

# Intressant just nu om bedrägerier

## Nationellt bedrägericenter



April 2020

Diarienummer: A116.272/2015

### Tema: Bedrägeri i katastrofens spår – hur utnyttjar bedragare krisen?

Bedragare har en lång historia av att utnyttja naturkatastrofer eller andra kriser för sin egen vinning. Varje lokal eller global händelse har olika förutsättningar och skeenden, men en dimension har dessa gemensamt; att vissa individer står redo att gagna sig själva på andras bekostnad.

I nyhetsbladet har det tidigare nämnts att det går att skönja så kallade ”coronabedrägerier” i spåren av den pågående pandemin. Detta är dock inte det första och säkerligen inte heller det sista exemplet på ”krisbedrägerier”. I efterdyningarna av finanskrisen 2008 utsattes exempelvis amerikanska medborgare för phishing, mejl med bedräglig information om hur man kunde motta ekonomiskt stöd från staten genom att fylla i sina personliga uppgifter på en hemsida. I USA, och i den övriga världen, utnyttjades den finansiella osäkerheten efter börskraschen även i bedrägliga investeringsupplägg, där brottsoffret övertalades att investera på ett sätt som uppgavs vara säkrare än aktiemarknaden.

Under finanskrisen 2008 utnyttjade bedragarna människors osäkerhet och rädsla för det ekonomiska läget. Under de omfattande skogsbränderna i Australien väddade, och väddar, istället bedragarna till människors goda vilja. Falska insamlingar för att bekämpa bränderna och för att undsätta det australiensiska djurlivet förekommer fortfarande i hög utsträckning. Dessa bedrägliga insamlingar kan bland annat bestå av förfalskade hemsidor som efterliknar genuina donationsrörelser, falska sociala mediekonton som utger sig för att representera genuina instanser, eller så kallade ”crowdfunding”, där en privatperson utger sig för att använda insamlade resurser för ändamålet.

I efterspelet av såväl orkanen Katrina i området runt New Orleans som orkanen Rita i Texas, tog bedragare sikte på offren för naturkatastroferna. Bedragare utgav sig för att vara hantverkare och kunde ta betalt i förskott för att sen genomföra undermåligt eller ibland inget återställningsarbete alls på brottsoffrets fastighet.

#### Internationell utveckling i corona-relaterade bedrägerier

En översikt av utvecklingen i andra länder kan ge en indikation om hur brottsligheten även i Sverige kan påverkas. En stor del av de modus som rapporterats om i andra länder har redan nått Sverige. Nedanstående är trender och modus som kan komma att bli aktuella här i framtiden, men som ännu inte observerats i Sverige.



**WHO**

WHO har gått ut med varningar om bedrägerimejl där bedragarna utger sig för att komma från WHO och ber om donationer. Situationen försvåras då det faktiskt finns en genuin ”solidarity response fund” dit man kan donera pengar, och som sköts av WHO.

**Kanada**

- ◆ Bedragare utger sig för att vara poliser, och utfärdar böter för de som har på sig ansiktsmasker. Böterna ska betalas omedelbart på plats.
- ◆ Bedragare som utger sig för att komma från kanadensiska Public Health Agency, anger att den uppringde har smittats av corona, och för att få ut recept på de mediciner man ska ta behöver man ge ifrån sig sina kortuppgifter. Det finns också fall där man erbjuder privat corona-testning för en större summa pengar.

**Schweiz**

- ◆ Falsa bokningssidor online där medborgare strandsatta utomlands pga. stängda gränser erbjuds hjälp att komma hem.
- ◆ Falsa annonser på sociala medier som erbjuder gratis streaming av Netflix för de som är i självkarantän.
- ◆ Falsa fakturor för dyra virustester skickas ut till företag, som luras att betala.

