Informasjonssikkerhet

FARTT – 2022

FJELLREGIONEN IKS

Hva er informasjonssikkerhet

- **Konfidensialitet**
  - Informasjon blir ikke kjent for uvedkommende
- **Integritet**
  - Informasjon blir ikke endret utilsiktet eller av uvedkommende
- **Tilgjengelighet**
  - Informasjon er tilgjengelig ved behov

Informasjonssikkerhet og personvern

En menneskerettighet

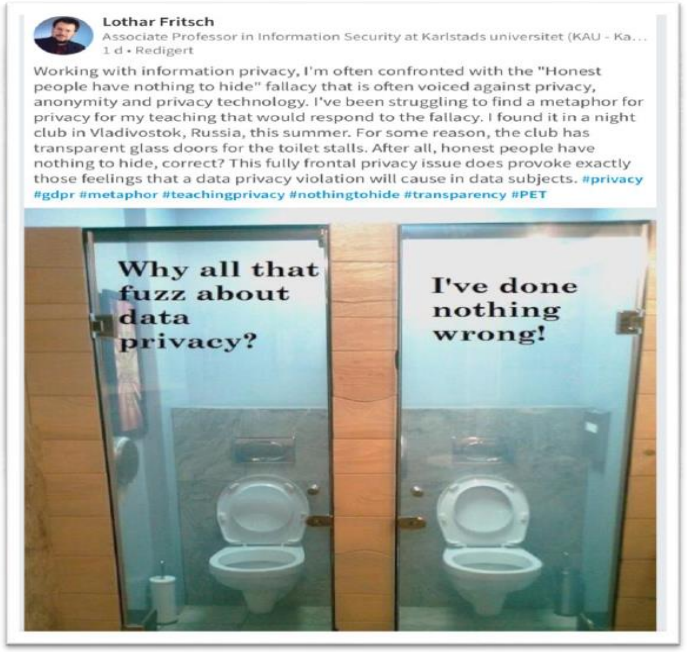
- Art. 8 Den europeiske menneskerettskonvensjon (EMK)
- Art. 12 FNs verdenserklæring om menneskerettigheter
- Paragraf 102 i Grunnloven:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.» (mai 2014)

Informasjonssikkerhet og personvern

Hva er personvern?

- Beskyttelse av privatlivets fred
- Ivaretakelse av den personlige integritet
- Retten til å bestemme over egne personopplysninger



Informasjonssikkerhet og personvern

Hva er en personopplysning?

Identitet: Navn, fødselsnummer, sivilstatus, høyde, vekt

Kontaktinfo: Adresse hjemme, adresse jobb, mobilnummer, e-post, etc.

Finans: Inntekt, skatt, gjeld, bankkonto, kontoutskrift, utgifter, kredittvurdering etc.

Pseudonymiserte opplysninger
mann, 57 år, Bærum, gift, en voksen sønn, hund, Datatilsynet, SPK, Statens informasjonstjeneste, Grimstad kommune, oppvokst i Eigersund

Aktivitet: Adferdsmønstre, interesser, hobbyer, utdanning, yrkesliv, lokasjon, posisjon, kjøpemønster, søkehistorikk, likes etc.

Kommunikasjon: MAC-adresse, IP-adresse, SMS, MMS, fotografier, videoer, sosiale medier, sosialt nettverk, kontakter, cookies etc.

Særlige kategorier:
Helseopplysninger, fagforeningsmedlemskap, politisk oppfatning, religion, seksuelle forhold/orientering, etnisitet/rase

Informasjonssikkerhet og personvern

Om sensitive personopplysninger?

Art. 9

- Særlige kategorier av personopplysninger
  - Rasemessig eller etnisk opprinnelse
  - Politisk oppfatning, religion, overbevisning
  - Fagforeningsmedlemskap
  - Genetiske opplysninger
  - Biometriske opplysninger med det formål å entydig identifisere en fysisk person
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering

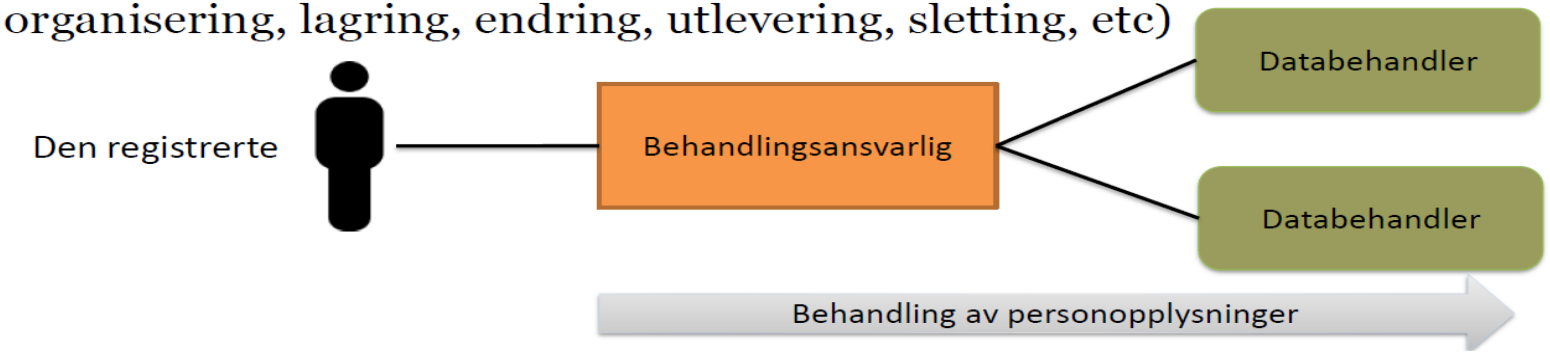
Art. 10

- (Personopplysninger om straffedommer og lovovertredelser)

Informasjonssikkerhet og roller

Kjenn din – og andres roller

- **Den registrerte:** Enkeltperson som det behandles personopplysninger om
- **Behandlingsansvarlig:** Virksomheten som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes
- **Databehandler:** Virksomhet som behandler personopplysninger på vegne av, (og etter avtale med) den behandlingsansvarlige
- **Behandling (av personopplysninger):** Enhver prosessering (innsamling, organisering, lagring, endring, utlevering, sletting, etc)



Hovedprinsipper for beskyttelse av personopplysningene til brukere, innbyggere og ansatte mv (de registrerte)

- Ikke lagre og bruke mere opplysninger enn nødvendig for tjenesten
- Kun de som har tjenestelig behov skal ha tilgang til opplysningene
- Opplysningene skal være korrekte og oppdaterte og beskyttet mot uautorisert endring
- Opplysningene skal være tilgjengelige når de trengs i tjenesten
- De registrerte skal kunne få innsikt hva vi har registrert på dem og hva vi bruker dataene til (åpenhet)
- Kun bruke data til det formålet de er innsamlet/ lagret for

Informasjonssikkerhet, rettigheter og plikter

Noen har rettigheter – andre har plikter

- De **registrerte** har **rettigheter**
- Behandlingsansvarlig, databehandler, underleverandører har **plikter**

Informasjonssikkerhet, rettigheter

Figur 18: Illustrasjon av de registrertes rettigheter etter GDPR.

