Så identifierar du nätbedrägerier

KULUTTAJALIITTO
KONSUMENTFÖRBUNDET

huijausinfo.fi

Med hjälp av detta utbildningspaket kan du lära dig mer om nätbedrägerier. När du har genomfört utbildningspaketet känner du de vanligaste bedrägerityperna, kan identifiera bedrägerier och vet hur du ska agera om du blir bedragen. Målet med utbildningspaketet är att stödja och uppmuntra till säker användning av nätet.

Utbildningspaketet kan användas för självstudier eller för utbildning av andra. Paketet får delas vidare till egna nätverk.

Detta utbildningspaket har genomförts som en del av Konsumentförbundets projekt för att få bukt med bedragare (Huijarit kuriin! STEA 2019–2021). Mer information om projektet och bedrägerier finns på www.huijausinfo.fi

Detta utbildningspaket har uppdaterats i december 2021.

Kuluttajaliitto ry – Konsumentförbundet rf är Finlands enda allmänna och för alla tillgängliga intressebevaknings-, utbildnings- och rådgivningsorganisation för konsumenter och användare av offentliga tjänster. Vi försvarar rättigheterna för konsumenter och användare av offentliga tjänster vid samhälleligt beslutsfattande.

Läs mer och bli medlem på: www.kuluttajaliitto.fi/sv/.

Innehåll

1. Allmänt om nätbedrägerier

Nätbedrägerier är olika bedrägerier som begås av brottslingar där digital utrustning (t.ex. dator, surfplatta, mobiltelefon) används och där offren förlorar pengar, personuppgifter eller användarnamn och lösenord.

Bakom bedrägerierna ligger ofta den internationella organiserade brottsligheten. Även om bedrägeriet sker på finska innebär det inte att det har begåtts i Finland. En stor del av bedrägerierna genomförs utanför Finlands gränser.

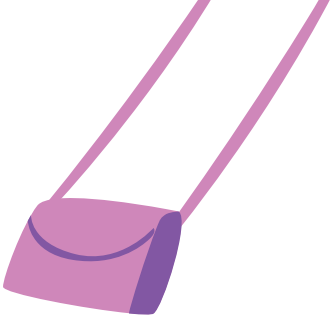
Syftet med bedrägerierna är att få ekonomisk vinning antingen på en gång eller genom att utnyttja information om den bedragna senare.

Nätbedrägerierna kan delas in i olika grupper på följande sätt:

- Näthandelsbedrägerier
- Bedrägerimeddelanden
- IT-stödbedrägerier
- Romansbedrägerier
- Investeringsbedrägerier
- Vd-bedrägerier (gäller förutom företag föreningar och organisationer)

Spelregler för säker användning av nätet

- Var noggrann och aktsam, tänk alltid efter vad du gör.
- Gör inte några förhastade beslut. Bedragarna utövar ofta påtryckningar på offren genom brådska och hot för att få dem att agera ovarsamt.
- Var kritisk och tro inte på allt som skrivs på nätet. Om något verkar för bra för att vara sant är det oftast inte sant!
- Kontrollera fakta: webbplatsens pålitlighet, sändaren av meddelandet, adresserna i länkarna.
- Sök mer information och lär dig identifiera olika bedrägerier.
- Fråga om hjälp om du inte vet något. Hjälp kan fås till exempel från bibliotek och digitalt stöd.
- Besök nätbanken eller myndigheters nättjänster via en sökmotor eller länkar i e-postmeddelanden!
- Öppna inte länkar som kommer från konstiga nummer eller adresser!



2. Näthandelsbedrägerier och beställningsfällor

Näthandelsbedrägerier

Numera kan nästan vad som helst köpas på nätet. Förutom pålitliga nätbutiker finns det dock även falska sidor och reklam på nätet. Även på loppmarknader på nätet, såsom Tori.fi och Facebook, finns bedragare som kan ge sig ut för att vara köpare eller säljare av begagnade varor.

Vid näthandelsbedrägerier skapar brottslingar webbplatser som ser ut som äkta webbutiker för att lura folk på pengar. På loppmarknader på nätet uppträder bedragarna under falska personuppgifter.

Falska nätbutiker kan sälja vilka tjänster och varor som helst som folk även annars köper (t.ex. kläder, semesterandelar, uthyrningsstugor, telefoner).

Gör inte några förhastade inköpsbeslut! Tänk igenom och kontrollera nätbutikens pålitlighet t.ex. med hjälp av en sökmaskin.