**UK**

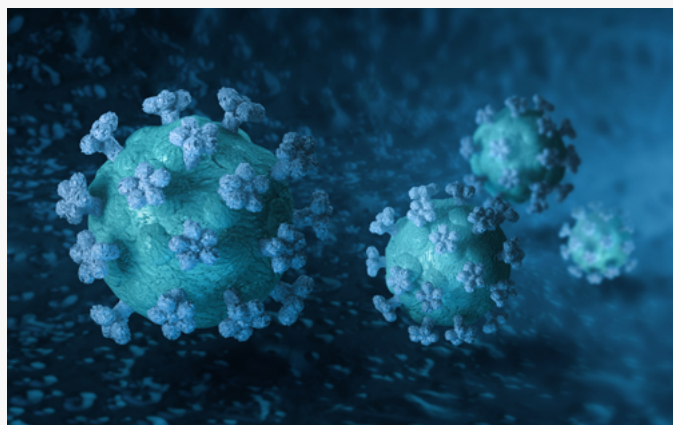
- ◆ Vårdanställda har blivit måltavlor för phishingmejl som ser ut att komma från sjukhusets IT-avdelning. Man ombeds att registrera sig på vad som ser ut att vara en intern sida för utbildning i corona-hantering, men som innebär att bedragarna kommer åt all personlig information.
- ◆ Mejl har skickats ut som ser ut att komma från brittiska Skatteverket, där man skriver att regeringen infört skatteåterbäring för de som drabbats ekonomiskt av coronaviruset. För att få tillgång till denna skatteåterbäring behöver man ge ifrån sig sina bankdetaljer.
- ◆ Officiella sms från brittiska regeringen har använts som mall för bedragare, som skickar ut snarlika sms med länkar till bedrägliga webbsidor.
- ◆ En corona-variant på Microsoftbedrägerier (fjärrstyrningsbedrägerier).

**Australien**

- ◆ Australian Cyber Security Centre flaggar för att många regeringsanställda som jobbar hemifrån kommer att bli måltavlor för framför allt phishing-försök. Samma varning har utfärdats i USA och i Kanada.

**USA**

- ◆ I USA förs redan nu diskussioner kring att skapa en s.k. task force för att hantera den våg av corona-bedrägerier man befärrar kommer att svepa genom USA efter att stimulanspaket och ekonomiska åtgärder liknande de vi har sett i Sverige genomförts.

**Corona-relaterade bedrägerier i Sverige**

I coronavirusets spår har vi fått särskilt utsatta grupper. Dessa utsatta grupper överlappar till viss del med den grupp som är extra utsatt för bedrägerier. Det finns en hög efterfrågan av produkter som inte finns tillgängliga, och en stor mängd information som går ut via sociala medier – både falsk och korrekt information.

Allt detta utgör en grogrund för bedrägerier. Det är viktigt att vi från myndigheternas sida upplyser, ger korrekt information och de verktyg våra medborgare behöver för att stå emot de bedrägeriförsök som uppkommer i krisens spår. Det är dock lika viktigt att sätta allt i ett perspektiv, så att oron inte överstiger risken att utsättas.

Ännu syns ingen anstormning av coronarelaterade bedrägerier. Den senaste månaden har endast ett sextiotal polisanmälningar gjorts.

### Vem drabbas?

De corona-relaterade bedrägerier som anmälts har haft olika målgrupper, i vissa fall har de riktats mot specifika grupper (äldre och självisolerade), i andra fall har man använt sig av ett väldigt stort nät, utan att rikta in sig mot någon särskild målgrupp. De som anmält har varit privatpersoner i alla åldrar och representanter för företag.

### Tillvägagångssätt

Majoriteten av anmälningarna består av redan existerande bedrägerityper som utvecklats med en corona-inriktning. De kan delas upp i tre grupper: fysiska besök, telefonkontakt och via digital kontakt. Det finns en tydlig variation på tillvägagångssätten som identifierats, men det handlar om relativt få fall av varje typ.

