Nätbedrägerier som brottsfenomen

En diskursanalytisk studie av hur nätbedrägerier framställs i media

Robin Klemets

4/2023

Polisyrkeshögskolans lärdomsprov / YH

REFERAT

Författare: Robin Klemets

Publikationens namn: Nätbedrägerier som brottsfenomen - En diskursanalytisk studie av hur nätbedrägerier framställs i media

Lärdomsprovets form: Undersökande lärdomsprov

Offentlighetsgrad: Offentligt

Handledare: Sabina Jordan & Christian Romberg

Examen: Polis (YH)

Syftet med denna undersökning är att ta reda på hur nätbedrägerier framställs i media genom att analysera olika nätartiklar och nätpublikationer, för att identifiera hurdan diskurs som förekommer i de olika texterna. I undersökningen redogörs också för de olika förebyggande råden som ges i texterna och de jämförs med råden som ges av myndigheterna, för att granska relevansen av råden i texterna. I undersökningen redogörs även för väsentlig lagstiftning och vanligaste formerna av nätbedrägeri.

I undersökningen används metoden diskursanalys för att analysera texterna. Diskursanalys är en forskningsmetod med vars hjälp man undersöker skriven och talad kommunikation inom ett ämne och hur de påverkar våra uppfattningar. Genom diskursanalys kan man identifiera vilka maktstrukturer, ideologier och normer som förekommer inom en given diskurs.

Undersökningens resultat tyder på att det i texterna förekommer flera underliggande mönster kring nätbedrägerier. Informationen i texterna bidrar till att öka medvetenheten och försiktigheten hos nätanvändare genom att förmedla relevant information och förebyggande råd angående nätbedrägerier.

Sidantal: 41 + 17

Månad och år då granskningen skett: 4/2023

Nyckelord: Bedrägeri, diskursanalys, media, nätbedrägeri, nätfiske, MittKanta

TIIVISTELMÄ

Tekijä: Robin Klemets

Julkaisun nimi: Nätbedrägerier som brottsfenomen - En diskursanalytisk studie av hur nätbedrägerier framställs i media

Opinnäytetyön muoto: Tutkimuksellinen opinnäytetyö

Julkisuusaste: Julkinen

Ohjaajat: Sabina Jordan & Christian Romberg

Tutkinto/kurssi: Polis (YH)

Tämän tutkimuksen tavoitteena on selvittää, miten media kuvailee verkkopetoksia, analysoimalla erilaisia verkkoartikkeleita ja -julkaisuja. Tekstien analyysillä pyritään tunnistamaan, minkälaista teksteissä esiintyvä diskurssi on. Tutkimuksessa esitellään myös tekstien ennaltaehkäisevät neuvot ja niitä verrataan viranomaisten suosituksiin, niiden asianmukaisuuden arvioimiseksi. Tutkimuksessa käsitellään myös keskeistä lainsäädäntöä ja yleisimpiä verkkopetosten muotoja.

Tutkimuksessa käytetään tekstien analysoimiseksi menetelmänä diskurssianalyysiä. Diskurssianalyysi on tutkimusmenetelmä, jolla tutkitaan kirjoitettua ja puhuttua viestintää tietystä aiheesta ja miten ne vaikuttavat näkemyksiimme. Diskurssianalyysin avulla voidaan tunnistaa tietyssä diskurssissa esiintyviä valtarakenteita, ideologioita ja normeja.

Tutkimuksen tulokset viittaavat siihen, että verkkopetoksia käsittelevissä teksteissä esiintyy useita taustalla olevia rakenteita. Tekstien sisältämä informaatio lisää nettikäyttäjien tietoisuutta ja varovaisuutta antamalla asianmukaista tietoa ja ennaltaehkäiseviä neuvoja verkkopetoksista.

Sivumäärä: 41 + 17

Tarkastuskuukausi ja vuosi: 4/2023

Avainsanat: Petos, diskurssianalyysi, media, nettipetos, tietojenkalastelu, OmaKanta

INNEHÅLL

Begrepp

Centrala begrepp som använts i undersökningen:

Oredlighetsbrott: Oredlighetsbrott innebär att en person på ett oärligt eller vilseledande sätt utnyttjar en annan person för att få ekonomisk vinning, vilket orsakar skada för den andra personen eller någon denne företräder. Exempel på oredlighetsbrott är bedrägeri, förskingring och utpressning.

Bedrägeri: ”Oredlighetsbrott som begås av den som genom vilseledning förmår någon annan till handling eller underlåtenhet som leder till vinning för gärningsmannen och skada för den vilseledde eller någon denne företräder.” (Nationalencyklopedin, bedrägeri). Bedrägeri betyder alltså att bedragaren försöker lura offret att göra något eller låta bli att göra något och på det sättet uppnå ekonomisk vinst.

Nätbedrägeri: Samlingsbegrepp för olika former av bedrägeri som sker på internet eller med hjälp av internet.

Phishing: ”*Nätfiske*, metod för IT-brottslighet där internetanvändare luras att lämna ut känslig information som sedan kan användas till bedrägerier, till exempel att tömma bankkonton på pengar.” (Nationalencyklopedin, phishing)

Kanta-nätsidan: Kanta.fi är en webbtjänst i Finland som samlar och lagrar elektroniska hälsodata för medborgarna. Tjänsten omfattar olika hälsovårdsregistren, såsom receptregister och patientjournaler, och gör dem tillgängliga för patienterna och hälsovårdspersonal.

MittKanta-nättjänsten: MittKanta, som tidigare kallades Mina Kanta, är en del av Kanta.fi-nätsidan. Det är en nättjänst för medborgare på vilken man ser egna hälso- och sjukvårdsuppgifter samt recept mm.

1 Inledning

Nätbedrägerier har blivit allt vanligare i dagens samhälle där allt fler transaktioner och kommunikation sker över internet. Detta har lett till en ökad medvetenhet om problemet och behovet av att förebygga och bekämpa nätbedrägerier. Bedrägerier som utförs med hjälp av internet har blivit alltmer vanliga och det är högst sannolikt att de kommer att fortsätta öka i antal. Under de första sex månaderna av år 2020 mottog polisen över hundra anmälningar om enbart romansbedrägerier och den totala summan pengar som förlorades på grund av dessa romansbedrägerier var närmare tre miljoner euro (Happonen, 2020).

Nya metoder av nätbedrägerier som brottslingarna använder sig av för att lura pengar av människor kommer hela tiden till kännedom. Vissa former av bedrägerier är enklare att utföra och det krävs inte mycket av kriminella för att de ska lyckas. Näthandelsbedrägerier utförs ofta av enskilda individer och två populära nätsidorna på vilka sådana bedrägerier utförs är bland annat Tori.fi och Facebook Marketplace.

En annan typ av nätbedrägeri är till exempel kärleksbedrägeri, som även kallas romansbedrägeri. Kärleksbedrägeri är en mer komplicerad form av bedrägeri, som kräver skicklighet av kriminella för att lyckas lura pengar av personer. Gärningsmännen är skickliga människokännare som utnyttjar människan naturliga behov av att hitta sällskap eller en partner. Bakom denna typ av bedrägeri kan ligga enskilda individer, men bedragarna kan även tillhöra organisationer för organiserad brottslighet. (Riku, 2023.)

Under år 2021 började det förekomma bedrägerier där kriminella även hittat på att bedraga människor genom att skapa falska sidor som liknar till exempel Kanta-nätsidan och dess nättjänst MittKanta. Målet har varit att få tag på personers person- och bankuppgifter genom nätfiske. Orsaken till detta kan vara att användningen av MittKanta-tjänsten ökade i samband med coronapandemin. (Kuukkanen, 2021.)

Jag har valt att skriva om detta ämne, eftersom bedrägeribrottsligheten utgör en stor del av brottsligheten som sker på internet. Av den anledningen är det viktigt att undersöka vilka variationer av nätbedrägerier det förekommer i Finland och på vilket sätt media informerar om dessa bedrägerier. Mitt intresse för ämnet väcktes när jag arbetade i brottsutredningen och anmälningsmottagningen under Polisyrkeshögskolans arbetspraktiksperiod. Då lade jag märke till

den stora mängden brott som sker på internet och som till en stor del utgjordes av bedrägerier och andra oredlighetsbrott. Jag blev förvånad av mängden brottsanmälningar på näthandelsbedrägerier som utförts bland annat på nätsidorna Tori.fi och Facebook Marketplace. Under tiden jag arbetade i anmälningsmottagningen så anmälde ett antal personer även att de blivit utsatta för kärleksbedrägeri och att de betalat tusentals euron åt en människa som de aldrig sett. På nyheterna läste jag även om bedrägerier där det skapats falska banknätssidor för att få tag på personers konfidentiella uppgifter. Jag förstod då även att det som är problematisk med tanke på bedrägerier som utförs på internet är att ett stort antal av dem utförs av någon från utlandet, vilket kan påverka förundersökningsåtgärderna som kan vidtas i Finland.

I detta lärdomsprov har jag redogjort för nätbedrägerier som sker i Finland och med hjälp av diskursanalys analyserat hur nätbedrägerier framställs i media. Ett av målen med denna undersökning är att få en djupare förståelse för nätbedrägerier som brottsfenomen, genom att analysera vilka underliggande ideologier som förmedlas via nätartiklar och nätpublikationer. Ett annat mål är även att undersöka hur relevant informationen i nätartiklarna och nätpublikationerna är med tanke på förebyggande av nätbedrägerier.

Media har en viktig roll i att förmedla information och därför är det viktigt att granska hurdan information som förmedlas om olika fenomen. Oavsett om det handlar om nyheter, sociala medier eller annan form av kommunikation så finns det alltid en baktanke eller ett syfte med informationen som förmedlas åt läsaren. Kritisk granskning av information hjälper läsaren att utveckla sin förmåga att granska och förstå information på ett mer nyanserat sätt. Detta är särskilt viktigt i dagens samhälle, där informationsflödet är enormt och det kan vara svårt att urskilja vilken information som är korrekt och pålitlig.

Nyttan med denna undersökning är att den ger läsaren en uppfattning om olika nätbedrägerier samt lagstiftning som är förknippad med dessa bedrägerier. Undersökningen fungerar även som ett informationspaket för svenskspråkiga poliser och polisstuderande som vill bekanta sig med brottsfenomenet. Undersökningen fungerar även som grund för Polisyrkeshögskolans svenskspråkiga studerande som vill forska vidare inom detta område, eftersom det inte finns undersökningar angående detta ämne på svenska i Polisyrkeshögskolan i Finland.

1.1 Syfte och forskningsfrågor

Syftet med den här undersökningen är att undersöka nätbedrägerier som brottsfenomen genom att analysera hur de framställs i media. Tanken med detta är att undersöka hur medias presentation av nätbedrägerier möjligen påverkar allmänhetens uppfattning och medvetenhet om dessa brott samt därmed öka förståelsen för hur man kan förebygga och bekämpa nätbedrägerier.

I undersökningen redogörs för de vanligaste variationerna av nätbedrägeri som förekommer i Finland, eftersom det är viktigt att känna till dem. Undersökningen är avgränsad till bedrägerier som utförs på internet eller med hjälp av internet. Jag vill även försöka få fram vilka påföljderna är för dessa brott och vad som är problematiskt i utredningen av dessa brott. För att beskriva detta brottsfenomen kommer jag att analysera nyhetsartiklar och nätpublikationer i vilka nätbedrägerier behandlas. Huvudfokus i de texter som jag valt att analysera ligger på nätbedrägerier som utförts genom nätfiske av uppgifter med hjälp av falska nätsidor som liknar Kanta.fi-nätsidan och dess nättjänst MittKanta. Genom denna undersökning vill jag få en djupare uppfattning om nätbedrägerier genom att analysera hurdan diskurs som förekommer i media angående ämnet.

Frågor som jag vill få svar på genom denna undersökning är:

1. Hurdana nätbedrägerier finns det och vilka av dem förekommer i Finland?
2. Hur beskrivs nätbedrägerier genom olika nyhetsartiklar och nätpublikationer samt hurdan är diskursen?
3. Hurdana råd förmedlas via media med tanke på förebyggande av nätbedrägerier och är informationen relevant?

1.2 Avgränsning

Media kan definieras som ”kanaler för förmedling av information och underhållning” (Nationalencyklopedin, media). *Massmedier* är något som är förknippat med ordet *media* och kan definieras som ”tekniska medier och mediaorganisationer som förmedlar information eller underhållning till en stor publik.” Exempel på massmedier är dagstidningar, veckotidningar, radio, TV och även internet (Nationalencyklopedin, massmedier). Denna undersökning är avgränsat till massmediet internet och därmed nyhetsartiklar samt nätpublikationer som jag hittat på internet.

Orsaken till detta är att det finns mycket information om undersökningsämnet på internet som når en stor del av den finska befolkningen. Om jag skulle inkludera andra former av massmedier i undersökningen så skulle lärdomsprovet bli för omfattande.

Undersökningsämnet är avgränsat till bedrägerier som utförs i nätmiljön och som är aktuella för tillfället. I denna undersökning behandlar jag olika metoder som bedragare använder sig av för att få tag på bankuppgifter, såsom bankkortsuppgifter och annan personlig information som kan användas för att komma åt individers pengar. Denna undersökning är avgränsad till de nätbedrägerier som förekommit i Finland under de senaste åren. Huvudfokus ligger på nätbedrägerier som utförts med hjälp av förfalskade sidor som gjorts på till exempel Kanta-nätsidan. Jag har valt att fokusera noggrannare på nätbedrägerier som är förknippade med Kanta-nätsidan och dess nättjänst MittKanta, eftersom det är finsk nätsida och det har utförts bedrägerier som avsiktligen riktats mot finländare och individer som använder denna tjänst.

Nyhetsartiklarna som använts i analysen är finsk- och svenskspråkiga nyheter och nätpublikationer som publicerats av finländska nätsidor och nyhetsförmedlare. För att samla så ny och relevant information som möjligt om brottsfenomenet, så har jag använt mig av finländska nätartiklar och nätpublikationer som blivit publicerade år 2021 och framåt.

1.3 Disposition

Detta lärdomsprov är uppbyggt av sex kapitel, som täcker olika aspekter av det valda undersökningsämnet. I det första kapitlet introduceras undersökningsämnet och syftet med undersökningen. I kapitlet tar jag också upp hur jag avgränsat undersökningen samt tidigare undersökningar som utförts inom ämnet i Polisyrkeshögskolan.

I det andra kapitlet redogörs allmänt om forskningsmetodik samt mera djupgående om diskursanalys, som jag valt att använda mig av för att utföra undersökningen. I kapitlet behandlas även materialinsamlingsmetod, validitet, reliabilitet och forskningsetik.

I tredje och fjärde kapitlet behandlas den teoretiska bakgrunden i ämnet, vilket är viktigt för att förstå innehållet i texterna som analyseras i femte kapitlet. I tredje kapitlet redogörs för väsentlig lagstiftning som är aktuell i utredningen av nätbedrägerier. I fjärde kapitlet redogörs för vanligaste

formerna av nätbedrägeri i Finland samt hur dessa nätbedrägerier utförs. Jag redogör även för ”MittKanta-bedrägeri”, som är en form av nätbedrägeri som utförs genom nätfiske av uppgifter. I slutet av fjärde kapitlet redogörs för förebyggande av nätbedrägerier.

I femte kapitlet har jag analyserat materialet som fungerat som grund för diskursanalysen. Texterna är nätartiklar och andra nätpublikationer av nyhetsleverantörer samt myndigheter, som huvudsakligen behandlar ”MittKanta-bedrägerierna”. I kapitel 5.1 har jag sammanfattat kapitlet och redogjort för undersökningens resultat.

I sjätte kapitlet har jag sammanfattat undersökningen samt redogjort för undersökningens huvudsakliga resultat. I kapitlet tar jag även ställning till resultatens validitet och reliabilitet samt utförande av arbetet. I kapitlet ger jag också förslag på vidare forskning inom ämnet.

1.4 Tidigare lärdomsprov vid Polisyrkeshögskolan

Under åren 2016–2021 har det gjorts flera lärdomsprov i vilka nätbrottslighet behandlas vid Polisyrkeshögskolan. Jag vill med min undersökning bygga på de lärdomsprov som gjorts, men också bilda en grund inom detta ämne för den svenskspråkiga utbildningen. För tillfället har det inte gjorts några lärdomsprov som behandlar nätbrottslighet inom den svenskspråkiga utbildningen i Polisyrkeshögskolan, vilket även är en motivering till varför jag valt det ämne som jag undersöker. Jag har i min undersökning valt en annorlunda synvinkel än i de andra undersökningarna, eftersom jag granskar hur nätbedrägerier framställs i media genom nätpublikationer och -artiklar.