Personvernombudets (PVO) oppgaver (art 39)

- Informere og gi råd – veilede og bidra til opplæring
- Kontrollere og ha oversikt, samt bidra til at virksomheten har oversikt over sine behandlinger av personopplysninger
- Gi råd og vurdere personvernkonsekvensvurderinger (DPIA): Behandlingsansvarlige pålegges å be PVO om råd (art 35)
- Samarbeide med Datatilsynet og være kontaktpunkt
- Kunne bidra til å vurdere personverntrusler både teknisk, organisatorisk, omgivelsesmessig og på andre måter

Personvernombudets (PVO) oppgaver (art 39)

- Bidra til at det implementeres internkontrollsystemer for informasjonssikkerhet og personvern
- Sørge for at det finnes et avviksregister
- Melde avvik til Datatilsynet (eller sørge for at andre gjør dette)
- Prioritere innsatsen dit hvor personvernrisikoen er høyest

Personvernombudets rolle

- Skal bistå med at virksomhetene holder seg innafor personvernregelverket
- Bidra til å utvikle «ryggmarksrefleks for personvern» hos ledere og ansatte
- Kommer vi dit at **alle tenker:**

«her tror jeg det er noe personverngreier- best vi undersøker litt» ,

- da har vi kommet langt!

Eksempler på personvernbrudd

- **Tilgangsstyring**
  - Elever får tilgang på andre elevers personopplysninger.
  - Leverandører får utilsiktet tilgang på sensitive data ved vedlikehold av datasystemer.
  - Ansatte uten definert behov har adgang på personopplysninger de ikke har bruk for.
- **Publisering av personopplysninger**
  - Informasjon til offentligheten (postliste) inkluderer personopplysninger eller opplysninger som kan settes samme slik at alle skjønner hvem det gjelder
  - Dokumenter med personopplysninger gjøres tilgjengelig på websiden til kommunen

Fødselsnummer på e-post

- **Skal ikke forekomme! Her syndes mye**
- Fødselsnummer er i personopplysningsloven definert som en ordinær personopplysning. Selv om fødselsnummer ikke hverken er sensitivt eller taushetsbelagt, er det beskyttelsesverdig. Det er lagt klare begrensinger på bruken av fødselsnummer og det skal kun anvendes når det er saklig behov for sikker identifisering av en person og når fødselsnummeret er nødvendig for å oppnå en slik identifisering.

Husk at fødselsnummer likevel kan være taushetsbelagt etter særlovgivningen, slik som eksempelvis NAV-loven § 7 og Lov om barneverntjenester § 6-7.»

Fødselsnummer på e-post

- Når fødselsnummer sendes i e-post eller ved hjelp av annen telekommunikasjon, skal det krypteres.
- Kryptering eller sikring av fødselsnummer er viktig også når fødselsnummer sendes gjennom usikrede nettverk. Kryptering er spesielt viktig når det sendes i e-post eller over internett. Alminnelig usikret e-post eller annen ukryptert internettkommunikasjon gir ikke tilfredsstillende informasjonssikkerhet.

Kryptering (Datatilsynet)

Feilsending av brev/e-post - eksempler

- **Feilsending av brev/e-post**
  - E-post/brev med personopplysninger sendes til feil privatperson.
  - E-post/brev med personopplysninger sendes til feil etat/instans.
  - E-post/brev med personopplysninger deles med flere enn nødvendig internt.
- **Bruk av personopplysninger uten samtykke**
  - Dere bruker bilder av barn/unge/beboere på oppslagsvegg uten samtykke
  - Dere distribuerer video om barn uten samtykke
  - Dere bruker sensitive personopplysninger (eksempelvis helseforhold) uten samtykke
- **Lagring av sensitive data på feil sted**
  - Sensitive data lagres utenfor angitt lagringsområde
  - Sensitive data ligger på pulter/hyller der mange har tilgang
  - Personopplysninger lagres på privat utstyr (PC/mobil/USB o.l.)

Brudd på retningslinjer

- **Hva gjør du hvis det oppstår eller det er mistanke om personvernbrudd**
  - Du skal straks varsle din leder
  - Dersom personvernbruddet kan føre til negative konsekvenser for den/de det gjelder skal disse varsles slik at de kan gjøre egne tiltak
  - Alvorlige brudd skal også meldes til Datatilsynet, innen 72 timer
  - Varsling til de registrerte og til Datatilsynet skal gjøres i eller i samråd med ledelsen
  - Personvernombudet skal ha varsel om alle personvernbrudd

Rutine på Compilo, Avviksbehandling personvernsaker

Avvik personvernregelverket meldes til Datatilsynet

- Melde avvik til Datatilsynet – gode rutiner må på plass
- PVO har tilgang til å melde avvik til Datatilsynet på vegne av den enkelte kommune
- Skjema på AltInn «Melding om avvik (Datatilsynet)DPA-01»
- Avvik meldt inn til Datatilsynet fra FARTT kommunene:
  2019 = 1
  2020 = 1
  2021 = 3

Melding om avvik

Datatilsynet

Innsender

Organisasjonsnummer	988448680
Navn	IKT FJELLREGIONEN IKS
Adresse	Tynset Kommune Rådhuset
Postnr og sted	2500 TYNSET

Melder din virksomhet dette avviket som behandlingsansvarlig eller databehandler? (•) Behandlingsansvarlig ( ) Databehandler

Beskrivelse av avviket

Hovedårsak til avviket	Annet		
Forklar årsaken til avviket	Usikkert hva årsaken er.		
Tidsrom for avviket	21.09.2019	til	24.09.2019
Når ble avviket oppdaget	21.09.2019	Kl.	17:00:00
Angi hvor mange personer som kan være berørt av avviket	1		

Beskriv hva som har skjedd. Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.

[redacted] fikk en epost på sin Ipad under ferie i Spania. Hun åpnet eposten, og et Skjema om søknad om øk sosialhjelp (kun første side av søknadskjemaet) "dukket opp". Skjemaet gjelder søknad fra en innbygger i Rendalen kommune om øk sos hjelp.

Hvordan oppstod avviket?

Vi prøver å finne det ut. Mottakeren av eposten har fått beskjed om ikke å slette noe fra Ipaden før hun kommer hjem fra ferie ca 7/10.

