Bromsa Bedragarna

Klara Arvidsson, Hadeel Ibrahim och Isabelle Rehn

Vilka är vi?

Vi är tre studenter vid Linköpings universitet som läser vår sista termin på kandidatprogrammet Språk, litteratur och medier. Bloggen är en del av ett projekt som ingår i utbildningen.

Nyttiga länkar för mer information om nätbedrägerier

- Polisen
- Näthatsgranskaren
- Brottsofferjouren
- Byrån mot diskriminering
- Näthatshjälpen

Sociala medier

Instagram
Youtube
Facebook

Detta är en återpublicering av bloggen https://bromsabedragarna.blogspot.com/.
Ett projektarbete i kursen *Att publicera i den medierade offentligheten* vt 2021 som publicerats av
Linköping University Electronic Press i serien: Linköping Electronic Press Workshop and Conference Collection, Nummer 28
ISSN: 2003-6523

Dagmar blev ett offer för Facebookbedrägeri

“Det kändes som jag hade haft inbrott i mitt hem. Det är så personligt”, så beskriver 44-åriga Dagmar hennes känsla efter att bedragare tog över hennes Facebookkonto och lurade hennes vänner på pengar.

Det hela började med att Dagmar Cerny (44) fick ett meddelande av en vän i Facebookchatten. Vännen, som Dagmar har en god relation till ber henne skicka sitt mobilnummer. Mitt i stressen och utan att tänka sig för en extra gång skickar hon mobilnumret. Vad Dagmar inte vet är att personen hon pratar med inte alls är hennes vän. Bakom skärmen sitter en bedragare som har hackat vännens konto med målet att lura till sig pengar och genom att Dagmar gör en så pass simpel sak som att ge ut sitt telefonnummer startas en serie av bedrägerier som både hon och hennes vänner ska komma att bli offer för. Ovetandes, blir hon en spelpjäs i bedragarens plan.

Efter att ha skickat telefonnumret får Dagmar ett sms innehållande en kod. Vännen ber henne att ta en skärmdump på koden och att sedan skicka skärmdumpen i chatten. Vilket hon gör. Det är ju hennes goda vän som ber henne. Vad som händer härnäst är att Dagmars eget konto blir hackat. Koden hon precis tagit en skärmdump av är en återställningskod för lösenordet till hennes Facebookkonto. Inte många minuter senare blir hon utkastad från kontot.

Strax innan Dagmars eget konto blir hackat får hon fler koder via sms, vilka vännen ber henne att ta skärmdumpar på. Några av de koderna som hon får kostar mellan 50 och 250 kr. Dagmar reagerar på detta och ringer upp sin Facebookvän och får då reda på att det inte är hennes vän som skrivit, utan en bedragare som utgett sig för att vara vännen.

— Jag ringde min vän som sa: “Skicka inte någon kod. Det där är inte jag. Det är en bedragare som tagit över mitt konto!” säger Dagmar

I och med att Dagmar blev misstänksam och ringde sin vän blev hon själv inte av med några pengar. Däremot blev flera av hennes vänner av med stora summor, vissa upp mot så mycket som 10 000 kr. Eftersom bedragarens plan involverade en tävling, skickade vissa av vännerna deras bankkortnummer för att “sätta in vinsten på ett konto” och blev på så sätt av med pengar.

Utöver det faktum att bedragaren valde att skriva till nära vänner, som offren ofta har kontakt med, var bedragaren också skicklig på att formulera sig på ett övertygande och familjärt sätt, vilket ledde till att få av de som utsattes för bedrägeri misstänkte något.

— Hon trodde hela tiden att det var jag. Vi skickade små hjärtan till varandra, säger Dagmar när hon beskriver hur hackaren “förklädd” som Dagmar skrev till hennes vän.

När bedragaren hackade Dagmars konto startades konversationer med flera av hennes nära vänner. Bilden nedan visar en konversation mellan bedragaren och en vän till Dagmar. Den blåa rutan är bedragaren som utger sig för att vara Dagmar.

Början av konversationen mellan offret och bedragaren

Offren fick skylla sig själva

Fler av Dagmars vänner blev av med pengar. Många runt 1000 kronor och, som mest, 10 000 kronor. Ingen av dem fick några pengar tillbaka. Dagmars polisanmälning slutade med att ärendet lades ner samma dag som hon anmälde, trots att hon samlade bevis och kontaktade flera företag utomlands.