#### Fysiskt besök

Vid ett fysiskt besök kan tillvägagångssätten se lite olika ut, men utgångspunkten är att gärningspersoner gör hembesök hos äldre. De kan exempelvis utge sig för att vara från sjukvården som behöver testa de boende för coronavirus. De kan också utge sig för att vara från hemtjänsten som ska städa och sanera lägenheten från coronavirus. Väl inne i lägenheten stjäls mediciner och värdesaker.

#### Telefonsamtal

Ett annat tillvägagångssätt är att äldre/självisolerade personer blir kontaktade av gärningspersoner som erbjuder sig att handla åt dem med anledning av coronaviruset. De drabbade ombeds ge ifrån sig kontanter och/eller kontokort med kod som sedan bedragarna tar för sig av.

Telefonbedrägerier har förekommit under en längre tid, men nu har polisen börjat se exempel på den här typen av bedrägerier med en corona-prägel. Samtal kommer exempelvis från "Folkhälsomyndigheten" där den drabbade ombeds logga in med e-legitimation, bedragaren för sedan över pengar från den drabbades konto till ett annat.

#### Digital kontakt

Företag tar emot mejl från bedragare som utger sig vara kunder eller leverantörer till företagen, och påstår att betalningsförfaranden ändrats på grund av coronasituationen. Meddelanden som ...”framtida betalningar ske till ett nytt konto istället för det vanliga bankkontot” har rapporterats. I andra fall har bedragare utgett sig för att vara företagsledare som ändrar på befintliga betalningsprocesser under pandemin.

Andra bedrägerier som fått corona-prägel inkluderar annonsbedrägerier, då bedragare lägger ut annonser om ansiktsmasker och handsprit till försäljning. Produkterna finns inte, och kan därför inte levereras. Det har också funnits exempel på falska insamlingar: mejl där man ber om donationer till Röda Korset och Karolinska Institutet med anledning av coronapandemin.



#### Deklarationstider – igen...

Den 4 maj 2020 är sista dagen att lämna in sin deklaration till Skatteverket angående deklarationsåret 2019.

I samband med att deklarationerna skickas ut varje år följs det av massutskick av falska mejl och sms. I dessa har man påstått sig vara från Skatteverket och fått personer att lämna ifrån sig skyddsvärd information, som koder och kortuppgifter.

Skatteverket har tidigare gått ut och varnat för bluffmejl/-sms med informationen:

”Om du har fått ett mejl eller sms som ser ut att komma från Skatteverket, men som du misstänker är falskt ska du

- inte klicka på länkar i det
- inte öppna bilagor
- inte svara på meddelandet.

Vår rekommendation är att du raderar mailet eller meddelandet.” ... ”Skatteverket efterfrågar aldrig dina kontouppgifter i mejl eller sms. Det gör vi endast via våra e-tjänster som du loggar in på med din e-legitimation.”

[Läs om vad du kan göra](#), om du misstänker att du har fått bluffmejl eller bluff-sms från Skatteverket.

Detta aktualiserar även frågan om vad som är viktigt gällande vår digitala identitet när allt fler deklarerar via nätet.

Din e-legitimation (exempelvis bank-id) bekräftar för, i det här fallet Skatteverket, att det verkligen är du som har skickat in din deklaration. Därför är det extra viktigt att du inte lämnar ifrån dig vare sig inloggningsuppgifter eller annat som kan kopplas till din e-legitimation.



En digital brevlåda kan vara ett bra sätt att snabbt få vetskap om något har ändrats i dina uppgifter hos exempelvis myndigheter. Hos Skatteverket kan du, förutom att anmäla dig till en digital brevlåda, också begära att din adress inte ändras annat än om du själv begär det och legitimerar dig med en e-legitimation.

Vill du komma i kontakt med Skatteverket – *ta kontakt via uppgifterna på deras hemsida.*

## Intern kontaktuppgift

Gäller för anställda inom Polismyndigheten  
nationellt-bedragricenter.stockholm@polisen.se



Följ oss på Facebook: [Polisen - bedrägeri](#)

## Extern kontaktuppgift

Lotta Mauritzson  
charlotta.mauritzson@polisen.se