Beskriv hva slags type personopplysninger som ble berørt av avviket

Navn , adr, fødselsnummer, kontonummer, hva pasienten søker støtte til og hvorfor, tannhelse, øk situasjon.

Hvilken relasjon har virksomheten til de personene som er berørt av avviket?

Bruker av sosiale tjenester i Rendalen kommune.

Beskriv hvor personopplysningene befinner seg etter avviket. Skriv også hvor mange og hvilken type mottakere som kan ha fått eller sett opplysningene.

På nettbrettet ti[redacted]og hun lovet å ikke vise det videre.

Konsekvenser

Beskriv mulige konsekvenser avviket har medført for de berørte personene.

Personopplysninger kommet uvedkommende i hende.

Tiltak

Beskriv hvilke tiltak som er gjort og planlagt for å forhindre at hendelsen skal skje igjen. Beskriv hva som er gjort for å redusere potensielle skadevirkninger.

Datatilsynet

IKT FJELLREGIONEN IKS
Tynset Kommune Rådhuset
2500 TYNSET

Deres referanse	Vår referanse	Dato
AR337046624	19/02873-2/MBA	15.10.2019

Melding om avvik - IKT FJELLREGIONEN IKS

Vi viser til avviksmeldingen dere har sendt inn.

Dere opplyser at dere har truffet tiltak for å lukke avviket og begrense konsekvensene, samt hindre at dette skal skje igjen i fremtiden.

Vi legger til grunn at dere følger opp at tiltakene dere har iverksatt fungerer og er tilstrekkelige. Det er viktig at organisatoriske og tekniske tiltak følges opp med god opplæring.

Vi avslutter saken med dette.

Med vennlig hilsen

Monica Barø
Monica Barø
rådgiver

Det er viktig å forstå

- Personvernkonsekvenser
  - Konsekvenser for den registrertes rettigheter og friheter
- Personvernrisiko
  - Hvor ille er / kan det bli for den registrerte?
  - Personvernrisiko vurderes høyere hvis
    - det gjelder barn
    - det er store mengder personopplysninger og/eller
    - det gjelder mange perso...

..husk!

Et hvert uoppdaget avvik, er et tapt forbedringspotensial.

Sørg for å ha interne rutiner for å oppdage avvik og for å ha rutiner for hendelseshåndtering når avvik har oppstått!

Opplæring ansatte informasjonssikkerhet

- Opplæring ansatte i IKT-sikkerhet: vi må kunne dokumentere at alle er opplært – Bra e-læringsprogram på KS-Læring
- KS Læring – kommunen skrive avtale med KS – Pris årlig 5000 + 0,95 pr innbygger + opplæring superbruker (priser 2020)
- Prøvd ut for alle på kommunehuset i Tolga 2021. Og alle som jobber i FARTT i 2022.

- Ellers: Se Datatilsynets sider- veldig mye bra info der !!

Sikkerhetsarbeid er som husarbeid - du ser det først når det ikke blir gjort !

Informasjonssikkerhet – ansvar og roller

Kommunen-behandlingsansvarlig

- Kommunen er etter loven den som bestemmer formålet med behandlingen av personopplysningene, hvilke hjelpemidler som skal brukes og er ansvarlig for at personopplysningsloven og personopplysningsforskriften følges
- I kommunen er det rådmann/kommunedirektør som er behandlingsansvarlig

IKT Fjellregionen IKS-databehandler

- IKT Fjellregionen IKS er databehandler for hver av FARTT kommunene og behandler personopplysninger på vegne av behandlingsansvarlige og må følge lover og plikter som gjelder for denne
- Databehanderavtalen regulerer forholdet mellom IKT Fjellregionen og kommune

Informasjonssikkerhet – ansvar og roller

«Behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsrett eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett. (Personopplysningsloven, 2018, artikkel 4 nr. 7).

Informasjonssikkerhet – ansvar og roller

«Databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. (Personopplysningsloven, 2018, artikkel 4 nr. 8).

Informasjonssikkerhet – IKT Sikkerhetsutvalget

Sikkerhetsutvalget består av en representant fra hver av FARTT kommunene, fra FARTT og skal være et rådgivende utvalg for:

- Deling av erfaringer og kunnskap om effektiv og praktisk håndtering av informasjonssikkerhet
- Koordinering og samordning av kommunenes arbeid med oppfølging av Personvernforordningen og Personopplysningsloven
- Utvikling og vedlikehold av felles strategier, maler, prosedyrer og annet verktøy for slik oppfølging

Informasjonssikkerhet – operativ drift i FARTT

I det daglige er arbeid med informasjonsikkerhet en viktig del av operativ drift i FARTT.

Operativ sikkerhetsgruppe i FARTT har stort fokus på dette og følger råd og retningslinjer fra flere sentrale aktører som driver operativt sikkerhetsarbeid i Norge:

- Nasjonal Sikkerhetsmyndighet (NSM), Nasjonalt Cybersikkerhetssenter (NCSC)
- HelseCERT, Norsk Helsenett
- KINS, Foreningen for kommunal sikkerhet
- KommuneCERT, ressurssenter for cybersikkerhet for kommuner og driftsleverandører med praktisk informasjonssikkerhetsarbeid
- Norm for Informasjonssikkerhet, bransjenorm for informasjonssikkerhet og personvern i helsesektoren
- Andre sentrale aktører i Norge som driver operativ overvåking og yter responstjenester dersom behov, f.eks. ATEA

Informasjonssikkerhet – beredskap

FARTT jobber hele tiden aktivt med overvåking i egen plattform og systemer

- Mottar jevnlig rapportering og varsling fra nasjonale sikkerhetsmyndigheter
- Følger nasjonale myndigheter råd og anbefalinger ift. Endringer i trusselbildet og rapporterer til ledelsen
- Beredskapsplanen, jobber videre på denne ift. å hensynta ulike hendelser og tiltak for å følge opp disse, fokus på hendelseshåndtering
- FARTT er del av nødnett, ansatte har gjennomført opplæring og øver nå på enkel samhandling internt, ønsker å samhandle gjennom felles beredskapsøvelser i kommuner/fylke med andre aktører
- Jobber med kartlegging av VA sektoren, sammen med KommuneCSIRT

Informasjonssikkerhet – trusselbildet

Angrepet på Østre Toten og andre lignende hendelser viser at det er viktig at FARTT og kommunene har fokus på sikkerhetsarbeidet, ulike trusler:

- Remote desktop, angriper kan overta servere eller sentrale maskiner i en virksomhet
- Sårbarheter i brannmur eller tekniske styringssystemer, servere og klientutstyr
- Phishing: E-post fra ukjente med vedlegg eller link til internett-tjenester med skadelig programvare
- SMiShing: SMS Svindel tilsendt pr SMS tilsvarende fishing (se over)
- Ransomware, løsepengevirus, bedrifter slutter å betale- trussel øker,
  - «Moderne Ransomware»: mange aktører som legger data ut for salg
- Større Cyberangrep på stater og virksomheter, ref krig i Ukraina
- Angrep på VA sektor eller annen kritisk infrastruktur

Informasjonssikkerhet – utfordringer i sikkerhetsbildet

Hvordan takler vi en hendelse/krise ?

