

## Fem tips för seniorer; hur skyddar man sig mot bedrägerier?



*Hur skyddar sig någon som inte växte upp omgiven av datorteknik mot några av de vanligaste typerna av nätbedrägerier?*

Den konventionella tankesättet är att många äldre människor löper högre risk att råka ut för bedragare än deras barn eller barnbarn. Oavsett om det [stämmer eller inte](#) att äldre personer är mer utsatta så är de sant att äldre luras på mycket stora belopp på olika sätt, inklusive stöld via internet, bedrägerier och utnyttjande. All statistik av detta slag utgör sannolikt endast en bråkdel av den verkliga skadan eftersom många brottsoffer skäms för att stiga fram och medge att de blivit lurade av bedragare.

Hur som helst, vad är det som gör äldre personer sårbara för nätbedrägerier? Bedragare kan bland annat [utnyttja deras naturliga tillit](#) och att åldrandet ibland leder till försämrad kognitiv förmåga. Självfallet kan bedragarna utnyttja det faktum att deras offer inte växte upp med teknik i sin omgivning och aldrig fått ens någon grundläggande utbildning i [datasäkerhet](#).

Problemen är allra högst närvarande även i trygga Sverige. Allt från telefonbedragarligheter som [lurat till sig stora belopp](#), svindlerier mot [yngre målgrupper och deras vanor](#) eller förhoppningar om romantik som visar sig vara [kostsamma bluffar](#).

### Var skeptisk

Ta aldrig för givet att en främling på nätet går att lita på. Faktum är att det är klokt att alltid överväga möjligheten att ett oväntat meddelandet kan vara ett bedrägeriförsök. I förlängningen bör du vara försiktig även om meddelandet kommer (eller ser ut att komma) från någon du känner, och detta gäller i lika hög grad för alla meddelanden som levereras via e-post, appar för direktmeddelanden eller sociala medier. Var uppmärksam på allt som verkar ovanligt med budskapet eller avsändaren. Det kan vara en

brottsling som har tagit över din väns inloggning och använder den för att skicka ut mängder av skadlig skräppost. Kasta meddelandet om du känner dig osäker!

### Klicka inte

Ett [phishing-angrepp](#), som är ett av de allra vanligaste bedrägerierna på nätet, inleds vanligtvis med ett oväntat meddelande via e-post eller något socialt nätverk, där bedragaren imiterar någon välkänd organisation och använder olika typer av [social manipulation](#) för att locka av dig olika känsliga uppgifter, såsom uppgifter om ett kreditkort eller inloggningsinformation. Många [bedragare har kommit mycket längre](#) än till att nöja sig med felstavade, textbaserade meddelanden. De skapar imitationer av hela webbplatser och Facebook-sidor som lockbeten för sina kampanjer. Ta aldrig för givet att något material som dyker upp oväntat är autentiskt, oavsett hur officiellt det än verkar. Därför ska du aldrig klicka på länkar eller öppna bifogade filer i e-post, även om meddelandet ser ut att komma från en känd och betrodd källa.

### Tacka nej ”gratispresenter”

På motsvarande sätt kan bedragare skicka dig ett e-postmeddelande där de gratulerar dig till en ”vinst” i något [lotteri](#) du inte ens deltog i. Icke desto mindre, för att du ska kunna erhålla ditt ”pris” kommer de att be om personlig information och/eller begära förskottsbetalning i en typ av ”bedrägeri med förskottsavgift”. Vanligtvis brukar sådana skrivelser sträva efter att få dig att känna att du måste skynda dig och att du behöver svara snabbt för att inte missa chansen. Kom ihåg att riktiga lotterier aldrig kräver att vinnarna betalar några avgifter för att erhålla sina vinster.

### Skicka aldrig pengar till främlingar

Bedrägerier genom svindleri eller romantik, där offret luras att skicka pengar eller personlig information till en falsk beundrare utgjorde år 2018 den näst dyraste typen av nätbedrägerier för personer i alla åldrar. Bedrägerier med användning av romantik har under många år legat högt upp på listan över de bedrägerier som oftast vänder sig till äldre personer. Det kanske är naturligt med tanke på att ensamhet är ett av de vanligaste problemen för många äldre.

### Lägg på

Vid [bedrägerier i samband med teknisk support](#) försöker ofta bedragarna övertyga dig att din dator har smittats av virus och att du behöver ge dem fjärråtkomst till din enhet för att de ska kunna åtgärda problemet. Det är givetvis falska svepskäl, men de påföljande skadorna – förlusten av personlig information och pengar – är högst konkreta och påtagliga. Ge aldrig någon främling fjärråtkomst till din dator, inte ens om de hävdar att de representerar någon tillverkare med gott rykte.

### Extratips

Vårt sista tips vänder sig huvudsakligen till dem av oss som är yngre – låt oss se till att hålla dialogen öppen med våra föräldrar och deras föräldrar och förklara grundläggande datorsäkerhet för dem på ett begripligt sätt. Utöver att de får bättre förståelse för farorna på nätet kommer många av dem också att känna sig mer engagerade och mindre ensamma, något som till syvende och sist kan hjälpa dem att skydda sig bättre på nätet. Polisen delar med sig av [utbildningsmaterial](#) både i text och video som med fördel kan användas.