

SE UPP FÖR BEDRAGARNA!

– så tänker du säkert på nätet



Bedrägerierna på nätet ökar. Här listar vi de vanligaste fällorna och vad du kan göra för att undvika dem.

AV SANDRA HOLMES FOTO ISTOCK

KORTBEDRÄGERIER

Den vanligaste formen av bedrägeri är att någon får tag i dina betal- eller kreditkortsuppgifter och tar ut pengar, eller handlar varor och tjänster med dem. Det kan t ex ske om nätbutiker blir hackade, eller genom så kallad skimming, då man stjälar kortuppgifterna med en avläsare.

Så skyddar du dig:

När du handlat på nätet, spara inte dina kortuppgifter i webbutiken. Och stäng ditt bankkort från nätköp och utlandsköp när du inte använder det. Det kan du göra i din banks mobilapp eller på bankens hemsida. Förlorar du ditt fysiska kort - spärra det direkt!



Stäng kortet för nätköp efter att du handlat!

ID-KAPNING

Bedragaren använder ditt namn, personnummer och adress för att t ex köpa varor, ta lån, spela eller skaffa kreditkort. Knäcker någon lösenordet till din mejladress och sociala medier så kan de dessutom skicka meddelanden till dina vänner och be om pengar.

Så skyddar du dig:

Ha ditt personnummer spärrat hos kreditupplysningsföretagen, och spärra obehörig adressändring hos Skatteverket, så att varor som beställs i ditt namn inte kan levereras till en annan adress. Använd starka lösenord för att skydda dina konton.

FEJKANNONSER

Falska annonser med prylar som inte finns, eller inte motsvarar det som står i annonsen, blir allt vanligare. Du kanske t ex hittar en lägenhet att hyra eller bil att köpa. Säljaren påstår att det är bråttom, så du hinner inte titta innan du bestämmer dig, och du behöver lägga en handpenning för att säkra köpet. Och så fort du har skickat pengarna går säljaren upp i rök.

Så skyddar du dig:

Betala aldrig privatpersoner i förskott! Är det ett företag som står bakom annonsen - googla då företagets namn, läs kundomdömen samt kolla om det har en adress, organisationsnummer och verklig kundtjänst. Välj nätbutiker som använder säkra betalningsmetoder som 3D secure, där du måste verifiera köpet med BankID.

BLUFFAKTUROR

Du luras att betala för något du inte har beställt, genom bluffakturor. Det kan hända

Känn igen bedrägarna!

3 VARNINGSTECKEN

1. De påstår att det är jättebråttom! Du behöver bestämma dig nu, annars är det för sent!
2. Erbjudandet låter för bra för att vara sant.
3. De respekterar inte ditt nej, utan försöker övertala dig.

utan tidigare kontakt, eller genom att t ex telefonförsäljare försöker ingå falska avtal med dig, där de ber dig att uppge dina personuppgifter. Samtalet kan klippas ihop på ett felaktigt vis, och du får hem en bluffaktura.

Så skyddar du dig:

Betala inte fakturan! I stället ska du bestrida den via brev eller mejl, med en kopia på fakturan bifogad, och göra en polisanmälan, annars riskerar du inkassokrav. Svara aldrig när ökända nummer ringer. Råkar du göra det, lägg på direkt om det verkar suspekt.

KÄRLEKS-BLUFFAREN

Romansbedragare, eller sol- och-vårare, brukar särskilt rikta in sig på medelålders kvinnor. De tar kontakt genom dejtingsajt eller Facebook, och blir snabbt kärvännliga. Det händer att de inleder relationer med kvinnorna i verkliga livet, men det vanligaste är att man aldrig träffas. Ofta utger de sig för att vara änkemän, med ett förtroendeingivande yrke som militär eller läkare, och befinner sig utomlands.



postnord

Ditt paket väntar på dig
Ditt paket med spåringsnummer #SE-SAM32013. Paketet har försökt levereras till dig.

