SVÅR-LURAD!

ETT INITIATIV AV SVERIGES BANKER

Innehållsförteckning

Svårlurad – i korthet

Det kan vara svårt att genomskåda skickliga bedragare som försöker lura dig. Här är tre tips för att minska risken att det sker.

1. **Lägg på om samtalet känns obekvämt, stressande eller konstigt.**
2. **Logga inte in med din säkerhetsdosa eller e-legitimation (exempelvis BankID) på någon annans uppmaning.**

   Lämna inte ut lösenord eller koder till någon.
3. **Banken ringer inte för att be dig logga in eller lämna ut personliga uppgifter.**

→ **Har du blivit utsatt för bedrägeri?** Kontakta din bank omgående!

→ **Polisanmäl alltid** ett bedrägeriförsök. Ring Polisen på 11414.

Skriv gärna ner numren till din bank och en närstående:

_____

_____

_____

Allt fler människor utsätts för bedrägerier och det finns ett stort behov av att informera om detta brett i samhället.

Bakom initiativet Svårlurad! står Sveriges banker och Svenska Bankföreningen. Initiativet syftar till att ge konkreta tips och information om hur man kan skydda sig själv och sina närstående mot bedrägerier.

Kontakta gärna din bank med frågor om säkerhet.
Läs mer på svårlurad.se

SVÅR-LURAD!
ETT INITIATIV AV SVERIGES BANKER

Så kan bedragare försöka lura dig

Bedrägeriförsöken ökar och metoderna ändras hela tiden. Ju mer du känner till om hur det kan gå till desto lättare är det att undvika att bli lurad. De senaste åren har det blivit vanligare att bedragaren utger sig för att ringa från din bank, polisen, företag, en myndighet eller påstår sig vara din närstående. Bedragarna kan manipulera telefonnummer så att det ser ut som att det exempelvis är banken som ringer.

Bedragarna kan försöka stressa dig, till exempel genom att påstå att du är utsatt för en situation som måste åtgärdas omedelbart. Ofta påstår bedragarna att det är mycket bråttom.

I nästa steg kan bedragaren erbjuda hjälp att lösa det påhittade problemet och rätta till situationen. Bedragaren kan be dig att lämna ut svarskoder från säkerhetsdosan, använda din e-legitimation (exempelvis BankID) eller skriva under en Swishbetalning.

Var på din vakt vid spontana kontakter! Bedrägeriförsök sker inte bara över telefon. Bedragare kan även försöka lura dig genom sms, i sociala medier eller mejl. Det kan också ske genom att de knackar på hemma. Tänk alltid igenom rimligheten i det personen ber dig om att göra – dela aldrig personlig information eller koder. Logga inte in om du känner dig det minsta osäker.

Bedragarna kan påstå att:

- De ska **stoppa ett pågående bedrägeri** på ditt konto eller kort
- De kan hjälpa till med **skatteåterbäringen**
- De ska hjälpa dig med **coronarelaterade tjänster,** som vaccinering
- De kan **ge tillbaka pengar** som du blivit lurad på
- Du har **vunnit pengar**
- En **närstående** har råkat illa ut och **behöver din hjälp**
- Din **dator har fått virus** eller andra problem som de säger sig kunna hjälpa dig med
- Du ska ladda ner en **programvara för att förhindra en pågående virusattack**

Så blir du svårlurad

Det är lätt att bli svårlurad – och alla kan bli det. Du kan alltid avbryta ett telefonsamtal som känns konstigt. Be att få återkomma och lägg på. Ring sedan din bank eller en närstående och berätta vad som hänt – sök hjälp och stöd hos någon du litar på. Här beskrivs några vanliga varningstecken och viktig information:

→ **Tänk på** att bedragarna kan säga sig ringa från banken, polisen, ett företag, en myndighet eller påstå sig vara en närstående.

→ **Väntar du samtal från banken eller det här företaget?** Om svaret är nej så bör du vara försiktig med vilken information du lämnar ut. Be att få återkomma om du är osäker på vem som ringer.

→ **Lägg på om samtalet känns obekvämt, stressande eller på något vis konstigt.**

→ **Logga aldrig in på någon annans uppmaning. När du använder e-legitimation** (exempelvis BankID) läs noggrant vilken tjänst du identifierar dig mot och vad du skriver under.

→ **När du använder säkerhetsdosan** tänk på att skydda din pinkod och att inte lämna ut svarskoder från den till någon annan.

Kom ihåg! Banken ringer inte upp dig för att be dig logga in eller lämna ut personliga uppgifter.

Detta kan du som närstående göra

Du som närstående spelar en viktig roll i att sprida information och kunskap. Prata med dina nära om risken att luras av bedragare och hur de bäst undviker det.

Dela gärna med dig av din erfarenhet till den som inte har samma kunskap som du. Du är ett viktigt skyddsnät för den som känner sig osäker och ovan. Tillsammans skapar vi en tryggare vardag för alla.

Läs mer på www.svårlurad.se

Scamaware – in brief

It can be tough to see through convincing scammers who are trying to trick you. Here are three tips to reduce the risk.

