Styrket kamp mot **digital svindel**

Det handler om tillit

nets | nexi

Nets ble etablert i 1972, og har 50 års erfaring med det norske betalingsmarkedet og er spesialist på å drive og styrke utviklingen av digitale betalinger. Vi knytter banker, bedrifter og forbrukere sammen i et internasjonalt nettverk som legger til rette for digitale betalinger. Gjennom vår tilstedeværelse i hele det nordiske markedet leverer vi en rekke kort- og kontobaserte tjenester samt betalingsløsninger for varehandelen.

Nets har vært en del av Nexi Group siden 2020 og er til stede i over 25 land.

Kamp på mange fronter mot svindel med betalingskort

Nets er Norges største leverandør av digitale betalingsløsninger, og vi har derfor et medansvar for å beskytte nordmenn mot digitale svindelforsøk. Vi arbeider målrettet med å undersøke og analysere omfanget, årsakene til og konsekvensene av digitale svindelforsøk - og bruker denne kunnskapen til å forebygge fremtidige svindelforsøk.

Her presenterer vi noen av de viktigste trendene innen digital svindel, viser omfanget av den og identifiserer de mest utsatte områdene. Vi belyser også nordmenns tillit til digitale løsninger - fordi digitale betalingssystemer i stor grad er tillitsbaserte.

Digitale svindelforsøk brer om seg. I takt med at nye teknologier tilgjengeliggjøres og sprer seg, blir kampen mot svindel enda mer kompleks. Derfor er det nødvendig at alle aktører på området samarbeider enda tettere. Vi deler her noen av våre innsikter om betalingsbedrageri for å bidra til dette arbeidet - og til en informert debatt om hvordan alle berørte aktører kan samarbeide enda tettere for å beskytte samfunnet mot betalingssvindel.

Nets ser behov for en spesialisert og mer operativ beredskap mot betalingssvindel, bestående av både offentlige og private aktører med innsikt i metodene de kriminelle bruker. Dette vil sikre en sterk og koordinert respons på forsøk på betalingssvindel gjennom nye initiativer.

Rapporten du nå leser er basert på data som vi i Nets har spesiell innsikt i, intervjuer med eksterne og interne eksperter, offentlig tilgjengelige data, samt en spørreundersøkelse gjennomført høsten 2024 i samarbeid med analyseselskapet Norstat.

Vi i Nets håper at dette kan bidra til en bredere debatt om hvordan vi kan styrke tilliten til digital betaling i det norske samfunnet - og forebygge svindel som trekker i motsatt retning.

Utvikling og trender i digital svindel

Digital svindel gir dårligere kår for norske virksomheter

Våre anbefalinger

I Nets setter vi sikkerhet først

Brukervennlige, pålitelige og sikre betalinger har hovedprioritet i Nets. Slik har det vært siden etableringen i Norge i 1972. Siden da har vi knyttet banker, bedrifter og forbrukere sammen i et sømløst nettverk for sikker og enkel betaling.

Sofistikert svindel
Gode betalingsløsninger som har tillit hos forbrukere og alle tilknyttede virksomheter er avgjørende for velfungerende samfunn. Med økt digitalisering og kompleksitet har svindleres angrepsflater blitt flere. Svindelmetodene er blitt mer sofistikerte, noe som gjør det vanskeligere for forbrukere å skille mellom ekte og falsk informasjon.

Manipulasjon utgjør en stor og økende andel av det totale svindelvolumet. I tillegg kommer sosial manipulering, hvor blant annet falske kampanjer i sosiale medier utnytter kjente ansikter og stemmer for å lokke mennesker til å investere eller kjøpe varer som ikke eksisterer.

Dette har ført til svekket tillit til digitale betalinger blant norske forbrukere. Da Nets spurte nordmenn om deres tillit til sikkerheten for betalinger og digital adferd, svarte en av tre at de har mindre tillit nå enn for tre år siden. Selv om bevisstheten om svindel øker, er det også økende skepsis til digitale løsninger.

Smart forebygging av svindel
Vi ser på den økende graden av svindel og svindelforsøk som et samfunnsproblem med store mørketall da ikke alle bedragerier blir anmeldt. I Nets jobber vi for at tilliten skal styrkes. Siden 2013 har vi benyttet kunstig intelligens (KI) for overvåking og forebygging av kortbasert svindel.

I 2019 snudde vi metoden for å avverge svindel på hodet da vi i samarbeid med KPMG utviklet Nets Fraud Ensemble. Denne KI-baserte løsningen stopper svindeltransaksjoner i realtid, uavhengig om kortet brukes fysisk eller om kort-informasjonen misbrukes. I løpet av 2024 forhindret vi svindelforsøk til en verdi av 1,1 milliard kroner, både i butikker og for bankens kunder.

Vårt ansvar innebærer at nye bedriftskunder fra første stund blir grundig vurdert for å sikre at de er legitime og ikke er involvert i ulovlige aktiviteter.

Vi ønsker at både forbrukere og forretninger skal oppleve økt trygghet når de møter våre betalingsløsninger. Enten det er fysisk i butikk eller på nett. Det innebærer at vi kontinuerlig utvikler nye, innovative løsninger for å ligge i forkant av kriminalitetsutviklingen.

Samarbeid styrker sikkerhet og tillit
For å styrke betalingssystemene ytterligere, må vi som samfunn – både bedrifter og myndigheter – styrke samarbeidet om rutiner og digitale løsninger ytterligere. Det vil styrke effektiviteten og bidra til enda sterkere vern mot svindel.

Forutsetningene for å styrke samarbeidet både nasjonalt og internasjonalt er gode. Siden Nets ble en del av Nexi Group i 2020, har vi samarbeidet med, lært av og dratt nytte av erfaringene fra betalingsløsninger i over 25 europeiske land.

Nets har også omfattende erfaring fra samarbeid med norske, nordiske og europeiske myndigheter. På nordisk nivå omfatter samarbeidet blant annet informasjonsdeling om digitale trusler, sårbarheter og sikkerhetshendelser gjennom Nordic Financial CERT (NFCERT).

Nets er medlem av Beredskapsutvalget for finansiell infrastruktur. Vi deltar dessuten i TIBER-testen. Dette for å avdekke styrker og svakheter i cybersikkerheten og øke motstandskraften til bank- og betalingssystemene mot angrep med systemiske konsekvenser. Nets Branch Norway er også underlagt DORA-loven (Digital Operational Resilience Act), som stiller felleseuropeiske krav til digital operasjonell motstandsdyktighet i finanssektoren. Både Nets Branch Norway og Nexi Group har implementert DORA-loven, som har bidratt ytterligere til å gjøre virksomheten motstandsdyktig mot tredjepartsrisiko.

Vinneroppskriften
Trygghet, brukervennlighet og tilgjengelighet forventes av Nets' betalingsløsninger. Samarbeid, kompetanse og teknologi er vår vinneroppskrift. I denne rapporten forteller vi om trusler og hvordan vi jobber for å motstå dem.

God lesning!

Lars Erik Tellmann
Administrerende direktør

Digital svindel i et av verdens mest tillitsfulle og digitaliserte samfunn

Norge er blant landene med høyest tillit mellom mennesker og institusjoner i hele verden – og dette gjenspeiles i vårt stadig mer digitaliserte samfunn.

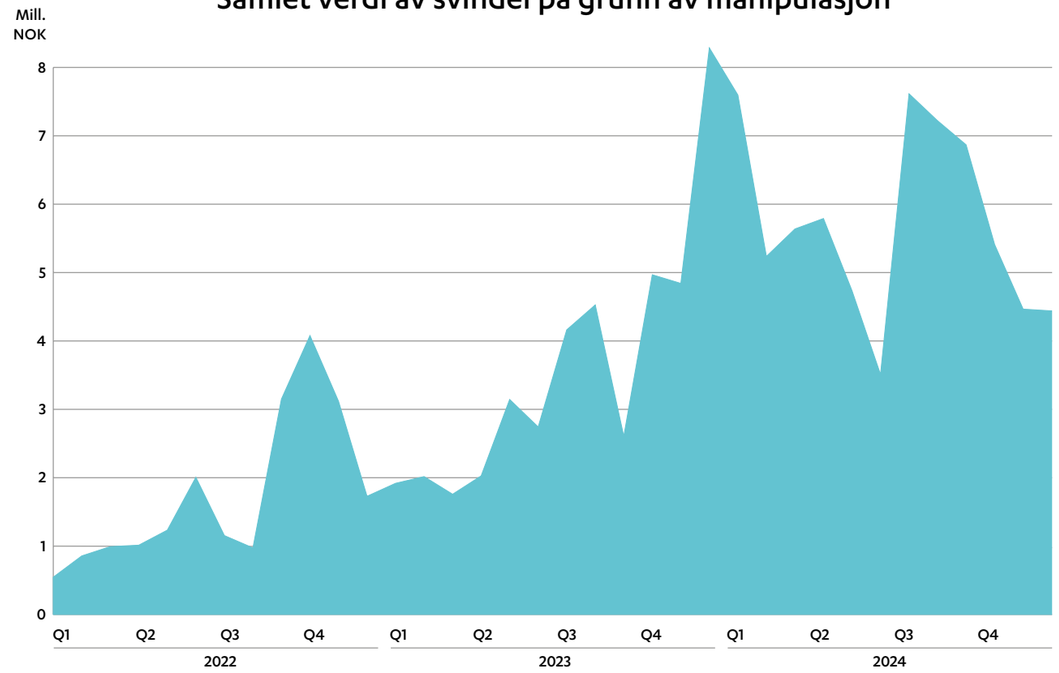
Tillit er en kjerneverdi i samfunnet og er grunnleggende for våre betalingsløsninger. Men digital svindel kan svekke tilliten mellom innbyggere, bedrifter og myndigheter.

Det er viktig at den enkelte forbruker er klar over den økte risikoen for svindel. Men det er kanskje enda viktigere at vi som samfunn – både på bedrifts- og myndighetsnivå – samarbeider i enda større grad for å opprettholde vårt tillitsbaserte samfunn – som er avgjørende for den økonomiske og sosiale utviklingen og effektiviteten i Norge.

En av de nyere metodene kriminelle bruker for å stjele penger innebærer bruk av sosial manipulering. I dag utgjør manipulasjonssvindel en betydelig – og fortsatt økende – andel av det totale volumet av digital svindel. Et eksempel på dette er falske kampanjer i sosiale medier, der ansiktene og stemmene til kjendiser manipuleres og utnyttes for å lokke intetanende individer til å investere store summer i varer, tjenester eller verdipapirer som ikke eksisterer. Falske nettbutikker som er til forveksling lik de originale, er en annen metode.

Svindel med betalingskort i kraftig vekst

Samlet verdi av svindel på grunn av manipulasjon



Manipulasjon driver utviklingen

En av hovedårsakene til økningen i økonomisk svindel er manipulasjon. Kriminelle manipulerer ofre gjennom sofistikert sosial manipulering for å overlevere informasjon eller overføre penger.

De siste årene har sikkerhetstiltakene rundt digitale betalinger blitt kraftig styrket – med økt regulering, 2-faktor autentisering for nettbetalinger, innføring av QR-koder i BankID-appen – og andre lignende initiativer. Paradoksalt nok har ikke omfanget av svindel blitt mindre, men tvert imot økt i samme tidsperiode.