Annina Lehtonen (2016) har i sitt lärdomsprov: *Nettipetosten kasvu 2010-luvulla. Nettipetokset selityksenä petosten kokonaismäärän kasvulle?*[1] undersökt hur nätbedrägerier ökat under 2010-talet. Syftet med lärdomsprovet har varit att påvisa att nätbedrägerierna är orsaken bakom att mängden bedrägeribrott har ökat. Lehtonen (2016) har i sitt lärdomsprov redogjort för hur man utför nätbedrägerier, vem som utför dem och vilka straff man ger åt gärningsmännen. Lehtonen (2016) samarbetade med Tori.fi och fick information om deras samarbete med polisen. Enligt Lehtonen (2016) så har nätbedrägerier spelat en stor roll i att bedrägeribrott har ökat under åren 2010 – 2015 (Lehtonen, 2016, s. 45 – 46). Lehtonen (2016) har huvudsakligen fokuserat på brottsbenämningen

[1] Nätbedrägeriers ökning på 2010-talet. Nätbedrägerier som förklaringar till ökningen av bedrägeriers totalmängd? (Min översättning)

bedrägeri och nätbedrägerier som utförts på bland annat Tori.fi-nätsidan. Jag har i min undersökning hänvisat till sådant i Lehtonens (2016) undersökning som är väsentligt med tanke på mitt ämne och använt det som teoretisk bakgrund i min undersökning.

Aki Somerkallio och Mari Takkinen (2018) har i sitt lärdomsprov: *Kyberrikollisuus ihmisen arjessa*[2] undersökt cyberbrottslighet från en vanlig nätanvändares synvinkel. I lärdomsprovet har de lyft fram olika brott på nätet, som vilken nätanvändare som helst kan bemöta i sin vardag. För teoribakgrunden har de intervjuat experter inom ämnet. I intervjuerna kom det fram att en utmaning i bekämpningen av cyberbrott är medborgarnas okunskap om brott som sker på internet. Slutresultatet av lärdomsprovet har blivit ett frågeformulär för ett online test, vars syfte är öka människors kunskap inom cyberbrott och genom det fungera som ett förebyggande projekt.

Aku Limnell (2021) har i sitt lärdomsprov: *Kyberrikollisuuden trendit nyt ja seuraavan kolmen vuoden aikana*[3] undersökt nuvarande trender och inom tre år förekommande cyberbrottslighetstrender. Limnell (2021) har i sitt lärdomsprov behandlat cyberbrottslighetens utveckling, uppfattningar som är centrala för lärdomsprovet, lagstiftning gällande cyberbrottslighet samt centrala aktörer och upphovsmän. Limnell (2021) har även behandlat lägesbilden och typiska fenomen inom cyberbrottligheten.

Jag hittade några lärdomsprov i vilka det använts samma metod som i min undersökning, alltså diskursanalys. Den senaste som är på svenska är ett lärdomsprov som är skrivet av Oscar Asikainen (2022).

Oscar Asikainen (2022) har i sitt lärdomsprov: *Polisen och allmänna sammankomster – Diskursanalytisk studie om på vilket sätt polisen framställs i traditionell media när det gäller demonstrationer* undersökt hur polisen framställs i media när det gäller demonstrationer. Asikainen (2022) har undersökt hur polisens verksamhet under allmänna sammankomster, och mer specifikt demonstrationer, framställs i traditionella medier. Syftet med studien var att granska hur medierna realiserar polisens kommunikationsstrategier i artiklarna och på vilket sätt polisen och dess åtgärder framställs. För att göra detta använde Asikainen (2022) diskursanalys, som är en metod som gör det möjligt att analysera både skriftlig och muntlig språkanvändning. Asikainen (2022) har

[2] Cyberbrottslighet i människors vardag (Min översättning)

[3] Cyberbrottslighetens trender nu och under följande tre års tid (Min översättning)

analyserat två artiklar var från tre olika nyhetsleverantörer: Hufvudstadsbladet, Helsingin Sanomat och Iltalehti. Enligt Asikainen (2022) tyder undersökningens resultat på att olika nyhetsleverantörer använder olika stilar för att framställa polisens ageranden, och att polisens kommunikationsstrategier framgår tydligt i de artiklar som han analyserat.

Det som skiljer min undersökning från Asikainens är att jag inte analyserat hur polisen framställs i de artiklar jag valt, utan jag har analyserat hur nätbedrägerier framställs i media genom de olika artiklarna. Syftet i min undersökning är att få en djupare uppfattning av själva nätbedrägerierna som brottsfenomen och hur de framställs via olika källor.

2 Material och metod

I detta kapitel redogör jag för material och vilken metod jag valt att använda för att kunna utföra undersökningen. Jag redogör för varför jag valt materialet som jag använt mig av i undersökningen och hur jag analyserat materialet samt för- och nackdelar med analysmetoden. I detta kapitel behandlas även forskningsetik och undersökningens validitet samt reliabilitet.

2.1 Forskningsmetodik

I boken *Metod helt enkelt: En introduktion till samhällsvetenskaplig metod* av Ann Kristin Larsen (2018) skriver Larsen (2018, s. 19) att metod är som ett verktyg eller redskap som används för att man ska få svar på frågor och därmed ny information inom ett område. De olika metoderna kan man anse att är olika verktyg som passar för olika ändamål och därmed måste man överväga vilken metod på bästa sätt tjänar målet som man vill nå i sin undersökning.

Forskningsmetoderna kan delas in i två olika huvudtyper; kvalitativa och kvantitativa metoder. Skillnaden mellan dessa metoder baserar sig på vilken data som samlas in för undersökningen och hur denna data analyseras. Kvantitativ metod innebär att man samlar in och analyserar data i form av numerisk information, som sedan bearbetas statistiskt. Denna forskningsmetod är vanligtvis inriktad på att studera samband mellan variabler och syftar till att kunna dra generella slutsatser om populationen utifrån den insamlade datan. En fördel med en kvantitativ metod är att den ofta ger hög grad av precision och objektivitet, eftersom den insamlade datan behandlas med hjälp av matematiska formler och statistisk analys. En nackdel med kvantitativ metod är dock att det är svårt

att fånga komplexa fenomen som inte kan mätas i numerisk form och att det kan vara svårt att fånga kontextuella faktorer som påverkar fenomenet. (Larsen, 2018, s. 31–35.)

Kvalitativ metod innebär däremot att man samlar in och analyserar icke-numerisk information, som till exempel intervjuer, observationer eller textmaterial. Kvalitativ forskning syftar till att förstå fenomen på djupet och fokuserar ofta på hur individer tolkar och upplever sin omvärld. Denna forskningsmetod ger vanligtvis mycket information om få enheter och presenteras vanligtvis i löpande text med citat. En fördel med den kvalitativa metoden är att den är lämplig för att undersöka komplexa fenomen som inte kan mätas i numerisk form. En nackdel är att den kan vara svår att generalisera till en större population. Det är viktigt att välja rätt metod beroende på forskningsfrågan, eftersom både kvantitativa och kvalitativa metoder har sina för- och nackdelar. (Larsen, 2018, s. 31–35.)

Jag har valt att använda mig av metoden diskursanalys i denna undersökning, eftersom det är den lämpligaste metoden för att analysera materialet som jag valt för undersökningen. Diskursanalys hör till kvalitativa metoder. Diskursanalys är en metod för att studera och analysera språkliga och icke-språkliga uttryck för makt och ideologi i samhället. Diskursanalys innebär att man undersöker hur språk och retorik används för att skapa, upprätthålla och förändra sociala normer och värderingar. I diskursanalys fokuserar man på hur texter och samtal konstruerar mening och betydelse, och hur de påverkar förhållanden mellan människor och grupper i samhället. (Fejes & Thornberg, 2019, s.91–92.)

2.2 Material och materialinsamlingsmetod

Jag samlade in materialet för undersökningen på basis av den metod som jag valt att använda mig av i undersökningen. Jag hade från första början tänkt använda en kvalitativ metod i min undersökning, eftersom frågeställningarna i undersökningen var anpassade för en kvalitativ forskning med tanke på att det inte går att svara på dem med ja eller nej svar.

I diskursanalys används textmaterial som datainsamlingsmetod för att analysera språkliga utsagor om verkligheten. Inom diskursanalysen betraktas alla texter som lika viktiga, eftersom de alla ger en beskrivning av verkligheten och har sanningsspråk. Forskaren är också en del av diskursen och påverkar vad som studeras och hur det studeras. Vilket material som används beror på

forskningsintresset och vilken aspekt av verkligheten som ska studeras. (Fejes & Thornberg, 2019, s. 94–96.)

Nyhetsartiklar och nätpublikationer kan med andra ord vara bra material för diskursanalys eftersom de ofta representerar och formar olika diskurser samt ideologier. Diskurser kan ses som de tankemönster och sätt att tala om och förstå världen som finns inom en viss kontext och nyhetsmedia är en viktig del av det offentliga diskursiva rummet. Genom att analysera nyhetsartiklar och nätpublikationer kan man få insikt i vilka idéer och värderingar som dominerar inom en viss samhällsfråga eller debatt, samt hur dessa idéer och värderingar representeras genom diskursen.

Jag har samlat in informationen för analysen från internet, eftersom det är lättast att hitta information om ämnet där. En stor del av befolkningen får nuförtiden sin information från massmediet internet, på grund av att det är lättillgängligare och en stor del av nyheterna är gratis. Det som kan vara problematiskt med källor på internet är att nästan vem som helst kan publicera nyheter där och de går inte nödvändigtvis genom likadana granskningar som nyheter från kända nyhetsleverantörer.

För att lyckas med min diskursanalys så har jag valt relevanta texter för den frågeställning och ämnesområde som jag har undersökt. Jag har samlat in totalt fem nätartiklar och nätpublikationer. Jag har valt texter från olika källor och olika perspektiv för att få en mer mångfacetterad bild om hurdan diskurs som används om nätbedrägerier i media. Jag strävade även till att hitta så ny information som möjligt om ämnet. Texterna har jag hittat genom att använda mig av sökorden ”Omakanta huijaus” och ”MittKanta bedrägeri” i webbläsaren och sedan valt de populäraste källorna som behandlar bedrägerifenomenet.

2.3 Diskursanalys som metod

Diskursanalys är en metod och ett teoretiskt perspektiv som används för att undersöka språkets betydelse och dess effekter på samhälle, människor och deras relationer. I stället för att betrakta språket som ett abstrakt system av regler och termer, ser diskursanalys språket som en handling som påverkar hur människor upplever, tänker, ser och känner. Diskursanalys används inom många akademiska ämnen, såsom historia, språkvetenskap, statsvetenskap, sociologi, företagsekonomi,

nationalekonomi och juridik. Metoden kan utföras på både makro- och mikronivåer och är lämplig när man vill undersöka språkets betydelse för människors identitet och subjektivitet. På makronivå undersöks det ”stora” språkbruket i samhället för att förstå vårt samhällsklimat, medan på mikronivå fokuseras på detaljerna i vardagliga samtal. (Svensson, 2019, s. 16.)

Kritisk diskursanalys är en av flera inriktningar inom diskursanalysen och det är en metod som Norman Fairclough utvecklade för att analysera hur språk och diskurser används för att skapa och upprätthålla maktrelationer. Kritisk diskursanalys fokuserar på att synliggöra de underliggande ideologierna och maktstrukturerna i samhället genom att analysera de språkliga praktikerna. Metoden är viktig inom samhällsvetenskaplig forskning eftersom den kan bidra till att utmana och förändra samhällets maktrelationer. (Svensson, 2019, s. 53–54.)

Det centrala i kritisk diskursanalys är att undersöka de olika nivåerna av diskursiva praktiker, inklusive text, diskurs och social praktik. Textnivån handlar om att analysera specifika språkliga handlingar, till exempel textens uppbyggnad, grammatik och vokabulär. Diskursnivån handlar om att analysera de bredare diskursiva praktikerna, inklusive de språkliga och icke-språkliga handlingar som används för att upprätthålla sociala och politiska strukturer. Den sociala praktiknivån handlar om att undersöka hur de bredare sociala och politiska strukturerna påverkar och formas av diskursiva praktiker. (Svensson, 2019, s. 55–56.)

2.4 Analysbeskrivning

Praktiska utförandet av diskursanalysen verkställdes genom att använda arbetsgången som beskrivs i boken *Diskursanalys* av Svensson (2019) på följande sätt:

1. Bekanta sig med det empiriska materialet
2. Organisera det empiriska materialet
3. Närläsning
4. Tematisering
5. Kontextualisering
   (Svensson, 2019, s.132.)

Metoden diskursanalys användes redan under insamlingsfasen av materialet, vilket innebar att materialinsamling och analysen sammanflätades. Jag inledde med att söka efter relevanta texter om ämnet genom att använda sökord som var relevanta med tanke på mitt forskningsområde. Eftersom det fanns många artiklar var jag tvungen att välja de mest relevant. Med relevans i detta sammanhang menar jag att jag valde de populäraste nätartiklarna och publikationerna som dök i webbläsarens sökresultat.

Det första jag gjorde med materialet var att jag samlade alla texter i ett dokument och sedan läste jag igenom alla fem texter. Dokumentet som jag gjorde är som bilaga i denna undersökning. Jag valde sedan att organisera materialet enligt den ordningen som de blivit publicerade för att se hur diskursen angående ämnet utvecklats med tiden. Enligt Svensson (2019, s. 135) kallas detta för *longitudinell* organisering, vilket betyder att materialet organiseras i en viss tidslinje, sekvens eller turordning. Svensson (2019, s 135) menar att denna typ av organisering kan vara att föredra i till exempel studier av debatter i media för att fånga utveckling av ett meningsutbyte.

Efter att jag organiserat materialet började jag med närläsningen. När jag läste materialet så fokuserade jag på de tre olika nivåerna som Faircloughs kritiska diskursanalys bygger på. De tre olika nivåerna är: text, diskursiv praktik och sociokulturell praktik (Svensson, 2019, s. 56). Jag gjorde en diskursanalys på varje text efter att jag läst dem och skrev ner resultaten för varje text i kapitel fem.

Utifrån de resultat som förekom i de enskilda diskursanalyserna så tematiserade jag det som jag upptäckt i texterna. Tematisering betyder att man sammanfattar det som man upptäckt i materialet och skapar teman som på bästa sätt beskriver det man upptäckt samt de forskningsfrågor som man formulerat (Svensson, 2019, s.142).

Kontextualisering syftar på att man placerar den språkliga diskursen i sitt rätta sammanhang. Det handlar om att förstå och analysera diskursen utifrån faktorer som påverkar dess betydelse. (Svensson, 2019, s 146.) Kontexten i texterna har jag redogjort för i kapitel 5.1.

2.5 Hermeneutik

Hermeneutik kan definieras som läran om tolkning och har sitt ursprung i det grekiska ordet hermēneutikē', vilket betyder "tolkningskonst". Hermeneutik tillämpas inom områden som teologi, rättsvetenskap och klassisk filologi, där det anses vara en samling regler som möjliggör tolkning av texter på det bästa möjliga sättet. (Nationalencyklopedin, hermeneutik.)

Hermeneutik kan användas både som metod och som teori beroende på hur forskaren väljer att använda den. Som metod kan hermeneutik användas för att försöka förstå tolkningar och tankar, medan den som teori används för att förstå ett vetenskapligt fenomen. Det är alltså upp till forskaren att avgöra hur den vill använda hermeneutiken i sitt arbete och vilken avgränsning som är mest relevant för den specifika forskningen. (Skoglund, 2012, s. 1.)

En hermeneutisk forskare närmar sig sitt forskningsobjekt subjektivt utifrån sin egen förförståelse, och ser förförståelsen som en tillgång snarare än ett hinder. Till skillnad från positivisterna, som studerar forskningsobjektet bit för bit, så försöker hermeneutikern se helheten i forskningsproblemet. Detta kallas för holism, och innebär att man försöker förstå helheten genom att se relationen mellan delarna för att få en så fullständig förståelse som möjligt. Hermeneutiken ses ofta som en motvikt till positivismens kvantitativa och naturvetenskapliga synsätt och betonar i stället kvalitativa förståelsesystem samt en subjektiv forskarroll. (Patel & Davidson, 2011, s. 28–30.)

2.6 Validitet, reliabilitet och forskningsetik

Reliabilitet och validitet är viktiga koncept inom forskning och viktigt även inom diskursanalys. Inom diskursanalys kan det vara svårt att uppnå reliabilitet, eftersom metoden ofta bygger på forskarens egna tolkningar av texter. Det innebär att olika forskare kan dra olika slutsatser från samma material. För att förbättra reliabiliteten kan man använda sig av etablerade teorier och metoder samt vara tydlig med hur forskningen utförs. I diskursanalys strävar man nödvändigtvis inte till att hitta en objektiv sanning, utan snarare att utforska och avslöja de underliggande ideologier, maktstrukturer och värderingar som formar och präglar diskurser. Validitet inom diskursanalys betyder att forskningen verkligen lyckas fånga de diskurser, ideologier och maktstrukturer som den syftar till att analysera och förstå. För att förstärka validiteten så har jag valt relevanta texter som

ger en tillräcklig bredd och variation av perspektiv och därmed en korrekt bild av de diskurser som undersöks. Texterna är även relevanta med tanke på forskningsfrågorna. Trots att jag valt relevanta texter så kan mängden av texter som jag valt påverka validiteten negativt.

