetsdosan** عليك أن تفكّر بحماية رقم التّعريف الشخصي Pinkod وأن لا تُعطي رموز الإجابة من جهاز الأمان لأي شخص.

تذكّر! إنّ المصرف (البنك) لا يتصل بك ويطلب منك تسجيل الدخول أو إعطاءهم بيانات شخصية.

يمكنك القيام بهذا بصفتك أحد الأقارب المقربين

كأحد الأقارب المقربين أنت تلعب دورًا مهمًا في نشر المعلومات والمعرفة. تحدّث إلى أقاربك المقربين عن مخاطر التعرض للاحتيال من قبل المحتالين وكيف يمكنهم تجنب ذلك على أفضل وجه.

لا تتردد في مشاركة تجربتك مع أولئك الذين ليس لديهم نفس المعرفة التي لديك. أنت تشكّل شبكة حماية مهمة لمن يشعر بالتردد وعدم الأمان وليس لديه خبرة كافية. معاً نخلقُ حياة يومية أكثر أماناً للجميع.

اقرأ المزيد في موقع الويب www.svårlurad.se