



SINTEF

Eksisterende undersøkelser

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim
Sentralbord: 40005100
info@sintef.no

Foretaksregister:
NO 919303808 MVA

VERSJON
1.0

DATO
2024-01-20

FORFATTERE
Stine Skaufel Kilskar
Marte Høyby
Per Håkon Meland

OPPDRAGSGIVER
Justis- og beredskapsdepartementet

OPPDRAGSGIVERS REFERANSE

PROSJEKTNUMMER
102027997

ANTALL SIDER OG VEDLEGG:
10

Overskrift sammendrag

Dette er et vedlegg til Kunnskapsoversikten som viser eksisterende undersøkelser relevante for estimering av omfang av cyberkriminalitet.

UTARBEIDET AV
Stine Skaufel Kilskar

SIGNATUR

GODKJENT AV
Geir Kjetil Hanssen

SIGNATUR

GRADERING
Åpen

COMPANY WITH
MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO 9001 • ISO 14001
ISO 45001



Innholdsfortegnelse

1	Eksisterende undersøkelser i Norge	3
1.1	Mørketallsundersøkelsen.....	3
1.2	Kriminalitets- og sikkerhetsundersøkelsen i Norge	4
1.3	Nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner.....	4
1.4	Bedrageri mot næringslivet (NTAES, 2019).....	5
1.5	Nasjonal trygghetsundersøkelse.....	6
1.6	Politiets innbyggerundersøkelse.....	7
2	Undersøkelser fra andre land.....	8
2.1	Crime Survey for England and Wales.....	8



1 Eksisterende undersøkelser i Norge

Delkapitlene under gir en oversikt over noen sentrale eksisterende undersøkelser i Norge som er relevante for estimering av omfang av cyberkriminalitet. I tillegg til å beskrive hensikten med og metoden for den enkelte undersøkelsen, listes spørsmål og/eller temaer som er direkte relevante for måling av cyberkriminalitet.

1.1 Mørketallsundersøkelsen

Mørketallsundersøkelsen 2022 ble gjennomført av Opinion på oppdrag for Næringslivets Sikkerhetsråd (NSR), og var med dette den 13. mørketallsundersøkelsen innenfor datakriminalitet og digitalisering av NSR. Undersøkelsen søker å gi en kvantitativ vurdering av omfanget av datakriminalitet i Norge som ikke blir politianmeldt. I tillegg har den som målsetning å beskrive den digitale sikkerhetstilstanden i norsk næringsliv samt noen offentlige virksomheter. Mørketallsundersøkelsen 2022 sin populasjon var norske virksomheter i privat og offentlig sektor med mer enn fem ansatte, og utvalget ble trukket fra Datafactory sin database som henter informasjon fra Enhetsregisteret. Det ble gjennomført 2500 telefonintervjuer mellom 3. mars og 12. mai 2022, og data ble vektet på størrelse (antall ansatte) og bransje (RIM-vektet). Siden det før undersøkelsen i 2016 ble gjort endringer i både spørsmål og datainnsamlingsmetode, sammenligner den siste studien kun resultater fra undersøkelsene i 2016, 2018 og 2020.¹

I undersøkelsen blir det lest opp informasjonssikkerhetshendelser som man blir bedt om å svare ja eller nei på om virksomheten har vært utsatt for i det foregående kalenderåret. For de fire siste undersøkelsene inkluderte disse om man har blitt utsatt for følgende:

- Forsøk på datainnbrudd/hacking (2022, 2020, 2018, 2016)
- Phishing eller andre sosial manipuleringsangrep (2022, 2020, 2018, 2016)
- Datainnbrudd/hacking (2022, 2020, 2018)
- Bedrageri (2022, 2020, 2018, 2016)
- Løsepengevirus (2022)
- Hendelse forårsaket av bedriftens ansatte (2022, 2020, 2018, 2016)
- Dataskadeverk (2022, 2020, 2018, 2016)
- Hendelse forårsaket av outsourcingsleverandør (2022, 2020, 2018, 2016)
- Hendelse forårsaket av manglende kontroll på administrativ informasjonssikkerhet (2022)
- Tyveri av IT-utstyr (2022, 2020, 2018, 2016)
- Misbruk av virksomhetens IT-ressurser (2022, 2020, 2018)
- Tyveri eller eksfiltrasjon av data (2022)
- Virus og/eller malwareinfeksjon (2020, 2018, 2016)
- Brudd på sikring av opplysninger om f.eks. brukere, ansatte, kunder, pasienter (2020, 2018)
- Tap av personopplysninger (2016)
- DDoS-angrep eller trusler om (2020, 2018, 2016)
- Penetrasjon av organisasjonens sikkerhetssystemer (2020, 2018, 2016)
- Tapt forretningshemmeligheter gjennom informasjonstyveri/digital spionasje (2020, 2018, 2016)

Det blir også stilt spørsmål om hva som var den mest alvorlige hendelsen i det foregående året.

¹ <https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen>



1.2 Kriminalitets- og sikkerhetsundersøkelsen i Norge

Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) har blitt gjennomført ti ganger i perioden 2006-2021. Den kartlegger kriminalitets- og sikkerhetstilstanden i privat og offentlig næringsliv, og bygger på et utvalg ledere og sikkerhetsansvarlige i 2000 private og 500 offentlige virksomheter. Datainnsamlingen blir gjennomført som telefonintervjuer med utgangspunkt i Datafactory sin database.²

I tillegg til å kartlegge aspekter rundt risikovurdering, trusselvurdering, kontroll av samarbeidspartnere og kontrolltiltak ved ansettelse, kartlegges i de tre siste undersøkelsene hvorvidt virksomhetene i løpet av de siste 12 månedene har blitt utsatt for følgende hendelser:

- Å få tilsendt fakturaer for varer som ikke er bestilt (2021, 2019, 2017)
- Løsepengevirus (2021, 2019)
- Direktørsvindel (2021, 2019, 2017)
- At bedriftens merkevare/logo har blitt misbrukt i falske annonser/kampanjer på nett, SMS eller i epost (2021, 2019)
- Fått tilsendt faktura for varer som er bestilt, men der mottakerkonto er endret til svindlers konto (2021)
- Overrumpende salg over telefon av bedriftsoppfølging i nettkatalog eller lignende (2017)
- Sagt ja til å motta uforpliktende tilbud, en fått tilbud utformet som en forpliktende faktura (2017)

Undersøkelsen for disse årene dekker også spørsmål om hvilken type kriminalitet virksomheten ikke anmeldte, der "kriminalitet i det digitale rom (løsepengevirus, tjenesteangrep, direktørsvindel" er et svaralternativ, samt årsaker til at lovbrudd ikke anmeldes.

1.3 Nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner

Vista Analyse gjennomførte i 2023 en nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner på oppdrag av Justis- og beredskapsdepartementet.³ Dette er en undersøkelse rettet mot private og offentlige virksomheter, og som har til hensikt å kartlegge oppfatninger av lovbruddsbildet samt egne offererfaringer. I tillegg til en elektronisk spørreundersøkelse rettet mot private og offentlige virksomheter og kommuner, er det gjennomført intervjuer med fagetater og representanter fra arbeidslivet. Spørreundersøkelsen ble gjennomført i perioden 14. mars til 23. april 2022 og ble mottatt av et representativt utvalg på 100 000 virksomheter trukket fra proff.no sin database. Svarprosent på første spørsmål var 8,4 prosent og på siste spørsmål 6.8 prosent. Det skiller i analysen mellom virksomheter med flere enn fire ansatte og virksomheter med null til fire ansatte, da de største er sammenlignbare med tidligere undersøkelser gjennomført av Statistisk sentralbyrå i 2003 og 2008.

Spørreundersøkelsen spør om utsatthet siste år, og spørsmålene er formulert slik at de er i tråd med gjeldende straffelov. Sentrale problemstillinger i undersøkelsen er kategorisert etter:

- Utsatthet for Kriminalitet – omfanget av økonomisk kriminalitet

² <https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino>

³ <https://www.regjeringen.no/globalassets/departementene/jd/dokumenter/rapporter-planer-og-strategier/nasjonal-omfangsundersokelse-av-okonomisk-kriminalitet-rettet-mot-virksomheter-og-kommuner.pdf>



- Konsekvenser av utsatthet
- Risiko for lovbrudd og forebyggende tiltak
- Utvikling over tid, i den grad det er metodisk forsvarlig å sammenligne.