Så undviker du näthandelsbedrägerier

- Kom ihåg att det finns inget på nätet som är gratis!
  I försäljningssituationer försöker bedragare luras med fantastiska erbjudanden och få personen att fatta snabba inköpsbeslut genom att utöva påtryckningar genom brådska.

- Handla på kända företags webbplatser eller kontrollera webbutikens pålitlighet och rykte: använd sökmaskiner (t.ex. google) för att i diskussionsforum läsa om andra användares kommentarer om företaget och se till att det finns tillräckligt med information om företaget i webbutiken.

- Köp inte om du är osäker på webbutikens pålitlighet.

- Betala alltid med kreditkort om möjligt. När du har betalat med kreditkort kan du vända dig till den bank som beviljat kreditkortet om du skulle bli bedragen och det inte skulle gå att reda ut frågan med nätbutiken.

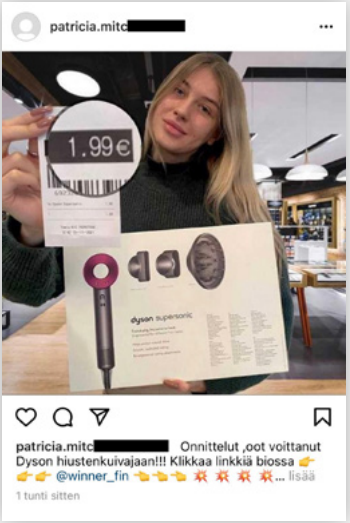
- Spara orderbekräftelserna, all kommunikation med försäljaren och butiksinnehavarens kvitto efter godkänd betalning.

- Läs beställningsvillkoren noggrant, alltid även den finstilta texten.

Bedragare kan ge sig ut för att vara finska företag. Dessutom finns det numera, framför allt i Instagram, många falska konton som påstår att personen har vunnit i ett lotteri och kan beställa eller köpa en viss produkt.

EXEMPEL

I bilden finns en falsk reklam i butikskedjan Giganttis namn där det påstås att personen har vunnit en elsparkcykel. Länken till inlösning av priset i annonsen leder till en falsk webbsida.



I bilden finns ett falskt konto som fanns på Instagram där det påstods att användare som taggats i bilden skulle ha vunnit en hårtork. Syftet med bedrägeriet är att leda användare till en falsk webbsida för att få kreditkortsuppgifter från personen.

Kontrollera alltid innan du köper att företaget tydligt anger följande uppgifter på sin webbplats, framför allt om det handlar om en webbutik som du inte tidigare känner till

- Företagsinformation och kontaktuppgifter (företagets namn, postadress, telefonnummer och e-postadress)
- Produktens eller tjänstens innehåll och pris (även leveranskostnader)
- Leveransvillkor och eventuella begränsningar kring produkten eller överraskande villkor som nämns i dem
- Leveranssätt och leveranstid för varan eller tjänsten
- Handlar det om en engångsbeställning eller förbinder man sig till en fortlöpande prenumeration vid inköp
- Hur sker betalningen och på vilka villkor
- Hur kan du ångra beställningen eller avsluta tjänsten efter inköp
- Vad har den beställda produkten för garanti- och underhållsvillkor

Beställningsfällor

Med beställningsfälla anses när konsumenter luras att omedvetet förbinda sig till fortlöpande prenumerationer antingen i telefon, i en webbutik eller till exempel med ett falskt meddelande.

Bedragarna kan påstå sig erbjuda gratisprover, avgiftsfria introduktionserbjudanden eller deltagande i utlottning på nätet, men i själva verket hamnar offret i en beställningsfälla. Personen som ringer kan berätta att det handlar om en marknadsundersökning där man kan få en viss produkt som tack genom att endast betala för portot.

Under produktens täckmantel luras konsumenter att förbinda sig till ett långt tidsbestämt avtal som innebär att de beställer varan eller tjänsten utan att de förstår eller vet om det själv.

Folk har hamnat i en beställningsfälla även genom falska meddelanden som skickats i till exempel Postens namn, när de har trott att de betalar en leveransavgift för en beställning. I själva verket har personen utan sin vetskap förbundit sig till en ”beställning” som innebär att ett visst belopp debiteras från personens konto.

I en beställningsfälla kan försäljarens kundtjänst vanligtvis inte kontaktas för att reda ut frågan. Därför går det vanligtvis inte att ångra beställningsfällan, och det kan vara svårt att stoppa debiteringarna.