Dette skyldes at kriminelle også forbedrer sine evner og metoder. Spesielt fremveksten og bruken av generativ kunstig intelligens har styrket kriminelles muligheter. Teknologien gjør det for eksempel lettere å lage falske stemmer, bilder, tekster og nettsider som fremstår som troverdige og autentiske.

Teknologiske fremskritt kan dermed utnyttes både til nytte og skade for den enkeltes økonomi – og vi ser et våpenkappløp mellom de kriminelle og vi som beskytter systemene og tilliten til betalingsløsningene i samfunnet.

SOSIAL MANIPULERING

Sosial manipulering er en metode for å utnytte menneskers psykologi, følelser og tillit – og har blitt et mer utbredt fenomen de siste årene.

Gjerningspersonene utgir seg for å være troverdige og pålitelige personer, selskaper eller myndigheter for å vinne offerets tillit. De bruker taktikker som etterligning og overtalelse for å få tilgang til sensitiv informasjon som passord, økonomiske data og tilgang til systemer. Gjerningsmennene vil i større grad enn tidligere være involvert i svindelen, for eksempel ved å foreta lengre telefonsamtaler der de skaper et bånd med offeret gjennom en fabrikkert historie.

Funn i Nets' undersøkelse fra høsten 2024 og i betalingsdataene som genereres hver dag, viser at alle aldersgrupper blir ofre for digital svindel. Det er ikke bare eldre eller digitalt uerfarne som rammes, men også unge og digitalt kompetente mennesker som blir svindlet. Svindlerne tilpasser angrepene sine til ulike målgrupper, situasjoner og digitale plattformer. De utnytter stresset, frykten, nysgjerrigheten eller grådigheten til ofrene for å få dem til å handle impulsivt eller uforsiktig.

Det er mange grunner til at forskjellige mennesker blir svindlet. Eldre kan være mer tilbøyelige til å stole på henvendelser som fremstår som «offisielle», mens unge og «digitalt innfødte» er så vant til å sveipe hele tiden at de kan gå glipp av advarsler med liten skrift. En ny trend er at unge mennesker i økende grad er i søkelyset til kriminelle. Vi ser at spesielt aldersgruppen 15-24 år ser ut til å ha fått høyere risiko enn før for å la seg lure – for eksempel lokket av utsiktene til store gevinster på kryptovaluta.

Nets har spurt nordmenn:

33 %
av nordmenn angir at de har mindre tillit til at sikkerheten er ivaretatt for betalinger og digital adferd sammenlignet med hva de hadde for tre år siden.

56 %
angir at de hverken er mer eller mindre tillitsfulle i dag sammenlignet med hva de var for tre år siden.

12 %
sier at de har mer tillit i dag.

Nets har spurt nordmenn:

62 %

av nordmenn er enten i svært eller stor grad bekymret for at kunstig intelligens kan brukes til økonomisk svindel eller misbruk.

3 %

sier at de i svært liten grad er bekymret.

Phishing, smishing, vishing og spoofing

Det er lett å la seg lokke av et godt tilbud, en falsk e-post eller en vennlig stemme på telefonen. Men digital svindel kan få store konsekvenser - både for lommeboken og privatlivet ditt.

E-poster, tekstmeldinger og samtaler – de fleste er nå kjent med disse svindelmetodene, spesielt phishing, som har blitt et vanlig begrep. Phishing involverer falske e-poster som ser ut som de kommer fra pålitelige kilder, for eksempel banker eller offentlige etater, men i realiteten "fisker" etter din konfidensielle informasjon. Smishing er den samme taktikken via tekstmeldinger, og vishing skjer gjennom telefonsamtaler der kriminelle utgir seg for å være en annen enn den de er – og at de ringer fra en annen virksomhet enn de faktisk gjør.

Mens phishing, smishing og vishing tar sikte på å lokke folk til å videreformidle informasjon, handler spoofing om å skape en troverdig fasade for svindleren. Her manipulerer personen sin egen identitet eller lokasjon for å fremstå som troverdig. Noen eksempler kan være:

Telefonspoofing: Det kan se ut som anropet kommer fra et vanlig norsk nummer, ofte fra en tilfeldig, intetanende innbygger. Hvis du prøver å ringe tilbake, vil anropet gå til denne personen som nummeret er "stjålet" fra og ikke til svindleren selv.

Forfalskning av e-poster og nettsteder: Svindleren manipulerer e-postadresser eller domenenavn til å se ut som offisielle kilder, for å iscenesette for eksempel interne e-poster eller meldinger fra familiemedlemmer.

GPS- og IP-spoofing: Svindleren skjuler posisjonen eller identiteten sin ved å manipulere tekniske data, noe som gjør dem vanskeligere å spore.

Tidligere var det påkrevet å ha både betydelig teknisk kunnskap og god språkforståelse for å utføre slike angrep. Men tilgang til avanserte verktøy og generativ KI har gjort svindelforsøk langt mer sofistikerte og vanskeligere å oppdage.

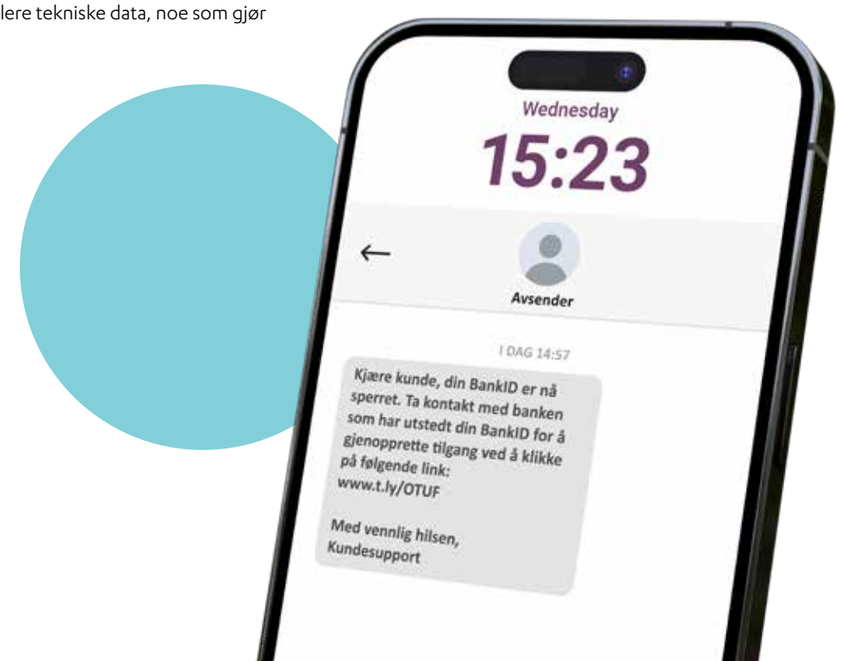
Svindelforsøk pleide å bli avslørt av tydelige språkfeil. Nå er disse ofte ikke-eksisterende, noe som gjør det vanskelig selv for digitalt kompetente personer å oppdage svindelen.

Samtidig har omfanget av svindelangrep økt betraktelig. Det har blitt mulig å automatisere og skalere svindelforsøk i et mye større omfang – og dermed produsere og sende ut store mengder falske meldinger og oppringninger. Dermed er det langt flere mennesker som utsettes for svindel-forsøkene som det kreves oppmerksomhet og bevissthet om for å kunne skille mellom sant og usant.

Falske hjemmesider

Ifølge Telenor er 7 av 10 nye nettsider som opprettes svindelnettsider. Kriminelle etterligner ordinære nettsteder for å lure forbrukerne til å oppgi personlig og økonomisk informasjon. Det kan være en tro kopi av den opprinnelige nettsiden med de samme produktene og bildene, men med en liten bevisst skrivefeil i firmanavnet eller URL-en. Her bestiller forbrukerne varer de er vant til, men mottar aldri noe.

På samme måte lager svindlere nettsteder som skal se ut som Nets eller andre leverandører av betalingsløsninger for å lure ofrene til å oppgi betalingskortopplysninger og annen konfidensiell informasjon. Nets stenger i gjennom-snitt 100 nettsteder i måneden som er forsøk på å kopiere Nets-nettsteder.



INTERVJU: ØKOKRIM

Kampen mot svindel er en del av totalforsvaret

Økokrim har utviklet en forebyggende modell for hvordan vi tenker. En Totalforsvar-tankegang innebærer at samfunnet løser utfordringene sammen. Politiet har mye av kunnskapen, mens andre aktører som Nets og bankene har muligheten til og ansvaret for å gjøre endringer i sine teknologiske systemer.

Om intervjupersonen Fredrik Lykken

ØKOKRIM

Fredrik Lykken er fagleder for forebygging i Økokrim, Norges nasjonale organ for økonomisk kriminalitet, miljøkriminalitet og inndragning.

Fagfeltet for forebygging samarbeider tett med fagfeltene for etterforskning og etterretning for å bekjempe kriminaliteten. Fagfeltene må også virke sammen med andre offentlige og private aktører for å bekjempe denne utfordringen.

Bedragerier utgjør fortsatt en stor andel av arbeidsmengden som havner på Lykkens pult.

Har Økokrims tilnærming til bekjempelse av digital svindel endret seg de siste årene, og i så fall hvordan?

På dette området har det vært stor endring. Økokrim har tradisjonelt vært en organisasjon som jobber med etterforskning for å fange kjeltringen. Nå har vi utviklet oss til å jobbe mer helhetlig med kriminalitetsbekjempelse, hvor etterretning, forebygging og etterforskning går hånd i hånd.

Hvordan tror du svindel påvirker folks tillit til samfunnet som helhet?

Det kommer inn rundt 30.000 anmeldelser på svindel i løpet av året, og veldig mange blir henlagt. Det er klart det gjør noe med tilliten i samfunnet. Et særlig problem har vært at mange er blitt svindlet via spoofing, etter å ha blitt oppringt av en svindler under dekke av å ringe fra politiet eller bank. Her er det nå gjennom Nasjonal ekspertgruppe for digital svindel laget et teknisk skjold som i stor grad har tatt ned denne muligheten for svindlerne.

Anmeldelsene er slik sett svært viktige for både vårt forebyggende arbeid, og for at vi skal få kunnskap om hvordan de kriminelle jobber. Ved å se saker i sammenheng, kan vi få tak i bakmennene og på den måten oppklare flere hundre saker i én etterforskning.

Vi er på feil vei når folk er redde for å ta telefonen fordi de ikke vet om det faktisk er banken eller politiet som ringer. Mye svindel skjer mens du sitter hjemme i stua, når du er på det antatt tryggeste. Kriminaliteten forflytter seg inn i den nærmeste sfæren, sier Lykken.

Hvordan har du observert at svindelmetoder har utviklet seg i takt med økende digitalisering?

Svindelvirksomhet kan nesten sammenlignes med en bedrift. Crime-as-a-service har kommet til et punkt der man kan kjøpe ferdige pakker. Det har utviklet seg ganske mye de siste årene, med at svindelen i Norge kan gjennomføres fra nær sagt hvor som helst. Nordic AntiFraud Corporation er et samarbeid for å bekjempe svindel på tvers av de nordiske landene. Også jobber vi med Europol opp mot de store sosiale mediene for å prøve å få dem til å rydde opp i hva som spres via deres kanaler.

