Vanliga nätbedrägerier

Vi har listat några av de vanligaste nätbedrägerierna. Här får du råd och tips om hur du undviker att bli lurad.

En person sitter framför datorn.

1. Samtal från utlandsnummer

Om du blir uppringd av ett utländskt nummer, svara inte om du inte förväntar dig ett samtal.

Och om du har ett missat samtal som inleds med ett utlandsnummer bör du inte heller ringa upp.

Samtalet är troligen ett bedrägeri och du riskerar att bli av med stora summor pengar.

2. Falskmejl om återbäring av skatt

Scenario: Du får ett mejl om att du är berättigad till skatteåterbäring och avsändaren påstår sig vara Skatteverket.

Avsändarens mejladress kan vara refund@skatteverket.se, skatt@skatteverket.se och liknande adresser. Du blir ombedd att klicka på en länk som ser ut att gå till skatteverket.

Bedragarens mål är att:
Få dig att lämna ut dina kontouppgifter och lägga beslag på dina pengar.
Så skyddar du dig:
Klicka aldrig på länkar i den här typen av mejl.
Den här typen av bedrägeri kallas för phishing eller nätfiske.

3. Samtal från Microsoft-supporten

Scenario: Du blir uppringd av en person som utger sig för att vara en representant från Microsoft eller Windows supportavdelning. Personen påstår att din dator är utsatt för virus eller liknande och att du riskerar att förlora all data på hårddisken. Du får sedan instruktioner om att skriva in komplicerade kommandon till din dator, det vill säga du accepterar att personen i andra änden får fjärrstyra din dator.
Bedragarens mål är att:
Få åtkomst till data som finns sparad på din dator, till exempel bilder, e-post, kontoinformation, ladda ner skadlig kod till din dator. Den gör att datorn kan kontrolleras på distans och att data du har sparat blir tillgänglig. Din dator kan dessutom bli en del av ett fjärrstyrt nätverk (botnet) som används för attacker mot mål på nätet,
du ska betala för utfört arbete, oftast genom att uppge ditt kortnummer. Många gånger dras sedan betalningen flera gånger.
Komma åt konto- och bankinformation för att kunna göra obehöriga överföringar från ditt konto
Så skyddar du dig:
Lägg helt enkelt på luren.
Ställ dig frågan om det troligt att ett stort it-företag ringer runt och erbjuder support? Vid minsta osäkerhet, be om personens namn och be att få ringa tillbaka senare.
Skulle du ändå ha följt instruktionerna, betala absolut inga pengar.
Koppla bort datorn från nätet. Ta hjälp av en expert som kan undersöka om något har installerats på datorn.

4. Låst dator

Scenario: Du surfar på internet när det plötsligt dyker upp ett meddelande från Rikspolisstyrelsen på dataskärmen. Det går inte att stänga ner meddelandet och varken tangentbord eller mus fungerar. I meddelandet står det att du begått ett brott på internet och att du måste betala en summa pengar för att datorn ska låsas upp igen.

Bedragarens mål är att:
Du ska tro att meddelandet kommer från Polisen och att du ska betala summan.
Så skyddar du dig:

Ställ dig frågan om detta verkar rimligt. Polisen skickar aldrig ut personliga meddelanden till internetanvändare, i synnerhet inte när någon misstänkts för ett brott.
Betala aldrig pengar till någon som kräver det via nätet om du inte beställt något eller ingått ett avtal.
Tänk på att datorn kan ha smittats med skadlig kod i samband med att meddelandet dök upp. Ta hjälp av en expert för att avgöra om datorn är fri från skadlig kod.

5. "Nigeriabrev"

Scenario: Du får ett mejl av en person som påstår sig ha en stor summa pengar som han eller hon behöver hjälp med att föra ut från ett annat land. Bedragaren hävdar att du kommer att bli rikligt belönad om du hjälper till.

Bedragarens mål är att:
Lura in dig i en händelsekedja där du tror att det är nödvändigt att betala mutor och avgifter för att få ut de utlovade pengarna.
Få dig att lämna ut dina kontouppgifter. De används sedan för att komma åt dina pengar och för att begå bedrägerier mot andra.
Så skyddar du dig
Ställ dig frågan om hur stor chansen är att just du, av alla internetanvändare, skulle bli tillfrågad om att delta i något som skulle ge stora penningsummor för nästan ingen motprestation?
Besvara aldrig den här typen av erbjudanden.

6. Romansbedrägeri, amerikansk militär eller desertör

Scenario: Du får ett mejl av en person som påstår sig vara en amerikansk hög militärofficer på uppdrag i olika delar av världen eller en desertör från armén i ett annat land. Personen skickar bilder på sig själv i syfte att utveckla en relation med dig. När relationen har etablerats ber personen om pengar för att kunna komma och träffa dig i Sverige.

Bedragarens mål är att:
Spela på känslor och förmå dig att skicka pengar.
Så skyddar du dig:
Ställ dig frågan om hur stor chansen är att en person, ofta från en annan kontinent, kontaktar just dig? Bilderna som används som bevis för att personen existerar är ofta hämtade från internet.
Du kan enkelt göra en bildsökning genom din webbläsare och se om bilden använts tidigare i andra sammanhang.
Gör även en sökning på personens namn.
Skicka aldrig pengar till någon som ber om det via internet.

7. Meddelande från din bank

Scenario: Du får ett mejl från din bank där det står att det har uppstått ett problem med ditt konto och att du ska skicka in dina kontouppgifter. Du uppmanas göra detta omgående annars blir dina tillgångar frysta i avvaktan på utredning. Bedragaren vill att du ska besvara mejlet och ange dina uppgifter alternativt klicka på en länk i mejlet. Länken går till en webbsida där du ska ange dina kontouppgifter.

Bedragarens mål är att:
Få dig att lämna ut dina kontouppgifter och lägga beslag på dina pengar.
Så skyddar du dig:
Banker och andra kreditinstitut begär aldrig in dina uppgifter via mejl. Är du osäker på om meddelandet kommer från din bank, ring banken och fråga.
Klicka aldrig på länkar i den här typen av mejl. Det finns en risk att din dator blir smittad med skadlig kod. Samma råd gäller för mejl där du påstås ha vunnit på lotteri, att du betalat in för mycket när du betalat en faktura eller där en advokat vill ha kontakt med dig angående ett arv från en tidigare okänd släkting i utlandet.