Anvisningar till dig som hamnat i en beställningsfälla

- Betala endast för det du har beställt! Det är bäst att regelbundet se över vilka debiteringar som gjorts från ditt konto.

- Konsumenten kan inte krävas betala, returnera eller förvara produkter eller prov som de inte beställt.

- Produkter och fakturor som skickats utan att de har beställts ska reklameras hos avsändaren.

- Kontakta din bank angående konstiga direktdebiteringar som gjorts från ditt konto eller kreditkort.

- På Konkurrens- och konsumentverkets webbplats (KKV, www.kkv.fi/sv/) finns anvisningar för hur du reklamerar. KKV:s Konsumentrådgivning hjälper till vid reklamationer. Med KKV:s reklamationstjänst kan du reklamera även själv (www.reklamaatioapuri.fi/sv/).

3. Bedrägerimeddelanden och nätfiske

Falska meddelanden är den vanligaste bedrägeriformen. Nästan alla får någon gång falska meddelanden. Falska meddelanden skickas via e-post, textmeddelanden i sociala medier och andra appar.

Brottslingarna försöker genom falska meddelanden fiska mottagarnas bank- och kreditkortsuppgifter, personuppgifter samt användaruppgifter (t.ex. användarnamn och lösenord till e-post).

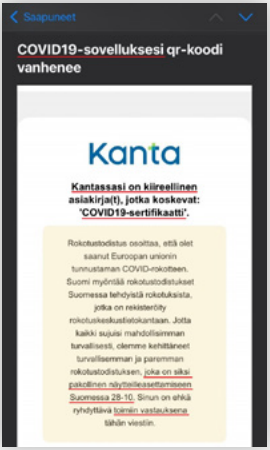
Med falska meddelanden skickas nästan alltid en länk som ska få offret att agera. Öppna aldrig någon länk i överraskande meddelanden!

Falska meddelanden via textmeddelanden kan i smarttelefoner hamna i samma kedja med äkta meddelanden (t.ex. Posten meddelanden). Det kan alltså vara svårt att skilja ett falskt meddelande från ett äkta meddelande.

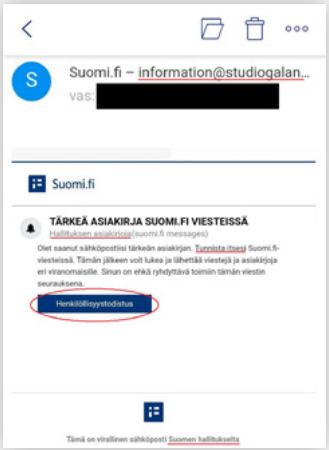
Falska meddelanden kan också skickas i myndigheters namn. I dessa meddelanden påstås att det finns ett dokument till exempel i suomi.fi-tjänsten, Kanta-tjänsten eller Skatteförvaltningens tjänst som ska läsas via en länk i meddelandet.

Meddelanden skickas också i alla finländska bankers namn där det hotas till exempel att bankkortet eller nätbanken kommer att stängas av om mottagaren inte uppdaterar sina uppgifter genom länken i meddelandet.

EXEMPEL



I Kanta-tjänstens namn skickades falska meddelanden när coronapasset infördes i Finland. Syftet var att leda mottagarna av meddelandet via länken i meddelandet till en falsk sida för att komma åt offrets nätbankskoder. I meddelandet fanns flera skrivfel och ovanliga termer.



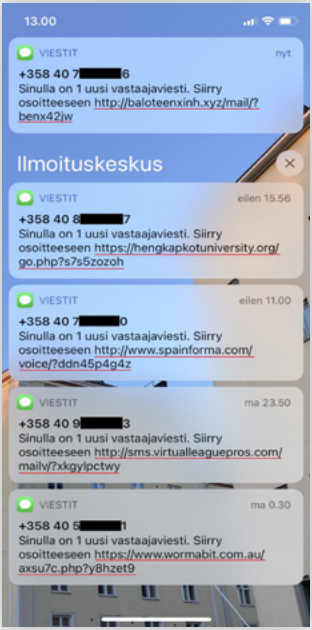
I suomi.fi-tjänstens namn skickas bluffmeddelanden där det påstås att mottagaren av meddelandet har ett viktigt dokument i tjänsten som måste läsas via länken i meddelandet genom att identifiera sig med bankkoder. Genom meddelandet sprids en falsk webbsida via vilken brottslingar kommer åt offrets nätbankskoder. Meddelandet innehåller skrivfel, flera ovanliga termer och påståenden om avsändaren som väcker misstanke.