Det norske samfunnet er tillitsbasert, det har nok svindlerne skjønt. I Norge kan de lettere lykkes med sosial manipulasjon, som å gi seg ut for å være en myndighetsperson eller en annen som kan hjelpe deg. Da spiller de på frykt og hast, noe som gjør at ofrene får lite tid til å tenke seg om.

For å stoppe disse metodene må alle spille på lag. Ofte er det bankene eller Nets som ser ting først. Da er det regelverket for informasjonsdeling ved offentlig/privat samarbeid som setter føringer for samarbeidet. Teleselskapene og bankene må ha sine sikkerhetsmekanismer, og hver enkelt av oss må være årvåken. Økokrim leder ikke an på teknologien, men vi følger med og gjør de grepene som må til, også på teknologi.

Hva er noen av de hyppigste formene for digital svindel som du har observert de siste 3-5 årene?

Investerings- og kjærlighetsbedragerier er en vanlig svindelform. Det har typisk vært at menn vil ha raske penger og damer vil ha kjærlighet, men også dette jevner seg ut. Det går fort noen kroner når man lar følelsene ta overhånd. Det har kommet ganske mange tips den siste tiden som tyder på at denne metoden har kommet mer tilbake etter at spoofing har stoppet litt opp. Det er ikke så lett for oss å forhindre svindel som går via sosiale medier. Her har de sosiale mediene selv et stort ansvar. I tillegg blir det opp til enkeltpersoner å være obs. Bankene har på sin side muligheter til å legge inn sperrer på overføring til utenlandske kontoer. Brukervennlighet er et interessant tema. For jo mindre friksjon det er for kunden, jo lettere kan det bli for de kriminelle. Økt sikkerhet i form av 2-faktor autentisering eller annen form for identifisering skaper mer friksjon, så hvor skal den grensen gå? Samfunnet, særlig det offentlige, har ikke vært gode nok på å vurdere brukervennlighet opp mot kriminalitet. Det er helt nødvendig at systemutviklere også tenker sikkerhet og kriminalitet.

Er det visse grupper som identifiseres som spesielt sårbare for nettsvindel? Hva gjøres for å beskytte/utdanne disse gruppene?

Dette kalles jo Olga-svindel av en grunn, nemlig at svindlerne fant ut hvem som har gammeldagse navn og jobbet veldig målrettet mot eldre og sårbare personer. Men vi ser en økning av yngre folk (35-55) som blir utsatt for bedragerier.

De yngste er litt utenfor målgruppen for emosjonell manipulasjon, men kan fort la seg lure på falske nettbutikker og gå på noen smeller de også. Det finnes en svindel for alle.

Det handler ofte om å treffe på folk på de mest sårbare tidspunktene, for eksempel i stressede situasjoner mellom jobb og henting i barnehage.

FEM GODE RÅD TIL NORDMENN FRA ØKOKRIM OG NETS

1
Ikke gi kontoopplysninger eller annen sensitiv informasjon til noen.
Ingen seriøse aktører vil be deg om dette.

2
Vær kritisk til nettsider og kampanjer du ikke kjenner til fra før.
Virker noe for godt til å være sant, så er det ofte det.

3
Ikke la deg stresse til å ta raske avgjørelser. Mye svindel skjer via sosial manipulasjon.
Ring heller banken via sentralbordnummeret og dobbeltsjekk først.

4
Hvis du er i tvil om noe kan være svindel,
forhør deg gjerne med folk du stoler på om hva de tenker.

5
Ring banken umiddelbart,
dersom du mistenker at du har blitt svindlet.

6
Anmeld til politiet.
Det gir oss verdifull kunnskap om hvordan kriminaliteten utvikler seg, og vi får bedre forutsetninger til å forebygge og etterforske.

"For å stoppe disse metodene må alle spille på lag. Ofte er det bankene eller Nets som ser ting først. Da er det regelverket for informasjonsdeling ved offentlig/privat samarbeid som setter føringer for samarbeidet. Teleselskapene og bankene må ha sine sikkerhetsmekanismer, og hver enkelt av oss må være årvåken."

Svindelforsøk rettes mot enkeltpersoner

Kriminelle utnytter kunstig intelligens til å velge ut ofre for kortsvindel med enestående presisjon. Ved å bruke generativ KI kan de identifisere mål og rette angrepene sine mot bestemte grupper mennesker, noe som gjør svindelen både mer effektiv og vanskeligere å oppdage.

For eksempel kan de rette seg mot eldre kvinner i et bestemt område, sende dem en overbevisende melding og deretter fysisk hente kortene deres, kanskje til og med ved å utgi seg for å være en pålitelig person med en tillitvekkende fremtoning.

Eksempler på hva kriminelle får hjelp av KI til å svare på:
- Hva er de vanligste norske navnene på kvinner født i 1945?
- Hva er interessene til en gjennomsnittlig, eldre norsk kvinne?
- Hvilke typer e-poster, tekstmeldinger eller brev mottar denne målgruppen ofte?

Med noen få enkle spørsmål kan svindlere lage svært målrettede angrep.

Basert på svarene kan de sende personlige meldinger eller e-poster som appellerer til ofrenes interesser eller livserfaringer. De kan lage meldinger som ser ut som de kommer fra kjente organisasjoner eller til og med venner og familie. Og de kan bruke språk og terminologi som virker troverdig for den spesifikke målgruppen. Derfra trengs det simpelthen å identifisere mulige ofre i spesifikke områder og kontakte dem.

Ved å forstå hvordan generativ KI brukes til å styrke svindlernes presisjon, blir det klart hvorfor det er så viktig å styrke forsvaret vårt mot digital svindel. Samtidig viser det hva vi kan gjøre for å motvirke svindelforsøk – og hvordan vi kan bruke KI som et motvåpen for å gjenkjenne svindel basert på spesifikke mønstre.

KI har akselerert våpenkappløpet mellom kriminelle og blant annet Nets, som på vegne av banker og bedrifter forsøker å bremse forsøk på kortsvindel.

Hva kommer?

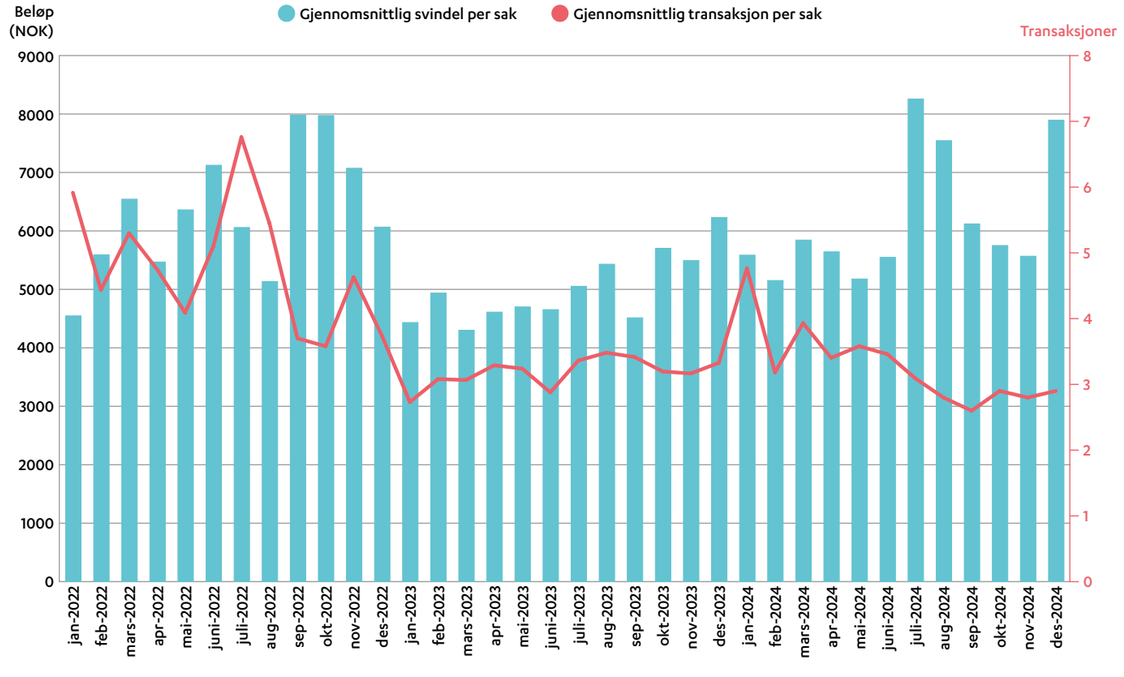
I takt med den teknologiske utviklingen ser vi at nye og mer avanserte svindelmetoder dukker opp. Her er noen av metodene vi kan forvente å se mer av i fremtiden:

Svindel som tjeneste: Vi ser økt profesjonalisering og organisering av kriminelle nettverk, som flere steder opererer som ordinære selskaper. Nettverkene selger «svindelsett» til betalende kunder, som dermed kan få tilgang til lokalt målrettede manualer og bruksanvisninger. Håndbøkene forklarer ulike metoder for å utføre svindel via nettbank eller kort. Dette stiller enda større krav til aktører som jobber med å bekjempe svindel.

Deepfakes: Utviklingen av deepfakes går også raskt. Allerede i dag ser vi at teknologi kan lage bilder og videoer av kjente personer som tilsynelatende promoterer visse kjøp eller handlinger. Videoene og bildene brukes til å lure folk til å tro at de mottar legitime meldinger fra pålitelige personer de stoler på, noe som gjør det enda vanskeligere å skille mellom ekte og falsk informasjon.

Med bruken av KI-drevne stemmegeneratorer kan kriminelle etterligne stemmene til kjente personer – eller til og med noen som ofrene kjenner personlig. Teknologien kan brukes til å foreta telefonsamtaler som høres autentiske ut og overbevise folk om å overlevere sensitiv informasjon eller overføre penger.

Det svindles for høyere beløp



Vi ser en tendens til at svindlere i dag gjør færre, men større transaksjoner enn før, med et stjålet betalingskort.

Trenden er spesielt tydelig ved kjøp av kryptovalutaer, reiser og elektronikk, hvor store pengesummer er vanlig – og dermed vanskeligere for sikkerhetssystemer å oppdage, slik at svindlere kan maksimere gevinsten.

Skiftet fra flere små til noen få store transaksjoner antyder en mer strategisk tilnærming fra svindlernes side. Tidligere brukte kriminelle ofte stjålne betalingskort til å gjøre mange små kjøp, da transaksjoner under en viss beløpsgrense ikke krever PIN-kode. Men sikkerhetstiltak hos oss i Nets kan fange opp dette mønsteret, for eksempel når det foretas mange lignende, små transaksjoner på samme betalingskort.

Vi begynner nå å se en endring i adferden til kriminelle. De legger ned en større innsats enn tidligere for å få tak i koden til betalingskortet – eller legge det stjålne betalingskortet inn i sin egen digitale lommebok, hvis de har fått tilgang til offerets BankID – og gjør deretter noen få større transaksjoner før kortet blir meldt stjålet.