- Egen beredskap/tiltak dersom f.eks. et større cyberangrep - ransomware, VA blir angrepet
- Har kommunene en plan B, dvs hvordan sikre drift på legekontor/legevakt dersom fagsystem/IKT systemene er nede over en uke ?
- Hva hvis VA, varme-ventilasjon, heisstyring, alarmsystemer ol blir ute av drift over en periode ?
- Hendelseshåndtering i kriser, viktig for både databehandler og behandlingsansvarlig
- Nedetid før man er operativ, hvilke prioriteringer gjelder ? Kommuneledelsen må prioritere
- Ikke bare produksjonsdata kan rammes, backup/sikkerhetskopi kan også bli utilgjengelig
- Øve sammen om aktuelle hendelser

Men det er vanskelig å være 100 % sikret til enhver tid

Informasjonssikkerhet – utfordringer i sikkerhetsbildet

Kunnskap om informasjonssikkerhet er viktig

- FARTT, sikkerhetsutvalg og kommuneledelse må jobbe sammen om å dele/spre kunnskap og erfaringer innafor informasjonsikkerhet
- Bidra til kompetanseheving blant ansatte
- Styrke digital sikkerhetskultur ute i organisasjonene

IKT sikkerhet

Digitalisering

- Nye systemer
- Ny teknologi
- Sømløse integrasjoner
- Nye fagsystemer
- Lovpålagte endringer

Alt handler om **Informasjonssikkerhet**

Hva jobber vi med?

- Bedre klientsikkerhet
- Innføring av to-faktor autentisering
- Passord policy
- Fjerne begrepet «sikker sone»
- Ny pålogging og arbeidsflater
- Veiledninger
- Varslinger og informasjon fra FARTT
- Mer synlig digitalt

Hva jobber vi med? [2]

- Risiko- og sårbarhetsanalyse av tjenester
- Beredskap
- Katastrofe gjenoppretting
- Prosedyrer og retningslinjer
- Avvik- og hendelseshåndtering
- Forbedre sikkerhetskultur (kunnskap & bevisstgjøring)
- Automatiserte prosesser -> digitalisering
- Anskaffelser

I henhold til eForvaltningsforskriften § 15 skal virksomheten ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet.

Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Omfang og innretning på internkontrollen skal være tilpasset risikoen.

DET KONGELIGE
KOMMUNAL- OG DISTRIKTSDEPARTEMENT

Kommuner
Fylkeskommuner
KS

Deres ref	Vår ref	Dato
	22/707-1	26. januar 2022

Digitalisering i offentlig sektor - orientering til kommunesektoren

Regjeringen ønsker en sterk og effektiv offentlig sektor som gir innbyggerne gode tjenester, valgfrihet og medbestemmelse. Alle innbyggere, uansett bosted, skal ha et godt tjenestetilbud i sitt nærmiljø. Digital infrastruktur blir avgjørende for å bygge landet videre i fremtiden. Staten vil ta et større ansvar for bredbåndsutbygging i områder der det ikke er lønnsomt. Regjeringen vil legge til rette for at folk kan bo der de vil, blant annet gjennom å sikre gode grunnleggende digitale tjenester for innbyggere og næringsliv.

Teksten nedenfor inneholder tema og tiltak som kommunal- og distriktsdepartementet (KDD) finner særlig relevant for kommuner og fylkeskommuner i deres digitaliseringsarbeid.

Oppfølging av Én digital offentlig sektor - Digitaliseringsstrategien for offentlig sektor 2019-2025
Digitaliseringsstrategien for offentlig sektor (2019-2025)– Én digital offentlig sektor er felles for kommunesektoren og staten. Offentlige tjenester skal dekke brukernes behov og oppleves sammenhengende og helhetlige for brukerne, uavhengig av hvilke offentlige virksomheter som tilbyr dem. Kommunal og statlig sektor må samarbeide på tvers av forvaltningsnivåer og sektorer for å lykkes med dette. Dette arbeidet er godt i gang.

Sentralt i strategien er utvikling av sammenhengende tjenester innenfor syv prioriterte livshendelser. Disse er *Få barn (AID), Alvorlig sykt barn (HOD), Miste og finne jobb (AID), Ny i Norge (AID), Starte og drive bedrift (NFD), Starte og drive frivillig organisasjon (KUD)* og *Dødsfall og arv (KDD)*. Øverste ansvar for livshendelsene er lagt til departementene i

Gode digitale hygieneregler

- Lange passord (min. 14 tegn)
- Autentisering (biometrisk & to-veis/MFA)
- Utlån av utstyr
- Privat bruk av e-post
- Sjekk avsender (e-post, SMS og telefon)
- Stopp. Tenk. Sjekk

IKT Sikkerhetsplakat, til oppslag på kontoret nær skjermen din! Revidert 18.3.2019

Datasikkerhet er DITT ansvar!

1. Beskytt passordet ditt; det er din personlige nøkkel
2. Lås pc/klientmaskin når du forlater kontoret, logg ut av nettet og slå av maskinen når du går for dagen
3. Lås kontordøra når du forlater kontoret
4. Ha kontroll på utskriftene dine
5. Sørg for sikker lagring av elektroniske data og papirdokumenter, vær nøye med makulering av fortrolig informasjon
6. Jobb-relatert informasjon skal ikke lagres på private lagringsmedier, som skytjenester, minnepinner etc.
7. Ikke send personsensitive opplysninger på e-post og sms
8. Vær bevisst i forhold til bruk av sosiale medier og internett
9. Meld fra dersom du oppdager sikkerhetsmessige avvik
10. La ikke sensitiv informasjon bli tilgjengelig for uvedkommende

Gjør deg kjent med FARTT kommunenes retningslinjer og regler for informasjonssikkerhet. Mer informasjon om dette finnes i kvalitetssystemet i kommunen.

Hvor privat skal du være?