Dessutom kan falska meddelanden skickas till exempel i Postens, transportföretags, butikers och operatörers namn. I meddelanden utövas påtryckningar genom brådska och hot om följder.

Falska meddelanden skickas i alla bankers namn. I meddelanden hotar och skrämmer avsändaren till exempel med att stänga av kontot eller kortet för att få offret att agera snabbt och ogenomtänkt. Det finns alltid en länk i meddelanden som leder till en falsk webbsida som ser ut som nätbanken. Texterna kan vara skrivna på dålig finska. Till exempel ett meddelande som skickades i Nordeas namn innehöll flera skrivfel och hot om avstängning av kontot.

- **Banker begär aldrig sina kunder att uppdatera några uppgifter genom ett vanligt e-postmeddelande – det gör bluffare!**
- **Meddelanden från banker skickas alltid via nätbanken och kan läsas under ”Meddelanden”. Om du får ett meddelande i bankens namn där du begärs göra något i nätbanken, gå alltid till nätbanken endast genom att skriva nätbankens adress i webbläsaren (t.ex. www.pankki.fi) eller genom bankens egna mobilapp.**
- **Öppna aldrig länkar i e-post- eller textmeddelanden, ladda aldrig konstiga bilagor i ett meddelande eller ge dina uppgifter om du inte är helt säker på att det inte handlar om ett falskt meddelande.**

EXEMPEL



Det kan komma flera falska meddelanden efter varandra. I falska meddelanden där det påstås att personen har ett nytt meddelande i svararen eller ett paket att skriva under finns ofta en konstig lång länk som leder till en falsk webbsida. Meddelandet ser ut att komma från ett nummer i Finland. Genom att öppna länken kan du komma att ladda ner ett skadligt program.

I ett falskt meddelande som skickats i Postens namn påstås att mottagaren har ett paket att hämta som måste skrivas under via länken i meddelandet.

Falska utpressningsmeddelanden

Falska meddelanden kan också innehålla utpressningar. Ofta påstår avsändaren att offrets dator eller e-postkonto har kapats eller att offret har smygfilmats genom kameran i datorn.

Bedragaren försöker pressa offret på pengar (vanligtvis kryptovaluta, såsom bitcoins) och hotar att publicera ”känsliga” bilder till offrets kollegor och närmaste krets.

Det handlar om ett bedrägeri och datorn har (oftast) inte blivit hackad eller kapad. Betala aldrig några pengar som krävs i ett utpressningsmeddelande. Gör en polisanmälan om utpressnings-meddelandet.

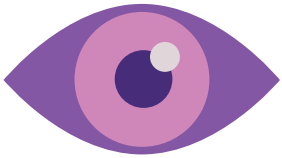
Så identifierar du bedrägerimeddelanden

Innan du reagerar på ett meddelande som du fått, fundera på följande:

- Pressas du med att det är bråttom och hotas med följder om du inte agerar som det begärs i meddelandet?
- Känner du avsändaren?
- Finns det en länk i meddelandet som du begärs använda?
- Finns det skrivfel i meddelandet?
- Väcker innehållet i meddelandet på något annat sätt misstankar?
- Ser den eventuella länken konstig ut?
- Skulle organisationen i fråga ta kontakt på det sätt som meddelandet är utformat?
- Låter erbjudandet eller lotteriet i meddelandet för bra för att vara sant eller följderna i meddelandet för hemska för att vara sant?

Gör så här om du fått ett suspekt meddelande

1. Öppna inte konstiga länkar i meddelandet.
2. Logga inte in i nätbanken eller myndighetstjänster via länkar i meddelanden.
3. Gå till en påstådd tjänst genom att skriva tjänstens adress i webbläsaren (t.ex. www.pankki.fi för att gå till en nätbank)
4. Om du inte vet om meddelandet är bluff eller inte kan du fråga om det genom att ringa till kundtjänsten för det företag som skickat meddelandet. Svara dock inte på meddelanden direkt utan leta kontaktuppgifter till kundtjänsten själv. Företag berättar oftast om lotterier och tävlingar på sin webbplats. Det är bäst att kontrollera om tävlingen eller lotteriet i meddelandet finns på riktigt.



4. IT-stödbedrägerier

Vid IT-stödbedrägerier ringer brottslingen och ger ut sig för att vara en IT-stödperson och påstår att personens dator är hotad. Bedragaren som ofta pratar engelska säger sig ringa från Microsofts IT-stöd och påstår att:

1. samtalet kommer från Microsofts huvudkontor där personens dator har övervakats,
2. offrets dator skickar någon signal om ett fel som måste åtgärdas,
3. datorn är smittad med skadlig programvara och konton har eventuellt kapats,
4. det är bråttom och endast IT-stödpersonen kan rädda personens dator.