Abonnementsfeller og falske nettsteder

Abonnementsfeller lokker brukere til å registrere seg for tjenester som ser ut til å være gratis eller billige, men som i realiteten resulterer i dyre abonnementer – ofte enten med et billig produkt eller ikke noe i det hele tatt – fordi det er falskt. Typiske eksempler på slike abonnementsfeller kan være hudpleieprodukter, fitness, populære «goodie bags» og andre ting som ofte annonseres gjennom sosiale medier. Forbrukerne signerer på vilkår og betingelser som med liten skrift beskriver vanskelige avbestillingsprosedyrer, gebyrer og urimelige priser.

Falske nettsteder etterligner legitime sider for å lure forbrukere til å oppgi personlig og økonomisk informasjon. Imitasjonene er vanskelige å oppdage, det kan være snakk om en tro kopi av en original nettside med de samme produktene og bildene, men kanskje med en liten, bevisst skrivefeil i e-posten, f.eks. kontakt@elkjopp.no. Her bestiller forbrukerne varer slik de er vant til, men mottar aldri noe produkt. Nettsteder utnytter ofte SEO-teknikker for å angere høyt i søkeresultatene og kan til og med pryde seg med falske anmeldelser for å fremstå mer troverdige. Svindlerne bruker også psykologiske manipulasjonsteknikker, som å skape en følelse av at det haster å gjennomføre handelen.

Bedrifter opprettes med svindel som eneste formål, og belaster betalingskort eller utsteder falske fakturaer. Bankene mottar bekymringsmeldinger fra sine kunder og Nets stenger deretter ned aktiviteten på de påklagede nettstedene. Omfanget er stort, det handler om mer enn 1 000 butikker i året, som Nets stenger basert på mistenkelig oppførsel.

Nets forebyggende tiltak mot digital svindel

Slik jobber Nets med KI og maskinlæring for å bekjempe svindel

Nets har i en årrekke brukt KI for å styrke overvåkingen av betalingssvindel, ettersom kriminelle stadig endrer metodene sine. Vi utvikler selvsagt systemene våre for hele tiden å være et skritt foran.

De siste årene har vi i Nets i samarbeid med KPMG utviklet den første modellen for et system som bruker maskinlæring, for i sanntid å identifisere uvanlige mønstre som mennesker kan overse eller ikke rekke å reagere på. Den første versjonen av modellen kunne oppdage svindel på omtrent 20 millisekunder – seks ganger raskere enn et blink med øye.

Modellen utvikles løpende, og er opplært til å identifisere normal atferd i stedet for svindelkarakteristikker. I stedet for å fokusere på spesifikke svindelmønstre, lærer modellen vår hva som er normalt og reagerer på atferd som faller utenfor den normen.

Dette gjør det mulig å oppdage svindel selv når de kriminelle endrer metoder. Med modellen har vi redusert uredelige transaksjoner med 40 prosent. Dette kommer på toppen av våre eksisterende tiltak for forebygging av svindel. Alle kortholderdata som brukes i modellen er anonymisert, og Nets bruker kun dataene til å gjenkjenne mønstre og stoppe svindel.

Nets har spurt nordmenn:

Nordmenn stoler på sikkerhetstiltakene som beskytter transaksjoner når de foretar nettbetalinger, som for eksempel verifisering av kjøp via SMS eller BankID.

74 %
av nordmenn stoler på at sikkerhetstiltakene i stor eller svært stor grad fungerer.

20 %
anser tillitten til sikkerhetstiltak som nøytral.

7 %
sier at de i liten eller svært liten grad har tillit til sikkerhetstiltakene.

INTERVJU: KREDITTBANKEN

Hyppige forsøk på manipulasjon

Om intervjupersonen Oddveig Kvål

Kredittbanken
Del av SpareBank 1 og Eika

Oddveig Kvål jobber som fagspesialist svindel i Kredittbanken – Del av SpareBank 1 og Eika. Hun er en del av et team på elleve personer som sitter i Trondheim og Gjøvik og hjelper sparebankenes kunder med deres reklamasjoner på kredittkort.

Inntil nylig jobbet de kun med Mastercard, men som følge av sammenslåingen med Eika Kredittbank på nyåret fikk de også Visa.

Hvordan har dere som finansinstitusjon opplevd utviklingen av digitale svindelmetoder de siste årene?

Det har vært en veldig stor økning av svindel etter korona-pandemien, og det blir mer og mer for hvert år. Før var det mer datainnbrudd og bruk av kort i utlandet, mens nå er det mer manipulering av kortholdere som lures til å gi fra seg kortopplysninger på nett og over telefon. Mange av de rammede er eldre personer, som generelt er oppegående og bevisste, men kanskje er litt naive og har begrenset teknologisk kompetanse. Dessuten ser vi mer hard, fysisk kriminalitet, der svindlerne kommer hjem til kortholder og lurer vedkommende til å gi fra seg betalingsopplysninger.

Falske nettsider er også et problem, men det er en tendens vi har sett i flere år.

Uttrykker kundene bekymring eller frykt for å bli offer for digital svindel? I så fall, hvordan håndterer dere disse bekymringene?

Vi er ikke i kontakt med alle, for ofte er det bankene som tar den kundedialogen.

Har dere erfart at den økende digitale svindelen kan ha innvirkning på kundenes tillit til banken? Hvordan påvirker dette forholdet mellom dere og kundene deres?

Kundene er absolutt blitt mer skeptiske. Vi anbefaler alle å gå inn og lese seg opp på svindel.no, som er godt oppdatert på svindelmetoder.

Utviklingen av svindelmetoder: Hvordan beskytter dere dere selv og kundene deres mot digital svindel?

Vi bruker Nets som overvåking, og de reagerer hele tiden på mistenkelige transaksjoner. Det kommer sjelden klager fra kundene når kort blir sperret, de har forståelse for det. Vi anbefaler alle kunder å bruke regionsperre når de ikke er på reise.

Hvordan ser dere på utviklingen sett innen digitale svindelmetoder og fremveksten av AI?

Vi ser særlig at stemmer manipuleres via telefonoppringninger. I tillegg så vil det nok komme flere BIN attack på bankenes kortnummer.

Kan du gi noen konkrete eksempler på hvordan overgangen fra fysisk til nettbasert svindel har påvirket bankens drift og forretningsmetoder? Har dere måttet endre deres interne prosedyrer eller investere i ny teknologi for bedre å motvirke denne trusselen?

Det er en kontinuerlig jobb å forbedre systemer, der får vi god hjelp blant annet fra Nets. Det går løpende på trender og brukersteder.

Mye er reiserelatert, at svindlerne får tak i kortnummer og sikkerhetskode for så å bestille seg en reise på en legal nettside. Dessuten er det mye pengeoverføringer via tjenester som Revolut.

Anbefalinger

Jobber dere aktivt med andre myndigheter og organisasjoner for å bekjempe digital svindel?

Der vi har felles kunder på både debet og kredit, da blokkeres begge fortest mulig.

Vi har veldig bra samarbeid med ukentlig dialog for å utveksle brukersteder som er fanget opp.

Hvordan ser du på datadeling som en mulig løsning for å bekjempe digital svindel på tvers av ulike interessenter, inkludert andre banker, myndigheter og betalingstjenesteleverandører?

Det ville vært fint å kunne dele mer informasjon mellom bankene, og det er noe myndighetene jobber med og som vi håper de får til fort. Finans Norge har et prosjekt gående med Økokrim, Datatilsynet, bankene og teleselskapene.

Hva er deres holdning til sosiale medieplattformer som Meta og deres ansvar i forbindelse med digital svindel? Mener du at slike plattformer bør ta større ansvar for å beskytte brukerne mot svindel, og i så fall, hvilke skritt bør de ta for å oppfylle dette ansvaret?

Vi har lite dialog med dem, fordi de er utfordrende å få tak i. Vi ser generelt at det på sosiale medier florerer med annonser og lenker til falske nettsider. Det kan typisk være for kjøp av sko, kjoler og kofferter. Typisk er slike nettsteder operative i 2-3 dager om gangen før de sperres ned og senere dukker opp igjen. Så det er en evigvarende kamp, men denne typen svindel kan gjenkjennes av årvåkne forbrukere. Det er bankene som eier kundeforholdene til kortholderne.

Hva kan dere utgi av statistikk, f.eks. av alder på de som rammes? Hva slags prosedyrer har dere selv? (Nets sjekker tredjepartsdata (kortholdere) i realtid.)

Når det gjelder ulike aldersgrupper, så ser vi at phishing i størst grad rammer de over 70, men det blir også flere og flere unge som går på denne type svindel.

Videre er det noen klassiske sesongvariasjoner, der en del lures av ekstra fakturaer under travle handelsperioder som black week, eller falske meldinger fra skattemyndighetene når det er sesong for det.

Slike falske meldinger er blitt stadig bedre på å etterligne seriøse aktører med tanke på korrekt språk og timing for utsendelse. Et rødt flagg er klikkbare lenker i eposter eller tekstmeldinger, for det er noe seriøse aktører prøver å unngå. Spamfilteret til de fleste epostleverandører fungerer for øvrig ganske godt på å filtrere ut uønsket kommunikasjon.

Hva koster denne svindelen banken deres i faktiske dekninger? Er det pliktig å opplyse om i årsrapporten?

Det blir rapportert til myndighetene, og det har vært en kraftig økning det siste året i antall saker, særlig for phishing som samlebetegnelse.

Noen tips til slutt for hvordan unngå å bli rammet av svindel?

Ikke bli stressa, tenk litt over det du mottar før du handler. Ta kontakt med banken og dobbeltsjekk hvis du er usikker.

Digital svindel rammer også butikkene

Når forbrukere handler på nett, forventer de å kunne betale trygt og enkelt med betalingskortet sitt. Dessverre utnytter kriminelle denne tilliten og prøver å svindle med falske eller stjålne kortdetaljer. Samtidig påføres mange selskaper økonomiske tap både gjennom ekstraarbeid og kostnader knyttet til reversering av uredelige transaksjoner og tap av solgte varer. Håndtering av svindelsaker krever betydelige ressurser som kan tynge driften i en virksomhet.

Kriminelle kan få tak i betalingskortopplysninger på flere måter, for eksempel:

- hacke en nettbutikk og stjele kundedata
- installere skadelig programvare på en forbrukers datamaskin eller mobil
- kjøpe stjålne kortdetaljer på det svarte markedet
- lokke informasjonen ut av kortinnehaveren ved hjelp av phishing og lignende

Regningen havner ofte hos bedriften: når en forbruker oppdager svindelen på kontoen sin og kommer med en innsigelse, fører det til en tilbakeføring, hvor banken returnerer beløpet fra selskapet til forbrukeren. Selskapet taper dermed både potensiell inntjening – og varer.

En annen indirekte måte selskaper taper inntekter på er gjennom markedet for forfalskede varer som kriminelle selger på falske nettsteder. Forbrukere som ellers ville ha kjøpt et originalt produkt fra et norsk selskap, ender i stedet opp med å kjøpe en kopi på en svindelside. Dermed mister de legitime selskapene potensielt salg, som kan utgjøre betydelige beløp over tid.

