Vanliga bedrägerier Skydda dig!

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

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. Meddelande från din bank

- **Scenario:**
- Du får ett mejl eller blir uppringd från din bank om 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.

3. Falskmejl om återbäring av skatt

- 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.

4. Samtal från Microsoft-supporten

- 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 och 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.
- Microsoft aldrig ringer dig om det är nåt fel på din dator,

5. Låst dator

- Polismyndigheten 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.

6. "Nigeriabrev"

- 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.

Exsempel på ett Nigeria brev:

- Exsempel på ett Nigeria brev:
- Salamu kwako,
- Jina langu ni Bwana James Morgan, kutoka Toulouse Ufaransa. Nimekuwa
- nikisumbuliwa na ugonjwa wa saratani na daktari anasema kwamba nina
- muda mfupi tu wa kuishi. Kwa miaka kumi na mbili iliyopita, nimekuwa
- nikishughulika na usafirishaji wa dhahabu, kabla ya kuugua kwa sababu
- ya Saratani. Nilipata pesa nyingi kutokana na mauzo ya Dhahabu na
- pamba, niliolewa na mke wangu marehemu baada ya miaka mingi ya ndoa
- hatukuwa na mtoto wetu. Nina mgonjwa sana na kulingana na daktari,
- sitaweza kuishi ugonjwa huo.
- Mbaya zaidi ni kwamba sina wanafamilia au watoto kurithi utajiri
- wangu. Ninaandika barua hii sasa kupitia msaada wa kompyuta kando ya
- kitanda changu cha wagonjwa. Nina Dola za Kimarekani Milioni 2.5
- zilizohifadhiwa katika Jumba la Fedha la Ng'ambo na niko tayari
- kufundisha kuhamisha mfuko huo kama Mdhamini wangu wa kigeni

Från shona till svenska:

Hälsningar till dig,

Jag heter Mr. James Morgan,

från Toulouse Frankrike. jag har varitlider av cancer och läkaren säger att jag harbara en kort tid att leva

Under de senaste tolv åren har jag varit dethantera transport av guld innan jag blev sjuk av en anledningav cancer

Jag tjänade mycket pengar på guldförsäljning ochbomull, jag gifte mig med min senaste ftu efter många års äktenskapvi hade inte vårt

7. Bedrägeriförsök Covid19-vaccination!

- Igår blev två Jämtlandsbor uppringda av personer som skulle hjälpa dem att boka tid för vaccination mot Covid19. Uppringarna ville att den uppringde skulle legitimera sig/logga in med bank-ID/bankdosa. Jämtlandsborna misstänkte dock bedrägeri och tack vare det lyckades inte bedragarna! Dessa två fall utreds nu av polisen.
- Region JH ringer INTE upp och ber att du ska legitmera dig med BankId eller bankdosa. Får du ett samtal där någon ber dig legitimera dig ska du helt enkelt bara lägga på luren och göra en anmälan om försök till bedrägeri.
- Vi är glada att ni vaksamma och har uppmärksammat varningarna, fortsätt så!

8. Nätfiske

- Den form av nätbedrägeri som troligen ökar mest är nätfiske. Nätfiske kommer oftast i form av en tvåstegsraket med ett e-postmeddelande som ofta länkar till en falsk inloggningssida. Syftet är oftast att stjäla inloggningsuppgifter. Man kan skydda sig mot denna typ av bedrägerier genom tvåfaktorsautentisering och/eller genom att tjänsten i fråga varnar dig om det sker ett inloggningsförsök från en enhet den inte känner igen sedan tidigare – den senare metoden är dock inte alltid vattentät. Använd alltid tvåfaktorsautentisering där du kan.
- Problemet med nätfiske är att bedragarna ofta, men inte alltid, är otroligt skickliga på att få både e-postmeddelandet och landningssidan att se väldigt äkta ut. Men eftersom de inte är äkta, finns det alltid sätt att kontrollera äktheten,
- Får du en epost från Google, Microsoft, Facebook eller vilken som helst av dessa tjänster, som ber dig att logga in via en länk i meddelandet, är det per definition ett bedrägeriförsök.

Några bra länkar

- Polisen: Information från polisen om ID-skydd - https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/identitetsintrang/
- Polisen: Identitetsintrång – utsatt - https://polisen.se/utsatt-for-brott/olika-typer-av-brott/bedrageri/identitetsintrang/
- Polisen: Anmäl brott till polisen - https://polisen.se/utsatt-for-brott/polisanmalan/
- Skatteverket: Information från Skatteverket om Identitetsintrång - https://www.skatteverket.se/privat/folkbokforing/identitetsintrang.4.35c34f651660af3747c3178.html
- Bolagsverket: Skydda ditt företag mot kapning - https://bolagsverket.se/ff/foretagsformer/skydda/kapning
- Bolagsverket: Bestrid en bluffaktura - https://bolagsverket.se/ff/foretagsformer/skydda/bestrid-en-bluffaktura-1.8828
- Företagarna: Vad är VD-bedrägerier? - https://www.foretagarna.se/juridisk-faq/bluffakturor-och-bedragerier/vad-ar-vd-bedragerier/
- Kronofogden: Bluffakturor - https://www.kronofogden.se/bluffakturor.html

Fler bra länkar

- Polisen: Försök inte lura mig, utbildningsmaterial
- URPLAY: Försök inte lura mig, UR-play

Ett tips

- Om du gillar att lägga pussel så följ denna länk :
- https://www.jigsawplanet.com/