1. **Hang up if the conversation starts to feel uncomfortable, stressful or strange.**
2. **Don't use your bank security device or electronic identification (like BankID) to log in at somebody else's request.**

   Don't tell anyone your passwords or security codes.
3. **Your bank will never phone you to ask you to log in or to provide personal details.**

→ **Have you been the victim of fraud?** Contact your bank immediately!

→ **Always report** attempted fraud to the police. Ring the police on 11414.

Write the phone numbers of your bank and a family member here:

_____

_____

_____

More and more people are being targeted by fraudsters, and there is a huge need to raise awareness about this broadly among the general public.

Scamaware! is an initiative by Sweden's banks and the Swedish Bankers' Association. The purpose of this initiative is to provide useful advice and information about how we can protect ourselves and our family members from scams and fraud.

Contact your bank if you have any questions about security. Read more at svårlurad.se

SVÅR-LURAD!
ETT INITIATIV AV SVERIGES BANKER

How scammers may try to trick you

Attempted fraud is on the rise and scammers are constantly changing their methods. The more you know how the scams work, the easier it will be to protect yourself from falling victim to them. In recent years, it has become more common for scammers to ring up and claim to be your bank, the police, a company, a government agency or even a member of your family. Fraudsters can manipulate phone numbers to make it look like it really is your bank that's calling.

They may try to make you feel stressed, for example by saying that you have a problem that needs to be resolved immediately. Fraudsters will often emphasise that time is short.

Next, the scammer tends to offer help solving their invented problem and getting the situation sorted out. They may ask you to share a security code from your bank security device, to use your electronic identification (like BankID) or to approve a Swish payment.

Be suspicious when somebody contacts you out of the blue! And remember, scams don't only happen over the phone. Fraudsters may also try to trick you via text messages, on social media or by using email. They may even knock at your door. Always think whether or not what you are being asked to do is reasonable – and never share personal information or security codes. Don't log in if you are even the slightest bit suspicious.

Fraudsters may say:

- They are **going to help you stop an existing scam** on your account or card
- They can help you with **your tax rebate**
- They can help you with **coronavirus services**, like vaccinations
- They can help you **recover money** that you have been scammed out of
- You have **won some money**
- A **family member** has got into a tricky situation **and needs your help**
- Your **computer has a virus** or some other problem that they say they can help you with
- You need to download **software to protect your computer from an on-going virus attack**

Be scamaware

It's simple to be scamaware – and everyone can learn how. You can always end a phone call that feels strange. Tell the caller you'll get back to them and hang up. Then ring your bank or a family member and explain what happened – seek help and support from somebody you trust. Here are some common warning signs to watch out for and some important information:

→ **Remember** that fraudsters may claim to be your bank, the police, a company, a government authority or they may even claim to be a family member.

→ **Are you expecting a call from your bank or the company the caller claims to represent?** If not, then be careful about what information you give out. Tell the caller you'll get back to them if you are unsure about the person calling.

→ **Hang up if the call starts to feel uncomfortable, stressful or strange in any way.**

→ **Never log in anywhere at somebody else's request. When using electronic identification** (like BankID), always make sure you read all the information about the service you are accessing and what you are agreeing to.

→ **When using your bank card reader,** remember to protect your PIN code and never share security codes with anybody else.

Remember! Your bank will never ring you to ask you to log in or give out personal information.

Supporting your family members

You can help play an important role in sharing information and knowledge with those close to you. Talk to your family members about the risk of being scammed and how best to prevent this from happening.

Share your own experiences with others who might not have the same knowledge as you. This is an important safety net for anybody who is feeling unsure or concerned. Together we can help keep each other safe and secure.

Read more at www.svårlurad.se

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

Nie daj się oszukać – skrócony poradnik

Jeśli trafisz na sprytnego oszusta, może Ci być trudno przejrzeć jego zamiary. Oto trzy rady, jak zmniejszyć ryzyko padnięcia ofiarą oszustwa.

1. **Rozłącz się, jeśli rozmowa jest dla Ciebie niewygodna, stresująca lub dziwna.**
2. **Nie loguj się za pomocą czytnika ani elektronicznego dokumentu tożsamości (np. BankID) na czyjąś prośbę.**
   Nie udostępniaj nikomu swojego hasła ani kodów.
3. **Bank nigdy nie dzwoni, żeby poprosić Cię o zalogowanie się lub o podanie danych osobowych.**

→ **Jesteś ofiarą oszustwa?** Skontaktuj się jak najszybciej ze swoim bankiem!

→ **Zawsze zgłaszaj na policję** próbę oszustwa. Zadzwoń na policję na numer 114 14.

Zapisz sobie numer do swojego banku i do bliskiej osoby:

_____

_____

_____

Coraz więcej ludzi pada ofiarą oszustów, dlatego trzeba koniecznie informować o tym ogół społeczeństwa.

Za inicjatywą Nie daj się oszukać! stoją szwedzkie banki oraz Szwedzkie Stowarzyszenie Bankowe (Svenska Bankföreningen). Inicjatywa ma na celu udzielanie konkretnych porad i przekazywanie informacji o tym, jak można chronić siebie oraz swoich bliskich przed oszustwami.