- Ha et klart skille mellom jobb og privat
  - Ingen private surfing i arbeidstid eller på jobb enheter
  - Privat e-post på privat enhet
- Ikke aksepter bruk av informasjonskapsler på nettsider
- Vær kritisk til informasjon du har på dine profiler i sosiale medier
- Ditt utstyr, nøkler, nøkkelkort, pinkoder og passord er personlig
- Ikke gjenbruk passord på jobb og privat
- Skru av karttjenester (Snapchat og Google)
- Reduser risiko

Klient sikkerhet

- Årvåkenhet
- Kjernekompetanse på IKT og sikkerhet
- Autentisering (multi/to faktor)
- Oppdatert programvare
- Registrering av utstyr (Intune)
- Ajourført IT-utstyr & mobiltelefoni

Investeringsbehov

- Windows 11 (2025)
- Nye antenner på trådløst nett (2025)

For å nå mål om informasjonssikkerhet

- Verktøy for analyse av logger og varsling (SIEM)
- Automatisering av prosesser for tjenester og lisenser (IAM)

Må bevilges penger til investeringer av utstyr og kompetanse

FJELLREGIONEN IKS

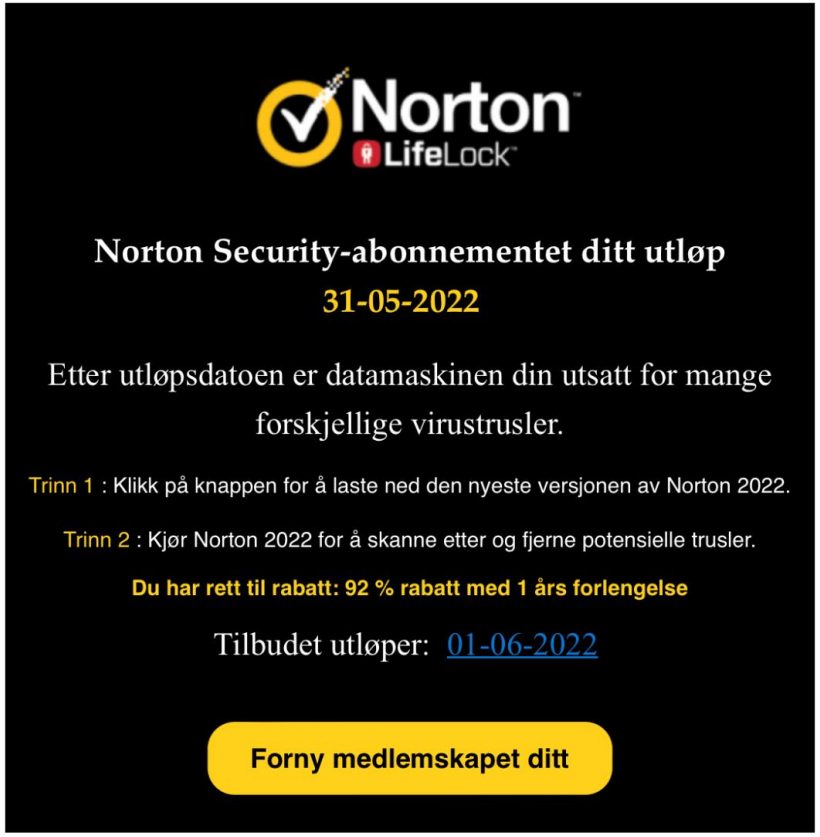
Sosial manipulasjon

Tillit	Fristelser	Frykt
• Kjent avsender • Stoler på avsender • Kjente merkenavn Kommer ofte på epost, SMS eller meldingstjenester	• Tilby noe som er gratis • For godt til å være sant • Konkurranser	• Skremme til å utføre en handling. • Laste ned noe (f.eks program for å fjerne virus, rydde opp på maskin m.m) • Følelsen om at noe haster

Mål: penger eller personopplysninger

Re: Risikoen for å bli høyere!! Forny nå begrenset konto. >>

N **Norton** 21:04
Til Deg



Løspengevirus

Ondsinnet program krypterer filer på datamaskin og krever løsepenger for å frigi disse. Skadevaren spres via lenker eller vedlegg i e-post eller infiserte nettsider

Vær kritisk til hva du laster ned og hvilke program du installerer på maskinen din (og telefon + nettbrett).

sanwaiWare 2021

Your files have been encrypted.

PAYMENT

Send **0.002077** BITCOIN to

bc1qjp5suqqk52fmlu0xa3vzfl34l3ghhp9v55drm6

AFTER PAYMENT

Once you have sent payment, open the Decryptor on your Desktop.
Attempting to reverse will result in your files being lost forever.

PAYMENT NOTICE

You have (48) hours from initial notice to make payment.
If payment is not made within the time frame, your files will be deleted.

Phishing

- Kriminelle lurer deg til å oppgi sensitiv eller personlig informasjon om deg selv eller din virksomhet
- Gjøres via epost eller SMS
- Lures inn på falsk nettside hvor du blir bedt om personlige opplysninger (f.eks. fødselsnummer og lignende)

Sjekk alltid avsender adresser, og oppgi ALDRI finansiell eller personlig informasjon via e-post


+44 7563 886844
Tekstmelding
19. okt. 2020, 11:49
Elkjop har valgt telefonen din (4798056100). Velg ditt produkt: http://avezek.com/U_68xsU


Emne: Du har mottatt ny post
oppdater bankid på mobil-informasjon (påkrevd handling)
hei,
SpareBank 1 , BankID-kunde Dessverre kunne vi ikke fornye kontoen din SpareBank1
Er dette kortet utløpt? Det er forskjellige grunner til at faktureringsadressen endres, noe av kontoinformasjonen din er feil, og du må bekrefte eiKa gruppen BankID-informasjonen din for å opprettholde kontoen din
Nå kan du sjekke kontoen din.
Logg Inn
Logg inn med BankID på mobil. Husk at tjenesten må være bestilt og mobilen slått på
BankID pålogging
Det advarer deg også om å låse kontoen din hvis du ikke bekrefter innen 24 timer.
Hvis e-postadressen til påloggingskontoen din ikke er logget inn
Kontakt: BankID Kundeservice.

Falske trusler og utpressingskrav

- Eposter med usanne påstander
- F.eks at de kriminelle har video av deg mens du ser på porno
- De truer med å offentliggjøre filmen dersom de ikke får betaling, gjerne via kryptovaluta

Vurder om eposten kunne ha blitt sendt til mange andre uten at teksten ble endret vesentlig. Betal aldri utpressere – uansett om trusselen er ekte eller falsk. Du har ingen garanti for at det vil løse problemet

Hallo!
Jeg er en hacker som har tilgang til operativsystemet ditt.
Jeg har også full tilgang til kontoen din.
Jeg har sett på deg i noen måneder nå.
Fakta er at du ble smittet med malware via et voksent nettsted som du besøkte.
Hvis du ikke er kjent med dette, vil jeg forklare.
Trojan Virus gir meg full tilgang og kontroll over en datamaskin eller annen enhet.
Dette betyr at jeg kan se alt på skjermen din, slå på kameraet og mikrofonen, men du vet ikke om det.