Den som ringer vill ge intrycket om att det är väldigt brådskande och att det är nödvändigt att lyssna och följa de anvisningar som IT-stödpersonen ger.

Oftast begär bedragaren offret att ladda ner ett fjärradministrationsprogram på sin dator med hjälp av vilket den som ringer kan hjälpa personen att rädda sin dator.

Om du får ett IT-stödbedrägerisamtal

1. Avsluta samtalet omedelbart. **Varken Microsoft eller någon annan instans övervakar konsumenters datorer eller erbjuder allmänt IT-stöd.** IT-stöd är en tjänst som används till exempel av företag men Microsoft erbjuder inte någon sådan tjänst.

2. Ladda aldrig fjärradministrationsprogram eller andra appar på din dator om du inte är helt säker på hur programmet används. Personer som plötsligt ringer och kräver att ladda ner ett program på datorn är alltid bedragare.

3. Tro inte på den som ringer även om personen påstår sig veta om information på din dator.

4. Om du har laddat ner ett fjärradministrationsprogram eller på något annat sätt agerat enligt det som IT-stödpersonen säger meddela din bank omedelbart om det och låt en professionell kontrollera din dator för skadeprogram.

5. Romansbedrägerier

I romansbedrägerier ger bedragaren ut sig för att vara en påhittad person med syfte att skapa en romans eller ett vänskapsförhållande mellan den påhittade personen och offret. Genom att utnyttja den romans som skapas försöker bedragaren få pengar från offret.

De som begår dessa brott är mycket skickliga människokännare och duktiga på att använda sig av datanätverk. De utnyttjar hänsynslöst människors naturliga behov att hitta sällskap eller en livskamrat.

Genom att skickligt vädja till människors känslor kan de lyckas lura åt sig även stora summor pengar. Många offer till romansbedrägerier förlorar tiotals eller till och med tusentals euro.

Romansbedrägerier kan pågå i flera år, och offret kan luras på alla sina besparingar och till och med att låna pengar.

Så här går romansbedrägerier till

1. Bedragaren närmar sig oftast offret via sociala medier (t.ex. Facebook eller Instagram) eller dejtingappar (t.ex. Tinder).

2. Kommunikationen sker i huvudsak via olika kommunikations-appar (WhatsApp, Hangouts, Messenger).

3. Bedragaren kan säga sig arbeta i något krisområde eller på en oljeplattform.

4. Profilen i bedragarens sociala medier föreställer ofta en stilig och förmögen officer eller en vacker skådespelare från till exempel USA eller Österuropa. Bilderna, personens namn och titel samt levnadshistoria är antingen upphittade eller stulna från någon annan persons konto från sociala medier.

5. Bedragaren berättar ofta sig veta mycket om Finland och vilja komma på besök. Resorna till Finland ställs dock alltid in på grund av olika olyckliga sammanträffanden.

6. Vanligtvis fungerar inte videosamtalen och vanliga samtal rings också bara sporadiskt.

7. Ofta berättar bedragaren sig nyligen ha fått en större summa pengar i arv eller på något annat sätt eller att personen är rik från början. Bedragaren kan dock av någon anledning inte använda sina pengar och begär därför offret att ”låna” pengar.

8. Ofta vill bedragaren att överföringen görs till någon annan persons konto, inte till bedragaren själv. Begäran på pengar kan också vara förknippade med något nödläge, som sjukhuskostnader, betalning av lön, tullavgifter, arbetslöshet, skilsmässa eller dödsfall av en närstående.

9. Bedragaren kan skuldbelägga eller hota offret om offret inte går med på att göra eller kan göra de begärda överföringarna och om offret ifrågasätter personens pålitlighet kan bedragaren spela kränkt och bli arg.

10. Bedragaren intygar sin pålitlighet och äkthet till exempel genom att skicka bilder på sig själv där bedragaren är i sällskap av djur eller barn eller i något arbete som väcker tillit. Bedragaren kan även presentera länkar till sitt företags webbplats. Ofta berättar bedragaren sig vara förmögen, ha ett bra arbete och i god fysisk kondition.