Skontaktuj się ze swoim bankiem w przypadku pytań o bezpieczeństwo. Więcej informacji na svårlurad.se

SVÅR-LURAD!
ETT INITIATIV AV SVERIGES BANKER

Jak oszust może próbować Cię oszukać

Prób oszustwa jest coraz więcej, a metody zmieniają się cały czas. Im więcej wiesz na ten temat, tym łatwiej będzie Ci uniknąć bycia ofiarą oszustwa. W ostatnich latach coraz bardziej powszechne stało się, że oszust dzwoni i podaje się za przedstawiciela banku, policji, firmy, urzędu lub za bliską osobę. Oszuści potrafią zmanipulować numer telefonu tak, aby wyglądało na to, że dzwoni na przykład bank.

Oszuści mogą próbować Cię zestresować, na przykład przekonując, że jesteś w sytuacji, która wymaga natychmiastowej interwencji. Oszuści często twierdzą, że sprawa jest bardzo pilna.

Następnie oszust może zaproponować pomoc w rozwiązaniu tego fikcyjnego problemu oraz naprawę sytuacji. Oszust może poprosić Cię o udostępnienie mu kodu zwrotnego z czytnika, o użycie Twojego elektronicznego dokumentu tożsamości (np. BankID) lub o potwierdzenie płatności przez aplikację Swish.

! **Zachowaj czujność** w przypadku niespodziewanych kontaktów! Próby oszustwa dzieją się nie tylko przez telefon. Oszuści mogą próbować oszukać Cię również przez sms, w mediach społecznościowych lub przez e-mail. Mogą również zapukać do drzwi Twojego domu. Zawsze zastanów się nad zasadnością tego, o co prosi Cię dana osoba – nigdy nie udostępniaj danych osobowych ani kodów. Nie loguj się, jeśli masz jakiekolwiek wątpliwości.

Oszuści mogą twierdzić, że:

- chcą **uniemożliwić oszustwo**, którego ktoś próbuje dopuścić się na twoim koncie lub karcie,
- mogą pomóc Ci ze **zwrotem podatku**,
- chcą pomóc Ci w **usługach związanych z COVID-em**, jak na przykład szczepienie,
- mogą **zwrócić Ci pieniądze,** które ktoś Ci ukradł,
- udało Ci się **wygrać pieniądze**,
- ktoś z Twoich **bliskich** popadł w tarapaty, i **potrzebuje Twojej pomocy**,
- Twój **komputer został zaatakowany przez wirus** lub masz inne problemy, które pomogą Ci rozwiązać,
- musisz zainstalować jakiś program, **aby zapobiec trwającemu atakowi wirusa**.

Jak możesz nie dać się oszukać

Nie daj się oszukać – to proste i każdemu może się udać. Zawsze możesz przerwać rozmowę telefoniczną, która wydaje Ci się dziwna. Poproś o możliwość oddzwonienia i rozłącz się. Następnie zadzwoń do swojego banku lub do bliskiej Ci osoby i opowiedz o tym, co się wydarzyło – szukaj pomocy i wsparcia u kogoś, komu ufasz. Tutaj opisujemy kilka powszechnych sygnałów ostrzegawczych oraz ważne informacje:

→ **Pamiętaj**, że oszuści mogą mówić, że dzwonią z banku, z policji, z firmy, z urzędu lub podawać się za bliską Ci osobę.

→ **Oczekujesz telefonu z banku lub z tej firmy?** Jeśli odpowiedź brzmi nie, uważaj na to, jakich informacji udzielasz. Poproś o możliwość oddzwonienia, jeśli nie masz pewności, kto do Ciebie dzwoni.

→ **Rozłącz się, jeśli rozmowa jest dla Ciebie niewygodna, stresująca lub w jakikolwiek sposób dziwna.**

→ **Nigdy nie loguj się na czyjąś prośbę. Kiedy używasz elektronicznego dokumentu tożsamości** (np. BankID), przeczytaj uważnie, jaką usługę potwierdzasz i co podpisujesz.

→ **Kiedy używasz czytnika**, pamiętaj, aby chronić swój kod pin oraz nie udostępniać nikomu kodu zwrotnego z czytnika.

! **Pamiętaj!** Bank nigdy nie dzwoni, żeby poprosić Cię o zalogowanie się lub o podanie danych osobowych.

Co możesz zrobić, aby wesprzeć bliską osobę

Będąc bliską osobą, odgrywasz ważną rolę w rozpowszechnianiu informacji i wiedzy. Rozmawiaj ze swoimi bliskimi o ryzyku padnięcia ofiarą oszustwa oraz jak tego uniknąć.

Dziel się Twoim doświadczeniem z tymi, którzy nie mają takiej samej wiedzy. Stanowisz siatkę bezpieczeństwa dla osób, które są niepewne lub nienawykłe do takich sytuacji. Razem budujemy bezpieczniejszą codzienność dla nas wszystkich.

Więcej informacji na www.svårlurad.se