Hvor bruker kriminelle andres penger?
Når kriminelle får tilgang til stjålet kortinformasjon, bruker de dem på steder der de raskt kan konvertere de stjålne midlene til penger eller verdifulle varer. Felles for disse bransjene er at de tilbyr lett omsettelige varer og tjenester som enten kan brukes direkte av svindlerne eller raskt selges videre.

Kontanter og pengeoverføringer
Favoritten blant kriminelle er pengeoverføringer og kontanter. Det inkluderer også kjøp av såkalte Quasi Cash, for eksempel gavekort, spillesjetonger eller forhåndsbetalte kontantkort. Quasi Cash er en stor favoritt fordi de raskt kan konverteres til andre varer eller kontanter – og enkelt kan kjøpes både i butikk og på nett.

Reise – fly og transport, hoteller og restauranter
Reise- og transportsektoren, inkludert hoteller og restauranter, er hardt rammet. Kriminelle bruker stjålet kortinformasjon til å bestille flybilletter og hotellrom, som enten brukes av de kriminelle selv eller selges videre til intetanende tredjeparter. Reise er en av de kriminelles foretrukne kategorier, da det kan ta lang tid før offeret oppdager at kortet deres har blitt misbrukt.

Detaljhandel og kjøpesentre
En annen viktig kategori er detaljhandel og kjøpesentre. Kriminelle bruker kredittkort til å kjøpe varer av høy verdi som enkelt kan selges videre på det svarte markedet. Det inkluderer alt fra elektronikk og smykker til luksusvarer med vedvarende høy etterspørsel og verdi.

Telekommunikasjon, IT og elektronikk
Innen telekommunikasjon, IT og elektronikk kjøper kriminelle dyre duppeditter som smarttelefoner, datamaskiner og andre høyteknologiske enheter. Produktene er både av høy verdi og enkle å videreselge.

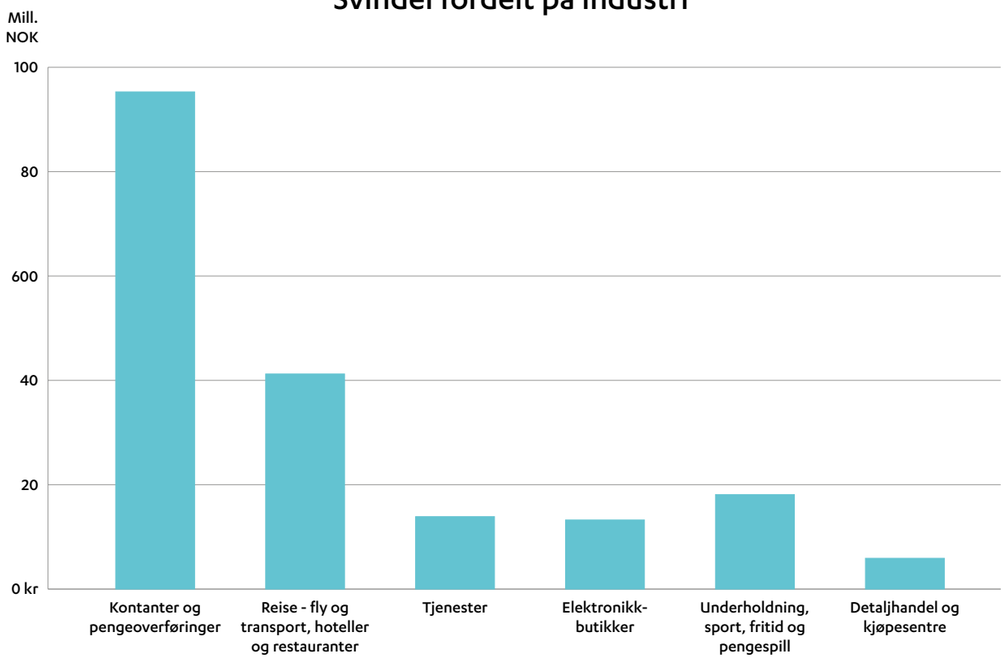
Underholdning, sport og fritid
Underholdning, sport og fritid er også en attraktiv kategori for svindlere. Det kjøpes billetter til arrangementer, abonnementer og medlemskap, som deretter selges videre. Videre er det lett for svindlere å kjøpe adgangsbilletter og tjenester knyttet til fornøyelsesparker og idrettsanlegg.

Tjenester
Tjenestesektoren dekker et bredt spekter av kategorier der kriminelle kan utnytte stjålet kortinformasjon, for eksempel private leger, skoler eller kurs. Selv om det kan virke som et overraskende mål, utgjør det et attraktivt alternativ for svindlere. For eksempel kan påmeldingsavgift til kurs betales med et stjålet kort, som deretter videreselges billigere til andre. Dette skaper økonomiske og administrative utfordringer for de berørte institusjonene og tjenesteyterne, som må håndtere konsekvensene av svindelen.

Pengespill
Kredittkortinformasjon som er stjålet kan for eksempel brukes til å finansiere pengespillaktiviteter, både på nett og i fysiske spillesteder hvor det kan være vanskelig å spore betalingsmidlenes opprinnelse.

Når man ser på spennet i bransjene og butikktypene som kriminelle foretrekker for bruk av stjålet kortinformasjon, blir det tydelig hvor omfattende og utbredt svindel er. For å beskytte både forbrukere og bedrifter er det avgjørende at både finansinstitusjoner, bedrifter og tjenesteleverandører kontinuerlig implementerer robuste sikkerhetstiltak.

Svindel fordelt på industri



INTERVJU: TELENOR

Høy spoofing-aktivitet: SMSer veldig verdifulle for de kriminelle

Telenorbutikken, med sine 82 filialer drevet av franchise-takere rundt omkring i Norge, er kunde av Nets.

Butikkene opplever i liten grad svindel knyttet til falske betalingskort, men desto flere forsøk via andre kanaler.

– SMSer er veldig verdifulle for de kriminelle.
Det er en mer personlig form for kommunikasjon.
I motsetning til e-post, som mange kanskje møter med større skepsis, forventer vi ofte raske svar på SMS, som innebærer en større forventning om rask respons.

Om intervjupersonen Thorbjørn Busch

Thorbjørn Busch er fagleder for teamet som har hovedansvaret for svindeldeteksjon og granskning av kriminalitet rettet mot Telenor og selskapets kunder, både digitalt og fysisk.

Svindeldomenet er enormt og omfatter alt fra identitetstyverier til målrettede phishingangrep med bruk av anrop og SMS. Teamet jobber kontinuerlig med å identifisere, analysere og håndtere disse truslene for å beskytte Telenor og selskapets kunder. Ansvaret til teamet består også av å håndtere suspekte hendelser knyttet til Telenors utstyr, inkludert samfunnskritisk infrastruktur som basestasjoner.

Folk på farten vil gjerne fikse ting fort, og da er det lettere å la seg lure. Svindlerne utnytter folks hastverk og manglende oppmerksomhet på detaljer som kunne ha avslørt svindel-forsøket, sier Busch.

Tidligere var det enklere å spoofe norske merkevarer via SMS. I verste fall kunne svindlernes tekstmeldinger havne i samme meldingstråd som du hadde med for eksempel banken din. Dette er i mindre grad et problem i dag, da Telenor har innført en tjeneste som hindrer at utsatte norske merkevarer kan få sitt navn misbrukt i SMS-er.

I 2023 ble for eksempel rundt 40 ulike filialer av Telenor-butikken oppringt av noen som utga seg for å være fra Telenor IT-support. Bare gjennom fjoråret blokkerte Busch sitt team 64 millioner SMS og 54 millioner uønskede anrop i Telenornettet.

Problemet med spoofing og useriøse anrop er fortsatt like relevant, men forsvaret er blitt betydelig bedre. Telenor og de andre telekomtilbyderne samarbeider godt, og har innført i november 2024 et felles Anti-spoofing proxy filter som har gjort det mulig å identifisere og blokkere spoofede anrop fra mobilnumre som hører hjemme hos andre operatører. Dette har gjort det svært vanskelig å misbruke norske mobilnumre til telefonsvindel, og kriminelle bruker ikke lenger ressurser på denne metoden.

Tiltaket vil bidra til å gjenopprette tilliten til norske mobil-numre blant befolkningen. Men når Telenor lukker en dør, åpner det seg en ny. Etter at den nye sikkerhetsløsningen ble aktivert, så selskapet en kraftig økning i utenlandske anrop, spesielt fra Sverige og Danmark - land nordmenn har tillit til.

På enkeltdager registrerte de opp mot 800 000 anrop fra Danmark daglig. Det normale ligger på rundt 5000 legitime anrop. Mye tyder på at denne taktikken heller ikke har lyktes, da anropene fra disse landene nå er tilbake på et normalt nivå. Telenor forventer at de kriminelle i stedet vil ta i bruk alternative kommunikasjonskanaler for å nå ofrene sine.