— Polisen var inte ett dugg intresserade och utifrån det mobiloperatören sa, kändes det som att vi fick skylla oss själva, säger Dagmar.

När Dagmar och hennes drabbade vänner ringde mobiloperatören fick de som svar att det är eget ansvar som gäller i sådana situationer. Ingen hade egentligen tvingat dem att skicka koderna.

Bedragaren i försök i att få offrets bankkortnummer

Hackaren hade tillgång till kontot i över tolv timmar

När bedragaren tog över Dagmars konto försökte hon kontakta Facebooks kundtjänst, men det ledde ingenstans. Dagmar som var rädd att fler skulle drabbas, började ringa runt till sina vänner för att varna dem, men bland hennes 250 Facebookvänner hade hon endast numret till ett tiotal. Det enda sättet att få tillbaka kontot var genom att anmäla att det hade blivit hackat. Det tog tolv timmar för kontot att stängas ner, vilket också gav bedragaren tolv timmar extra till att lura fler vänner och hacka fler konton.

Dagmars trovärdighet skadades

— Andra gången jag ringde polisen grät jag. Det kändes som att jag hade haft inbrott i mitt hem. Det är så personligt. Jag har bilder på mina barn på Facebook. Det var jätteobehagligt. Dessutom kände jag skuld mot de som blivit av med pengar och att det var på grund av mig de hade blivit lurade. Jag erbjöd mig att hjälpa till att betala de summor mina vänner blivit av med. Mina nära vänner förstod

att det inte var mitt fel, men det fanns också personer bland de som blev utsatta som inte kände mig på det sättet, som jag tidigare hade kontaktat för att köpa saker via Blocket. Jag förklarade situationen, men de trodde nog inte på mig. Så absolut, min trovärdighet blev skadad.

Dagmar väljer att dela med sig av sin berättelse för att sprida kunskap och förståelse om hur sådana brott sker. Själv kände hon att hon hade agerat annorlunda om hon hade haft mer kunskap om bedrägerier:

— Hade jag hört av någon säga “akta dig, skicka inte koder” hade jag inte gjort det. Jag var ju 100% säker att det var min vän. Det första man gör är inte att misstänka att det är någon annan bakom skärmen. Jag tvivlade inte för en sekund, säger hon.

Vem som helst kan drabbas

—Jag har en gammal kompis som är vd för ett företag, även han skickade koderna, trots att vi inte haft kontakt på flera år. Det är inga dumma människor som drabbas, när man är stressad och får en uppgift av vad man tror är en vän, gör man det snabbt för att bli av med det, avslutar Dagmar.

Texten skapad av: Hadeel Ibrahim, Isabelle Rehn och Klara Arvidsson

Ökande IT-brott: Nätfiske

Vad är bedrägerier?

Bedrägeri, även kallat oredlighetsbrott, är ett brott som karaktäriseras av att gärningsmannen utnyttjar och vilseleder en användare till att utföra en oaktsam handling för att själv göra ekonomisk vinst på detta. Denna handling leder till skada för offret eller offrets närmaste krets. Bedrägeri kan handla om att gärningsmannen till exempel manipulerar olika digitala verktyg (som datorer och bankomater) för att komma åt känsliga uppgifter som i sin tur utnyttjas av bedragaren för ekonomisk vinning.

Dagens digitaliserade samhälle har gjort det möjligt för bedragare att bedriva verksamhet på nätet. Nätbedrägeri innefattar bedrägerimetoden **nätfiske (phishing),** vilket härstammar från den engelska motsvarigheten fishing och hänvisar till "att fiska efter något". Begreppet är ett paraplybegrepp för olika typer av IT-brott och går ut på att gärningsmannen manipulerar offret till att ge ut känslig information via till exempel mejl eller chatt för att sedan använda informationen för att begå bedrägeri. Med känslig information menas exempelvis bankkontonummer, personnummer eller lösenord. Nätfiske är en typ

av **identitetsstöld** då gärningsmannen gömmer sig bakom en falsk identitet genom att påstå sig vara till exempel en myndighet, ett företag eller en nära vän. Medan nätfiske hänvisar till en bredare attack mot flera människor, på till exempel ett företag, finns det andra metoder som riktar in sig på specifika personer. En av dessa kallas **Harpun-fiske** (**Spear-phishing)**, som går ut på att gärningsmannen riktar in sig på en enskild person och skräddarsyr attacken efter personen, för att komma åt så mycket känslig information som möjligt. Förutom mejl och chatt är de vanligaste tillvägagångssätten för att utföra bredare eller smalare nätfiskeattacker följande:

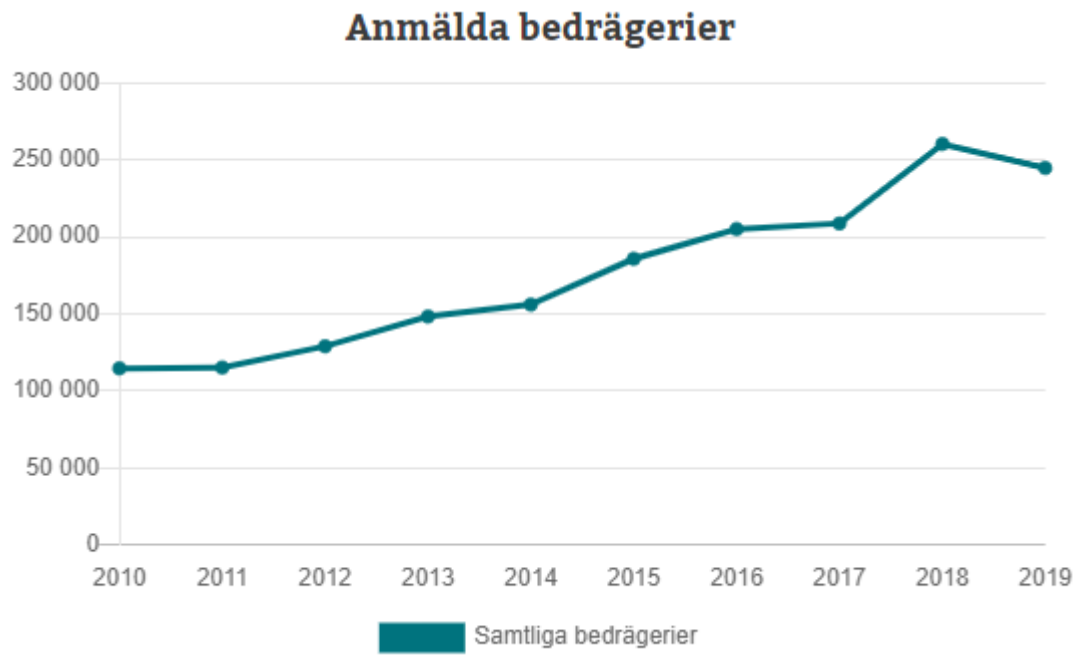
- **Pharming** - En sofistikerad attack där angriparen manipulerar servrar kopplade till en utvald webbadress. Användaren omdirigeras till webbadressen och ombeds att uppge lösenord och användarnamn.
- **Facebookbedrägeri** - Bedrägeriet går ut på att genom nätfiske, lösenordsgissning eller annat sätt komma åt en användares uppgifter på Facebook. Bedragaren studerar användarens chattloggar för att sedan fråga användarens Facebook-vänner om hjälp. (hänvisa till intervjun)
- **Falskt nödrop** - Efter att en bedragare har kommit över en användares inloggningsuppgifter skickas ett påhittat nödrop ut till alla kontakter. Nödropen handlar ofta om att personen är i behov av att låna pengar då denne har blivit bestulen eller råkat ut för en olycka i utlandet.
- **Dejtingbedrägeri** - Bedrägeriet börjar med en falsk profil på en dejtingsida. Målet med dejtingbedrägeri är att få en användare att falla för en fiktiv person (ofta en framgångsrik man), för att sedan få offret att betala en sjukhusräkning eller föra över pengar för en flygbiljett.

Längre ner i detta inlägg finns tips på hur man kan skydda sig mot dessa attacker och vad man kan se upp för.

Vem drabbas?