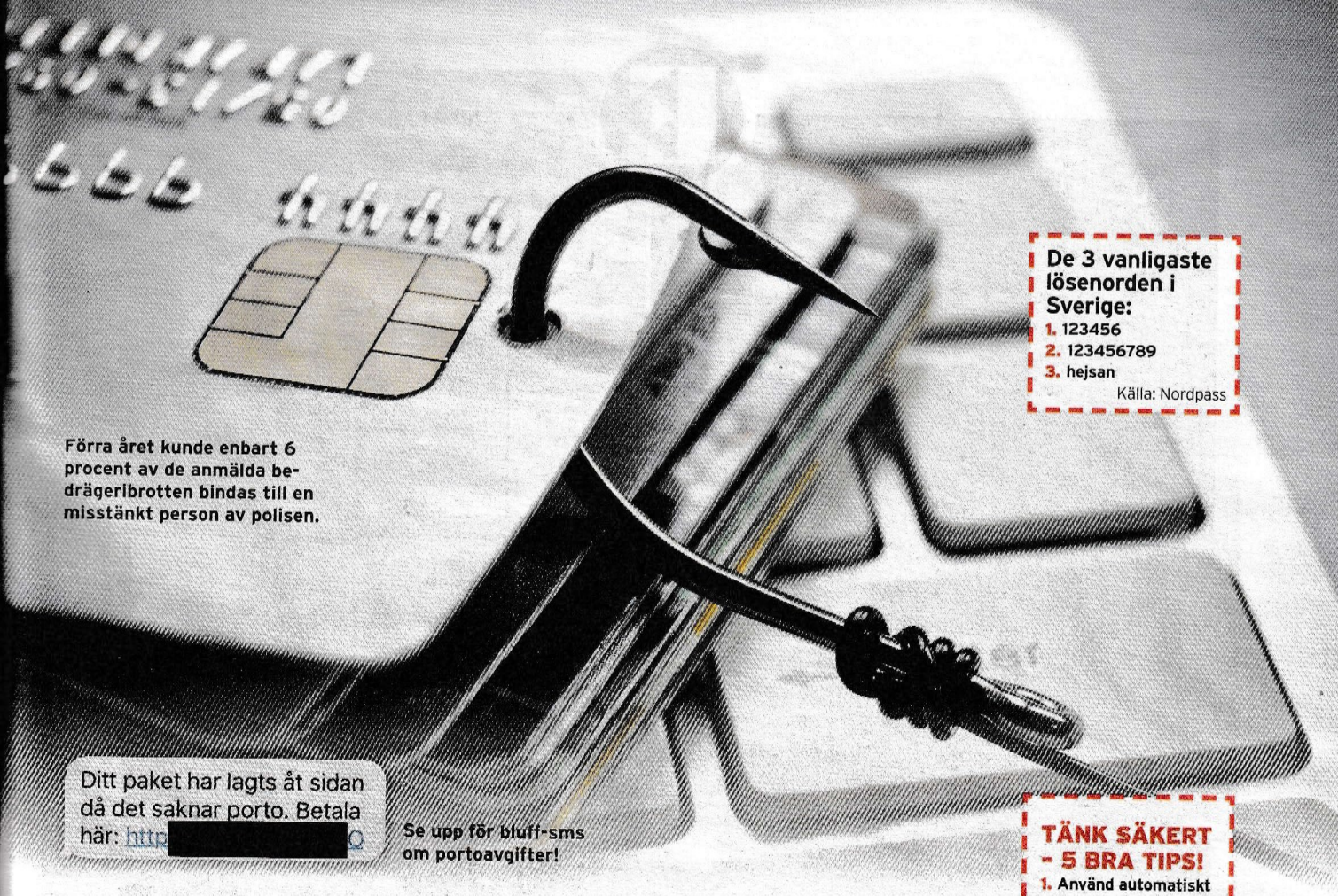
Vi har därför infört en avgift på 5 kronor.
När det är betalt får du ett formulär som måste överlämnas till posten.

Om paketet inte kommer ut tas emot inom 14 arbetsdagar, har PostNord rätt att krävs erstatning från dig.

Du kan hitta om förfarandet och villkoren för paketet lagring i närmaste kontor.

Betal frakt

Varning för sådana här falska mejl!



De 3 vanligaste lösenorden i Sverige:

1. 123456
2. 123456789
3. hejsan

Källa: Nordpass

Förra året kunde enbart 6 procent av de anmälda bedrägeribrotten bindas till en misstänkt person av polisen.

Ditt paket har lagts åt sidan då det saknar porto. Betala här: <http://...>

Se upp för bluff-sms om portoavgifter!

Plötsligt säger de sig hamna i en akut knipa och behöver låna pengar.

Så skyddar du dig: Låna aldrig ut pengar till någon du inte har träffat eller nyligen lärt känna. Och var skeptisk när någon du inte vet vem det är vill lägga till dig som vän på Facebook. Vill personen inte ställa upp på videosamtal är det också ett tecken på att något inte stämmer.

DEN FALSKA HJÄLPEN

Du får falska samtal eller mejl från t ex banken som påstår att det har försvunnit en större summa från ditt konto, eller kreditinstitut som hävdar att någon har ansökt om lån i ditt namn. De säger att de kan hjälpa dig att stoppa det, om du uppger dina lösenord, eller om du aktiverar din bank-

dosa eller mobila BankID. Men syftet är att komma åt pengarna på ditt konto. Du kan också bli uppringd av Microsoft eller Windows falska supportavdelning, som hävdar att din dator har blivit utsatt för virus och att de kan hjälpa dig genom att fjärrstyra datorn. Går du med på det kan bedragaren leta upp din känsliga information, och lägga in skadlig kod på datorn.

Så skyddar du dig: Avfärda alla sådana här mejl och samtal. Bank och myndigheter skulle aldrig be dig att lämna ut dina lösenord, och datasupporten skulle aldrig ringa upp dig! Klicka inte på några länkar i suspekta mejl, de kan innehålla virus.



TÄNK SÄKERT - 5 BRA TIPS!

- 1. Använd automatiskt skärmlås** på din mobil och dator, så gör du det svårare för tjuven att komma över din privata information om du blir bestulen.
- 2. Välj starka lösenord:** minst 12 tecken långa och en kombination av versaler, gemener, siffror och symboler. Aldrig lösenord som "12345", eller ord som finns i ordlistan.
- 3. Ha olika lösenord** för olika tjänster. För att göra det enkelt kan du spara dem i lösenordshanterare, t ex 1Password eller LastPass, som erbjuder en gratisversion.
- 4. Ha antivirusprogram** på datorn, och uppdatera din mjukvara regelbundet när du blir ombedd. Utvecklarna av din programvara kan ha upptäckt säkerhetsbrister i den gamla versionen.
- 5. Undvik gratis wifi** på t ex flygplatser och kaféer. Det är lätt för bedragare att koppla upp sig mot dem och ta sig in i din dator och mobil.

ANMÄL TILL POLISEN!

Blir man utsatt för bedrägerier är det viktigt att höra av sig till sin bank, betaltjänsten och företaget där man handlat, och att göra en brottsanmälan till polisen.

FÅ GRATIS RÅDGIVNING!

På Svenska Stöldskyddsföreningens sajt Sakerhetskollen.se hittar du info om aktuella bedrägeriförsök m m.



Känner du dig pressad av uppringaren ska du bäcka, tipsar polisen.

Källa: BRÅ, Polismyndigheten, SSF