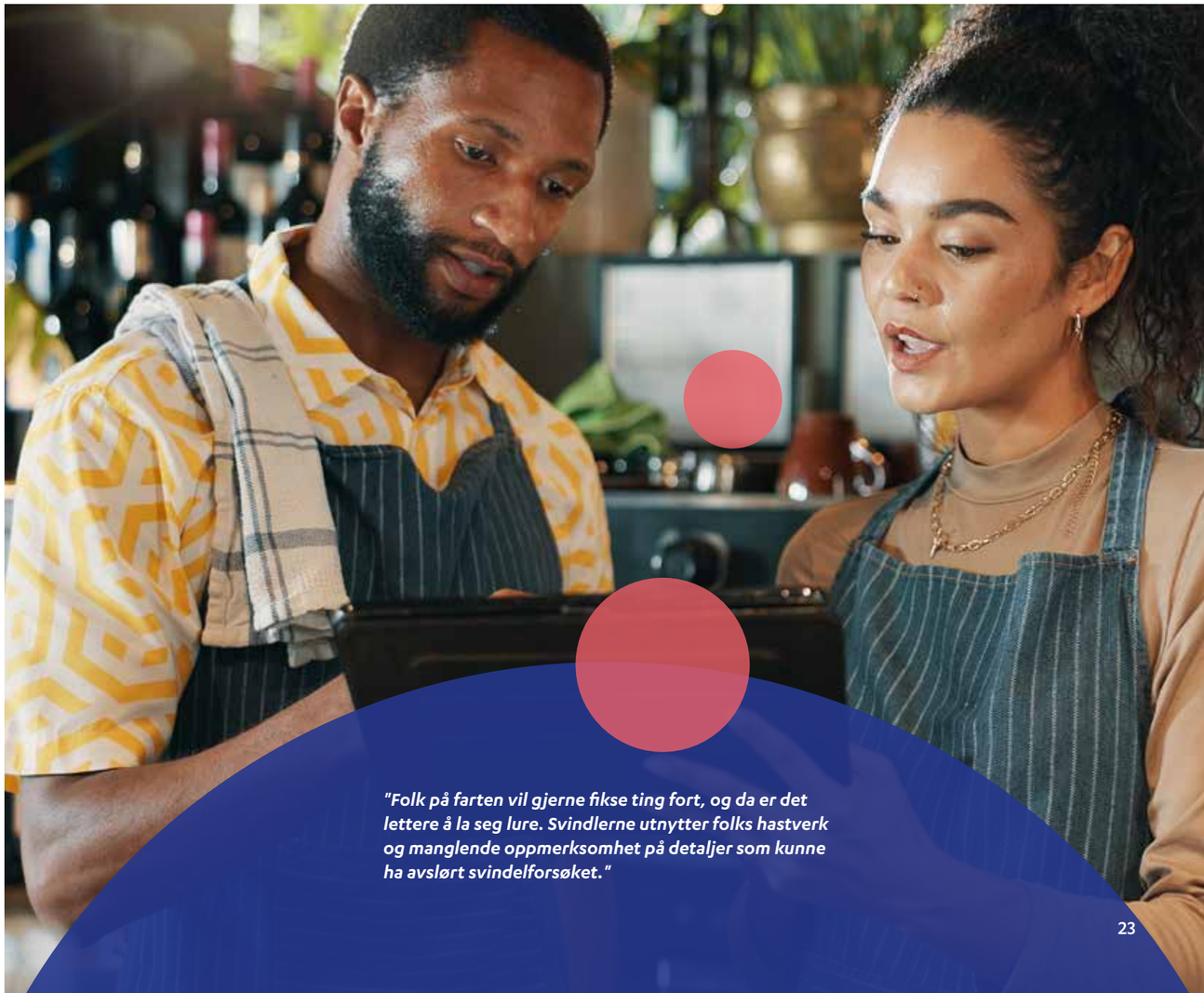
Cybercrime-as-a-Service

Spoofing har vært en landeplage for nordmenn i mange år. Når et telefonnummer blir misbrukt til spoofing, er det to ofre: Den som blir forsøkt lurt, og den som får nummeret sitt misbrukt. Noen kan være mer bekymret for å få telefonnummeret sitt på avveie enn person-nummeret, da telefonnummeret ofte fungerer som en identifikasjon for hvem du er.

Hvem er det så som står bak disse svindelforsøkene?

Anropssvindel kan skje fra mange land, men Telenor er kjent med at det også er skandinaviske kriminelle som står bak flere av svindeloperasjonene. Dette er kriminelle som opererer på tvers av landegrensene. Kriminelle som tidligere drev med tradisjonell kriminalitet bytter nå kanskje beite til digitale bedragerier. Lavere straffer, vanskeligere å bli oppdaget, forbedret tekstinnhold med bruk generativ AI kan være noen av årsakene.

En annen faktor er fremveksten av Crime-as-a-Service, som har gjort det mye enklere å begå kriminalitet på nett og mobil. De kriminelle kan kjøpe tjenester og verktøy som phishing-sett uten å ha teknisk ekspertise. Dette gjør det mulig for både erfarne og uerfarne kriminelle å utføre sofistikerte angrep med minimal innsats. Det er den moderne teknologiens bakside.



"Folk på farten vil gjerne fikse ting fort, og da er det lettere å la seg lure. Svindlerne utnytter folks hastverk og manglende oppmerksomhet på detaljer som kunne ha avslørt svindelforsøket."

Nets har spurt nordmenn:

37 %

av nordmenn sier at de er bekymret for å bli utsatt for svindel eller misbruk når de blir bedt om å taste inn personlige opplysninger, eller betalingsopplysninger, ved betaling på nett.

Forskjellen mellom fysisk og nettsvindel

I dag er nettsvindel den vanligste formen for økonomisk svindel.

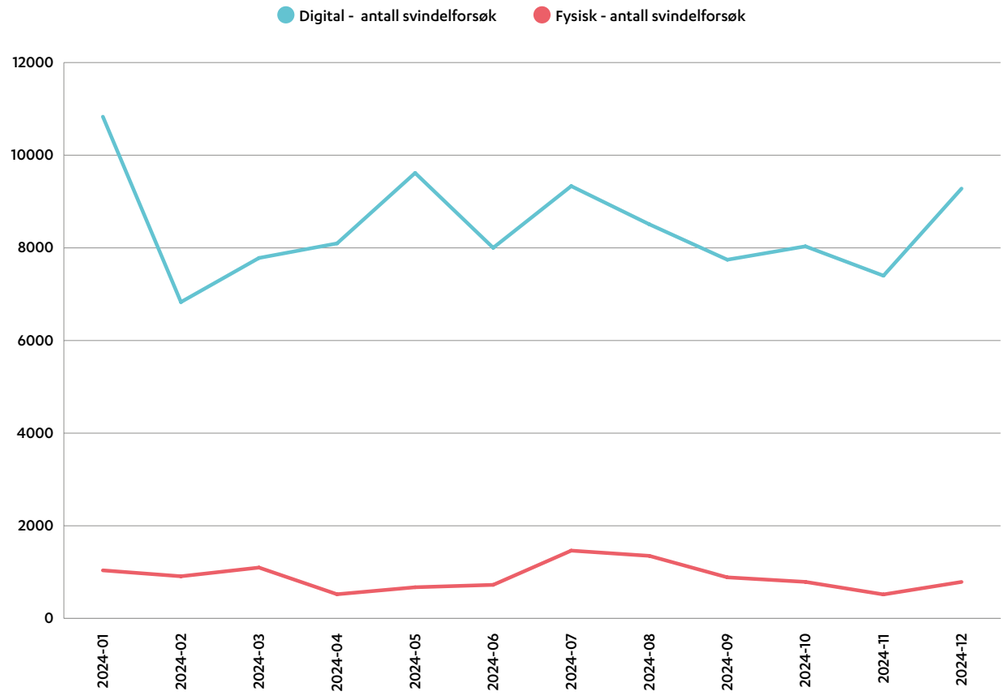
For kriminelle er det mindre risiko forbundet med å operere på nettet. De kan for eksempel bestille varer til anonyme postbokser eller adresser og jobbe fra hvor som helst i verden.

En nyere svindelmetode er at kriminelle stjeler eller kjøper kortopplysninger på det mørke nettet og legger dem inn i sin egen digitale lommebok på telefonen - og dermed har et digitalt betalingskort på telefonen. På denne måten kan de gjennomføre transaksjoner uten å ha det fysiske kortet.

Historisk sett har svindelmetodene endret seg i takt med at nye sikkerhetstiltak har blitt implementert. Dette betyr også at når den digitale sikkerheten strammes inn, kan svindlerne flytte fokuset tilbake til fysiske metoder. Denne skiftende dynamikken kan komme i bølger, med vekslende hyppighet av svindel på nettet og fysisk svindel. Forbrukernes tillit til både digitale og fysiske betalingssystemer er avgjørende. Derfor er det viktig å fortsette å utvikle og forbedre sikkerhetstiltakene på begge fronter for å beskytte mot svindel og opprettholde tilliten.

Den pågående innsatsen mot svindel viser seg også å ha en positiv effekt. Tall fra Den europeiske sentralbanken og Den europeiske banktilsynsmyndigheten viser at Norge har et lavere svindelnivå sammenlignet med gjennomsnittet i EU (2024 Report on Payment Fraud).

Dynamikken mellom fysisk og digital svindel



INTERVJU: DYREPARKEN

Hvordan jobbe mer aktivt mot svindel?

IT-sjef Vidar Skåra i Dyreparken har ikke opplevd forsøk på kortsvindel i sine 20 år i jobben. Likevel har han nok å gjøre for å sikre parken og de besøkende best mulig mot kjeltringer.

Om intervjupersonen Vidar Skåra

Vidar Skåra har siden 2012 hatt rollen som IT-sjef i Dyreparken.

Han er ansvarlig for IT drift, utvikling og koordinering av behov innenfor Dyreparkens hovedsystemer, samt maskinvare og infrastruktur.

Hvordan jobber dere for å sikre dere mot svindel?

De siste årene har vi vært langt mer proaktive enn tidligere. Vi setter av mer tid til risikovurdering for å avdekke potensielle svakheter i våre systemer og redusere risikoen for å bli svindlet. Dette blir vi stadig bedre på.

Opplever dere endring i trusselbildet?

Det finnes mange former for svindel, og vi opplever at våre ansatte utsettes for mer phishing enn før. Vi jobber derfor aktivt med å utdanne våre ansatte om dette og vise dem hvordan svindel kan ta form i forskjellige digitale kanaler. Vi har tidligere opplevd at svindlere utgir seg for å være en direktør i Dyreparken og kontakter regnskapsavdelingen for å få utbetalt penger som haster. Men de har aldri lyktes, da vi har gode rutiner for verifisering av identitet. Samtidig jobber vi forebyggende med bruk av brannmur, overvåkning av maskinvare og brukere.

Utsettes også kunder av Dyreparken for svindelforsøk?

Det vi ser mer av, er personer som forsøker å videreselge produkter de ikke har eller eier via markedsplasser på nett. Dette gjelder særlig salg av reelle billetter til Dyreparken som blir forsøkt solgt flere ganger. Det skjer iblant, men vi fanger det opp da vi aktivt overvåker markedsplassene for å sjekke salg av våre produkter.

Det er også tilfeller av falske fakturaer der det er forsøk på å kjøpe et produkt med kredittkort fra andre enn seg selv, slik at man selv ikke mottar regningen. Om lag 95 prosent av våre kunder er norske, og vi ser at svindelforsøkene i all hovedsak involverer norske personer. Det har vært økt pågang de siste årene, men det er få forsøk på svindel i forhold til antall besøkende og omsetning. I løpet av et år er det 1-2 svindelforsøk som går gjennom, og de blir politianmeldt.

Hvilke tiltak har dere iverksatt for å forebygge svindelforsøk?

Vi har bedret beskyttelsen mot hackerangrep. Til vår fordel har vi spesifikke produkter, som hotellrom, billetter til forestillinger og til parken med dato og klokkeslett. Dette gjør at forsøk på svindel i stor grad fanges opp før selve gjennomføringstidspunktet. Med andre ord er det mulig at dette gjør det vanskeligere for svindlere å gjennomføre et svindelforsøk mot oss.

Dessverre har det vært noen vellykkede svindelforsøk med tilgang til betalingsmidler i nettbutikken vår. Derfor overvåkes bookingen og kjøp på nettbutikken, som er vår absolutt største kanal. Vi får varsler med en gang noe oppfattes som mistenkelig.

Hvordan samarbeider dere med Nets og andre for å forebygge svindel?

Jeg kan faktisk ikke huske at vi har opplevd svindelforsøk med kortbetaling i de 20 årene jeg har jobbet her. Vi samarbeider godt med Nets og opplever kortbetaling som en svært trygg kanal. Samtidig har det hjulpet at myndighetene har satt krav til blant annet autorisering, som har gjort kortbetaling enda tryggere enn tidligere.

Nets' svindelbekjempelse

Anti-svindelteamet i Nets består av 20 nordiske medarbeidere som sammen med svært kraftige dataverktøy jobber døgnet rundt med å minimere svindel ved å overvåke transaksjoner og identifisere potensielle svindelmønstre for bank- og bedriftskundene våre.