Med utgangspunkt i Økokrim sin definisjon av økonomisk kriminalitet, skal den lovstridige handlingen være profittmotivert. Dette innebærer at profittmotiverte lovbrudd i kategorien datainnbrudd kan karakteriseres som økonomisk kriminalitet. Undersøkelsen viser at datainnbrudd er den nest største kategorien etter bedrageri. Undersøkelsen kartlegger videre hvilke metoder som ble benyttet i gjennomføringen av det siste tilfellet av bedrageri og datainnbrudd, der svaralternativene inkluderer:

- Kapring av nettside
- Falsk nettside
- Falsk avsender (spoofing)
- Datasnoking (phishing)
- Tjenestenektangrep
- Skadevare (virus e.l.)
- Løsepengevirus
- Datainnbrudd (hacking)

1.4 Bedrageri mot næringslivet (NTAES, 2019)

Nasjonalt tverretattlig analyse- og etterretningssenter utga i 2019 en rapport om bedrageri mot næringslivet etter oppdrag fra Det sentrale samarbeidsforum.⁴ Analysen ble utført med tanke på foretak som er registrert i Norge og som har virksomhet i Norge. Anmeldelser av bedragerier er lagt til grunn i analysen av omfang og utvikling samt i analysen av kjennetegn ved gjerningspersoner og fornærmede. Analysene tar også i bruk koder fra straffelovens kapittel om *informasjon og informasjonsutveksling* knyttet til datainnbrudd og identitetstyveri, som ofte finnes i bedragerisammenheng. Analysen omfatter blant annet:

- Antall anmeldelser for et utvalg av lovbruddstyper underlagt straffelovens kapittel 21, Vern av informasjon og informasjonsutveksling i 2016-2018: Ubertettiget befatning med tilgangsdata, data-program mv.; Identitetskrenkelse, befatning med annens identitetsbevis; Identitetskrenkelse, opptre med annens identitet; Innbrudd i datasystem.
- Prosentandel hvor private foretak er fornærmet i utvalgte kriminalitetstyper i 2018 (samme typer kriminalitet som over).
- Estimert angrepssum på bedrageri fordelt på transaksjoner gjennomført eller forsøkt gjennomført i 2016-2018: Bedrageri, transaksjon i nettbank; Bedrageri, korttransaksjon.
- Estimert angrepssum for transaksjoner foretatt gjennom nettbank i 2018 fordelt på modus: Fakturabedrageri; Kjærlighetssvindler og svindel via sosiale medier; Direktørsvindel; Investeringsbedrageri; Falsk IT-support; Phishing; Skadevare; Annet.
- Estimert angrepssum for transaksjoner foretatt gjennom nettbank og med kort i 2018, fordelt på modus: Kortbedrageri; Investeringsbedrageri; Fakturabedrageri; Direktørsvindel; Phishing; Skadevare; Annet.
- Antall rapporterte phishing-e-poster og phishing-websider 2012-2018.

⁴ <https://ntaes.no/reports/NTAES%20Rapport%20bedrageri%20n%C3%A6ringslivet.pdf>



1.5 Nasjonal trygghetsundersøkelse

Nasjonal trygghetsundersøkelse kartlegger uro og selvopplevd utsatthet for lovbrudd i den norske befolkningen. Undersøkelsen er gjennomført to ganger i Norge, henholdsvis våren 2021 (med spørsmål som refererer til 2020) og våren 2023 (med spørsmål som referer til 2022). Utvikling og gjennomføring av undersøkelsen er gjort av forskere og utredede fra NOVA og NIBR ved OsloMet, Frischsenteret og Ideas2evidence. Undersøkelsen er finansiert av Justis- og beredskapsdepartementet. Lovbrudd som blir kartlagt er lovbrudd med personofre, som tyveri, vold, hatkriminalitet og seksuell vold.⁵

