

SVÅR- LURAD,

ETT INITIATIV AV
SVERIGES BANKER





Allt fler utsätts för telefonbedrägerier 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.

Läs mer på svarlurad.se

Så kan bedragare försöka lura dig

- **Bedrägeriförsöken ökar** och metoderna ändras hela tiden.
- **De senaste åren** har det blivit vanligare att bedragaren utger sig för att ringa från din bank, polisen, företag, myndighet eller påstå sig vara en närstående.
- **Bedragarna kan manipulera** telefonnummer så att det ser ut som att det är exempelvis banken som ringer.
- **Bedragarna kan försöka** stressa dig, till exempel genom att påstå att du är utsatt för en situation som måste åtgärdas omedelbart.
- **Bedragaren kan be dig** att lämna ut svars-koder från säkerhetsdosan, använda din e-legitimation (exempelvis BankID) eller skriva under en Swishbetalning.
- **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.

Några vanliga situationer

**SVÅR-
LURAD,**



Telefonbedrägerier

Någon ringer och påstår sig vilja hjälpa dig stoppa en transaktion från ditt konto. Det är brådskande och du ombeds att logga in med ditt BankID eller säkerhetsdosa för att lösa problemet. Vänta, stopp! Det är någon som försöker luras.



SMS-bedrägerier

Du får ett sms från en avsändare som verkar tillförlitlig. I meddelandet uppmanas du att göra något, som att klicka på en länk, ringa upp någon eller ta emot ett samtal. I själva verket ger du ut personlig information som används för att begå brottsliga handlingar mot dig.



Hembesök

Det ringer från vad som du tror är polisen. Enligt uppringaren sker det just nu ett stort antal stölder i ditt bostadsområde. De kan hjälpa dig säkra ditt hem – du behöver bara öppna dörren åt en kollega om några minuter. Gör inte det, någon försöker lura dig.

Bedragarna kan påstå att:

- De ska **stoppa ett pågående bedrägeri** på ditt konto eller kort
- De kan hjälpa till med **skatteåterbäringen**
- De kan hjälpa dig med **utbetalning av elstöd**
- De ska hjälpa dig med **corona-relaterade tjänster**, som vaccinering
- De kan **ta 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**
- De ska **lämna ut ett paket** till dig

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. 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 svars-koder från den till någon annan.

Svårlurad i korthet

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.

Så här kan du minska risken för sms-bedrägerier

Risken att bli utsatt för sms-bedrägerier ökar och metoderna ändras hela tiden, vilket gör det svårare att identifiera bedragares avsikter. Hur vet man om ett sms egentligen är ett försök att komma åt känslig information?

→ **Läs alltid sms noggrant** och tänk efter om innehållet är rimligt.

→ **Var uppmärksam** på avsändaren och språket i meddelandet.

→ **Klicka inte** på länkar och ring inte upp okända nummer på någon annans uppmaning

**SVÅR-
LURAD,**

Så här kan sms-bedrägerier se ut

Hej,

Vi har upptäckt oväntad aktivitet på ditt bankkonto. Kontakta oss på [076-128 93 42](tel:076-128 93 42)

Mvh Din Bank

→ Ring inte upp

Bedragaren kan försöka stressa fram ett beslut genom att göra dig orolig.

Grattis i efterskott! Du har ett paket som väntar på dig. För att bekräfta upphämningsplats klicka här: <http://straighttoyou247.com/collect/GIFT433/>

Mvh Din Bank

→ Klicka inte på länken

Bedragare kan luras genom att göra dig positivt överraskad.

Anmäl ditt bankkonto och få skatteåterbäringen utbetald redan i mars. Logga in på: www.skatteverket.net/deklaration

→ Klicka inte på länken

Bedragare kan utnyttja aktuella händelser för att luras och manipulera avsändare att se trovärdiga ut.

Läs mer på svarlurad.se

**SVÅR-
LURAD,**
ETT INITIATIV AV
SVERIGES BANKER