

FÖRSÖK INTE LURA MIG

På nätet



Tips och råd på hur du kan förebygga bedrägeri på nätet, via telefon eller e-post.

Försök inte lura mig - mötespaket i tre delar

- På stan
- I hemmet
- **På nätet**



Polismyndigheten i samarbete med

BROTTSOFFER
JOUREN
0200-21 20 19

PRO

SENIORERNA

SKPF
pensionärerna



På nätet

Att handla på nätet har många fördelar. Du får tillgång till ett större utbud av varor och tjänster och du kan få varor hemskickade. Det som är mycket viktigt att tänka på när du näthandlar är att du inte ska lämna ut eller spara dina kortuppgifter på vilken webbsida som helst. Om du blir misstänksam gällande en webbsida, kan du söka på omdömen och varningar om webbsidan.

I de flesta fall blir det säkrare för dig om den näthandel du använder har en betalningsförmedlare som till exempel Klarna, Dibs eller Paypal, som sköter kortbetalningarna.

Tänk på att annonser på hemsidor inte behöver vara äkta. Ibland skapar bedragarna falska företags- sidor på nätet eller lägger ut falska annonser och erbjudanden på andra företags äkta webbplatser för att locka dig till att lämna ifrån dig uppgifter. Här är det bra att vara kritisk. Om något verkar vara för bra för att vara sant så är det troligtvis det.

Falsk e-post eller falska sms

Nätfiske är ett sätt för gärningspersoner att samla in person- eller kortuppgifter som de sedan använder för att genomföra ett bedrägeri. Gärningspersonen skickar falsk e-post eller falska sms till en stor mängd mottagare. Syftet är att lura dig att öppna en bifogad fil eller klicka på en länk som leder till en sida där du ska lämna ifrån dig personliga uppgifter eller så är sidan smittad med skadlig programvara. Här följer några exempel på hur uppmaningarna på e-post och sms kan vara.

- **Du är utvald och har vunnit ett presentkort.** För att få presentkortet behöver du klicka på en länk och fylla i dina kortuppgifter. Något presentkort existerar i själva verket inte.
- **Dina användaruppgifter behöver uppdateras.** Din bank informerar om att du ska gå in på en hemsida och där lämna ifrån dig personlig information. Hemsidan är inte äkta även om det ser ut så. Banker begär aldrig att den här typen av information lämnas på ett sådant sätt.
- **Skatteverket ger skatteåterbäring.** Du uppmanas att klicka på en länk och därefter fylla i dina kortuppgifter för att få din återbäring per omgående. Skatteverket begär aldrig in uppgifter på det här sättet.
- **Vi har ändrat våra betalningsrutiner.** Ett välkänt företag uppger att de har ändrat sina betalningsrutiner och du uppmanas klicka på en länk för att där fylla i dina kortuppgifter. Ta först reda på om det är ett seriöst meddelande innan du går vidare.

Falska telefonsamtal

Vid bedrägeri genom falska telefonsamtal lurar bedragaren till sig inloggningsuppgifter och koder till din internetbank för att på din banksida genomföra överföringar av dina besparingar till andra konton. De som ringer utger sig oftast för att vara från banken, polisen, en mäklarfirma eller en välkänd butik. De säger ofta att det är bråttom med ärendet. De kan säga att en större transaktion på ditt konto uppdragats eller att någon handlat varor i ditt namn. Om du uppger inloggningsuppgifter och koder från din bankdosa säger de sig kunna "hjälpa dig" att avsluta transaktionen och återföra pengarna till ditt konto. Bedragaren vilseleder dig till att ta snabba beslut och vidta felaktiga åtgärder.

En annan variant är att gärningspersoner ringer och erbjuder sig att komma förbi i ditt hem och hjälpa dig att ta ut pengar. Om du släpper in dem tar de ditt bankkort och din kod och kommer inte tillbaka. Istället tömmer de ditt konto via uttagsautomaten.

Ytterligare en variant av bedrägeri för att komma över dina tillgångar är att du vilseleds till att investera i exempelvis ett företag som

- inte existerar
- saknar värde, eller har ett lägre värde än utlovat.

Kontakten tas oftast via telefon, sociala medier eller en webbsida. Bedragarna arbetar metodiskt och över lång tid, och inte sällan förmår de personer att investera vid flera tillfällen. Lita på din kritiska magkänsla och var skeptisk till försäljare som kontaktar dig på telefon, i synnerhet på kvällstid, och försöker sälja investeringar.