Jeg har også tilgang til alle dine kontakter og all korrespondanse.
Hvorfor oppdaget ikke antivirusprogrammet skadelig programvare?
Svar: Min malware bruker driveren, jeg oppdaterer signaturene hver fjerde time slik at antiviruset ditt er stille.

Jeg lagde en video som viste hvordan du tilfredsstiller deg i venstre halvdel av skjermen, og i høyre halvdel ser du videoen du så på.

Med ett museklikk kan jeg sende denne videoen til alle e-postmeldinger og kontakter på sosiale nettverk.

Jeg kan også legge inn tilgang til all e-postkorrespondanse og messenger du bruker.
Men ikke bekymre deg for mye. Det er en måte vi kan løse dette personvernproblemet på. Alt vi trenger er en Bitcoin-betaling på £6,860.00 GBP, som jeg tror er en rimelig pris med tanke på omstendighetene.

Bitcoin-adresse for å foreta betalingen er: **[BITCOIN-ADRESSE]**

MERKNAD: HUSK Å GODKJENT BITCOIN-ADRESSEN MED USA FØR du utfører betaling for å unngå å betale to ganger.

Hvis du ikke forstår bitcoin, kan du gå på YouTube og søke etter “hvordan kjøpe bitcoin” eller google for “lokale bitcoins”, er det ganske enkelt å gjøre det.
Etter å ha mottatt betalingen, vil jeg slette videoen, og du vil aldri høre fra oss igjen.
Jeg gir deg 48 timer å betale. Jeg har et varsel om å lese dette brevet, og tidtakeren vil fungere når du

Direktørsvindel

Svindleren sender en epost eller SMS til økonomimedarbeider, tilsynelatende fra en direktør eller annen sjef i virksomheten og ber om en større pengeoverføring

Dersom det anmodes om penger, les gjennom e-posten flere ganger og sjekke med sjefen din om henvendelsen er reell

Gavekort

Fra: bestyrelsesprivat@gmail.com <bestyrelsesprivat@gmail.com> På vegne av Erling Strålberg
Sendt: torsdag 5. mai 2022 15:23
Emne: SV: Hastegavekort

Kan du hjelpe meg med å kjøpe gavekort på nett? Kan du kjøpe nå

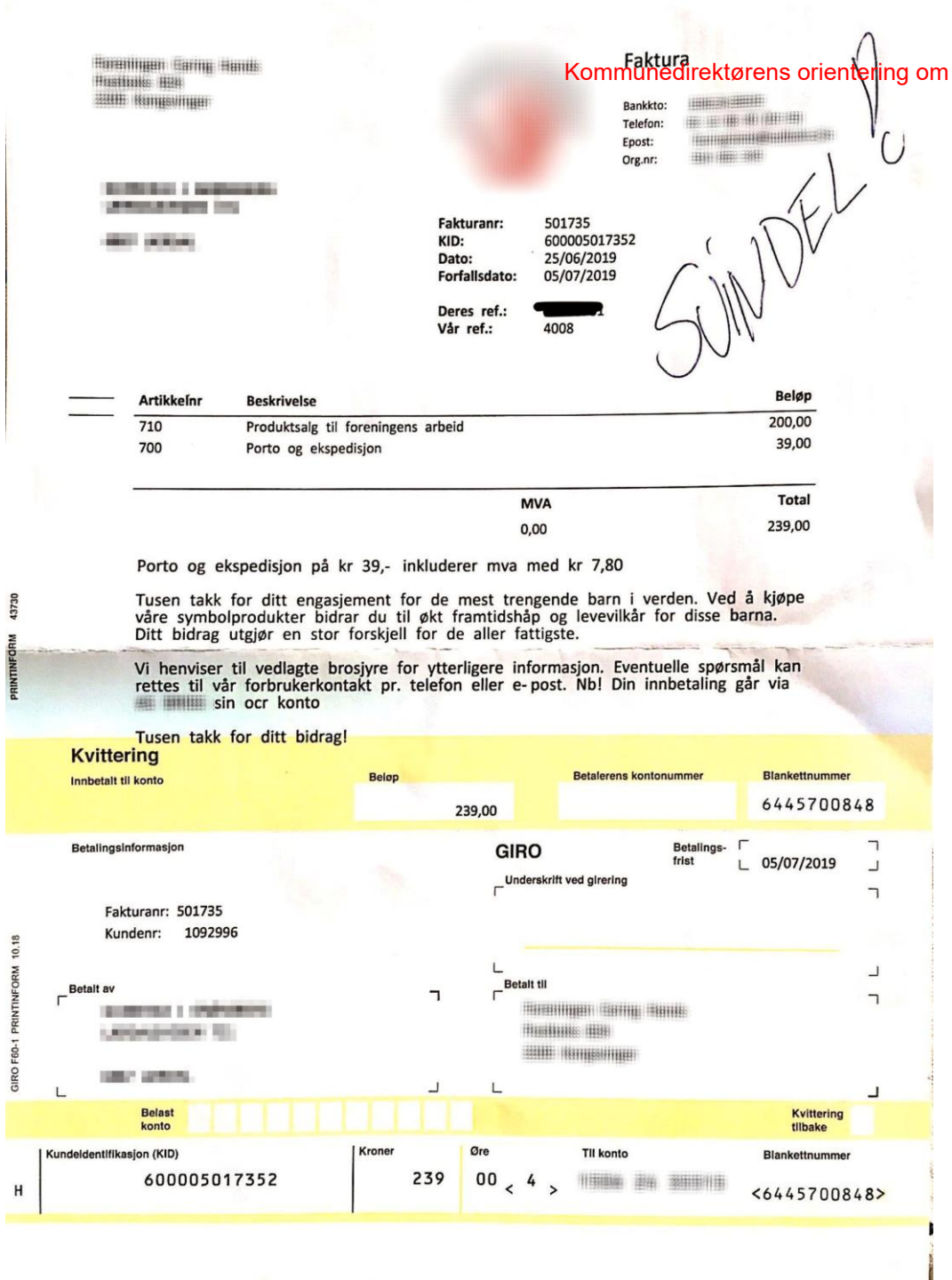
Vennlig hilsen

Erling Strålberg

Fakturasvindel

- Svindlere sender ut fakturaer for reelle tjenester eller produkter mottatt av andre, men med deres eget kontonummer.
- Den falske fakturaer blir oversendt etter lengre tids sosiale manipulering, ofte via e-post

Sjekk alltid med leverandøren som har byttet kontonummer om dette stemmer. Gjør det per telefon, ikke e-post



Faktura

Bankkto:
Telefon:
Epost:
Org.nr:

SVINDEL

Fakturanr: 501735
KID: 600005017352
Dato: 25/06/2019
Forfallsdato: 05/07/2019

Deres ref.:
Vår ref.: 4008

Artikkelnr	Beskrivelse	Beløp
710	Produktsalg til foreningens arbeid	200,00
700	Porto og ekspedisjon	39,00

MVA	Total
0,00	239,00

Porto og ekspedisjon på kr 39,- inkluderer mva med kr 7,80

Tusen takk for ditt engasjement for de mest trengende barn i verden. Ved å kjøpe våre symbolprodukter bidrar du til økt framtidshåp og levevilkår for disse barna. Ditt bidrag utgjør en stor forskjell for de aller fattigste.