Om du hyser misstankar om din nätbekants pålitlighet fråga dig själv dessa frågor

- Varför blir just jag kontaktad?
- Vet jag på riktigt vem min nätromans är?
- Har jag någonsin träffat min nätromans?
- Kan jag kontakta personen via telefon eller videosamtal?
- Begärs jag på pengar med vädjan till eventuella resekostnader, anskaffning av pass eller olika dramatiska händelser och berättelser?
- Är begäran på pengar präglade av påtryckningar, bråttom eller utpressning?

Om något verkar för bra eller för hemskt för att vara sant är det oftast inte sant!

Så här kan du undvika romansbedrägerier

- Var försiktig när du bekantar dig med nya människor på nätet. Framför allt om du plötsligt får meddelanden från en helt främmande person. Tro inte för lätt på alla berättelser som din nya bekantskap berättar.

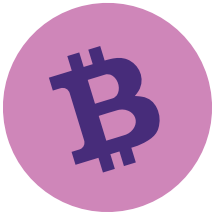
- Kontrollera nätbekantskapens bakgrund till exempel genom att söka på personens namn i Google och använda Googles omvända bildsökning. Försök att försäkra dig om personens identitet.

- Skicka inte pengar eller bilder på ditt pass till en ny bekantskap.

- Kräv att få träffa personen och att personen själv bekostar sin resa till dig.

- Prata med personen i olika kanaler. Idag har alla möjlighet att ringa videosamtal och vanliga samtal.

- Prata med dina närstående om din nya bekantskap.



6. Investeringsbedrägerier

Vid investeringsbedrägerier lockas personer genom extremt lönsamma investeringserbjudanden att köpa till exempel aktier, masskuldebrevslån eller kryptovaluta.

Ofta presenteras specialinvesteringen som ett specialerbjudande bara för dig. Erbjudandet sägs gälla endast en kort tid och du lovas snabba pengar.

Bedragarna skapar på löpande band falska nyheter och annonser på nätet där bilder på kändisar som finländarna upplever som pålitliga används och där de påstås ha blivit rika genom att investera i virtuella valutor eller rekommenderar Bitcoin-investeringar (t.ex. Matti Rönkä, Mika Anttonen, Sauli Niinistö och Sanna Marin, Ville Haapasalo).

Investeringsbedragarna gör även reklam på Tinder och i sök-maskiner, som Google.

Vid investeringsbedrägerier förlorar offren ofta stora summor pengar, upp till tio- och hundratusentals euro.

Så här går investeringsbedrägerier till

1. Investeringsbedrägerier börjar ofta i en falsk annons i sociala medier där man gör reklam för mycket lönsamma investeringsobjekt i vilka det är bäst att investera på en gång, eftersom tillfället endast gäller en kort stund.

2. Reklamen leder till en falsk sida som kan ha skapats så att den ser ut som till exempel webbplatsen för Yles nyheter. På sidan ges noggranna instruktioner på hur investeringen går till. När offret anger sina kontaktuppgifter börjar bedragarna kontakta offret och utöva påtryckningar med syfte att få så mycket pengar som möjligt av offret.

3. Offret luras att investera pengar på något som i verkligheten inte finns.

4. Därefter ringer bedragarna och skickar e-post där de begär extra investeringar till ett utländskt bankkonto eller en växlingstjänst för virtuella valutor.

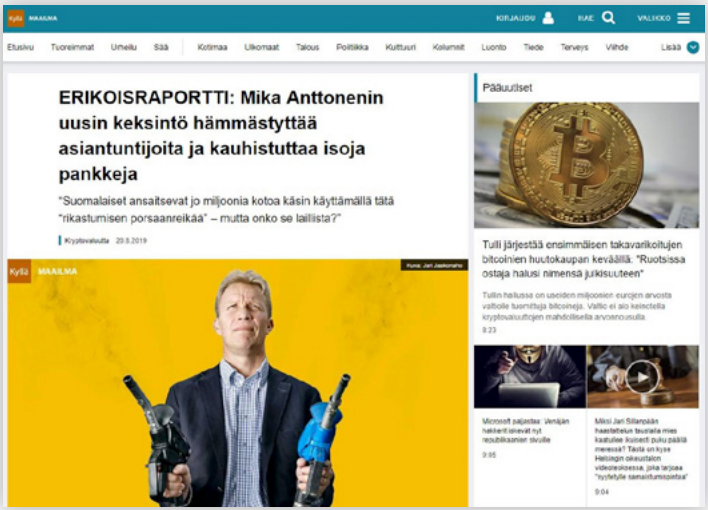
5. Offret erbjuds alltid större vinster och som ”bevis” visas bilder på påhittade börsdiagram eller webbplatser enligt vilka investeringen går bra.