Nets vern mot betalingssvindel

- Transaksjonsovervåking 24/7
- Regelbasert overvåkning basert på kunstig intelligens og maskinlæring
- Forbrukerbeskyttelsestjeneste som forhindrer autorisasjoner fra butikker som promoterer f.eks. abonnementsfeller og distribusjon av falske varer
- Identifisering av misbrukte betalingskort, sperring og kommunikasjon med banker og kortholdere
- Overvåkning av mistenkelige butikker og nettsteder
- Kontinuerlig oppdatering av svindellister

Etterforskning

- Løpende samarbeid med politiet for å forebygge og oppklare svindelsaker
- Samarbeid med internasjonale etterforskningsenheter for å bekjempe og forebygge svindel
- Deltakelse i nasjonale, regionale og internasjonale fora for svindelbekjempelse

Analyse

- Implementering av beskyttelse mot alle kjente svindelmønstre, der mistenkelige kjøp som avviker fra etablerte betalingsvaner raskt stoppes
- Analyse av mistenkelig kortholderatferd som oppdages og flagges
- Analyse av de nyeste svindeltrendene

Opplæring og utdanning

- Løpende kundemøter og veiledning om bedre svindelbeskyttelse
- Fokus på kampanjer og samarbeid med myndigheter
- Informasjon til bank- og personkunder om de nyeste svindeltrendene

"Det finnes mange former for svindel, og vi opplever at våre ansatte utsettes for mer phishing enn før. Vi jobber derfor aktivt med å utdanne våre ansatte om dette og vise dem hvordan svindel kan ta form i forskjellige digitale kanaler."

Nets jobber hver dag for å beskytte samfunnet mot digital svindel

I Nets er vi bevisst på vår særegne rolle i det norske betalingssystemet og i kampen mot digital svindel - både som partner for bankene og som leverandør av betalingsløsninger.

I begge tilfeller jobber Nets-medarbeidere hver dag proaktivt for å beskytte samfunnet mot digital svindel. Vi ønsker å motvirke de enorme økonomiske og sosiale omkostningene ved betalingskriminalitet - for den enkelte som rammes, for den lille eller store bedriften og for det generelle samholdet og tilliten i samfunnet.

Nets ønsker å bidra til å forsvare samfunnet og kundene våre mot kriminelle - både før, under og etter et eventuelt svindelforsøk:

Før:
Nets arbeider for å forhindre så mye svindel som mulig ved å overvåke transaksjoner og identifisere mistenkelige betalingsforsøk. Systemene våre er utviklet for raskt å identifisere potensielle svindelforsøk, og vi samarbeider tett med bankene for å kontinuerlig oppdatere sikkerhetskoder basert på de nyeste svindeltypene. I tillegg gjennomfører vi en grundig onboarding og kontroll av nye bedriftskunder for å sikre at de er legitime og ikke er involvert i ulovlige aktiviteter som salg av ulovlige varer eller hvitvasking av penger.

Under:
Når mistenkelige aktiviteter oppdages mens de skjer, kan vi raskt gripe inn. Vi kan for eksempel varsle butikker og forhandlere før de sender varer som er kjøpt med mistenkelige kort. Det daglige samarbeidet med forhandlerne bidrar til å forhindre svindel før den skjer. Vi samarbeider også tett med både banker og politi når systemene våre oppdager mistenkelige mønstre.

Etter:
Etter en svindelsak hjelper etterforskningsenheten vår politiet med å spore opp gjerningsmennene. Vi undersøker hvordan kortdata har havnet i hendene på kriminelle, for eksempel ved å identifisere datalekkasjer slik at vi kan forhindre misbruk av andre kort som kan ha blitt berørt. Ved å analysere data og mønstre fra svindelsaker, forbedrer vi kontinuerlig systemene våre, slik at vi kan oppdage og reagere enda raskere på nye svindelmetoder.

1,1 milliard kroner spart i løpet av 2024

*gjelder butikkene og bankenes kunder

Økt sikkerhet for forbrukere og bedrifter

Nets' forbrukerbeskyttelsestjeneste bidrar til å beskytte bankene og deres kunder mot økonomiske tap og ulemper. Med denne tjenesten stoppet vi svindelforsøk som i 2024 resulterte i en samlet besparelse på over 750 millioner kroner.

Tjenesten reduserer risikoen for at forbrukere engasjerer seg i risikofylte transaksjoner som kan være bedragerske eller ugjennomsiktige - for eksempel datingsider, forfalskede varer og abonnementsfeller. Mange av disse transaksjonene presenteres som attraktive tilbud eller «gode kjøp» som i virkeligheten er utformet for å lure forbrukeren. Ved å analysere advarselsmønstre og oppdage potensielt skadelige transaksjoner og misbruk beskytter Nets kortinnehaveren mot å bli fanget i økonomiske feller som det ofte er dyrt og vanskelig å komme seg ut av.

Eksempler på dette er datingsider som lokker forbrukerne til å chatte med profiler som er automatiserte chatbots - for deretter å ta betalt for videre «kommunikasjon». Vi ser også varer som selges til en brøkdel av den opprinnelige prisen, men der produktet enten er en kopi av dårlig kvalitet eller ikke finnes i det hele tatt. Abonnementsfeller er en annen vanlig felle der et tilsynelatende billig tilbud fører til dyre avtaler.

Med denne tjenesten beskytter vi kortinnehaveren mot fallgruver der et tilbud som ser for godt ut til å være sant, viser seg å være nettopp det - en felle.

Dette er en del av vårt kontinuerlige arbeid - og samarbeid med bankene - for å styrke svindelbeskyttelsen. I Nets er vi opptatt av å gjøre det stadig vanskeligere for kriminelle å lykkes med sine svindelforsøk, og vi leter hele tiden etter nye måter å forbedre sikkerheten og tilliten til betalings-systemene på.

Hva er abonnementsfeller?

Abonnementsfeller er villedende tilbud som lokker forbrukere til å registrere seg for tjenester som ser gratis eller svært billige ut, men som i virkeligheten resulterer i dyre abonnementer. Typiske produkter er hudpleieprodukter, treningsabonnementer og populære goodie boxes, som ofte annonseres på sosiale medier. Brukerne godtar vilkår som skjuler kompliserte avmeldingsprosedyrer, høye gebyrer og urimelige priser i det som står med liten skrift.

INTERVJU: NETS

Slik jobber Nets for å bekjempe svindel i Norge

Om intervjupersonen Herman van Den Weghe

Herman van Den Weghe jobber som Head of Fraud & Transaction Monitoring i Nets, noe som i praksis innebærer at han har det overordnede lederansvaret for å bekjempe svindelforsøk rettet mot Nets' kunder i de nordiske landene.

Fortell litt om rollen din og teamet du leder. Hva slags mandat har dere?

Vi er et team på 20 personer som dekker Norden og Baltikum. I utgangspunktet har vi ansvaret for alt som har å gjøre med transaksjonsovervåkning på vegne av våre kunder. Da er det snakk om forretninger og butikker som tar seg betalt for ting, men ikke banker.

Mandatet mitt er å ha kontroll på riktig og effektiv bruk av ressursene våre og kontroll på vår risiko relatert til svindel.

Hvordan er samspillet med kundene?

Vi har lite direkte dialog med kundene. Jobben vår handler mer om å ha kontroll på om svindel er økende innen spesielle områder, kanaler eller typer butikker. For eksempel kan det plutselig komme et oppsving innenfor blomsterhandel, der det tradisjonelt har vært få utfordringer. Da blir vi veldig årvåkne og lurer på hva det er som foregår. Ofte vil det være startskuddet for en nærmere etterforskning fra vår side.

Det er veldig stor forskjell i hvordan kundene selv bidrar til håndteringen, men mye av overvåkingen er automatisert. Vi forholder oss til regelverket fra aktører som Visa og Mastercard.

Vanligvis ser vi på utvikling over 13 måneder for å kunne sammenligne samme måned over to år på rad. Det er fordi det er viktig å ta hensyn til en del sesongmessige effekter, som for eksempel salg av vinterdekk. Med den nevnte blomsterhandelen er imidlertid sammenligningsgrunnlaget lite, så da skal det mindre til for at vi fatter mistanke.

De aller fleste kundene våre bruker relativt få ressurser på denne typen overvåking, så en etterforskning vil sjelden utløses av at det er kunden som innrapporterer mistanke til oss.

Noen interessante eksempler?

Det er klart vi ser noen absurde utslag av og til. Vi har hatt kunder som har laget nye markedsplaner basert på det de tror har vært sterk kundevekst i et gitt land, men så har det vist seg å faktisk være ren svindel. Det er slike ting Nets fanger opp, men som veldig få kunder ser selv.

For mange virksomheter er det tross alt dyrt og uaktuelt å sette av mye interne ressurser til bekjempelse av svindel. Unntaket er veldig profesjonaliserte aktører som Norsk Tipping og Vipps, som er regulert av myndighetene.

Hvordan samarbeider dere med andre aktører?

Det varierer jo litt fra land til land, men en del ting er felles.

Alle bankene og andre aktører som bruker kortnettverkene har mange forpliktelser. Når kortselskapene får meldt inn et stjålet eller mistet kort, går meldingen videre til Nets. I de fleste tilfeller vil vi ha ligget i forkant og allerede kontaktet dem. Uansett får vi alltid fasiten derfra som kan bekrefte eller avkrefte mistankene våre, transaksjon for transaksjon, og da kan vi lære av det og justere saker vi har hatt oppe til vurdering.

Det meste av svindelen er det naturlig at vi fanger opp etter at den er begått. Slik betalingsnettverket med BankID er skrudd sammen er sannsynligheten for svindel liten. Og når det først skjer blir banken involvert, som har flere ressurser og kjenner kortholders identitet.

PSD2 er et EU-direktiv som regulerer betalingsformidlingen i EU og EØS. I praksis styrer det hvem som taper pengene ved svindel og hva som må sikres med løsninger som BankID.

Herman forteller at teamet hans grovt sett ser to ulike tilnærminger til svindel: enten mange små transaksjoner eller få store.

De som skjønner systemet, har noen smutthull de kan utnytte. For eksempel er det unntak for små transaksjoner under 500 kroner ved tæpping, der trengs det ikke verifikasjon i form av pin-kode. Ved e-handel er terskelen nede på 300 kroner. Men da kan man typisk gruppere mange små handler, for eksempel av gavekort som man i ettertid kan be butikken om å veksle inn i kontanter.

Samtidig vil det være en enorm samfunnsøkonomisk trade-off å eliminere denne risikoen helt, fordi man kan ikke la det bli for tungvint å handle med kort. Denne typen svindel involverer ikke proffene, men småkjeltringer som er fornøyd med noen tusenlapper her og der.

De er plagsomme, men det er ikke der slaget står.

Hvordan skiller Norge seg fra de andre nordiske landene, og hvorfor?

Jeg kan bare svare på hva norske butikker blir utsatt for, så må bankene svare på hva norske kortholdere utsettes for.

Mye av svindelen skjer hos de store internasjonale selskapene, mens det tidligere var vanlig med fysiske kopier av betalingskort som ble brukt i Asia.