Vi henviser til vedlagte brosjyre for ytterligere informasjon. Eventuelle spørsmål kan rettes til vår forbrukerkontakt pr. telefon eller e-post. Nb! Din innbetaling går via sin ocr konto

Tusen takk for ditt bidrag!

PRINTINFORM 43730

Kvittering

Innbetalt til konto | Beløp: 239,00 | Betalerens kontonummer | Blankettnummer: 6445700848

Betalingsinformasjon

GIRO

Betalings-frist: 05/07/2019

Underskrift ved girering

Fakturanr: 501735
Kundenr: 1092996

GIRO F60-1 PRINTINFORM 10.18

Betalt av

Betalt til

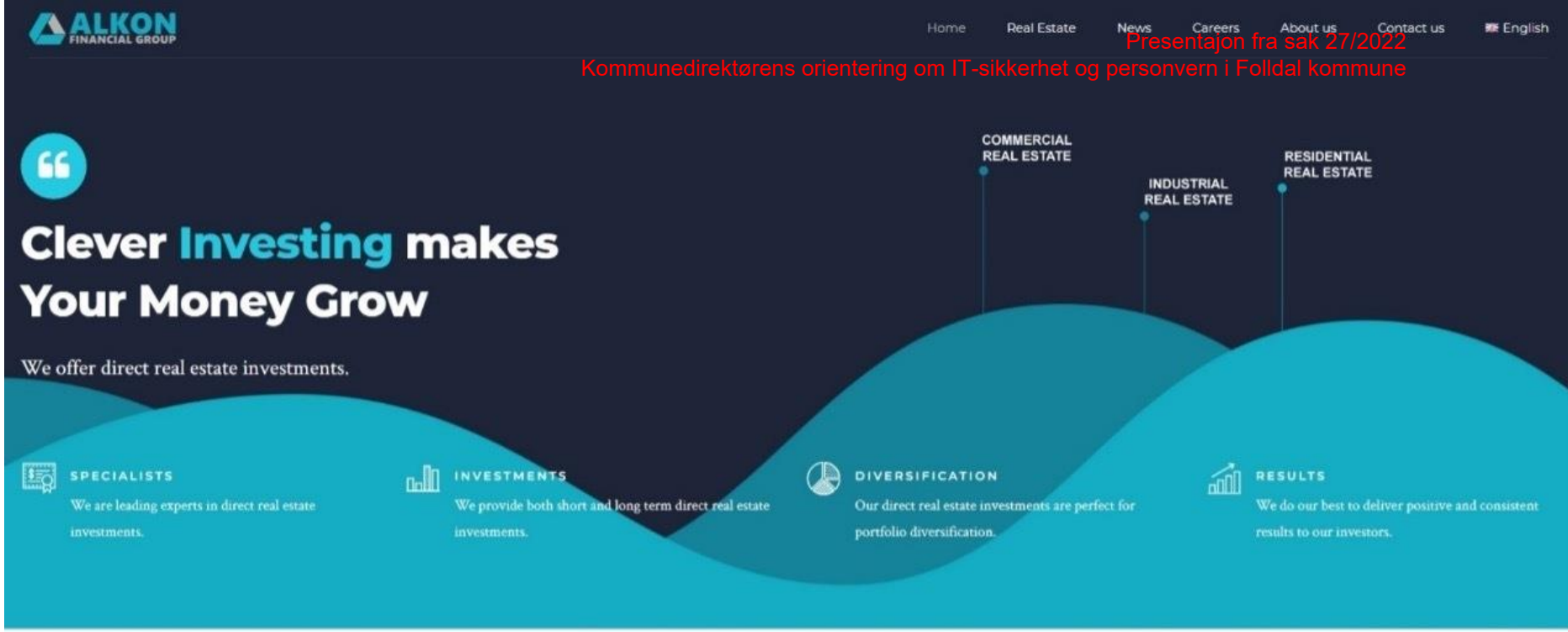
Belast konto | Kvittering tilbake

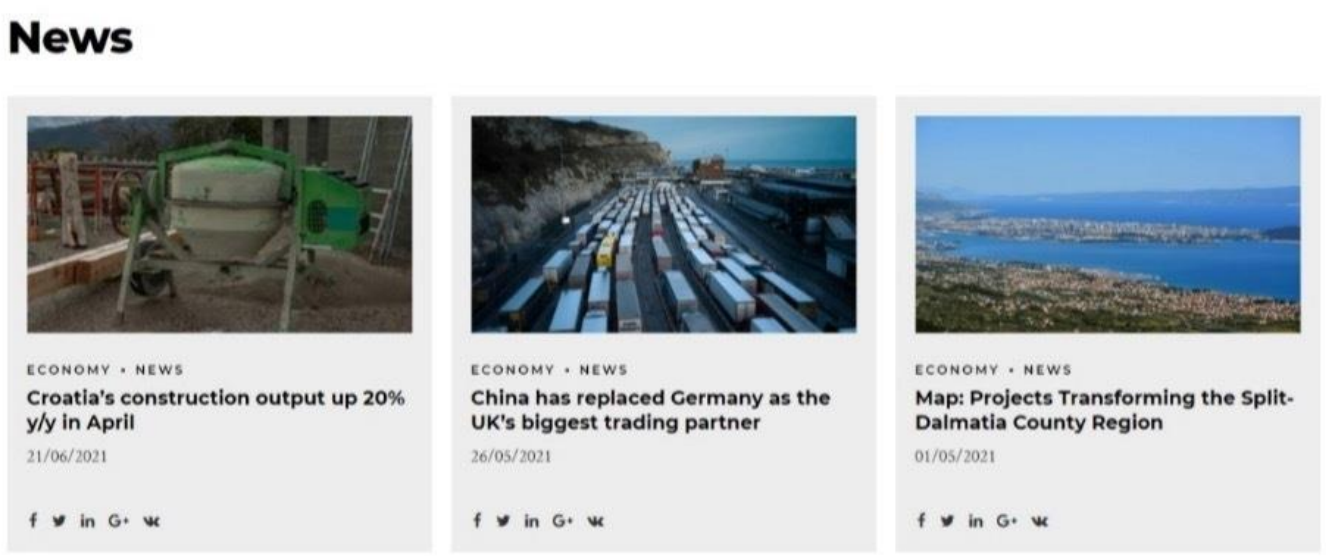
	Kundeidentifikasjon (KID)	Kroner	Øre	Til konto	Blankettnummer
H	600005017352	239	00 < 4 >		<6445700848>

Investeringsbedrageri

- Du lokkes til å investere pengene dine på nett, ofte i produkter eller tjenester som få har kunnskap om, som kryptovaluta eller valutaspekulasjoner
- Ofte fabrikeres det falske nyheter i sosiale medier om dette, gjerne med kjente personer som forteller hvor mye de har tjent

Gjør et Google søk på firmaet og den kjente personen som fronter annonsen. Hvem driver nettsider? Har andre lagt ut advarsler mot firmaet?