Det är även viktigt att forskning bedrivs på ett visst sätt och därmed måste forskningar uppfylla vissa krav. Forskningsetiska principer inkluderar fyra huvudkrav: informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. Informationen som ges till individer som berörs av undersökningen ska inkludera syftet med undersökningen, innebörden av medverkan och hur undersökningen genomförs. Samtycke från deltagarna ska samlas in och de ska informeras om att de har själv rätt att bestämma över sin medverkan. Konfidentialitetskravet innebär att alla deltagare i undersökningen ska ha rätt till fullständig konfidentialitet och att data ska lagras på ett sådant sätt att det inte går att identifiera enskilda personer. Nyttjandekravet innebär att uppgifter som samlas in bara får användas för forskningsändamålet. (Patel & Davidson, 2011, s. 62–64.)

I denna undersökning har jag inte behövt tillämpa forskningsetiska principerna såsom de beskrivs ovan, eftersom jag endast använt skriftliga källor i undersökningen. Jag har tillämpat forskningsetikens principer genom att korrekt hänvisa till alla författare och texter som använts, noggrant granska varje artikel och dess ursprung samt presentera materialets innehåll så att det stämmer överens med det ursprungliga sammanhanget och vad som faktiskt har skrivits. Allt material i detta lärdomsprov har samlats in från öppna källor på internet samt skriftligt material och det finns ingen sekretessbelagd information. Lärdomsprovet publiceras på tjänsten för yrkeshögskolornas examensarbeten i Finland: Theseus. Undersökningen har genomgått en plagiatkontroll med hjälp av programmet Ouriginal.

3 Lagstiftning

I detta kapitel redogörs för vilka av strafflagens paragrafer som rör nätbedrägerier. Lagstiftningen har behandlats på en grundläggande nivå för att läsaren skall få en bild av hur de olika brottsbenämningarna skiljer sig åt samt vad som krävs för att de olika brotten ska uppfyllas.

Strafflagen har inte någon skild lagstiftning för bedrägerier som sker på internet, utan de går under samma paragrafer som till exempel *bedrägeri, betalningsmedelsbedrägeri* och

betalningsmedelsbrott. Genom nätbedrägerier kan även brottet *identitetsstöld* bli aktuellt om individers person- och bankuppgifter missbrukas. Dataintrång är ett brott och betyder olagligt intrång i informationssystem och det kan i sin tur leda till bedrägerier. Det vanligaste sättet att utföra dataintrång är att stjäla inloggningsinformation av en användare genom nätfiske. (Poliisi, 2023.) Ett känt fall av dataintrång i Finland är Vastaamo-fallet där personers konfidentiella klientuppgifter läckte ut (Yle, 2020). Det är viktigt att förstå skillnaden mellan dessa olika brottsbenämningar för att förstå vilka brott som kan förekomma i samband med nätbedrägerier. Bekämpning av bedrägeribrottsligheten är viktigt, eftersom känslig information som avslöjas i samband med nätbedrägerier gör det möjlig för kriminella att utföra andra brott.

3.1 Bedrägeri

Bedrägeri är enkelt förklarat ett brott som går ut på att gärningsmannen försöker lura en annan person att göra något eller inte göra något som personen annars skulle göra. Gärningsmannen strävar ofta efter att uppnå ekonomisk eller att orsaka ekonomisk skada för den som bli lurad. I Strafflagens 36 kap. 1 § beskrivs bedrägeri på följande sätt:

> Den som för att bereda sig eller någon annan orättmätig ekonomisk vinning eller för att skada någon annan, genom att vilseleda eller utnyttja misstag, förmår någon att göra eller underlåta något och därigenom orsakar ekonomisk skada för den som misstagit sig eller den vars intressen han kunnat förfoga över, skall för *bedrägeri* dömas till böter eller fängelse i högst två år. (Strafflag 39/1889, 36 kap. 1 §)

Bedrägeriförsök är straffbart. Under denna paragraf går även bedrägerier som utförs i nätmiljön. I allmänhet är syftet med olika nätbedrägerier att uppnå ekonomisk nytta. I de flesta fall av nätbedrägerier kommer denna paragraf i fråga. När man bedömer om ifrågavarande brottskriterier uppfylls, så måste man även beakta vilken gärningsform brottet är. Lindrigt bedrägeri (Strafflagen 36:3) kommer i fråga om bedrägeriet som en helhet anses vara lindrigt när man tar i beaktande den eftersträvade nyttan eller den orsakade skadan samt andra omständigheter som har och göra med brottet.

Enligt Lehtonen (2016, s. 11) har gränsen för enskilda fall av lindrigt bedrägeri brukat vara 500 euro, medan grundformen av bedrägeri uppfylls i fall av nätbedrägerier, i vilka gärningspersonen fått brottsnytta på över 500 euro. Lehtonen (2016, s.11) nämner även att gränsen för grovt bedrägeri brukar ligga vid >10 000 euro.

3.2 Betalningsmedelsbedrägeri

Betalningsmedelsbedrägeri uppfylls då någon olovligt använder, överlåter åt någon annan eller missbrukar betalningsmedlet så att täckningen eller maximikreditbeloppet överskrids. Betalningsmedelsbedrägeri kan hänga ihop med bedrägeri i sådana fall om någon blir bedragen eller bestulen på sina bankkortsuppgifter och dessa kortuppgifter sedan används olovligt. (Minilex, 2022.) I Strafflagens 37 kap. 8 § beskrivs betalningsmedelsbedrägeri på följande sätt:

> Den som för att bereda sig eller någon annan orättmätig ekonomisk vinning 1) använder ett betalningsmedel utan tillstånd av dess lagliga innehavare, med överskridande av den rätt tillståndet ger honom eller henne eller annars utan laglig rätt, 2) använder ett falskt eller förfalskat betalningsmedel, eller 3) matar in, ändrar, förstör, skadar, överför eller raderar data i anslutning till ett betalningsmedel eller på något annat sätt ingriper i ett informationssystems funktion så att resultatet av överföring av pengar eller penningvärde förvanskas och därigenom orsakar någon annan en ekonomisk skada, ska för *betalningsmedelsbedrägeri* dömas till böter eller fängelse i högst två år. (Strafflag 39/1889, 37 kap. 8 §)

Betalningsmedelsbedrägeri kan anses vara grovt om det orsakar avsevärd eller synnerligen kännbar skada, brottet begås särskilt planmässigt eller brottet begås som en del av organiserad kriminalitet. Utöver dessa kriterier ska brottet som en helhet anses vara grovt. (SL 37 kap. 9 §.) Lindrigt betalningsmedelsbedrägeri uppfylls då den orsakade skadan och andra omständigheter som en helhet anses vara ringa.

3.3 Betalningsmedelsbrott

Betalningsmedelsbrott beskrivs i strafflagens 37 kap. 12 § på följande sätt:

> Den som 1) olovligen tillägnar sig ett betalningsmedel, 2) framställer ett falskt betalningsmedel eller förfalskar ett betalningsmedel för utförande av ett betalningsmedelsbedrägeri eller med vetskap om att användningssyftet är utförande av ett betalningsmedelsbedrägeri, eller 3) anskaffar, köper, i landet inför, innehar, säljer, sprider, överför, transporterar, överlåter eller ur landet utför ett olagligt anskaffat, falskt eller förfalskat betalningsmedel för utförande av ett betalningsmedelsbedrägeri eller med vetskap om att användningssyftet är utförande av ett betalningsmedelsbedrägeri, ska för *betalningsmedelsbrott* dömas till böter eller fängelse i högst två år. (Strafflag 39/1889, 37 kap. 12 §)

3.4 Identitetsstöld

Identitetsstöld beskrivs i strafflagens 38 kap. 9 a § på följande sätt:

> Den som i syfte att vilseleda en tredje part obehörigen använder någon annans personuppgifter eller identifieringsuppgifter eller andra motsvarande uppgifter som identifierar personen, och därmed orsakar ekonomisk skada eller mer än ringa olägenhet för den som uppgifterna gäller, ska för *identitetsstöld* dömas till böter. (Strafflag 39/1889, 38 kap. 9 a §)

Identitetsstöld innebär att någon använder sig av någon annans personuppgifter utan deras tillstånd i syftet att vilseleda en tredje part och därmed orsaka ekonomiska skada för den som uppgifterna egentligen hör till. Identitetsstöld kan vara ett följdbrott av nätbedrägeri. Det kan vara möjligt för kriminella att begå identitetsstöld, om de har fått tag på någons person- eller bankuppgifter genom till exempel nätfiske av uppgifter.

3.5 Dataintrång

Dataintrång betyder att någon olovligen eller utan tillstånd får tillgång till data eller system som inte är avsedda för allmänheten. Dataintrång kan även innebära olovlig manipulering av data eller system. Dataintrång kan få allvarliga konsekvenser för offret, som exempelvis att personlig information läcker ut. Dataintrång beskrivs i strafflagens 38 kap. 9 § på följande sätt:

> Den som genom att göra bruk av en användaridentifikation som han eller hon inte har rätt till eller genom att annars bryta säkerhetsarrangemang obehörigen tränger in i ett informationssystem där information eller data behandlas, lagras eller överförs elektroniskt eller med någon annan sådan teknisk metod eller i en särskilt skyddad del av ett sådant system, ska för *dataintrång* dömas till böter eller fängelse i högst två år. (Strafflag 39/1889, 38 kap. 9 §)
>
> För dataintrång döms också den som utan att tränga in i ett informationssystem eller en del av ett sådant
> 1) med hjälp av tekniska specialanordningar, eller
> 2) annars med tekniska metoder genom att ta sig förbi säkerhetsarrangemangen, utnyttja informationssystemets sårbarhet eller använda annars uppenbart svikliga medel, obehörigen tar reda på information eller data som finns i ett sådant informationssystem som avses i 1 mom. Försök är straffbart. (Strafflag 39/1889, 38 kap. 9 §)

Vanligaste sättet att utföra dataintrång är genom att stjäla personers inloggningsinformation genom nätfiske. Personers känsliga inloggningsinformation kan samlas in genom falska sidor på internet som tar vara på den känsliga informationen. Känslig information som samlas in används vanligtvis till att utföra bedrägerier eller andra brott där man kan utnyttja offrets information. (Poliisi, 2023.)

4 Nätbedrägerier

I detta kapitel redogörs för olika sätt som nätbedrägerier kan utföras på och vanligaste formerna av nätbedrägeri som förekommer i Finland samt viktiga begrepp inom bedrägeribrottsligheten. I detta kapitel går jag även mer djupgående in på så kallade MinaKanta-bedrägerierna som tagits upp i nyheterna från och med år 2021. I det sista delkapitlet behandlas även förebyggande råd som ges på internet samt vad man ska göra om man blivit utsatt för nätbedrägeri.

Enligt statistiken så påverkar nätbedrägerier samhället på en bred front. Under år 2021 rapporterades totalt 2500 fall av nätbedrägeri till polisen och finländska medborgare förlorade ungefär 47 miljoner euro till bedragare. Summan kunde ha varit större, men 25 miljoner euro

lyckades stoppas från att överföras till bedragare och återbetalades till de ursprungliga offren. Detta var möjligt på grund av bankernas och myndigheternas samarbete. Bedrägerierna som orsakade de största ekonomiska förlusterna var IT-supportbedrägerier, VD-bedrägerier, kärleksbedrägerier, dokumentbedrägerier, investeringsbedrägerier och bankbedrägerier. Under första kvartalet av 2022 minskade antalet anmälda fall och bedrägeriernas ekonomiska förluster med över 40 % jämfört med samma period förra året. (Finanssiala, 2022.)

4.1 De vanligaste formerna av nätbedrägeri

Nätbedrägerier är brott som sker med hjälp av datateknik och datanät. I dagsläget finns det många variationer av nätbedrägerier som brottslingar använder sig av. Exempel på vanliga typer av nätbedrägerier är näthandelsbedrägeri, kärleksbedrägeri samt olika bedrägerimeddelanden och e-post. Nätfiske är en form av bedrägeri i vilken en bedragare försöker lura till sig känslig information från en person genom att skapa en falsk webbsida eller ett e-postmeddelande som ser ut att vara från en pålitlig källa, som en bank eller en myndighet. Offret uppmanas att lämna ut personliga eller finansiella uppgifter, som lösenord eller kreditkortsinformation, och bedragaren använder sedan denna information för att begå bedrägeri eller identitetsstöld. I följande tre delkapitel redogör jag för de olika typerna av nätbedrägeri.

4.1.1 Näthandelsbedrägeri

Näthandelsbedrägeri kan inträffa i samband med försäljning, köp eller uthyrning av varor och tjänster. Bedragarna lockar med snabba tidtabeller och lockande priser för att få offret att agera snabbt och riskfyllt. Offret betalar för varan eller tjänsten till bedragarens angivna konto, men sedan kan det visa sig att varan inte levereras eller inte motsvarar vad man kommit överens om, och säljaren går inte att få tag på. Bedrägeriet kan röra sig om olika typer av tjänster och produkter, som bostäder, biljetter till evenemang och konserter. (Poliisi, 2023.)

Ett kännetecken för näthandelsbedrägeri är att en person säljer en produkt mycket billigare jämfört med andra. Detta brukar ofta vara tillräckligt för att väcka köparens intresse. Ett annat kännetecken är att person säger att den bor på en annan ort och därmed kan inte produkten hämtas direkt av försäljaren. Om köparen går på att betala produkten i förväg så slutar försäljaren att svara på kontaktförsöken och produkten anländer aldrig till köparen. Näthandelsbedrägerier kan även

utföras andra vägen. Bedragaren köper en produkt genom att förfalska ett kvitto för att påvisa att den skulle ha betalat eller påstår att produkten har gått sönder under transporteringen och kräver tillbaka pengarna. (Lehtonen, 2016, s. 11–12.)

4.1.2 Kärleksbedrägeri

Kärleksbedrägeri är en form av bedrägeri som innebär att bedragare utnyttjar människors naturliga behov av att hitta sällskap eller en livspartner genom att manipulera och lura dem att skicka pengar. Bedragarna är ofta skickliga nätanvändare och människokännare som kontaktar offren via sociala medier och utger sig för att ha en gemensam framtid i Finland. De ber om pengar för olika nödsituationer och lovar att överföra en stor summa pengar till offren, vilket kräver att offren skickar pengar till bedragarna först. Största delen av offren är kvinnor och offren kontaktas ofta via Facebook, men även via dejtingsidor och diskussionsforum. (Riku, 2023.)

Enligt kriminalkommissarie Hannu Kortelainen (Kortelainen, 2020) består romansbedrägeri av tre olika skeden:

1. Bedragaren skapar förtroende genom att skapa ett förhållande med offret via sociala medier och sedan föreslår att de flyttar diskussionen till andra plattformar, som till exempel e-posten, Hangouts eller Whatsapp. Detta skede kan vara i veckor eller till och med månader.
2. Bedragaren berättar om en tragisk händelse eller en nödsituation och på grund av detta behövs det pengar. Syftet med detta är att vädja till offrets känslor.
3. Bedragaren ber om pengar för att lösa den påstådda nödsituationen. Offret uppmanas att agera snabbt och det kan finnas fantasifulla förklaringar till varför pengar behövs. (Kortelainen, 2020.)

4.1.3 Nätfiske av uppgifter

Nätfiske, som på engelska kallas phishing, är en typ av bedrägeri som syftar till att lura människor att lämna ut känslig information som bankuppgifter, lösenord, kreditkortsnummer eller personuppgifter. Bedrägeriet utförs oftast via e-post, sms eller sociala medier och det är vanligt att bedragarna försöker övertyga mottagaren att klicka på en länk eller ladda ner en bilaga. När mottagaren klickar på länken eller öppnar bilagan styrs de ofta in på en falsk webbplats som ser ut

som den riktiga, till exempel en banknätsida. Där uppmanas de att fylla i sina känsliga uppgifter, vilket bedragarna sedan kan använda för att genomföra bedrägerier och få ekonomisk vinning. (Poliisi, 2023.)

Ett vanligt exempel på nätfiske är att en person får ett e-postmeddelande av någon som utger sig att vara en myndighet, ett företag eller bank. Meddelandet kan innehålla en begäran om att personen ska uppdatera sina konto- eller betalningsuppgifter. Det kan också innehålla en begäran om att personen ska skicka sina användarnamn och lösenord för att bekräfta sin identitet. Bakom dessa e-postmeddelanden ligger oftast utländska kriminella ligor och på grund av det kan språket i meddelanden vara bristfälligt översatt och meningarnas uppbyggnad kan vara konstig. (Haasio, 2017, s. 82–83.)

Phishing är ett samlingsnamn för alla typer av nätfiske, men det kan delas in i olika kategorier som baserar sig på hurdana metoder som används. Enligt artikeln: *Vad är nätfiske?*[4] av antivirusprogramföretaget F-Secure, så kan nätfiske delas in tre olika varianter: Spear-phishing, smishing och vishing. (F-Secure, 2023.)

Spear-phishing är en metod i vilken bedragare riktar in sig på en specifik person i stället för att skicka massutskick av e-post och skräddarsyr e-postmeddelandet för att lura personen att avslöja känslig information. Bedragaren kan använda sig av information från sociala medier och företagswebbplatser för att utge sig att vara en affärskontakt eller kollega och det kan vara svårt att upptäcka. (F-Secure, 2023.)