I och med att metoder för it-bedrägerier ständigt uppgraderas kan det idag vara svårt att avgöra vad som är ett bedrägeri och inte. Att bedragare dessutom har en tendens till att på ett skickligt sätt manipulera och vilseleda användare leder det till att i princip vem som helst kan drabbas. Under åren

2016 till 2019 uppges omkring fem procent av befolkning ha utsatts för it-bedrägerier och mellan 2010 och 2019 har bedrägerierna ökat med 113 % enligt Brottsförebyggande rådet. Vidare visar statistiken att vissa grupper är mer utsatta än andra. Antalet män som utsatts är större än antalet kvinnor. Dessutom ökar antal offer markant i takt med ålder fram till medelålder och uppåt, sedan sjunker siffrorna för åldersgruppen 75 år och uppåt, alltså bland personer som har låg internetanvändning.



Ökning av bedrägerier åren 2010-2019 (Källa: Brå)

Nätfiske/it-bedrägerier och Corona

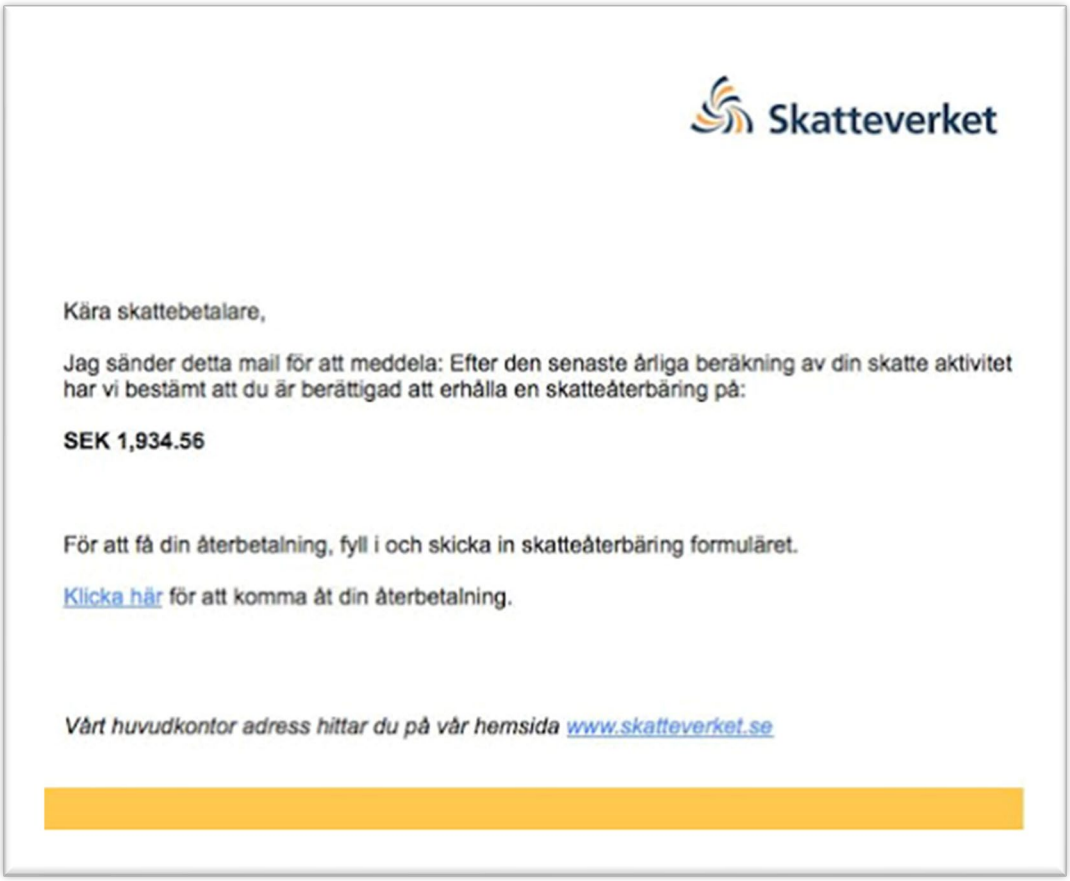
Nätfiske och andra avancerade bedrägerier är något som förekommer allt mer frekvent under pandemin. Bedragare utnyttjar covid-19 för att komma över känslig information. En vanlig strategi är att de utger sig för att vara ett lands folkhälsomyndighet. Varje dag skickar bedragare 18 miljoner mejl och 240 miljoner meddelanden relaterade till pandemin. I och med pandemin minskar fysiska möten mellan människor söker sig också allt fler ovana användare till de digitala plattformarna för att hålla kontakt med nära och kära, vilket ökar antalet potentiella brottsoffer.