I den siste av undersøkelsene ble et representativt utvalg på 68 000 personer fra 16 til 84 år trukket tilfeldig fra Folkeregisteret og invitert til å delta. Av disse, deltok 25 420 personer, som gir en svarprosent på 37 %. Bakgrunnsvariabler i studien inkluderte kjønn, alder, utdanning og innvandringsbakgrunn. Undersøkelsen ble distribuert som et digitalt spørreskjema. Innen temaet digital kriminalitet beskriver hovedrapporten fra Nasjonal trygghetsundersøkelse 2022 følgende:

- Andel utsatt for digital kriminalitet
- Andel utsatt for digital kriminalitet, etter sentralitet
- Andel utsatt for digital kriminalitet, etter politidistrikt
- Andel utsatt for digital kriminalitet, etter lovbrudd, hhv.
 - Misbruk av kortopplysninger
 - Bedratt ved kjøp av varer eller tjenester
 - Utsatt for kontaktbedrageri
 - Misbruk av personopplysninger eller identitetstyveri
 - Opplevd at bilder eller videoer har blitt videresendt eller spedt på internett
 - Utsatt for gjentakende trakasserende oppførsel
- Andel blant utsatte som anmeldte til politiet, etter lovbrudd
- Viktigste årsaker til å ikke anmelde lovbrudd, etter lovbrudd
- Økonomisk tap ved vinningslovbrudd (medianverdi)
- Økonomisk tap i ved vinningslovbrudd (medianverdi), etter anmeldelse

Under seksuell vold, skilles "Digital seksuell vold" ut som en egen kategori, der undersøkelsen kartlegger:

- Andel utsatt for minst én seksuell voldshandling mot sin vilje, etter lovbrudd, deriblant:
 - Tatt bilde av eller filmet under seksuelle handlinger
 - Truet med deling av seksualiserte bilder eller videoer
 - Deling av seksualiserte bilder eller videoer
 - Tvunget til å sende eller strøme seksualiserte bilder eller videoer
 - Tvunget til å utføre seksuelle handlinger over telefon eller internett
- Andel blant utsatte som anmeldte til politiet, etter lovbrudd
- Viktigste årsaker til å ikke anmelde lovbrudd, etter lovbrudd

I tillegg dekker undersøkelsen spørsmål om hvorvidt man i 2022 bekymret seg for å bli utsatt for svindel eller bedrageri på internett, for å bli utsatt for identitetstyveri eller for at bilder, videoer eller opplysninger om deg skal bli spredt mot ens vilje (via internett eller andre steder).

⁵ Nasjonal trygghetsundersøkelse 2022. NOVA-rapport 14/23. Oslo: NOVA, OsloMet (oda.oslomet.no)



1.6 Politiets innbyggerundersøkelse

Politiets innbyggerundersøkelse gjennomføres av Kantar Public på oppdrag for Politidirektoratet, og er en årlig kartlegging av innbyggernes oppfatninger av politiet i Norge. Undersøkelsen ble gjennomført første gang i 2004, men i 2022 ble det gjort vesentlige endringer. Tidligere har undersøkelsen blitt gjennomført som telefonintervjuer, mens den fra 2022 gjennomføres digitalt. Dette er derfor også vurdert som et nullpunkt for å se utviklingstrekk over tid.⁶

Oppsummeringsrapporten fra Politiets innbyggerundersøkelse 2022 inkluderer et eget kapittel om «Digital trygghet og politiets digitale tilstedeværelse» som oppsummerer funnene fra følgende spørsmål:

- Alt i alt, hvor trygg føler du deg når du bruker digitale tjenester? – etter alder kjønn og utdanning?
- I hvilken grad er du bekymret for at følgende kan ramme deg ved bruk av digitale tjenester?
 - Svindel eller bedrageri
 - Identitetstyveri
 - Deling av bilder eller videoer uten tillatelse
 - Trusler
 - Hatkriminalitet
 - Skremmende eller plagsom atferd
 - Seksuelle overgrep eller krenkelser
- Har du i løpet av det siste året lagt merke til politiet på noen av de følgende plattformene?
Svaralternativer: Facebook, Nettaviser, Twitter, TikTok, Politiets hjemmesider, Instagram, Snapchat, YouTube, Reddit.