Smishing är en form av bedrägeri som kombinerar sms och phishing. Bedrägeriförsöket utförs via sms i stället för e-post. Bedragarna utnyttjar mobiltelefonen för att komma åt privatpersoners kontouppgifter och annan privat information genom att skicka falska sms som innehåller länkar till falska webbplatser eller får användaren att installera skadlig programvara. Många svarar på sms snabbt och har högre tillitsgrad när de använder telefonen, vilket gör att bedragarna kan lura användare att lämna ifrån sig sina personuppgifter eller installera skadlig programvara. (F-Secure, 2023.)

[4] https://www.f-secure.com/se-sv/articles/what-is-phishing.

Vishing är en kombination av engelska orden ”voice” och ”phishing” och syftar alltså på samtalsfiske. Bedragarna använder sig av telefonsamtal för att få tag på konfidentiell information av personer. Bedragaren kan ringa upp personer och påstå sig representera exempelvis banken eller polisen för att lura till sig lösenord, bankkoder eller personuppgifter. (F-Secure, 2023.)

4.2 ”MittKanta-bedrägeri”

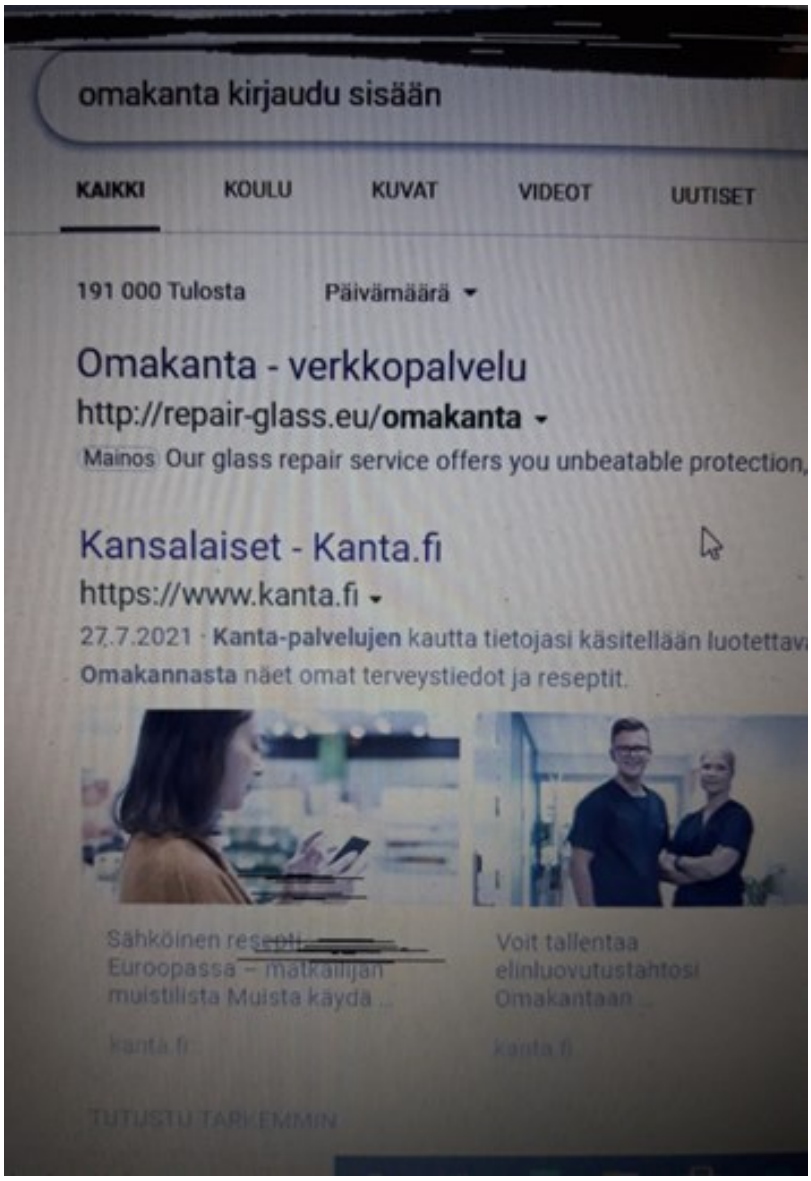
Begreppet MittKanta-bedrägeri är inte en etablerad term inom nätbedrägeri, men jag vill i denna undersökning använda termen för att beskriva nätfiske av uppgifter som utförts genom falska nätsidor med syfte att få tag på konfidentiella uppgifter som tillhör användare av Kanta.fi nätsidan och MittKanta-nättjänsten.

Kanta-tjänsterna är digitala tjänster avsedda för medborgare samt social- och hälsovården. I MittKanta-nättjänsten ser man sina egna hälso- och sjukvårdsuppgifter samt recept mm (Kanta, 2023.) Till MittKanta-nättjänsten loggar man in genom elektronisk identifiering med Suomi.fi identifieringstjänsten. Suomi.fi-identifikation är en gemensam tjänst för autentisering som används inom den finska offentliga förvaltningen för att säkerställa användarnas identitet när de loggar in i olika e-tjänster. Identifikationen används i alla tjänster där användarens identitet behöver verifieras. För identifieringen i tjänsten kan man använda finländska bankkoder, mobilcertifikat eller certifikatkort. (Suomi, 2022.) Det som är problematiskt med elektronisk identifiering är att identifieringsuppgifterna lätt råkar i kriminellas händer om man råkar logga in på en falsk nätsida.

Första nyheterna om MittKanta-bedrägerierna publicerades i september år 2021. Detta är baserat på sökresultaten som hittas med sökorden ”Omakanta huijaus” i Googles sökmotor. Det finns inte information om när exakt MittKanta-bedrägerierna har börjat, men på basis av de nyheterna som finns om ämnet på internet så kan man anta att bedrägerierna blivit aktuella under år 2021. Polisen publicerade 2.9.2021 nyheten: *Poliisi varoittaa Omakanta-huijauksesta – näin tunnistat kalasteluyrityksen*[5]*.* I nyheten står det att polisen fått kännedom om åtminstone ett fall i vilket en person lurades på pengar med hjälp av en annons i sökmotor som liknade MittKanta-tjänsten. Enligt nyheten sökte personen efter MittKanta-sidan på sökmotorn Bing och styrdes in på en falsk

[5] Polisen varnar om MittKanta-bedrägeriet – så här känner du igen nätfiske försöket (Min översättning)

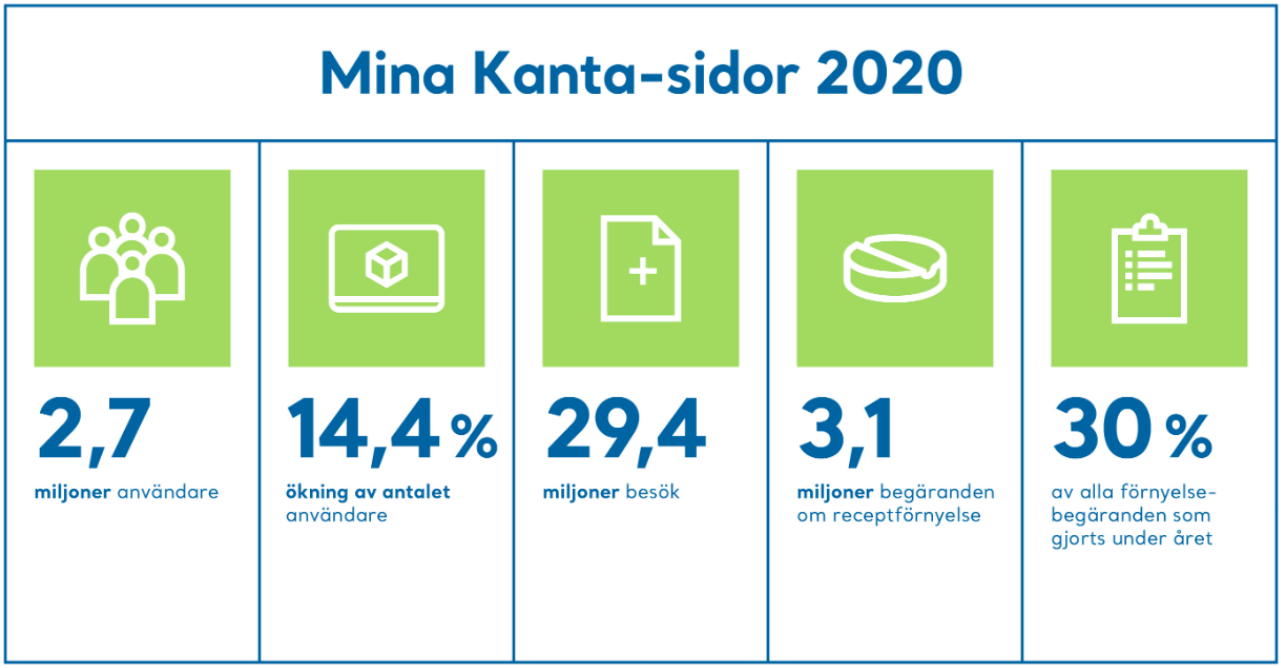
webbplats som samlade in personuppgifter och bankkoder. Offrets konto hade tömts på tusentals euro. I samband med nyheten publicerades en skärmdump (Figur 1) på resultaten i en sökmotor där man ser hur en bluffannons kan se ut:



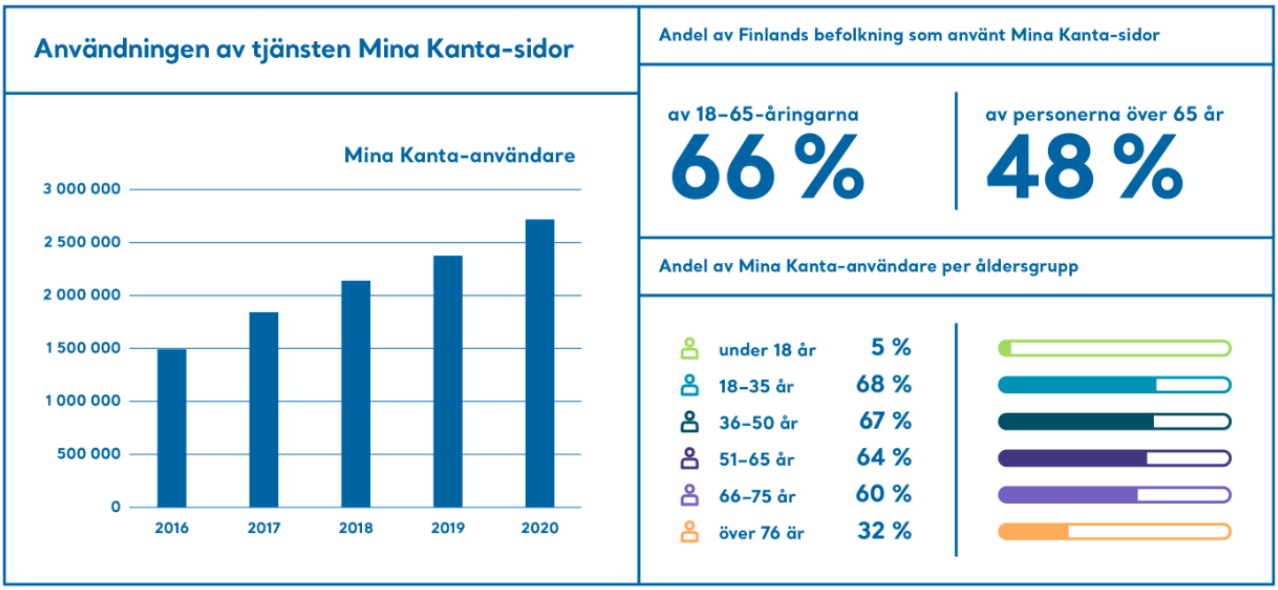
Figur 1: Sökmotorresultat för sökorden "omakanta kirjaudu sisään". (Poliisi, 2021.)

I figur 1 ser man två olika sökresultat. Det första är den falska annonsen som leder kunden till en webbplats där syftet är att samla in personuppgifter och bankuppgifter. Det andra sökresultatet är

den rätta adressen som man skall använda för att logga in på MittKanta-tjänsten: Kanta.fi. (Poliisi, 2021.)



Figur 2: Användningen av Mina Kanta-sidorna år 2020. (Kanta, 2021)



Figur 3: Användningen av Mina Kanta-sidorna år 2016–2020 samt åldersfördelningen år 2020. (Kanta, 2021)

I samband med meddelandet: *Coronaåret lyfte användningen av Mina Kanta-sidor till en ny nivå – se siffrorna för 2020* (Kanta, 22.4.2021), publicerades denna statistik som illustrerar användningen av Mina Kanta-sidorna år 2020 (Figur 2) samt antalet användare av tjänsten Mina Kanta-sidor år 2016–2020 och åldersfördelningen år 2020 (Figur 3). År 2020 användes tjänsten av 2,7 miljoner användare och sidorna besöktes mer än 29 miljoner gånger. I figur 3 ser man att nästan hälften av alla personer över 65 år använde tjänsten år 2020. I meddelandet (Kanta, 2021) betonas även att användningen av tjänsten ökat i samband med coronaepidemin. Denna statistik är väsentlig, eftersom den visar att en stor del människor använder tjänsten och användningen har ökat, vilket i sin tur ökar mängden potentiella offer för MittKanta-bedrägerierna. Tjänstens popularitet och det faktum att tjänsten använder stark autentisering för inloggning, kan vara bland de största orsakerna till att bedragare gjort falska sidor som liknar tjänsten. Det finns inte för tillfället någon mobilapplikation för tjänsten, vilket skulle vara säkrare med tanke på att man inte skulle behöva logga in till tjänsten via webbläsaren och därmed riskera att logga in på en falsk nätsida.

4.3 Råd för förebyggande av nätbedrägerier

I detta delkapitel redogörs för de förebyggande råden som ges av myndigheterna i Finland samt andra finska nätsidor. I delkapitlet har jag sammanställt och sammanfattat de förebyggande råden som ges på nätsidorna: Kyberturvallisuuskeskus.fi[6] och Suomi.fi[7].

4.3.1 Cybersäkerhetscentrets råd för förebyggande av nätbedrägerier

Cybersäkerhetscentret ger råd om hur man skyddar sig mot nätbedrägerier i anvisningen: *Så skyddar du dig mot nätbedrägerier.* (Kyberturvallisuuskeskus, 2020.) Anvisningen kan sammanfattas enligt följande lista:

[6] https://www.kyberturvallisuuskeskus.fi/sv

[7] https://www.suomi.fi/hemsidan

Hur man kan känna igen en nätbedragare:

1. Man får tomma löften. En överraskande kontakt innehåller något av följande: fantastiska och unika erbjudanden, lottovinster, arv, affärs- och placeringsmöjligheter eller möjligheter till lättförtjänta pengar.
2. Man hotas och utpressas, med påståenden om att bedragaren har känsligt material om en själv eller ens företag.
3. Man styrs in på en bluffsida, med en webbadress som är nästan identisk med den riktiga och innehåll som nästan ser äkta ut.
4. Man uppmanas att vidta åtgärder eller lämna ut uppgifter under förevändning av att det är bråttom eller en undantagssituation.

Hur man kan skydda sig mot bedrägerier:

1. Man borde inte lita blint på avsändaruppgifterna i ett e-postmeddelande.
2. Man borde inte lita på alla webbplatser och man borde granska villkoren för erbjudandet och webbplatsen.
3. Man borde kontrollera adressen i webbläsaren och man borde mata in adressen direkt i webbläsaren och granska att adressen är rätt skriven.
4. Man borde kontrollera att datatrafiken i webbläsaren är krypterad genom att kontrollera låsikonen och https:// i adressfältet.
5. Man borde byta hackade lösenord omedelbart och man borde ändra lösenord för andra tjänster om man har använt samma lösenord där.
6. Man borde använda olika lösenord för olika tjänster och man borde satsa på viktiga lösenord som används för att återställa lösenord som du glömt.

Vad man borde göra om man blir lurad:

1. Man borde göra en polisanmälan.
2. Man borde underrätta andra berörda parter, som en bank eller ett finansinstitut, om bedrägerier som utförts i deras namn.
3. Man borde förhindra ytterligare skador genom att byta lösenord och spärra kort.

4. Man borde söka hjälp på andra webbplatser, som Brottsofferjouren[8] och Konsumentförbundets bedrägeriinformation[9].
5. Man borde anmäla falska webbplatser för att förhindra att andra blir lurade. Detta kan göras på Cybersäkerhetscentrets sidor[10]
   (Kyberturvallisuuskeskus, 2020.)