6. Offret kan begäras installera ett fjärradministrationsprogram på sin dator med hjälp av vilket investeringssäljaren garanterar sig kunna ge bättre service. I verkligheten gör offret olovliga överföringar från offrets bankkonto och eventuellt tömmer offrets hela konto.

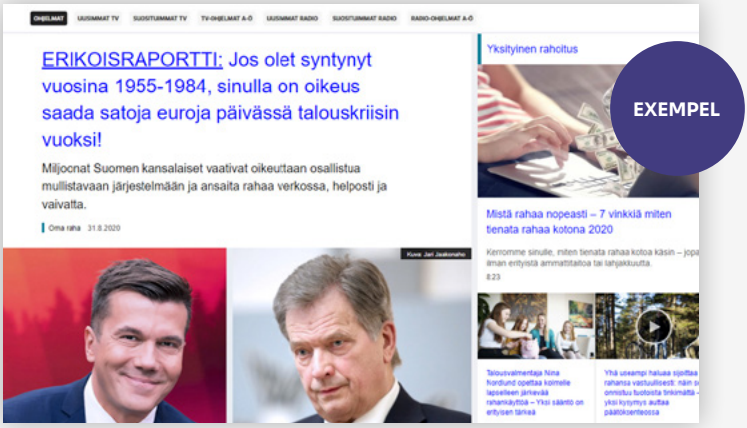
7. Kommunikationen kan vara väldigt intensiv och aggressiv och offret kan inte få ut sina pengar även om offret skulle vilja ta ut sin investering eller sina ”vinster”.

Vid investeringsbedrägerier skapas ofta en nyhetssida där man gör reklam för bedrägeriet med en bild på någon känd finländsk person. Sidorna är ofta maskerade som till exempel Yles nyheter och innehåller exakta instruktioner på hur investeringen går till och reklam på kryptovalutor. Ofta finns det skrivfel på sidorna och länkarna till andra artiklar fungerar inte. Annonser för falska sidor finns till exempel i Facebook och Google.

EXEMPEL



Vid investeringsbedrägerier skapas ofta en falsk sida som man gör reklam för i sociala medier. På sidan i exemplet försöker man väcka tillit till kryptovalutor och bedragarens tjänster samt ges detaljerade uppgifter om investeringen. På den falska sidan används företagsledare Mika Anttonens namn och bild.



I bedrägerier har även president Sauli Niinistös bild och namn använts för att marknadsföra ett investeringsobjekt som inte finns. På den falska sidan som ser ut som Yles nyheter påstås att finländare av en viss ålder skulle ha en särskild rätt att investera i den annonserade kryptovalutan, vilket i verkligheten är en bluff.

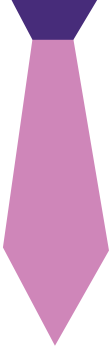
Om du misstänker ett investeringsbedrägeri

- Kom ihåg att ingen erbjuder mycket lönsamma investeringsobjekt eller investeringstips gratis till vanliga människor via telefon. Endast bedragare ringer och erbjuder investeringsobjekt.

- Investera inte dina pengar utifrån en annons på nätet (t.ex. i Facebook).

- Kontrollera bakgrunden och pålitligheten av investeringsobjektet och det företag som sköter det. Du kan fråga om hjälp till exempel från din egen bank om du inte själv vet om det handlar om ett äkta eller falskt objekt.

- Investera aldrig i objekt som du inte förstår dig på. Det gäller att vara försiktig framför allt vid investering i kryptovalutor, eftersom de ofta är förknippade med bedrägerier och risker.



7. Vd-bedrägerier

Vd-bedrägerier är riktade mot företag, föreningar, organisationer eller anställda.

Vid bedrägerier ger brottslingen ut sig för att vara en ledande person i din organisation och begär dig att överföra pengar utomlands under föregivande av något eller frågar först om saldot på organisationens bankkonto och begär därefter att en överföring görs.

Bedragaren kan vädja till att det är bråttom eller känsligt och på olika sätt utöva påtryckningar på offret för att betalningen ska genomföras.

Vanligtvis skickar bedragaren ett e-postmeddelande i en sådan persons namn som är i ledande ställning. E-postmeddelandet kan se ut att komma från chefens e-postadress även om chefen inte själv har skickat det.

Om meddelandet väcker den minsta misstanke, eller om det verkar väldigt egendomligt, fråga och kontrollera genom att ringa eller skicka e-post till den person i vars namn meddelandet har kommit.