I tillegg til å kartlegge innbyggernes bekymring for ulike typer kriminalitet, kartlegger undersøkelsen også innbyggernes opplevelse og utsatthet for i alt ni kategorier av negative hendelser, samt tilbøyelighet til anmeldelse for de ulike hendelsestypene man har blitt utsatt for. Disse inkluderer vold/mishandling, trusler, voldtekt, seksuelle overgrep eller krenkelser, skremmende eller plagsom atferd, tyveri på offentlig sted, utpressing, identitetstyveri, svindel eller bedrageri, og deling av bilder eller videoer uten tillatelse. Hendelser innen flere av disse kategoriene kan dreie seg om datakriminalitet – men trenger ikke å gjøre det.

Undersøkelsen 2021 inkluderte derimot konkrete spørsmål om hvilke typer nett- eller datakriminalitet man har opplevd eller blitt utsatt for, med følgende svaralternativ: Bedrageri/svindel eller forsøk på dette via internett eller mobiltelefon; Virus eller annen type skadevare; Datainnbrudd; ID-tyveri, Mobbing eller trakassering på internett eller mobiltelefon; Utpressing på internett eller mobiltelefon; Seksuelle overgrep eller seksuelle krenkelser digitalt, Annet, Vet ikke. Undersøkelsene 2018-2020 inkluderte følgende datakriminalitetsrelaterte svaralternativer i et mer generelt spørsmål om hvorvidt man i løpet av siste år har vært personlig utsatt for typer kriminalitet: Svindel eller bedrageri på Internett (2020, 2019, 2018); Mobbing eller trakassering på Internett (2020, 2019, 2018); Seksuelle overgrep eller krenkelser på Internett (2020, 2019, 2018) og Identitetstyveri (2020, 2019, 2018). Noen av disse var inkludert i undersøkelsene 2016-2017, mens det i året før var ett datakriminalitetsrelatert svaralternativ: Datakriminalitet eller kriminalitet på Internett (2015). 2014-undersøkelsen dekket ikke dette aspektet under spørsmål om opplevd kriminalitet.⁷

⁶ <https://www.politiet.no/om-politiet/tall-og-fakta/innbyggerundersokelsen/#endring-av-metode-og-utvalg-button>

⁷ <https://www.politiet.no/om-politiet/dokumenter-strategier-og-horinger/dokumenter/?tema=164&enhet=829>



2 Undersøkelser fra andre land

2.1 Crime Survey for England and Wales

Crime Survey of England and Wales (CSEW) er en undersøkelse der folk bosatt i husholdninger i England og Wales blir spurt (ansikt-til-ansikt) om deres opplevelser med ulike typer kriminalitet de siste 12 månedene før intervjuet. Respondentene blir også spurt om egne holdninger til ulike kriminalitetsrelaterte tema, som politi og rettssystem, samt oppfatninger av kriminalitet og antisosial atferd. Et representativt utvalg på totalt 31 183 intervjuer ble gjennomført som del av undersøkelsen 2022-2023.⁸ Disse brukes til å lage estimater på nasjonalt nivå. Resultatene fra denne perioden ble publisert i oktober 2023.⁹ Neste utgivelse kommer 25. januar 2024.

I følge Kantar Public UK¹⁰ er *The Crime Survey for England and Wales* svært viktig for å forstå det faktiske nivået av kriminalitet blant befolkningen. Den kritiske verdien ligger i evnen til å finne ut om kriminalitet som ikke blir rapportert til eller registrert av politiet. Det argumenteres også for at undersøkelsen fanger opp ny og fremvoksende kriminalitet, bedrageri og online kriminalitet, i tillegg til tradisjonell kriminalitet som tyveri og overfall/overgrep.