Det er mye likt mellom Norge og Norden, men enn så lenge er vi ganske heldige med at det ikke er så veldig mange store profesjonelle aktører som har satt inn støtet her i landet. Det virker som det i Danmark og Sverige er en vesentlig større andel selskaper som opprettes uten noe legitimt formål, for eksempel med falske nettsider som promoteres på sosiale medier. Det er gjerne tilbud som er for gode til å være sanne, for enkle produkter som boxershorts. I realiteten har ikke disse virksomhetene noen produkter overhodet, de har kun en betalingsløsning. Pengene renner inn en kort periode og så forsvinner de. Det største problemet er at kortholder aktivt deltar i handelen, slik at kortet ikke er misbrukt. I Norge ser vi altså heldigvis mindre av dette.

Hva slags bransjer skiller seg ut?

Reiseliv er en klassiker for stjålne kortdetaljer. Hvis du kan reise gratis med taxi i stedet for å ta bussen, så gjør du det. Det er også ganske utbredt med leie av hotellrom for prostitusjonsvirksomhet. En natts opphold kan være nok tid til at vi kan kontakte politiet for å arrestere vedkommende, men bakmennene slipper som regel unna.

"Jobben vår handler mer om å ha kontroll på om svindel er økende innen spesielle områder, kanaler eller typer butikker. For eksempel kan det plutselig komme et oppsving innenfor blomsterhandel, der det tradisjonelt har vært få utfordringer. Da blir vi veldig årvåkne og lurer på hva det er som foregår. Ofte vil det være startskuddet for en nærmere etterforskning fra vår side."

Våre anbefalinger

Betalingssvindel er ikke bare en trussel mot den enkelte forbruker eller virksomhet - men også mot grunnleggende verdier i det norske samfunnet. Tillit og økonomisk samhørighet berøres.

Som samfunn må vi gjøre vårt ytterste for å ligge i forkant av de kriminelle. Det er et permanent våpenkappløp som krever at vi handler raskere og mer fleksibelt.

Engangstiltak og tradisjonelle reguleringsprosesser holder ikke lenger mål. Vi trenger en mer smidig tilnærming der offentlig og privat sektor samarbeider for å reagere på nye trusler så snart vi ser dem.

Vi håper at beslutningstakere, bedrifter og publikum vil ta dem som en invitasjon til videre dialog. Vi er også interessert i å høre andre forslag som kan bidra til å styrke innsatsen vår.

1. Etablere operativ beredskap for å styrke offentlig-privat samarbeid i kampen mot digitalt bedrageri
2. Styrke den offentlige norske motstandskraften mot digitalt bedrageri
3. Styrke det juridiske rammeverket

1

Etablere et operativt innsatsteam for å styrke offentlig-privat samarbeid i kampen mot digitale bedragerier

Vi foreslår at næringsministeren tar initiativ til å etablere et operativt innsatsteam mot betalingssvindel med beslutningsmyndighet til å sette i gang tiltak, dele data og implementere teknologiske løsninger for forebygging og bekjempelse. Innsatsteamet bør samarbeide tett med både nasjonale og internasjonale aktører. Medlemmene bør bestå av både offentlige og private aktører som har kompetanse og ressurser til å bekjempe svindel på en effektiv måte. Betalingsleverandører, banker, telekombransjen, sosiale medieplattformer og andre - med myndighetene i spissen. Det er viktig at medlemmene i responsgruppen har mandat til å implementere løsninger i sine egne organisasjoner.

Konkrete tiltak beredskapsorganisasjonen kan sette i gang for å styrke kampen mot digitale svindelforsøk:

a) Utvikling og bruk av kunstig intelligens

- Utvikle et felles forsvar mot digital svindel ved hjelp av mønstergjenkjenningsteknologi som kan analysere og gjenkjenne mønstre i store mengder transaksjonsdata. Systemet skal kunne samle inn data som aktørene i dag er forhindret fra å dele med hverandre, og dele anbefalinger med enkeltaktører.
- Utvikle et nettsted, en app eller annen teknologi som bruker kunstig intelligens til å hjelpe innbyggerne med å vurdere om bestemte nettsteder, lenker, tekstmeldinger eller e-poster er svindel. Dette vil også redusere innbyggernes reaksjonstid og forhindre forhastede klikk.

b) Kunnskapsdeling og trusselvurdering

- Etabler sikre kanaler for datautveksling mellom alle deltakende aktører. I dag hindrer legitime bekymringer om datasikkerhet og konkurranse et effektivt arbeid mot svindel. En definert gruppe bør ha muligheten til å dele svindelrelatert kunnskap med relevante interessenter for å kunne forebygge svindel bedre og raskere.
- Regelmessige møter for å diskutere det aktuelle trusselbildet og dele innsikt om nye svindelmetoder, samt diskutere og implementere nye initiativer i kampen mot svindel.

2

Styrke Norges motstandsdyktighet mot digital svindel

For effektivt å bekjempe digital svindel - og beskytte tilliten til offentlig sektor - er det nødvendig å styrke utdanning, ressurser og kompetanse i offentlig sektor.

Foreslåtte tiltak:

a) Utdanning og forskning

Utvikling og bruk av kunstig intelligens er avgjørende i kampen mot digital svindel. Dette krever at vi utdanner flere mennesker med de nødvendige ferdighetene for å forberede fremtidige generasjoner på å bekjempe digital svindel. Vi foreslår at kunnskapsministeren tar initiativ til å inkludere cybersikkerhet og kunstig intelligens som viktige temaer i kommende reformer i videregående skole og på universitetene. Det bør også gis større støtte til forskning og utvikling innen digital sikkerhet og kunstig intelligens.

b) Økt samarbeid og koordinering

Vi oppfordrer justisministeren til å bevilge tilstrekkelige ressurser til Økokrim og andre relevante myndigheter for å kunne bekjempe digital svindel på en effektiv måte. Bedre koordinering mellom Økokrim og Skatteetaten er avgjørende for å kunne bekjempe tverrgående svindelmetoder. Økt internasjonalt samarbeid gjennom Interpol er nødvendig ettersom digitale bedragerier opererer globalt og krever en koordinert innsats.

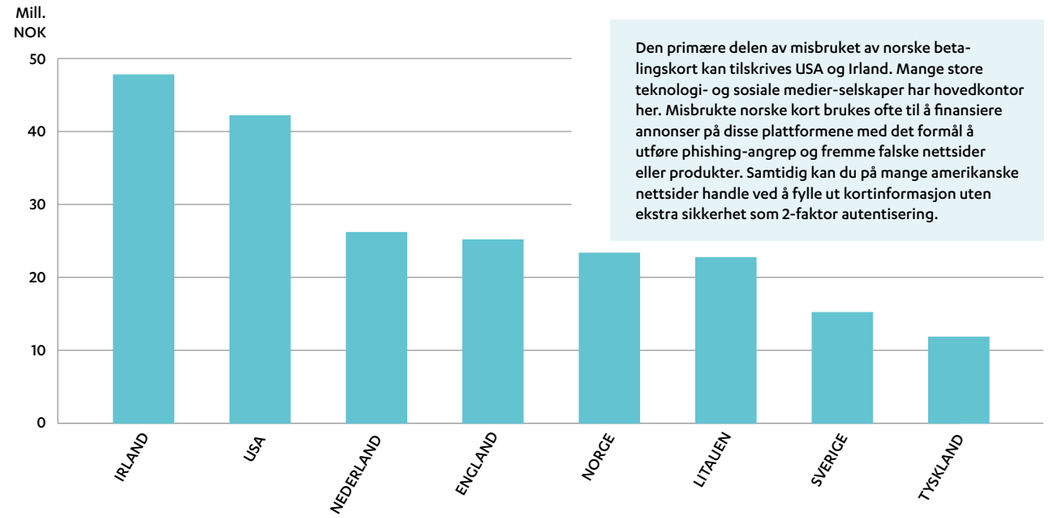
3

Styrke det juridiske rammeverket

a) Regulere sosiale medier

En stor del av digital svindel skjer gjennom bruk av sosiale medier. Vi foreslår at digitaliseringsministeren tar initiativ til å etablere et tydelig juridisk rammeverk som muliggjør en mer effektiv bekjempelse av digitale bedragerier på sosiale medier. Dette bør inkludere krav om at aktører som Meta skal reagere innen en viss varslingstid dersom det foreligger en begrunnet mistanke om svindel på deres plattform. I Nets er vi klare til å støtte dette arbeidet ved å hjelpe Meta og andre plattformer med å identifisere svindel.

Svindel opprinnelsesland



Den primære delen av misbruket av norske betalingskort kan tilskrives USA og Irland. Mange store teknologi- og sosiale medier-selskaper har hovedkontor her. Misbrukte norske kort brukes ofte til å finansiere annonser på disse plattformene med det formål å utføre phishing-angrep og fremme falske nettsider eller produkter. Samtidig kan du på mange amerikanske nettsider handle ved å fylle ut kortinformasjon uten ekstra sikkerhet som 2-faktor autentisering.

b) Regler for tilbakeholdelse av betalinger

Nets er i dag forpliktet til å gjennomføre en betaling senest én virkedag etter kjøpstidspunktet, noe som er regulert i EUs PDS2-direktiv. Nets foreslår at i tilfeller der det foreligger en begrunnet mistanke om svindel, får Nets og andre betalingsleverandører 3-4 dager på seg til å undersøke om mistanken om svindel er berettiget før betalingen gjennomføres. For å styrke kampen mot digital svindel bør reglene for hvor lenge betalingstilbydere kan holde tilbake betalinger ved begrunnet mistanke om svindel justeres. Dagens korte tilbakeholdelsesfrister er ofte utilstrekkelige til å gjennomføre en grundig etterforskning, noe som øker risikoen for at svindeltransaksjoner blir gjennomført og fører til økonomiske tap.

c) Bruk av interne data i kunstig intelligens

I dag finnes det mange ulike reguleringer knyttet til bruk av data i teknologiske løsninger basert på kunstig intelligens. Nets har forståelse for samfunnets legitime ønske om å beskytte borgernes personvern, men økt bruk av persontilpassede kjøpemønstre i vår maskinlæringsovervåkning av transaksjoner vil styrke kampen mot digital svindel. Vi foreslår at myndighetene innfører lovendringer som gjør det mulig for betalingsleverandører å bruke personopplysninger i sine KI-baserte metoder for svindelbekjempelse på en ansvarlig måte. Dette inkluderer strenge retningslinjer og sikkerhetstiltak for å beskytte brukernes personvern og sikre at data kun brukes til svindelbekjempende formål.

d) Nye produkter og teknologier må inneholde en obligatorisk vurdering av konsekvensene av svindel

For å beskytte mot bedrageri bør alle nye produkter og tjenester kreve en vurdering av konsekvensene av bedrageri. For eksempel har innføringen av deepfake og stemmegjenkjenning blitt mye brukt av kriminelle til å begå svindel, men verken EUs forordning om digitale tjenester (DSA) eller forordningen om kunstig intelligens fokuserer på svindel. Regjeringen bør arbeide for å innføre tiltak i EU-lovgivningen som sikrer mot potensielt misbruk av produkter i forbindelse med digital svindel.

nets | nexi

Nets Branch Norway • Lysaker Torg 45 • 1366 Lysaker

payments.nets.eu/nb-NO