Hur kan man skydda sig?

I takt med att nätbedrägerier blir ett allt vanligare brott utvecklas också nya, mer avancerade metoder, vilka kan göra det ännu lättare för internetanvändare att trilla dit/drabbas. Många gånger handlar det om att bedragare lyckas hacka konton och vidare utnyttja användarens konto för att begå olika bedrägerier. Att vi är mitt i en vaccinationsprocess är också något som bedragare utnyttjar. Vi har sammanställt fakta från myndigheter i form av tips som alltid är bra att bära med sig online:

- Var alltid försiktig med att lämna ut känsliga uppgifter (telefonnummer, personnummer och kontouppgifter) över medier. Även till vänner.
- Lämna inte ut kontouppgifter via mejl. Varken banker, kreditinstitut eller Försäkringskassan begär uppgifter via mejl.

- Klicka inte på länkar från okända mejladresser.
- Vaccination för Covid-19 är gratis och om någon vill att du ska betala för en vaccination handlar det om bedrägerier.
- Om du ska handla online, var försiktig med att lämna ut kortnummer.



Skatteverket

Kära skattebetalare,

Jag sänder detta mail för att meddela: Efter den senaste årliga beräkning av din skatte aktivitet har vi bestämt att du är berättigad att erhålla en skatteåterbäring på:

SEK 1,934.56

För att få din återbetalning, fyll i och skicka in skatteåterbäring formuläret.

Klicka här för att komma åt din återbetalning.

Vårt huvudkontor adress hittar du på vår hemsida www.skatteverket.se

Bluffmejl från Skatteverkets hemsida.

Texten skapad av: Hadeel Ibrahim, Isabelle Rehn och Klara Arvidsson

Svårt för polisen att utreda IT-bedrägerier

- Brott sker där människor finns, säger Karl-Johan Lantz, bedrägeriutredare hos Polisen i Linköping.

Under den senaste tiden har allt fler sökt sig till nätet och olika sociala plattformar. Som en följd har antalet IT-bedrägerier ökat markant. Har man blivit utsatt för ett bedrägeri vänder man sig till polisen i hopp om att få tillbaka pengar eller sätta dit skurken bakom skärmen, men många gånger leder utredningar ingenvart och ärenden läggs ner nästan omedelbart. Hur kommer det sig att det är så svårt att utreda IT-bedrägerier? Karl-Johan Lantz ger oss en inblick i faktorerna som försvårar polisens utredningsprocesser av IT-bedrägerier och vad man som privatperson kan göra för att undvika att bli ett offer.

Inte alla anmälningar utreds

När vi frågar Lantz om hur processen ser ut, från att en brottsanmälan kommer in till att ärendet antingen läggs ner eller utreds, berättar han att det första som görs är en initialbedömning av en förundersökningsledare. Är det uppenbart att brottet inte går att utreda hela vägen fram eller att prognosen för att hitta en misstänkt person är dålig kan ärendet läggas ner i ett tidigt skede för att inte ta tid och resurser från andra ärenden, som går att utreda. Summan pengar som ett offer blir av med kan också vara en faktor till att ett ärende läggs ner i ett tidigt stadie.

- Om det gäller ett bedrägeri på en tusenlapp eller några hundra kronor, då kan man ifrågasätta om det är värt en utredning, men det är alltid en avvägning, säger Karl-Johan Lantz.

Bedragaren kan sitta var som helst i världen

Bedrägerier handlar oftast om att utnyttja någon ekonomiskt, alltså att komma åt någons pengar. Om det har gjorts en betalning är det ofta där polisen börjar sin undersökning. De följer pengaströmmen och försöker koppla den till en person som delges misstanke. Många gånger leder strömmen till en person utomlands, vilket försvårar bevisinhämtningen. Polisen måste i vilket fall som helst hitta en fysisk person som är misstänkt, hålla förhör och delge misstanke. Det ska dessutom tydligt kunna bevisas att det är denna person som ligger bakom brottet.

“Brottscenen” ägs oftast av amerikanska företag

Många IT-bedrägerier sker via sociala medier som till exempel Facebook. Flera av de här företagen har amerikanska ägare, baserade i USA, alternativt har de ett dotterbolag i andra länder. Här försvåras utredningen då polisen inte får hämta in uppgifter hur som helst från olika användare och att de måste begära hjälp via en åklagarkammare för att få så kallad internationell rättslig hjälp.