Detaljert informasjon om datasettene som er brukt for å sammenstille kriminalitetsstatistikken er inkludert i «*User guide to crime statistics for England and Wales: March 2023*».⁸ Datasettet «*Crime in England and Wales: Appendix tables*» kan lastes ned fra nettsiden til Office for National Statistics.¹¹ Under gir en oversikt, hentet fra dette datasettet, over hvilke cyberkriminalitetsrelaterte data som inngår. Merk at det er her trukket ut både *fraud* og *computer misuse*, selv om svindel ikke trenger å være datarelatert.

- Summary Table 1: Police recorded crimes - rates, numbers and percentage change.
 - Total fraud and computer misuse offences

- Worksheet A1: Trends in CSEW incidents of crime, people aged 16 and over/households with percentage change and statistical significance of change.
 - Fraud
 - Bank and credit account fraud
 - Consumer and retail fraud
 - Advance fee fraud
 - Other fraud
 - Computer misuse
 - Computer virus
 - Unauthorised access to personal information (including hacking)

⁸<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/userguidetocrimestatisticsforenglandandwales>

⁹ [Crime in England and Wales: year ending June 2023](https://www.criminology.co.uk/en/AboutTheSurvey.html)

¹⁰ <https://www.criminology.co.uk/en/AboutTheSurvey.html>

¹¹<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>



- Table A1C: Trends in CSEW incidents of crime, people aged 16 and over/households with percentage change and statistical significance of change compared to the year ending June 2022
 - Fraud
 - Computer misuse

- Worksheet A2: Trends in CSEW incidence rates, people aged 16 and over/households, with percentage change and statistical significance of change.
 - Fraud
 - Bank and credit account fraud
 - Consumer and retail fraud
 - Advance fee fraud
 - Other fraud
 - Computer misuse
 - Computer virus
 - Unauthorised access to personal information (including hacking)

- Worksheet A3: Trends in CSEW percentages of people aged 16 and over/households who were victims once or more (prevalence risks), with percentage point change and statistical significance of change.
 - Fraud
 - Bank and credit account fraud
 - Consumer and retail fraud
 - Advance fee fraud
 - Other fraud
 - Computer misuse
 - Computer virus
 - Unauthorised access to personal information (including hacking)

- Table A4a: Police recorded crime by offence, year ending March 2003 to year ending June 2023 and percentage change between year ending June 2022 and year ending June 2023.
 - Total fraud and computer misuse offences
 - Total fraud offences recorded by the police
 - Fraud and computer misuse offences recorded by Action fraud
 - Fraud offences referred to NFIB by Cifas
 - Fraud offences referred to NFIB by UK Finance

- Table A4b: Police recorded crime by offence, July 2019 to June 2023
 - Total fraud and computer misuse offence
 - Fraud and computer misuse offences recorded by Action fraud
 - Fraud offences referred to NFIB by Cifas
 - Fraud offences referred to NFIB by UK Finance

- Table A5: Fraud and computer misuse number of offences recorded by Action Fraud or referred to the National Fraud Intelligence Bureau (NFIB), with percentage change.



- Total fraud offences
 - Banking and credit industry fraud
 - Business trading fraud
 - Insurance fraud
 - Telecom industry fraud (misuse of contracts)
 - All charity fraud
 - Advance fee payments
 - Financial investments
 - Consumer and retail fraud
 - Corporate fraud
 - Pension fraud
- Computer Misuse Offences
 - Computer viruses/malware
 - Denial of service attack
 - Denial of service attack (extortion)
 - Hacking – server
 - Hacking – personal
 - Hacking - social media and email
 - Hacking - PBX/dial through
 - Hacking (extortion)
- Table A7: Police recorded crime rates, rates per 1,000 population from year ending March 2003 to year ending June 2023
 - Total fraud and computer misuse offences
 - Fraud and computer misuse - police and Action Fraud
 - Fraud – Cifas
 - Fraud - UK Finance
- Worksheet A8: Trends in CSEW victims of crime, people aged 16 and over/households with percentage change and statistical significance of change
 - Fraud
 - Bank and credit account fraud
 - Consumer and retail fraud
 - Advance fee fraud
 - Other fraud
 - Computer misuse
 - Computer virus
 - Unauthorised access to personal information (including hacking)