4.3.2 Suomi.fi-nätsidans råd för förebyggande av nätbedrägerier

På Suomi.fi-nätsidan finns guiden; *Mina personuppgifter har stulits eller läckt ut* (Suomi, 2023), som ger råd om vad man ska göra om man misstänker att egna personuppgifter har kapats eller läckt ut. I guiden har det sammanställts fyra olika skeden som man ska gå igenom. De olika skeden i guiden (Suomi, 2023) kan sammanfattas enligt följande lista:

Man borde identifiera situationen:

- Om personuppgifter hamnar i fel händer så borde man vidta åtgärder omedelbart för att minimera eventuella ekonomiska skador. Man borde fokusera på att hantera en sak åt gången i stället för att göra allt samtidigt.
- Personuppgifter kan missbrukas på flera sätt, till exempel genom bedrägerier där någon gör inköp och skickar fakturan till en själv, obehörig användning av ens bank- och kreditkortsuppgifter, någon som utger sig för att vara en själv på e-post, Facebook eller andra webbtjänster, samt utpressning med stulna känsliga uppgifter såsom patientinformation.
- Om situationen blir överväldigande när man hanterar problemet, borde man söka samtalshjälp för att få stöd och hjälp att orka igenom processen.

[8] https://www.riku.fi/sv/

[9] https://www.kuluttajaliitto.fi/hankkeet/huijarit-kuriin/

[10] https://www.kyberturvallisuuskeskus.fi/sv/anmal

Vad man borde göra för att förhindra skador:

- Om ens uppgifter missbrukas, borde man omedelbart anmäla till den berörda organisationen och samla bevis. Man borde dokumentera händelser, ta skärmdumpar och spara kontoutdrag om pengar stulits. Polisen kommer att behöva dessa uppgifter för brottsutredningen**.**
- Om ens personuppgifter råkar i fel händer, borde man byta lösenord för e-post och andra nättjänster som man använder. Man borde även kontrollera att återställningsinställningar för e-post och konton inte har ändrats.
- Om man misstänker att man utsatts för brott som bedrägeri, dataintrång eller utpressning, borde man göra en brottsanmälan till polisen och inkludera insamlade bevis. Vid stöld av pengar från ens konton, eller hot mot ens hälsa eller liv, så ska man omedelbart göra en anmälan vid närmaste polisstation. I andra fall kan anmälan göras via polisens elektroniska ärendehanteringstjänst.

Nödvändiga förbud som man borde göra:

- Personuppgifter kan användas för identitetsstöld eller bedrägerier. Man borde förhindra missbruk genom att överväga att göra förbud, särskilt om personbeteckning eller adress blir tillgänglig till obehöriga.
- Man borde överväga kreditförbud som en avgiftsbelagd tjänst, som tillhandahålls av två företag: Suomen Asiakastieto och Bisnode. För att säkerställa ett omfattande skydd är det rekommenderat att införa kreditförbud hos båda företagen samtidigt.
- För att skydda ens integritet kan man införa förbud mot utlämnande av kontaktuppgifter från olika register. Detta förhindrar att obehöriga får tillgång till ens adress och kontaktinformation genom dessa tjänster.
- För att förhindra obehöriga flyttanmälningar bör man blockera sådana ändringar hos Myndigheten för digitalisering och befolkningsdatas befolkningsdatasystem samt Posti. Genom att blockera båda förhindrar man att någon kan göra en adressändring i ens namn.
- Genom att göra ett registreringsförbud hos Patent- och registerstyrelsen förhindrar man att brottslingar kan anmäla en som ansvarig person för ett företag, en förening

eller en stiftelse. Dock kan förbudet orsaka problem om man är företagare, till exempel som revisor.

Vad man borde göra efter den akuta situationen:

- Man borde anmäla kränkningar av informationssäkerheten till Traficoms Cybersäkerhetscenter när ens personuppgifter har stulits eller fiskats på webben, eller ens konto i en webbtjänst har hackats. Cybersäkerhetscentret utreder och förebygger sådana kränkningar med hjälp av anmälningar.
- Man borde ta hand om informationssäkerheten genom att använda stark eller tvåfaktorsautentisering i webbtjänster där det är möjligt, vara uppmärksam på lösenordens säkerhet och komma ihåg att myndigheter eller företag aldrig frågar efter ens lösenord.
- Man borde hantera ens uppgifter på webben genom att begränsa tillgänglig information om en själv, vara misstänksam vid kontakter som frågar efter personuppgifter, överväga vad man delar på webben, be sökmotorer radera uppgifter om en själv och be webbplatsadministratörer ta bort onödig information om en själv.
- Om ens personuppgifter stjäls, sprids eller används utan ens tillstånd kan man ha rätt till ersättning. Man borde bokföra uppkomna skador, ta reda på vem som är ansvarig för ersättning och kontrollera om ens försäkring täcker skador eller kostnader.
- Om man misstänker att ens egen eller ens familjs hälsa eller säkerhet är hotad kan man ansöka om spärrmarkering. När spärrmarkeringen är aktiverad kommer ens adress-, boningsort- och hemkommunsuppgifter endast att delas med myndigheter och inte lämnas ut ur befolkningsdatasystemet till andra.
- Personbeteckning kan bytas, men inte enbart på grund av att den har hamnat i händerna på utomstående. Man kan dock begära en ändring om tre villkor uppfylls: upprepat missbruk av personbeteckning, betydande ekonomiska eller andra olägenheter orsakade av missbruket, och att en ändring kan förhindra fortsatt missbruk. Man kan även begära att byta personbeteckning om ens hälsa eller säkerhet är utsatt för ett bestående hot.

  (Suomi, 2023.)

5 Hur nätbedrägerier framställs i media

I detta kapitel presenterar jag nyhetsartiklar och nätpublikationer i vilka nätbedrägerier som är förknippade med Kanta.fi-nätsidan och dess nättjänst MittKanta behandlas. Texterna behandlas i den ordningen som de blivit publicerade. Texterna finns som bilaga i denna undersökning.

Publikation 1: Artikel i Iltasanomat:

23.9.2021 publicerades artikeln: [11]*KRP varoittaa ovelasta Omakanta-huijauksesta – toimi näin suojautuaksesi*[12] (Huttunen, 2021). Huttunen (2021) skriver i artikeln att Centralkriminalpolisen på deras Twitter-konto har berättat att det förekommer falska nätsidor på internet som påminner MittKanta-tjänsten och med vilka man försöker fiska efter personers bankuppgifter.

Informationen som presenteras i artikeln baserar sig huvudsakligen på Centralkriminalpolisens cyberenhets Twitter-inlägg vilket ger artikeln en större grad av tillförlitlighet genom att hänvisa till information som en myndighet har publicerat om fenomenet. Huttunen (2021) har i artikeln även hänvisat till vad Kanta.fi-nätsidan meddelat om fenomenet och har placerat en länk i texten som leder till deras nätsida där de varnar om bedrägeriet. (Huttunen, 2021.)

I artikeln betonas vikten av att vara försiktig när man loggar in på elektroniska tjänster med sina bankuppgifter och det ges råd om att inte använda länkar som skickats via e-post eller som dykt upp i sökresultaten. I stället rekommenderas att användare lägger till rätt webbadress som ett bokmärke i webbläsaren. Artikeln syftar till att varna användare om bedrägerisidor och ger råd om hur man kan undvika att avslöja sina bankuppgifter och fokuserar främst på individuella åtgärder som kan tas för att hantera riskerna. Det nämns inte i artikeln vem som ligger bakom dessa falska sidor eller vem som är målgruppen för artikeln. Råden som ges i artikeln är i linje med de råden som behandlas i kapitel 4.3.1.

Artikeln är skriven på finska och är ganska kort samt ger inte alltför noggrann information om vad man skall vara aktsam för, men det förekommer ändå tillräckligt med information för att man blir

[11] https://www.is.fi/digitoday/tietoturva/art-2000008285667.html

[12] CKP varnar om ett listigt MittKanta-bedrägeri – gör så här för att skydda dig (Min översättning)

medveten om att det pågår bedrägeriförsök med hjälp av falska nätsidor som påminner MittKanta-tjänsten. I artikeln finns inte bilder som skulle visa hur de falska nätsidorna ser ut.

Publikation 2: Artikel i Yle

11.10.2021 publicerades artikeln: ***[13]****Useat suomalaiset ovat haksahtaneet Omakanta-huijaukseen – Kelan mukaan huijausmainoksia saatu poistettua netistä*[14] (Kuukkanen, 2021). Kort sammanfattat handlar artikeln om att ett flertal finländare blivit offer för nätbedrägeri genom att ha loggat in på en falsk nätsida som påminner om MittKanta-tjänsten som är upprätthållen av myndigheterna.

Huvudtemat i artikeln är MittKanta-bedrägeriet, som enligt Kuukkanen (2021) utförs av utländska kriminella ligor genom falska nätsidor och reklam för dessa nätsidor. Syftet med bedrägeriet är att avslöja personers bankuppgifter och stjäla pengar från deras konton. I artikeln nämns att användningen av MittKanta har ökat under coronapandemin, vilket kan ha bidragit till att göra tjänsten till ett attraktivt mål för bedragare. I artikeln nämns också att äldre och pensionärer är särskilt sårbara för sådana bedrägerier, men att personer i alla åldrar kan drabbas. Det ges flera råd för att skydda sig mot dessa bedrägerier, såsom att undvika att använda sökmotorer för att komma åt MittKanta och att vara försiktig med länkar som skickas via e-post eller SMS. Råden i artikeln är få, men relevanta, eftersom det betonas att man skall granska att webbadressen är korrekt, vilket även är ett av råden som framkommer i kapitel 4.3.1.

Diskursen kring MittKanta-bedrägeriet behandlar aspekter som internationella kriminella ligors inblandning och att vissa riskgrupper är mer sårbara för att bli lurade. I artikeln tas även fram vad som kan ligga som orsak bakom denna typ av bedrägeri. Det nämns att användningen av MittKanta-tjänsten har ökat i samband med coronapandemin, eftersom människor till exempel har hämtat intyg på coronavaccinationer från tjänsten.

Artikeln är skriven på finska och den är skriven på ett tydligt och informativt sätt. I artikeln används citat från en arbetstagare vid Folkpensionsanstalten och en polis, för att ge en trovärdig bild av

[13] https://yle.fi/a/3-12138550

[14] Flera finländare har fallit för MittKanta-bedrägeriet – enligt FPA har flera av bedrägeriannonserna blivit raderade från nätet (Min översättning)

situationen och förmedla deras råd om hur man kan undvika att bli utsatt för bedrägerier. I artikeln finns två bilder på Kanta-nätsidan, men det finns inte bilder på den falska nätsidan.

Publikation 3: Varning från Cybersäkerhetscentret

29.10.2021 publicerades varningen: *Bedragare kapar bankkoder i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn*[15] (Kyberturvallisuuskeskus, 2021). Texten är en varning från Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom om pågående bedrägerier i vilka bedragare kapar bankkoder i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn.

I texten nämns att bedragarna tidigare använt olika bankers namn för att utföra dessa bedrägerier, men att de nu verkar ha ändrat metoden och använder nu i stället Mina Kanta och Suomi.fi-tjänsternas namn. Det nämns inte noggrannare varför de ändrat på metoden eller vem som ligger bakom dessa bedrägerier. I texten beskrivs också att de falska sidorna är nästan identiska med de riktiga nätsidorna eller att det kan vara svårt att se skillnad på dem. Detta tyder på att bedrägerierna är sofistikerade och bedragarna är skickliga och investerar tid för att göra sina bedrägerier trovärdiga. I varningen finns det två bilder (se bilaga 3) som visar hur falska nätsidorna kan se ut och det påpekas att man ska läsa webbplatsens adress noggrant. Bilderna är dock på falska banknätsidor och inte på falska nätsidor som liknar Mina Kanta och Suomi.fi, vilka enligt varningen blivit aktiva.

Risker och konsekvenser för användarna betonas i texten, med fokus på allvarliga konsekvenser som identitetsstölder. I texten nämns att inloggningsuppgifter till nätbanken är värdefulla för brottslingarna, eftersom de även möjliggör stark autentisering. I slutet av varningen beskrivs olika förebyggande åtgärder för att hjälpa användare att skydda sig mot bedrägerier. Det nämns bland annat att man inte ska klicka på länkar till nätfiskemeddelanden och att man inte ska svara på dem.

I slutet av varningen nämns följande åtgärds- och begränsningsmöjligheter för denna typ av bedrägerier:

[15] https://www.kyberturvallisuuskeskus.fi/sv/bedragare-kapar-bankkoder-i-mina-kanta-tjanstens-och-suomifi-tjanstens-namn

- Man ska inte klicka på länkar till nätfiskemeddelanden och man ska inte svara på meddelanden.
- Man ska inte logga in på nätbanken eller tjänsten direkt via sökmotorresultat eller länkar som man fått via e-post eller textmeddelande.
- Om man blivit offer för ett betalningsmedelsbedrägeri som gjorts i bankens eller finansinstitutets namn, så ska man anmäla detta till finansinstitutet.
- Även om banker och företag vars namn används för bedrägerier inte är bakom bedrägerierna tar de gärna emot information om bedrägerier så att de kan varna andra kunder om dem.
- Därefter lönar det sig att man gör en brottsanmälan. Den kan man göra på nätet eller på den lokala polisstationen.
  (Kyberturvallisuuskeskus, 2021.)

Åtgärds- och begränsningsmöjligheterna är i linje med de råd som behandlas i kapitel 4.3.1. Råden som behandlas i kapitel 4.3.2 är även till vissa delar i linje med det som nämns i varningen. På basis av att informationen i varningen är i linje med råd från olika källor, så kan den anses vara relevant med tanke på förebyggande av nätbedrägerier.

Språket och stilen i varningen är formell och informativ, vilket passar syftet att informera allmänheten om bedrägerierna och hur man kan skydda sig mot dem. I varningen används korrekt och tydlig svenska och i den beskrivs detaljerat bedrägeriernas tekniker och risker. Det framgår också att bedragarna använder vårdad finska i sina bedrägerimeddelanden, vilket gör det svårare för användare att upptäcka nätfisket. Detta understryker hur viktigt det är att vara uppmärksam och följa de förebyggande råden som ges i texten.

Publikation 4: Artikel i Yle

24.1.2022 publicerades artikeln: *Kärleksbedrägerier, artiga samtalare och en telefon i tvättmaskinen – nätbedrägerierna blir allt vanligare* (Wikström, 2022). Artikeln handlar om att nätbedrägerier har ökat och om vad man kan göra för att undvika att bli lurad på nätet. Wikström (2022) har i artikeln återgett olika tips som polisen har publicerat i samband med ett pressmeddelande. I artikeln behandlas olika former av nätbedrägerier på en allmän nivå.

Tipsen som nämns i artikeln handlar om hur man kan skydda sig själv och sina närstående från bedragare som kontaktar en via telefon, sms, mejl eller sociala medier. I artikeln nämns tips av kriminalkommissarie Niina Eränen som ger exempel på vad man ska tänka på när man använder webbplatser som kräver inloggning eller nätbankskoder, och hon varnar också för artiga bedragare som försöker skapa förtroende för att sedan begära pengar eller personuppgifter.

Artikeln är informativ, med ett fokus på att ge råd och tips till läsaren för att undvika att bli lurad på nätet. Nätbedrägerierna behandlas på en allmän nivå. Språket är enkelt och lätt att förstå, vilket gör artikeln tillgänglig för en bred publik. Artikeln innehåller två källor, kriminalkommissarierna Niina Eränen och Janne Saari. Källorna används för att ge läsaren myndighetsråd för att förstärka budskapet om vikten av att vara uppmärksam på nätet.

I artikeln nämns även exempel på fall av nätbedrägerier. I det första exemplet behandlas kärleksbedrägeri och i det andra ett fall av nätfiske av uppgifter som utförts med hjälp av WhatsApp. Dessa exempel är effektiva i förmedlandet av artikeln budskap, eftersom det står att bedrägerier kan låta trovärdiga och att det är lätt att bli lurad, även för någon som är uppmärksam.

I artikeln betonas också att det är viktigt att be om hjälp om man har blivit lurad på nätet och anmäla händelsen till myndigheterna. Detta budskap är viktigt eftersom många människor kan känna skam eller skuld över att ha blivit lurade, vilket kan hindra dem från att söka hjälp. Genom att betona att det inte är offrets fel och att bedragarna är skickliga, kan artikeln hjälpa läsare att känna sig mindre ensamma och skuldbelagda.

Publikation 4: Meddelande från Kanta

29.3.2022 publicerades meddelandet: *Bedragare fiskar fortfarande efter bankkoder och personuppgifter i Mina Kanta-sidors namn* (Kanta, 2022). I meddelandet informeras det om att nätfiske av bankkoder och personuppgifter fortfarande fortsätter i Mina Kanta-sidors namn. Det nämns inte vem som skrivit meddelandet, men det publicerats i Kanta-sidans namn.

Meddelandet är uppdelat i två huvuddelar: I den första delen beskrivs de senaste nätfiskebedrägerierna som använder sig av Mina Kanta-sidors och FPA:s namn för att komma åt

personuppgifter och bankkoder, medan den i den andra delen ges råd om hur man kan undvika att falla offer för nätfiskebedrägerier och vad man ska göra om man har blivit utsatt för dem.