- Det är en ganska stökig process, säger Karl-Johan Lantz.

Karl-Johan Lantz, utredare, Bedrägerigrupp1, Linköping, OP Östergötland

Svårt att spåra det som sker via nätet

Ett sätt att hitta bedragaren är att spåra pengarna, men många gånger omvandlas pengarna till något annat. Det kan till exempel handla om att köpa kryptovaluta för pengarna. IP- och mejladresser är andra spår man kan gå på, men ofta byts de ut snabbt. Dessutom kan adresserna vara lätta att spåra till en enhet eller användare men desto svårare att spåra till en person.

- Det kanske går att spåra en IP-adress hem till en person. Då har det använts av en enhet i personens bostad, men var det den personen egentligen som använde enheten? Kan det ha funnits någon annan i bostaden? Det är en hänsyn som vi måste ta, förklarar Karl-Johan Lantz.

Lagen skyddar inte det man gör frivilligt

Många IT-bedrägerier, speciellt de då identitetsbedrägeri har begåtts, handlar om att offret kanske inte har varit försiktig nog. Ibland ger man ifrån sig vissa uppgifter frivilligt och då blir det ännu svårare för polisen att hjälpa personen. Enligt Linköpingspolisen är det en viktig faktor i utredningsprocessen.

- Det handlar lite grann om hur man som målsägare har agerat. Man kanske har varit slarvig med sina kortuppgifter eller liknande. Det är mycket vi väger in, säger Karl-Johan Lantz.

Internationell lagstiftning krånglar till det

- Lagstiftningen är inte internationellt anpassad. Om en svensk polisbil jagar en misstänkt brottsling och denne åker in i Norge säger internationell lagstiftning att den svenska polisen måste avsluta jakten på brottslingen. Istället får svenska polis ringa norsk polis, som får fortsätta jaga bilen. Brott som sker via nätet fungerar på samma sätt, förklarar Lantz.

Han menar att lagstiftningen borde ändras för ett ökat internationellt samarbete. Att hämta användaruppgifter är tekniskt sett lätt och lagen försvårar arbetet.

- Det blir krångligt, dyrt, omständligt och tar lång tid, tillägger Karl-Johan Lantz angående lagstiftningen som försvårar utredningar av it-bedrägerier.

Att lagen ser ut som den gör nu har med integritetsskäl att göra och att vissa länder helt enkelt inte är villiga att samarbeta.

Linköpingspolisens råd till privatpersoner

I och med att det finns många faktorer som försvårar polisens arbete och att brottsanmälningar i stor utsträckning läggs ner i ett tidigt stadie är det viktigt att var och en gör sitt yttersta för att förebygga potentiella bedrägeribrott. Här är Polisens egna tips och råd:

· Man ska aldrig behöva göra en egen bedömning av vad som är värt att anmäla eller inte. Upplever man sig ha blivit utsatt för ett brott då ska man anmäla och sen gör polisen och i vissa fall en åklagare bedömningen om ärendet går att ta vidare eller inte.

· Låter någonting “för bra för att vara sant” ska man stanna upp, tänka och sedan reagera.

- Får man ett meddelande eller ett erbjudande som verkar för bra eller lite konstigt, fundera en extra gång eller ring upp personen, säger Karl-Johan Lantz och uppmanar till att alltid ringa personen som har skickat ett meddelande som ser lite ovanligt ut.

· Många bedragare skickar mejl som ser ut som att de kommer från en viss myndighet eller ett institut. De använder en falsk kopia helt enkelt och då är det viktigt att man är uppmärksam på detaljerna.

· För varje gång man ska uppge kortuppgifter på nätet skadar det inte att göra lite research om sajten man vill handla på. Oftast skriver andra användare recensioner och de kan vara värda att läsa innan man ger ut känsliga uppgifter.

· Om man blir uppringd ska man göra inte göra signeringar med bank-id eller sin bank-dosa på uppmaning av någon annan, som du själv inte har kontaktat. - Det ska man aldrig göra, avslutar Lantz.

Texten skapad av: Hadeel Ibrahim, Isabelle Rehn och Klara Arvidsson