Falska fakturor

Att drabbas av en bluffaktura kan väcka stor oro, speciellt om du blir hotad med inkasso, betalnings- anmärkningar, Kronofogden eller stämning till tingsrätten. Följden av det blir ofta att fakturan betalas, och bedragarna lyckas i sitt uppsåt.

Om ett företag kontaktar dig via telefon i syfte att du ska ingå ett avtal krävs det att du bekräftar erbjudandet skriftligen för att avtalet ska vara giltigt. Du kan endast bli betalningsskyldig för produkter du skriftligen har bekräftat även när du fått erbjudandet via telefon.

Id-kapning

En id-kapning är när en person använder dina personuppgifter till att göra affärer. Ibland har de även skaffat sig en falsk identitetshandling med dina personuppgifter. De kan öppna konton, ta lån, köpa varor på kredit – allt i ditt namn. Fakturan kommer till dig medan varan hämtas ut av gärningspersonen på utlämningsstället.

Det finns flera varningssignaler som du kan vara uppmärksam på:

- Ett kreditupplysningsföretag informerar dig om att en kreditupplysning har gjorts på dig fast du själv inte sökt kredit eller lån.
- Du får faktura på varor du inte beställt.
- Du får meddelande om att mobilabonnemang tecknats i ditt namn.
- Du saknar post du väntat på, eller får ingen post överhuvudtaget.

Skydda dig mot bedrägeri på nätet

- Lämna aldrig ut kortuppgifter, koder eller andra känsliga uppgifter till någon. Kortuppgifter och koder är nycklar till dina pengar.
- Använd aldrig din bankdosa eller ditt bank-id på uppmaning av någon som kontaktar dig.
- Kontakta din bank och hör vilka säkerhetåtgärder de har för ditt bankkort, som t.ex. att spärra ditt kort för internetköp.
- Lagg på luren om någon ringer och du blir osäker. Det gäller oavsett om personen utger sig för att vara en nära släkting, från banken, ett företag eller en myndighet. Ring tillbaka på ett nummer som du själv tar reda på.
- Var misstänksam mot nätbutiker eller annonser som erbjuder varor och tjänster till mycket låga priser.
- Sök på nätet på varningar och omdömen om nätbutiker. På så vis kan du skaffa dig en uppfattning om företaget förekommit i bedrägliga sammanhang tidigare.
- Spara inte dina person- och kortuppgifter i appar eller på webbsidor. Det är säkrare att mata in uppgifterna varje gång du handlar.
- Klicka bara på för dig kända länkar.
- Skaffa en digital brevlåda. Då får du snabbare tillgång till din post från bland annat myndigheter.
- Anmäl dig till obehörig adressändring för din folkbokföringsadress hos Skatteverket. Tjänsten förhindrar att någon obehörig ändrar din adress.
- Skaffa adresslås via Adressändring. Med adresslåset förhindrar du att någon obehörig adress ändrar, lagrar eller eftersänder din post.

Vart ska jag vända mig om jag behöver hjälp?

Polisen

Vid pågående brott ring 112, för kontakt med polisen ring 114 14 eller besök en polisstation.

Banken

För att spärra ditt bankkort ska du snarast kontakta din bank eller den som är kortutgivare.

Brottsofferjouren

För kontakt med Brottsofferjouren ring det nationella telefonnumret 0200-21 20 19 som i sin tur kan hänvisa vidare till en brottsofferjour på din ort.

Hallå konsument!

Vänd dig till Hallå konsument! när du har frågor om köp av varor och tjänster, reklamationer och annat som du som konsument behöver hjälp med. Tjänsten samordnas av Konsumentverket. www.hallakonsument.se.

Bestrid faktura

Om du fått en bluffaktura gå in på www.bestrid.nu och följ instruktionerna för hur du bestrider en faktura eller be någon om hjälp att besöka sidan.

Egen telefonlista

Skriv upp viktiga telefonnummer, t.ex. till polisen, anhöriga, grannar, fastighetsskötaren och din bank. Förvara listan där du lätt kan hitta den.

-
-
-
-
-

Polisen 112 vid pågående brott, 114 14 för att annars komma i kontakt med polisen.