I meddelandet nämns att det fortfarande skickas meddelanden och länkar som leder till webbplatser som upprätthålls av brottslingar. I meddelandet nämns det inte noggrannare vem brottslingarna är och det visas inte heller hur deras webbplatser ser ut. Texten i meddelandet är skriven på svenska med en relativt enkel och tydlig språkstil. Språket är formellt och sakligt, med få uttryck för känslor eller åsikter. Texten innehåller många tekniska termer och uttryck som är specifika för datasäkerhet och nätfiske, vilket kräver att läsaren har en viss kunskap om ämnet. Stilen är också informativ, vilket tyder på att texten är avsedd att ge råd till läsarna för att förebygga dessa nätbedrägerier.

Texten ger en detaljerad beskrivning av problemet med nätfiskebedrägerier som utövas i Mina Kanta-sidors och FPA:s namn för att lura människor att lämna ut sina personuppgifter och bankkoder. Texten innehåller konkreta råd om hur man kan skydda sig mot nätfiske och vad man ska göra om man har blivit utsatt. Textens budskap är att människor måste vara mycket försiktiga när de loggar in på nätet och att de måste vara medvetna om de senaste nätfiskebedrägerierna för att undvika att falla offer för dem.

Textens syfte är att informera och utbilda människor om nätfiske och hur man kan skydda sig mot dem. Målgruppen för meddelandet specificeras inte, utan den är riktad åt allmänheten.

5.1 Sammanfattning av kapitlet och resultat

I de fem texterna behandlas nätbedrägerier kopplade till Kanta.fi och Mina Kanta-tjänsten samt andra former av nätbedrägerier på varierande sätt. Informationen i texterna tyder på att bedrägerierna är sofistikerade och utförs av skickliga bedragare, vilket innebär att användare måste vara uppmärksamma när de till exempel letar efter MittKanta-tjänsten via webbläsaren.

En av forskningsfrågorna i denna undersökning var att reda ut vilka råd som ges i media med tanke på förebyggande av nätbedrägerier och därigenom försöka bedöma om informationen är relevant. Råden som ges i texterna för att skydda sig mot nätbedrägerier inkluderar att vara försiktig med e-postmeddelanden och SMS som uppmanar mottagaren att ange sina bankuppgifter eller

personuppgifter och att vara uppmärksam på avsändarens e-postadress och att inte klicka på länkar i misstänksamma meddelanden. Dessutom rekommenderas det att användare sparar den korrekta webbadressen för Mina Kanta-sidor som ett bokmärke i sin webbläsare för att undvika att besöka falska webbsidor.

I de fem texterna ges råd på varierande nivå om nätbedrägerier, men det nämns konkreta råd i varje text. Då man jämför texterna med de råd som framgår i kapitlen 4.3.1 och 4.3.2 så kan man konstatera att råden står i linje med de råd som Cybersäkerhetscentret och Suomi.fi-nätsidan ger om förebyggande av nätbedrägerier. Det är dock värt att nämna att råden som ges i texterna huvudsakligen behandlar nätbedrägerier som utförs genom nätfiske av uppgifter och därmed är råden fokuserade på denna typ av nätbedrägeri.

Informationen i texterna är relevant för att förebygga nätbedrägerier, särskilt de som utförts i MittKanta-tjänstens namn genom nätfiske av uppgifter. Genom att presentera information om hur bedrägerier utförs, vilka metoder som används och hur man kan skydda sig, bidrar texterna till att öka medvetenheten om riskerna och hjälper användare att vidta försiktighetsåtgärder.

Texterna är skrivna på ett informativt och lättförståeligt språk, men det kan anses att de olika termerna som används skulle behöva förklaras mer djupgående, eftersom flera av begreppen kan vara svåra att förstå och det kan leda till att de som läser texterna kan bli osäkra på exakt vilka åtgärder de ska vidta. Det finns också en brist på bilder som skulle visa hur de falska nätsidorna ser ut.

I texterna betonas vikten av att be om hjälp och anmäla händelsen till myndigheterna om man har blivit lurad på nätet. Detta är viktigt eftersom många människor kan känna skam eller skuld över att ha blivit lurade, vilket kan hindra dem från att söka hjälp.

Sammanfattningsvis så kan man identifiera flera underliggande mönster i texterna som behandlar MittKanta-bedrägerier och nätbedrägerier. Jag har utifrån min egen analys av texterna identifierat följande underliggande mönster:

1. Fokus på individuella åtgärder: I texterna betonas vikten av att användare tar personligt ansvar för att skydda sig mot bedrägerier, genom att följa säkerhetsråd och

vara försiktiga när de använder nätbankstjänster eller andra elektroniska tjänster som kräver inloggning.

2. Myndighetsperspektiv: I texterna hänvisas det ofta till myndigheternas råd och varningar om bedrägerier, vilket ger dem en större grad av trovärdighet och auktoritet. Detta understryker också vikten av att samarbeta med och lita på myndigheterna i kampen mot nätbedrägerier.

3. Uppmärksamhet på sårbara grupper: I texterna kommer det fram att vissa grupper, såsom äldre och pensionärer, är mer sårbara för bedrägerier. Detta skapar en känsla av empati och solidaritet med de drabbade och betonar vikten av att skydda dessa grupper.

4. Internationella kriminella ligor: I texterna nämns att internationella kriminella ligor ofta ligger bakom nätbedrägerier, vilket understryker den gränsöverskridande och komplexa karaktären av detta problem. Det kan också skapa en känsla av oro och osäkerhet kring användning av nättjänster.

5. Corona-pandemins inverkan: I texterna tas det upp hur coronapandemin har bidragit till en ökad användning av elektroniska tjänster såsom MittKanta, vilket kan ha gjort dem mer attraktiva för bedragare. Detta visar på hur yttre omständigheter kan påverka säkerhetsrisker på nätet.

6. Skam och skuld: I vissa texter betonas vikten av att inte känna skam eller skuld över att ha blivit lurad, och att anmäla händelserna till myndigheterna. Detta hjälper till att avdramatisera situationen och uppmuntrar människor att söka hjälp om de har blivit offer för bedrägeri.

7. Fokus på förebyggande: I texterna ges råd och tips om hur man kan förebygga nätbedrägerier, vilket visar att förebyggande åtgärder anses vara viktiga för att hantera detta problem.

6 Sammanfattning och diskussion

I denna undersökning har jag undersökt nätbedrägerier som brottsfenomen genom att använda metoden diskursanalys för att analysera nätartiklar och andra nätpublikationer i vilka nätbedrägerier som sker i Finland behandlas. Gemensamma nämnaren i de texter som analyserades var att de handlade om nätbedrägerier och en viss metod av nätbedrägeri i vilken man använt falska sidor som påminner Kanta.fi-nätsidan och dess nättjänst MittKanta. Syftet med dessa falska sidor har varit att få tag på personers konfidentiella uppgifter, såsom nätbankskoder och personbeteckningar.

För att få svar på hur nätbedrägerier framställs i media så använde jag mig av följande forskningsfrågor:

1. Hurdana nätbedrägerier finns det och vilka av dem förekommer i Finland?
2. Hur beskrivs nätbedrägerier genom olika nyhetsartiklar och nätpublikationer samt hurdan är diskursen?
3. Hurdana råd förmedlas via media med tanke på förebyggande av nätbedrägerier och är informationen relevant?

I undersökningen förklarades olika typer av nätbedrägerier och de behandlas i kapitel 4. Materialet som användes i undersökningens analys var 5 texter från varierande källor på internet och dessa texter analyserades med hjälp av metoden diskursanalys. Metoden diskursanalys användes för att analysera hur nätbedrägerier framställs i media, genom att analysera språket i texterna.

Utifrån texterna som analyserades, så kan man dra den slutsatsen att bland annat nätfiske av uppgifter förekommer i Finland och det har utvecklats en metod för denna typ av nätbedrägeri genom att skapa falska nätsidor som liknar Kanta.fi-nätsidan och MittKanta-tjänsten. I texterna förklarades hur denna typ av nätbedrägeri fungerar.

Analysen av texterna i kapitel 5 visar att nätbedrägerier beskrivs på ett informativt och lättförståeligt sätt, men att det finns utrymme för mer detaljer och bilder. Diskursen i texterna inkluderade flera underliggande mönster, såsom fokus på individuella åtgärder, myndighetsperspektiv, uppmärksamhet på sårbara grupper, internationella kriminella ligor, coronapandemins inverkan, skam och skuld, samt förebyggande åtgärder.

I undersökningen kom jag fram till att informationen i texterna är relevant för att förebygga nätbedrägerier, särskilt de som är kopplade till den finska Kanta.fi-nätsidan och MittKanta-tjänsten. Genom att förmedla information om bedrägeriernas metoder och hur man kan skydda sig bidrar texterna till ökad medvetenhet och försiktighet bland användare. Råden som ges i texterna är i linje med råd som ges av myndigheterna med tanke på förebyggande av nätbedrägerier.

Jag anser att resultaten i undersökningen är tillräckligt reliabla och valida med tanke på den metod som jag använt mig av för att analysera materialet. Fastän diskursanalys huvudsakligen bygger på forskarens egen tolkning av materialet så anser jag att andra forskare kunde få liknande resultat. Jag anser att de resultat som jag kommit fram till är tillförlitliga, eftersom jag har strävat till att behandla texterna så objektivt som möjligt och också tänkt på min egen position i förhållande till diskurserna som förekommer i texterna och hur detta kan påverka tolkningen av materialet. Jag har bifogat de texter som jag analyserat i denna undersökning som bilaga för att den som läser denna undersökning ska möjlighet att ta del av de ursprungliga texterna.

Detta är första lärdomsprovet som jag har gjort och jag anser att det har varit utmanande, men även lärorikt, eftersom undersökningen har krävt mycket eget tankearbete och analysering med tanke på metoden som jag använt.

Jag nämnde i inledningen att en av orsakerna till att jag valde att undersöka nätbedrägerier var på grund av att det inte gjorts undersökningar inom ämnet på den svenskspråkiga utbildningen i Polisyrkeshögskolan. Jag hoppas denna undersökning kan inspirera studerande att forska vidare inom nätbedrägerier, men även allmänt inom cyberbrottslighet, eftersom det utan tvekan kommer att bli mer aktuellt inom polisens arbete i samband med teknologiutvecklingen.

Möjligheterna för vidare forskning inom cyberbrottslighet är oändliga. Med tanke på att det i texter som jag analyserade nämndes att coronapandemin kunde ha haft en inverkan på nätbedrägerier har ökat så kunde man till exempel göra en statistisk analys av mängden nätbedrägerier som förekommit i Finland under de senaste 5 åren och hur coronapandemin möjligen påverkat mängden nätbedrägerier. Med tanke på utbildning inom cyberbrottslighet så kunde man undersöka och jämföra hur cyberbrottslighetsutbildningen skiljer sig mellan polisutbildningen i Finland och Sverige/Norge och därmed försöka hitta förbättringsförslag för utbildningen i Finland.

REFERENSER

Asikainen, Oscar. (2022) *Polisen och allmänna sammankomster – Diskursanalytisk studie om på vilket sätt polisen framställs i traditionell media när det gäller demonstrationer.* Tammerfors: Polisyrkeshögskolan. Lärdomsprov.

Feijes A. & Thornberg R. (2019) *Handbok i kvalitativanalys analys* (3 uppl.) Liber.

Finanssiala ry (7.7.2022). *Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua.* Tillgänglig: https://www.finanssiala.fi/uutiset/varo-varmista-ja-varoita-nettihuijaukset-ja-tietojenkalastelu-muuttavat-muotoaan-mutta-niilta-on-mahdollista-suojautua/. (Hämtad 3.1.2023)

Finlex. *Strafflag.* Finlex (19.12.1889/39). Tillgänglig: https://www.finlex.fi/sv/laki/ajantasa/1889/18890039001. (Hämtad 24.7.2022).

F-Secure. *Vad är nätfiske?* Tillgänglig: https://www.f-secure.com/se-sv/articles/what-is-phishing. (Hämtad 2.2.2023.)

F-Secure. *Vad är smishing?* Tillgänglig: https://www.f-secure.com/se-sv/articles/what-is-smishing. (Hämtad 2.2.2023.)

F-Secure. Vad är vishing? Tillgänglig: https://www.f-secure.com/se-sv/articles/what-is-vishing. (Hämtad 2.2.2023.)

Haasio, Ari (2017). *Verkkorikokset.* Vantaa: Avain.

Happonen, Päivi (11.7.2020). *Salaperäinen boksi, satoja viestejä ja kyyneleitä: "Oli kohtaloni, että avasin sen viestin" – Aino menetti rakkaushuijarille 90 000 euroa.* Tillgänglig: https://yle.fi/a/3-11430085. (Hämtad 25.8.2022)

Huttunen, Otso (23.9.2021). *KRP varoittaa ovelasta Omakanta-huijauksesta – toimi näin suojautuaksesi.* Tillgänglig: https://www.is.fi/digitoday/tietoturva/art-2000008285667.html. (Hämtad 24.11.2022)

Kanta (2023). *Vad är Kanta-tjänsterna?* Tillgänglig: https://www.kanta.fi/sv/vad-ar-kanta-tjansterna. (Hämtad 12.2.2023)

Kanta (22.4.2021). Coronaåret lyfte användningen av Mina Kanta-sidor till en ny nivå – se siffrorna för 2020. Tillgänglig: https://www.kanta.fi/sv/meddelande/-/asset_publisher/cf6QCnduV1x6/content/koronavuosi-nosti-omakannan-k-c3-a4yt-c3-b6n-uudelle-tasolle-katso-vuoden-2020-luvut. (Hämtad 5.1.2023)

Kanta (23.9.2022). *Bedragare fiskar fortfarande efter bankkoder och personuppgifter i Mina Kanta-sidors namn.* https://www.kanta.fi/sv/meddelande/-/asset_publisher/cf6QCnduV1x6/content/omakannan-nimissa-kalastellaan-yha-pankkitunnuksia-ja-henkilotietoja. (Hämtad 24.7.2022)

Kela. *Brottslingar fiskar efter finländarnas bankkoder - tips för säker användning av tjänster.* Tillgänglig: https://www.kela.fi/web/sv/aktuellt-privatpersoner/-/asset_publisher/M6wYRe4QRiL1/content/brottslingar-fiskar-efter-finlandarnas-bankkoder-tips-for-saker-anvandning-av-tjanster. (Hämtad 9.3.2022.)

Kortelainen, Hannu (8.9.2020). *Rakkaushuijaus: Tästä se yleensä lähtee*. Tillgänglig: https://poliisi.fi/blogi/-/blogs/rakkaushuijaus-tasta-se-yleensa-lahtee. (Hämtad 7.8.2022).

Kuukkanen, Tatu (11.10.2021). *Useat suomalaiset ovat haksahtaneet Omakanta-huijaukseen – Kelan mukaan huijausmainoksia saatu poistettua netistä.* Tillgänglig*:* https://yle.fi/uutiset/3-12138550. (Hämtad 24.10.2022)

Kyberturvallisuuskeskus. *Bedragare kapar bankkoder i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn.* Tillgänglig: https://www.kyberturvallisuuskeskus.fi/sv/bedragare-kapar-bankkoder-i-mina-kanta-tjanstens-och-suomifi-tjanstens-namn. (Hämtad 20.11.2023)

Kyberturvallisuuskeskus (13.10.2020). *Så skyddar du dig mot nätbedrägerier.* Anvisning. Tillgänglig: https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-skyddar-du-dig-mot-natbedragerier. (Hämtad 13.4.2023)

Larsen, Ann Kristin (2018) *Metod helt enkelt: en introduktion till samhällsvetenskaplig metod.* 2 uppl. Gleerups utbildning AB.

Lehtonen, Annina (2016) *Nettipetosten kasvu 2010-luvulla: Nettipetokset selityksenä petosten kokonaismäärän kasvulle?* Tammerfors: Polisyrkeshögskolan. Lärdomsprov.

Minilex (2022). *Petos vai maksuvälinepetos.* Tillgänglig: https://www.minilex.fi/a/petos-vai-maksuv%C3%A4linepetos. (Hämtad 24.7.2022.)

Nationalencyklopedin, *bedrägeri.* Tillgänglig: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/bedr%C3%A4geri. (Hämtad 7.3.2023.)

Nationalencyklopedin, *hermeneutik.* Tillgänglig: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/hermeneutik. (Hämtad 26.2.2023.)

Nationalencyklopedin, *massmedier*. Tillgänglig: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/massmedier. (Hämtad 7.3.2023.)

Nationalencyklopedin, *media.* Tillgänglig: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/media. (Hämtad 7.3.2023)

Nationalencyklopedin, *phishing*. Tillgänglig: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/phishing. (Hämtad 7.3.2023)

Patel, R., Davidson, B. (2011). *Forskningsmetodikens grunder. Att planera, genomföra och rapportera en undersökning. (4 uppl.).* Studentlitteratur AB. Lund.