Svara dock aldrig meddelandet direkt utan skicka ett nytt meddelande för att din fråga för säkert går till den person som du vill och inte till en bedragare!

8. Anvisningar till bedragna

Om du har förlorat pengar, personuppgifter eller bankkoder

1. Kontakta kundtjänsten vid din bank så fort som möjligt och berätta om bedrägeriet. Banken kan spärra ditt bankkonto och dina bank- och kreditkort om uppgifterna har hamnat i bedragarens händer.
2. Gör en polisanmälan, www.poliisi.fi

Sök hjälp

- Håll det inte för dig själv! Prata med bedrägeriet med dina närstående. Du kan också prata om bedrägeriet genom att ringa till Brottsofferjouren (www.riku.fi/sv/).
- Konkurrens- och konsumentverket hjälper till vid utredning av bedrägerier om bedragaren är ett inhemskt företag (www.kkv.fi/kuluttajaneuvonta/sv/).
- Vid gränsöverskridande handel inom EU kan du få hjälp av Konsument Europa Finland (www.ecc.fi/sv/).

Eget kreditförbud och spärr mot marknadsföring i telefonen

Om du har förlorat dina personuppgifter till brottslingar till följd av ett bedrägeri kan du lämna ett avgiftsbelagt frivilligt kreditförbud för 2 år.

- Eget kreditförbud förhindrar inköp på kredit.
- Du kan själv avbryta eget kreditförbud när som helst.
- Det finns två serviceleverantörer i Finland, Suomen Asiakastieto Oy och Bisnode

Spärr mot marknadsföring i telefonen

- Direktmarknadsföring kan begränsas genom att anmäla sig till en spärrtjänst mot direktmarknadsföring. Tjänsterna kan vara avgiftsbelagda.
- Mer information finns bland annat på Konkurrens- och konsumentverkets webbplats på www.kkv.fi/sv/.

Hantering av skamkänslor hos bedragna och hjälp till bedrägerioffer

Personer som blir bedragna är offer för bedrägeribrott och det är inget man behöver skämmas för.

Att bli bedragen kan jämföras med att bli utnyttjad, eftersom offren för utnyttjande upplever skam. Vanligtvis lägger bedrägerioffer skulden för bedrägeriet på sig själv.

Det viktigaste vid hantering av skamkänslor är att prata om bedrägeriet och söka professionell hjälp vid behov. Det gäller att vara väldigt försiktig när man möter en person som redan från början känner skam.

9. Mer information om bedrägerier

Konsumentförbundets webbplats om bedrägerier
www.huijausinfo.fi

Polisen
https://poliisi.fi/sv/blev-du-bedragen

Brottsofferjouren
https://www.riku.fi/sv/olika-brott/natbedragerier-kan-drabba-vem-som-helst/

Trafik- och kommunikationsverket Traficoms Cybersäkerhetscenter
https://www.kyberturvallisuuskeskus.fi/sv/

Konkurrens- och konsumentverkets konsumentrådgivning
https://www.kkv.fi/sv/konsumentarenden/konsumentradgivning/

Konsument Europa Finland
www.ecc.fi/sv/

Medborgarrådgivning hos Myndigheten för digitalisering och befolkningsdata
tfn 0295 000

Om bedrägerier varnas till exempel på Huijausinfos och Cybersäkerhetscentrets samt polisens sociala kommunikationskanaler och webbplatser

Huijausinfo
på Twitter och Facebook @huijausinfo

Cybersäkerhetscentret
på Twitter @CERTFI och på Facebook @NCSC-FI

Polisen
på Twitter och Facebook @Suomenpoliisi

Om bedrägerier varnas även till exempel
i appen 112 Suomi

Yle Vetamix Digiträning, material om bedrägerier

Lurendrejeritest: https://svenska.yle.fi/artikel/2019/06/07/digitraning-blir-du-lurad-pa-natet-testa-hur-bra-du-klarar-av-fallorna

Vet du hur man shoppar säkert på nätet: https://svenska.yle.fi/artikel/2017/10/02/digitraning-vet-du-hur-man-shoppar-sakert-pa-natet

På konsumentförbundets webbplats och YouTube-kanaler finns flera utbildningsfilmer om bedrägerier

www.huijausinfo.fi eller
www.youtube.com, sökord ”huijausinfo”

Läs mer om bedrägerier på huijausinfo.fi

huijausinfo.fi

KULUTTAJALIITTO
KONSUMENTFÖRBUNDET