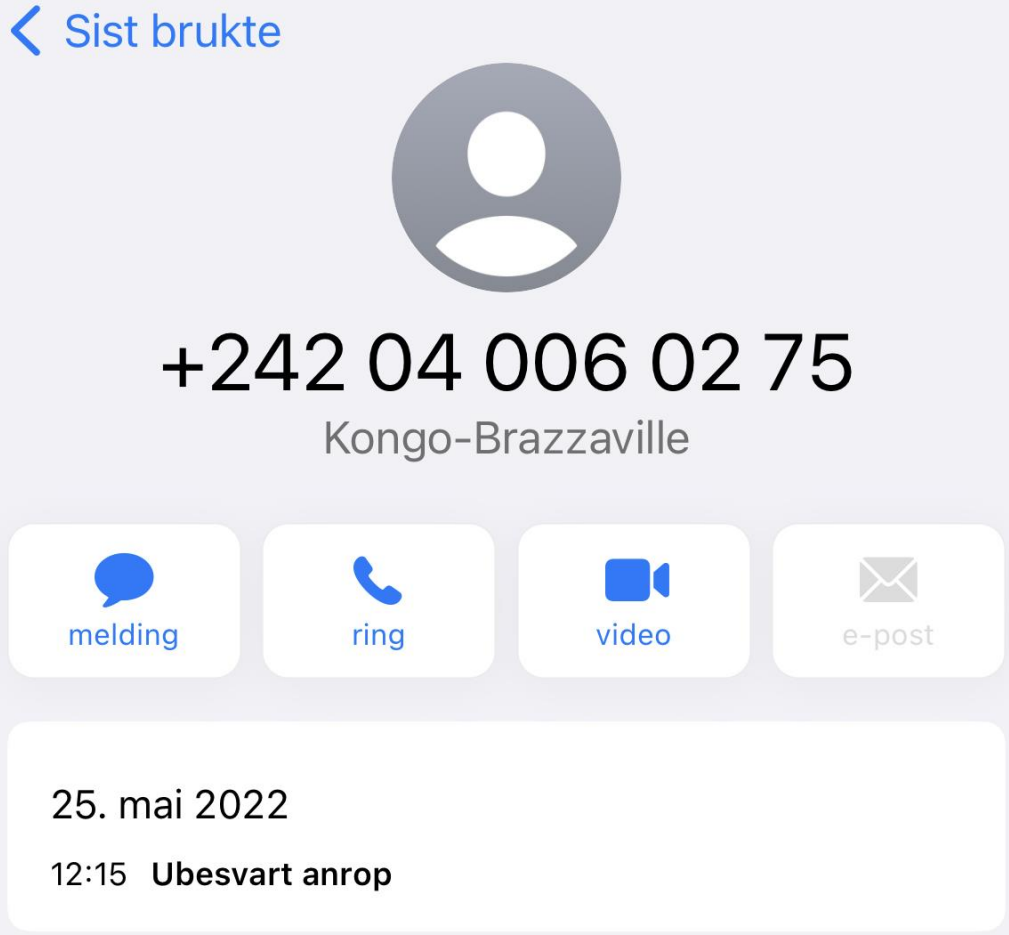

ALKON FINANCIAL GROUP
Home
Real Estate
News
Careers
About us
Contact us
English
Clever Investing makes Your Money Grow
We offer direct real estate investments.
COMMERCIAL REAL ESTATE
INDUSTRIAL REAL ESTATE
RESIDENTIAL REAL ESTATE
SPECIALISTS
We are leading experts in direct real estate investments.
INVESTMENTS
We provide both short and long term direct real estate investments.
DIVERSIFICATION
Our direct real estate investments are perfect for portfolio diversification.
RESULTS
We do our best to deliver positive and consistent results to our investors.


News
ECONOMY • NEWS
Croatia's construction output up 20% y/y in April
21/06/2021
ECONOMY • NEWS
China has replaced Germany as the UK's biggest trading partner
26/05/2021
ECONOMY • NEWS
Map: Projects Transforming the Split-Dalmatia County Region
01/05/2021

Telefonsvindel

- Du blir ringt opp fra et ukjent utenlandsk telefonnummer
- Etter at det har ringt et par ganger, blir det lagt på. Ringer du opp igjen er det ofte et høytakstnummer som belaster deg med en svært høy minuttpris

Ikke ring opp igjen!
Blokker abonnement for betalbare tjenester på telefon og SMS


Sist brukte
+242 04 006 02 75
Kongo-Brazzaville
melding
ring
video
e-post
25. mai 2022
12:15 Ubesvart anrop

Falske konkurranser

Falske sider på Facebook/Instagram som logger med premier dersom du «liker og deler» kan stjele dine personopplysninger

Må du dele innhold og tagge venner for å delta, er det mest sannsynlig en falsk konkurranse. Det strider mot Facebook regler for konkurranser. Er premien for god til å være sann, er det også en indikasjon på at konkurransen er falsk


Expert - Norge
Expert - Norge

Enkle tips fra FARTT

- Ikke klikk på lenker i SMS, meldingsAPPer og e-post
- Sjekk avsender (adresse & navn)
- Varsle på unormal aktivitet og hendelser
- Retningslinjer for bruk av utstyr
- Sikre enheter
- Passord & autentisering
- Lås maskin
- Varsle hvis enheter forsvinner
- Del kunnskap med dine kollegaer

Økende trend
Vær på vakt!

PODKAST

Nasjonal sikkerhetsmyndighet (NSM)

Nasjonal sikkerhetsmyndighet (NSM)

PODKASTEPISODE

STRENGT HEMMELIG - Veien inn - Episode 1 - Franzen filen

Nasjonal sikkerhetsmyndighet (NSM)

Spørsmål?