Poliisi (2023). *Bedrägeribrott.* Tillgänglig: https://poliisi.fi/sv/bedrageribrott. (Hämtad 10.1.2023)

Poliisi (2023). *Dataintrång.* Tillgänglig: https://poliisi.fi/sv/dataintrang. (Hämtad 10.1.2023)

Poliisi (2.9.2021). *Poliisi varoittaa Omakanta-huijauksesta – näin tunnistat kalasteluyrityksen.* Tillgänglig: https://poliisi.fi/-/poliisi-varoittaa-omakanta-huijauksesta-nain-tunnistat-kalasteluyrityksen. (Hämtad 16.12.2022)

Riku (2023). *Kärleksbedrägerier på nätet.* Tillgänglig: https://www.riku.fi/sv/olika-brott/karleksbedragerier-pa-natet/. (Hämtad 11.1.2023.)

Skoglund, Crister (2012) *Hermeneutik i praktiken. En kortfattad sammanfattning av hur en hermeneutisk forskningsprocess kan gå till*. Tillgänglig: http://doczz.net/doc/6926981/hermeneutik-i-praktiken.pdf. (Hämtad 27.2.2023)

Somerkallio, Aki & Takkinen, Mari. (2018) *Kyberrikollisuus ihmisen arjessa*. Tammerfors: Polisyrkeshögskolan. Lärdomsprov.

Suomi (1.11.2022). *Vad är Suomi.fi-identifikation?* Tillgänglig: https://www.suomi.fi/anvisningar-och-stod/identifikation/vad-ar-suomifi-identifikation. (Hämtad 13.1.2023)

Suomi (2023). *Mina personuppgifter har stulits eller läckt ut.* Tillgänglig: https://www.suomi.fi/guider/informationslacka/skeden. (Hämtad 12.4.2023)

Svensson, Peter (2019). *Diskursanalys*. Studentlitterattur AB. Lund.

Wikström, Malin (24.01.2022). *Kärleksbedrägerier, artiga samtalare och en telefon i tvättmaskinen – nätbedrägerierna blir allt vanligare.* Tillgänglig: https://svenska.yle.fi/a/7-10011923. (Hämtad 24.7.2022)

Yle (28.10.2020). *Dataintrånget mot Vastaamo: Det här har hänt och det här vet vi nu*. Tillgänglig: https://svenska.yle.fi/a/7-1496439. (Hämtad 25.7.2022)

BILAGOR

BILAGA 1

KRP varoittaa ovelasta Omakanta-huijauksesta – toimi näin suojautuaksesi

Poliisi kehottaa noudattamaan varovaisuutta pankkitunnuksilla sähköiseen palveluun kirjauduttaessa.

JAA

Omakanta-palvelun kautta pääsee tarkastelemaan omia terveystietojaan. KUVA: MARTTI KAINULAINEN / LEHTIKUVA

Otso Huttunen

23.9.2021 21:15 | Päivitetty 23.9.2021 22:13

VERKKOON on ilmestynyt Omakanta-terveystietopalvelua muistuttavia valesivustoja, joiden avulla yritetään kalastella pankkitunnuksia, keskusrikospoliisi (KRP) kertoo Twitterissä.

Huijaussivustot saattavat KRP:n mukaan näkyä hakukoneen tuloksissa oikeaa Omakanta-sivustoa ylempänä. Poliisi kehottaa varovaisuuteen kirjauduttaessa pankkitunnuksilla sähköiseen palveluun.

KRP:n kyberrikosten torjuntakeskus ohjeistaa ihmisiä olemaan kirjautumatta sähköisiin palveluihin saatujen linkkien tai hakukoneiden hakutulosten kautta.

Palveluiden oikeat osoitteet kannattaa lisätä selaimen suosikkeihin, ja ilmiöstä on hyvä muistuttaa myös läheisiä. Oikea Omakannan osoite on kanta.fi/omakanta.

MYÖS Kanta-palvelut varoittaa liikkeellä olevasta huijauksesta.

– Tietoturvasyistä arkaluonteisia tietoja, kuten henkilötunnusta, ei pidä koskaan lähettää sähköpostitse. Kanta-palvelut tai Kela ei koskaan kysy niitä sähköpostilla tai tekstiviestillä, tiedote muistuttaa.

Mikäli on jo vahingossa päätynyt epäilyttävälle sivustolle tai saanut kirjautumista pyytävän tekstiviestin, kehottaa Kanta-palvelut toimimaan seuraavasti:

1. Älä vastaa viestiin tai syötä tietojasi vaadittuihin kenttiin.

2. Älä klikkaa viestissä olevia linkkejä.

3. Jos epäilet, että luottokorttitietosi tai pankkitunnuksesi ovat joutuneet vääriin käsiin, ota yhteyttä pankkisi asiakaspalveluun.

KRP kertoi aiemmin, että poliisiin on perustettu valtakunnallinen petosrikollisuuden torjuntaan keskittyvä tutkintaryhmä. Päätös liittyy kevään ja kesän aikana havaittuun rikosvyyhtiin, jossa verkkorikolliset kalastelevat pankkitunnuksia. Teot ovat kohdistuneet useaan suomalaiseen pankkiin ja niiden asiakkaisiin.

Kokonaisuudessa on tämän vuoden aikana kirjattu noin 700 rikosilmoitusta. Rikosvahingon määrä on lähes seitsemän miljoonaa euroa.

Uuden tutkintaryhmän pääasiallisina tavoitteina on pankkitunnuksien kalasteluun liittyvän rikoskokonaisuuden epäillyn tekijän selvittäminen sekä lisävahingon syntymisen estäminen.

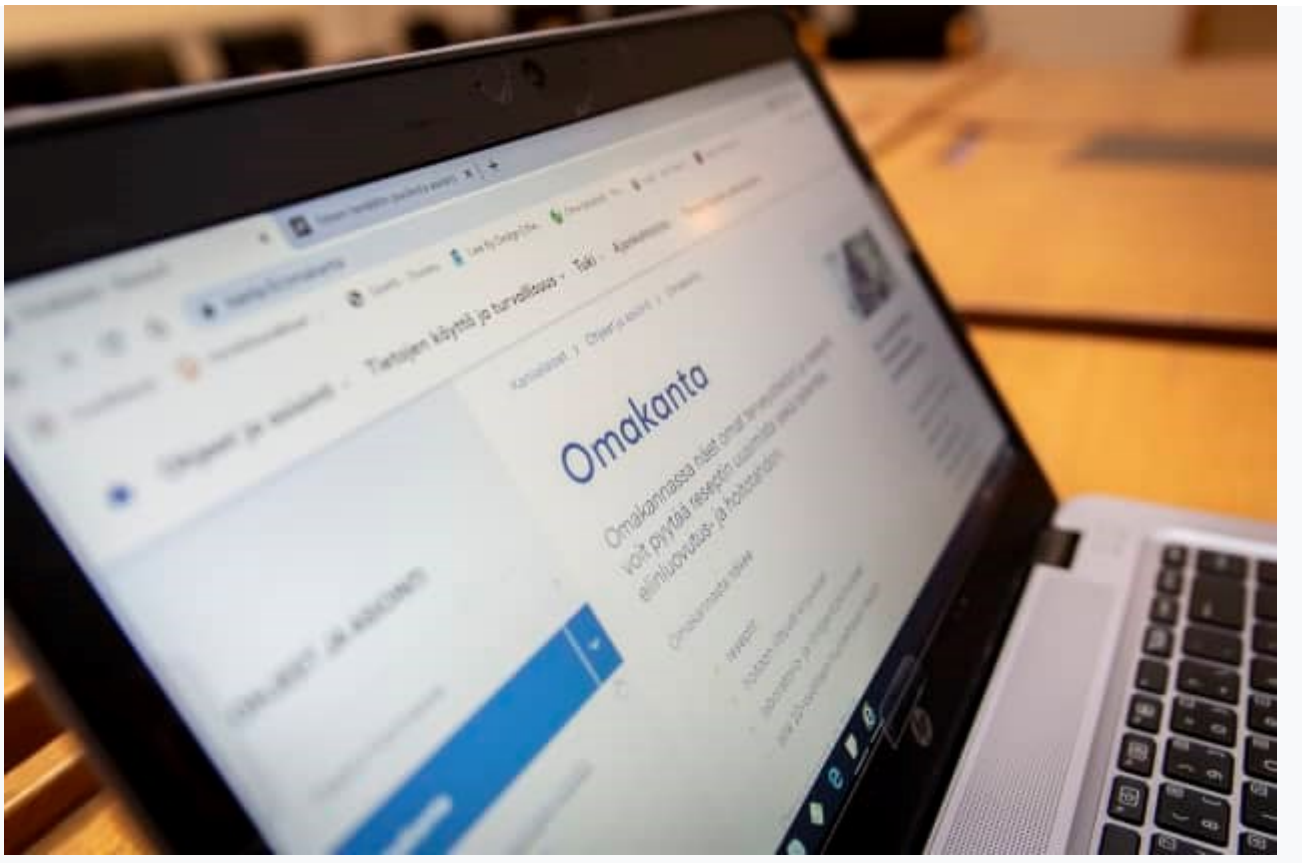
LUE LISÄÄ KIRJOITTAJALTA

Otso Huttunen

BILAGA 2

Useat suomalaiset ovat haksahtaneet Omakanta-huijaukseen – Kelan mukaan huijausmainoksia saatu poistettua netistä

Omakanta-sivusto joutui huijauksen uhriksi syyskuussa. Ulkomaiset rikollisliigat avasivat Omakantaa muistuttavan huijaussivuston ja kalastelivat sen kautta rahaa. Nyt huijaussivustojen mainoksia on saatu poistettua hakukoneista, Kelasta vakuutetaan.



Omakanta -sivuston käyttö on lisääntynyt korona-aikana, ja rikolliset ovat huomanneet tilaisuuden huijaukseen. Arkistokuva. Kuva: Ilkka Klemola / Yle

TATU KUUKKANEN

11.10.2021•Päivitetty 12.10.2021

Useat suomalaiset ovat joutuneet kuluvana syksynä uudenlaisten verkkohuijausten uhriksi. Ulkomaisten rikollisliigojen pyörittämässä huijauksessa ihmisiä on houkuteltu valesivustolle, joka muistuttaa viranomaisten ylläpitämää Omakanta-terveystietopalvelua.

Kun netin käyttäjä on kirjoittanut internetselaimen hakukenttään Omakanta, ensimmäiseksi linkiksi on noussut oikean Omakannan sijaan Omakantaa ulkoisesti muistuttavan huijaussivuston mainos ja sitä kautta henkilö on päätynyt rikollisten huijaussivustolle.

Kun henkilö on sitten kirjautunut huijaussivustolle verkkopankkitunnuksillaan, rikolliset ovat saaneet hänen pankkitunnuksensa haltuun ja sen avulla tyhjentäneet kaikki rahat pankkitililtä. Omakantaan, kuten muihinkin viranomaispalveluihin, kirjaudutaan pankkitunnuksilla, eli niin sanotun vahvan tunnistautumisen avulla.

Rikostarkastaja **Jukkapekka Risu** Helsingin poliisin kyberrikoksiin keskittyvästä ryhmästä kertoo, että aiemmin vastaavia valesivustohuijauksia on tehty esimerkiksi pankkien nimissä. Koska pankit ovat viime aikoina aktiivisesti varoitelleet huijauksista, rikolliset ovat keksineet uuden tavan huijata Omakannan avulla.
KRP on perustanut syyskuussa (siirryt toiseen palveluun) pankkihuijausten takia oman valtakunnallisen tutkintaryhmän, johon on kerätty edustajia kaikista poliisilaitoksista. Omakantaan liittyviä rikoksia tutkitaan Helsingin poliisin kyberrikosryhmässä ja useissa Suomen poliisilaitoksissa. Omakanta-huijauksessa rikolliset ovat tiettävästi saaneet valesivuston mainoksen hakutulosten kärkeen nimenomaan Microsoftin Bing-hakukoneessa. Monet ihmiset menevät erilaisiin nettipalveluihin juuri hakukoneita käyttämällä.

Varttuneempi väestö riskiryhmää huijauksille, mutta kuka tahansa voi mennä vipuun

Rikostarkastaja Jukkapekka Risu Helsingin poliisista arvioi, että esimerkiksi vanhemmat ihmiset eivät välttämättä ymmärrä, mikä on internetselaimen hakukone tai mitä eroa on Microsoftin tai Googlen hakukoneella, ja he ovat siksi riskiryhmää huijauksille.

Kelan palvelutoiminnan päällikkö **Outi Lehtokari** arvioi, että Omakantaan liittyviin huijauksiin ovat tiettävästi päätyneet antamaan tietojaan kaikenikäiset ihmiset.
Miksi juuri Omakanta? Risun mukaan luultavasti syynä on se, että Omakannan suosio on nyt noussut koronan aikana, kun ihmiset ovat hakeneet sieltä esimerkiksi todistuksia koronarokotuksista.

Kelan Lehtokari vahvistaa poliisin arvion. Omakannan käyttäjämäärät ovat peräti kaksinkertaistuneet syyskuussa.

Ennen koronaa Omakantaa käytti noin 700 000 eri henkilöä kuukaudessa ja viime kuussa 1,4 miljoonaa eri henkilöä. Sama on käynyt kirjautumisille. Ennen koronaa Omakannan kirjautumisia oli noin 1,5 miljoonaa kuukausittain ja nyt 3 miljoonaa kuukaudessa.

Poliisin mukaan huijaussivuston taustalla on kansainvälinen rikollisuus. Kuva: Ilkka Klemola / Yle

Tekijöinä ulkomaiset ammattirikolliset

Helsingin poliisissa kyberrikosten tutkinnanjohtajana työskentelevä Risu kertoo, että tämänkin huijauksen taustalla ovat ulkomaiset ammattimaiset rikollisliigat.

– Kun henkilö antaa pankkitunnuksensa rikollisten käsiin, rahat katoavat tililtä usein välittömästi ja ne siirretään ympäri Eurooppaa, hän sanoo.

Poliisi kertoi syyskuun alussa ensimmäistä kertaa Omakanta-huijauksista. Monet huijatuista ovat ikäihmisiä ja eläkeläisiä, mutta joukossa on kaikenikäisiä uhreja.

Jotta huijaukselta voi välttyä, Omakantaan mennessä ei kannata käyttää hakukoneita, vaan kirjoittaa selaimen osoitekenttään oikea osoite: kanta.fi.

– Toinen ohje on, että sähköisiin palveluihin ei kannata kirjautua ikinä sähköpostilla tai tekstiviestillä saatujen linkkien kautta, sillä ne ovat usein huijauksia. Pankit tai terveydenhuolto eivät lähetä kirjautumislinkkejä koskaan sähköisesti.

Rikostarkastaja Jukkapekka Risu Helsingin poliisista muistuttaa, että jos rikolliset saavat henkilön pankkitiedot käsiinsä, ne voivat tilin tyhjennyksen lisäksi tehdä monenlaista ikävää sähköistä tunnistusta käyttämällä, kuten ostaa netistä tavaraa henkilön nimiin tai nostaa pikavippejä.

Kela: Huijaussivustojen mainokset on poistettu hakukoneista

Kelan palvelutoiminnan päällikkö Outi Lehtokari kertoo, että suomalaisviranomaiset, kuten Kela, KRP ja Kyberturvallisuuskeskus ovat onnistuneet poistamaan Omakantaan liittyvien huijaussivustojen mainosten näkymisen internetin hakukoneissa ainakin toistaiseksi yhteistyössä hakukoneita operoivien Googlen ja Microsoftin kanssa.

– Enää valesivustoille ei pitäisi päätyä, jos yrittää mennä Omakantaan.

Lehtokari arvioi, että huijaussivusto ja sen mainokset ovat olleet uskottavia. Hänen mukaansa oikea tapa suojautua vastaavilta huijauksilta on välttää hakukoneita, kuten Googlea tai Bingiä, ja mennä Omakantaan kirjoittamalla kanta.fi selaimen osoitepalkkiin.

Lehtokari ei tiedä, onko huijaussivusto poistunut netistä kokonaan. Varmaan kuitenkin on, että huijaussivuston mainokset on onnistuttu poistamaan hakukoneista.

Omakanta on ollut käytössä 11 vuotta. Tämä on ensimmäinen kerta, kun järjestelmä on ollut yhdistettynä huijaukseen.

Lehtokari vinkkaa, että internetselaimen sivuhistoria kannattaa tyhjentää ja kirjautua ulos aina, kun lopettaa Omakannan käytön.

– Samat ohjeet pätevät kuin pankkiasiointiin. Huijauksista kannattaa ilmoittaa myös lähiomaisille, hän sanoo.

Juttua tarkennettu 12.10. kello 11.00 Jutussa kerrottiin aiemmin huijaussivustojen poistamisesta. Tarkennettu, että puhutaan huijaissivustojen mainosten poistamisesta.

BILAGA 3

Kyberturvallisuuskeskus

VARNING 3/2021

Bedragare kapar bankkoder i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn

Publicerad 29.10.2021

Bedragare försöker stjäla användarnas bankkoder i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn via förfalskade länkar i e-postmeddelanden. Om du använder tjänsten med en webbläsare, logga alltid in på tjänsten genom att skriva tjänstens hela adress i webbläsarens adressfält. Du undviker nätfiske efter bankkoder också genom att använda en mobilapplikation.

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom har under de senaste dagarna fått anmälningar om bedrägerimeddelanden som ser äkta ut. Med meddelanden försöker kriminella få tag på användarens bankkoder. Bedrägerimeddelanden skickas nu i Mina Kanta-tjänstens och Suomi.fi-tjänstens namn.

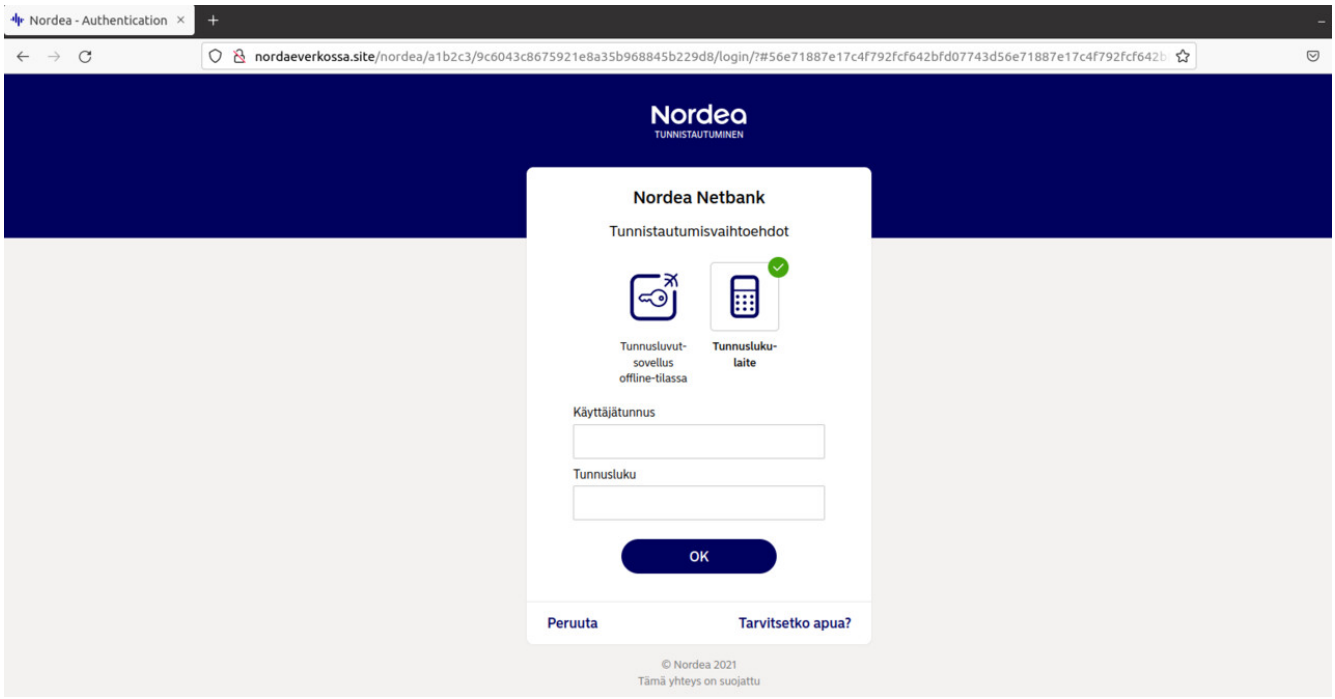
Bedrägerier där man försöker stjäla bankkoder har pågått under flera veckor. Bedragarna har agerat i bankers eller allmänt kända tjänsters namn.

Nätfiske efter bankkoder har redan pågått i två veckor

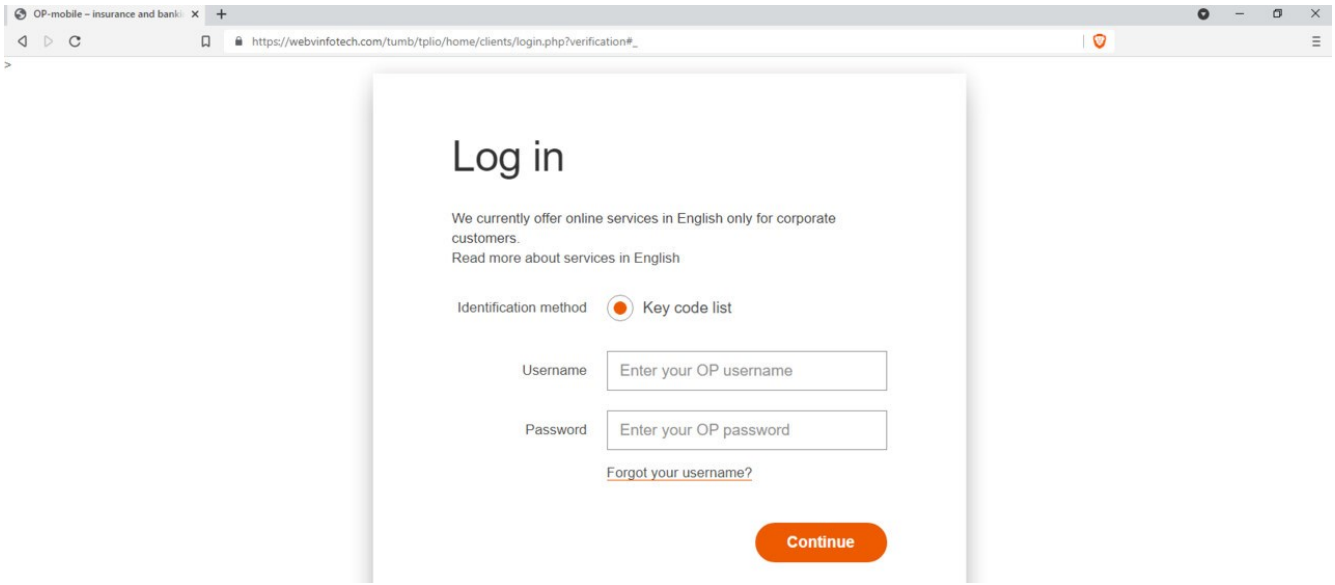
Denna nätfiskekampanj har samma särdrag som det nätfiske som vi informerade om tidigare. De använda meddelandetyperna och verksamhetsmodellerna verkar vara samma. Det ser ut som om bedragarna har bytt ut bankernas namn mot ovan nämnda Mina Kanta och Suomi.fi-tjänster.

Språket i meddelandena är bra och det framgår inte direkt att det skulle vara fråga om nätfiske. Om läsaren klickar på länken i meddelandet hamnar hen till en trovärdig falskwebbplats. De falska

sidorna verkar vara identiska med de genuina sidorna eller sidorna är så pass likadana att det är svårt att se skillnaden mellan den genuina och den falska webbsidan.



I nätfiskesyfte registrerar bedragarna domännamn som ser nästan likadana ut och med nästan samma namn som de ursprungliga domännamnen (till exempel nordea.fi vs. noreda.fi). Läs webbplatsens adress noggrant.



Ge inte dina uppgifter på webbsidor om du inte vet om de är äkta

Målgrupp för varningen

Brottslingarna försöker komma över personers bankkoder. Inloggningsuppgifterna till nätbanken är värdefulla för brottslingar därför att inloggningsuppgifterna kan användas förutom för att stjäla pengar också för stark autentisering. Om autentiseringsverktygen hamnar i fel händer kan det leda till exempel till identitetsstölder.

Tjänster eller banker i vilkas namn man gör bedrägerier har ingenting att göra med själva bedrägerierna trots att deras namn utnyttjas i meddelanden.

Bedrägerimeddelandena är bra finska

I Suomi.fi-meddelanden påstås det att ett viktigt dokument har kommit till Suomi.fi-tjänsten. I meddelandet uppmanas mottagaren att identifiera sig så att mottagaren ska kunna läsa dokumentet och skicka meddelanden till myndigheter i framtiden. Nätfiskesidan Suomi.fi är mycket bra gjord och är skriven på ganska felfri finska.

I Mina Kanta-sidors namn har bedragarna skickat e-postmeddelanden som uppmanar användare att logga in via länken i meddelandet. I meddelandena pratas det också om covid-19-certifikatet och om coronavaccinationsintyget. Trots sådana meddelanden bör man alltid logga in på Mina Kanta via adressen kanta.fi.

Nätfiske gäller i sig inte de tjänster som nämns i meddelandet utan brottslingar utnyttjar bekanta och offentliga tjänsters namn för att locka offer att ge sina uppgifter.
Hotet med tanke på bekanta tjänster är skada för anseendet när tjänsters namn används för nätfiske.

Åtgärds- och begränsningsmöjligheter

- Klicka inte på länkar till nätfiskemeddelanden och svara inte på meddelanden.
- Logga inte in på nätbanken eller tjänsten direkt via sökmotorresultat eller länkar som du fått via e-post eller textmeddelande.
- Om du blivit offer för ett betalningsmedelsbedrägeri som gjorts i bankens eller finansinstitutets namn, anmäl om detta också till finansinstitutet.
- Även om banker och företag vars namn används för bedrägerier inte är bakom bedrägerierna tar de gärna emot information om bedrägerier så att de kan varna andra kunder om dem.
- Därefter lönar det sig att göra en brottsanmälan. Den kan du göra på nätet eller på den lokala polisstationen.

BILAGA 4

Kärleksbedrägerier, artiga samtalare och en telefon i tvättmaskinen – nätbedrägerierna blir allt vanligare

Publicerad 24.01.2022 12:03.

Bild: imago stock&people/ All Over Press

Malin Wikström

Nätbedrägerierna har fortsatt att öka under de senaste åren, och polisen påminner därför om vad du kan göra för att slippa bli lurad på nätet.

Om du blir uppringd, får ett sms, ett mejl eller blir kontaktad via sociala medier av en okänd person ska du vara uppmärksam. Polisen i västra Nyland ger i ett pressmeddelande tips om vad du kan gör för att undvika att du blir lurad. Först och främst ska du fråga dig själv varför den här personen hör av sig till just dig.

Om du har en äldre närstående som inte nås av myndigheternas varningar i medierna eller på sociala medier ska du hjälpa den här personen.

Kriminalkommissarie Niina Eränen ger några tips på vad det lönar sig att fundera på:

-Lämna aldrig ut nätbankskoderna per telefon, oberoende av vem som frågar.
-Klicka inte på länkar i mejl eller textmeddelanden. Om du är tvungen att kolla upp något, till exempel läsa användarvillkor eller följa upp var ett paket finns, gör det på företagets egna webbsidor.
-När du använder en webbplats som kräver inloggning eller nätbankskoder, så som exempelvis FPA, banktjänster, Posti eller Mina kanta-sidorna, ska du inte använda en sökmotor. Skriv istället in den fullständiga url:adressen eller använd ett bokmärke som du har skapat tidigare.
-Om någon vill att du ska ge pengar, eller frågar efter en kopia på ditt pass eller körkortsfoto kan du prata med någon i din närhet. Diskutera om det här är något du ska ta på allvar. Fundera på vem som har skickat begäran.

Låt dig inte luras av artiga bedragare

Ofta försöker bedragaren att samtala artigt.

– Särskilt för äldre personer är det i viss mån en hederssak att samtala och betjäna en annan människa på bästa möjliga sätt. Förbrytaren attackerar sedan genom att utnyttja precis den här viljan, säger kriminalkommissarie Janne Saari.
Nätbedrägerier har fortsättningsvis blivit allt vanligare, och på sociala medier förekommer också så kallade kärleksbedrägerier. Enligt Janne Saari är en vanlig historia att en person utger sig för att vara en fredsbevarare, och befinner sig utomlands.

Bedragaren kontaktar en person och ber om pengar, efter att det har uppstått ett förtroende mellan dem. Bedragaren säger sig behöva pengar, till exempel för att bedragaren själv eller en familjemedlem har skadats. En del säger att de behöver pengar för att kunna komma och träffa personen som kontaktas.

– En målsägare förlorade i fjol 22 000 euro av sina egna pengar. Dessutom tog målsägaren lån på över 70 000 euro och skickade pengarna till bedragaren, berättar Saari.

Om skadan är skedd – be genast om hjälp

En del av bedrägerierna låter harmlösa och vardagliga. I slutet av 2021 fick en mamma ett meddelande via Whatsapp där en person utgav sig för att vara hennes dotter. Personen sade att telefonen hade hamnat i tvättmaskinen, och det hade lett till obetalda räkningar. “Dottern” bad att mamman skulle överföra cirka 4 000 euro till ett konto, och det gjorde mamman.

Enligt polisen kan det löna sig att inte svara på samtal från okända telefonnummer, utan i stället kolla upp vems numret är via en nummerupplysningstjänst.

Om bedrägeriet redan har inträffat ska du genast be om hjälp. Meddela genast din bank om du blivit av med dina pengar, det kan bli svårare att få tillbaka de stulna pengarna om du väntar länge. Ta kontakt med polisen, och spara bevis så som samtalsuppgifter och mejl.

Om personen är din vän på Facebook eller följer dig på Instagram ska du inte ta bort personen. Vid behov kan du begränsa personens rätt att se din profil.

– Även om du redan har blivit offer för bedrägeri ska du inte tveka att be om hjälp. Bedragarna är skickliga och det är inte ditt fel att du har blivit offer för brottet, säger kriminalkommissarie Niina Eränen.

BILAGA 5

Bedragare fiskar fortfarande efter bankkoder och personuppgifter i Mina Kanta-sidors namn

Meddelande - Medborgare Skrivet 29.03.2022

I Mina Kanta-sidors namn sprids fortfarande meddelanden och länkar som leder till webbplatser som upprätthålls av brottslingar. Också i FPA:s namn har bedragare fiskat efter bankkoder och personuppgifter. Det är endast tryggt att logga in på Mina Kanta-sidor på adressen www.kanta.fi och i MittFPA på adressen www.fpa.fi.

I slutet av 2021 informerade FPA om att bedragare använder Mina Kanta-sidors och FPA:s namn för att komma över personuppgifter och bankkoder. När offret uppger sina nätbankskoder på en falsk webbplats kommer bedragarna åt offrets nätbank och kan stjäla pengar från hans eller hennes konto. Länkar som leder vidare till webbplatser som upprätthålls av brottslingar har förekommit i sociala medier och sökmotorer på internet. Vissa har fått e-postmeddelanden med en länk som leder till en sida som används för nätfiske. FPA har fått anmälningar om nätfiske i Mina Kanta-sidors namn också i år.

– Nya bedrägerier uppdagas hela tiden och bedragarnas metoder förändras. Det räcker inte med att se upp för skumma meddelanden. Man måste göra det till en vana att logga in på olika tjänster endast via organisationens officiella webbplats, säger **Jouni Ihanus** som är chef för FPA:s säkerhetsoperationscenter.

Ihanus påminner om att webbplatser som upprätthålls av nätfiskare till utseendet kan likna FPA:s och Kanta-tjänsternas eller andra myndigheters webbplatser. Bluffmeddelanden och innehållet på falska webbplatser skrivs allt oftare på ett gott språk.

– Det är viktigt att alltid vara försiktig och att försäkra sig om att det säkert är en pålitlig tjänst man loggar in på, summerar Ihanus.

Ihanus hoppas att de som blivit offer för bedrägerier anmäler detta till Cybersäkerhetscentret och till den organisation i vars namn brottslingarna har fiskat efter uppgifter. Även om skadan redan är skedd kan man genom att anmäla och varna om saken förhindra att andra råkar ut för samma sak.

Logga in tryggt i MittFPA och på Mina Kanta-sidor

Det är tryggt att logga in på Mina Kanta-sidor på adressen www.kanta.fi och i MittFPA på adressen www.fpa.fi(Öppnar nytt fönster). Man ska aldrig logga in på dessa tjänster via länkar som man fått per e-post eller sms eller via en sökmotor på internet. Det finns ingen särskild mobilapplikation för MittFPA eller Mina Kanta-sidor.

Av datasäkerhetsskäl ska man aldrig skicka känsliga uppgifter, såsom personbeteckningar, per e-post. Varken Kanta-tjänsterna eller FPA ber någonsin om sådana uppgifter per e-post eller sms.

På fpa.fi och kanta.fi finns anvisningar för trygg inloggning:

- Hur sköter man ärenden tryggt på Mina Kanta-sidor?
- Sköta ärenden tryggt i MittFPA (fpa.fi)(Öppnar nytt fönster)

Gör så här om du har utsatts för försök till nätfiske

Om du har kommit in på en webbplats som verkar skum eller om du har fått ett meddelande med begäran om inloggning ska du gå till väga på följande sätt:

- Svara inte på meddelandet och fyll inte i dina uppgifter i de fält som finns på webbplatsen.
- Klicka inte på de länkar som finns i meddelandet eller på webbplatsen.
- Om du misstänker att dina bankkoder har hamnat i fel händer ska du genast kontakta din banks kundservice och därefter göra en polisanmälan.
- Om den skumma webbplatsen utger sig för att representera FPA eller Mina Kanta-sidor ska du meddela FPA.
- Gör en anmälan till Cybersäkerhetscentret (kyberturvallisuuskeskus.fi)(Öppnar nytt fönster).
- Varna dina bekanta för bedrägeriet.
- Besök också webbplatsen Dataläckagehjälp (tietovuotoapu.fi)(Öppnar nytt fönster).