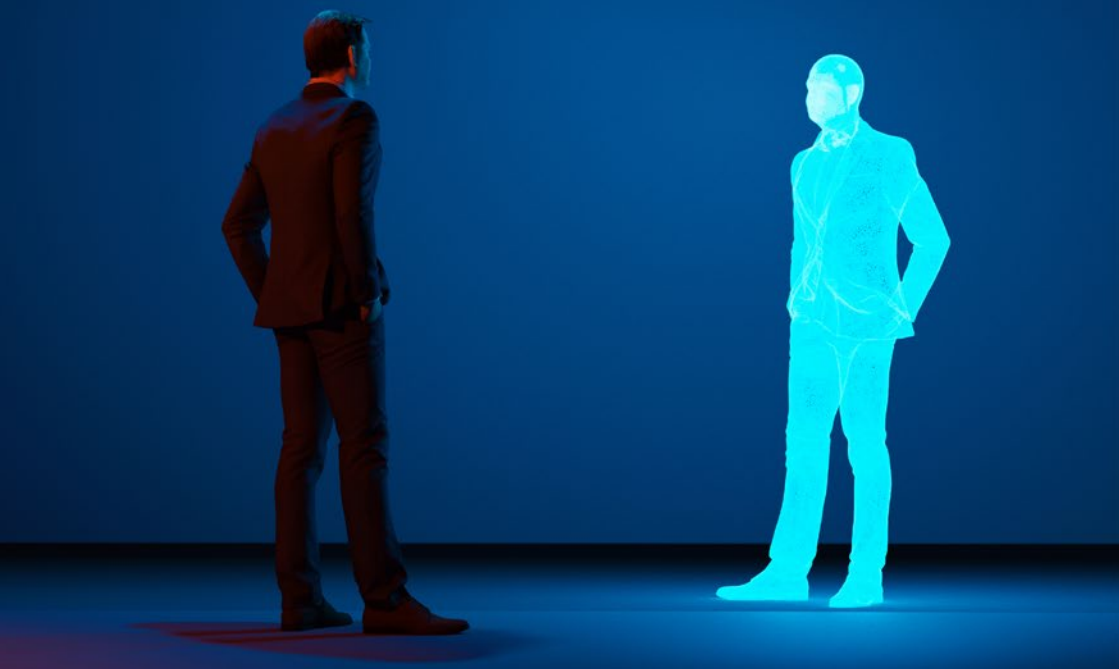
POLITIET telenor DNB

# Hvordan unngå bedrageri mot din virksomhet?

Bedrageri mot små og store virksomheter blir mer målrettet og stadig vanskeligere å avsløre.



Uoppmerksomhet kan påføre virksomheten tap i millionklassen.
I verste fall er det kroken på døren.

**Direktør- og fakturabedragerier utgjør en betydelig risiko for norsk næringsliv. De kriminelle blir stadig mer avanserte i sine angrep, og bruker en kombinasjon av datainnbrudd, moderne teknologi og sosial manipulasjon. Dette kan ramme alle, uansett om man er en stor eller liten virksomhet.**
**Her gir vi deg klare tips og råd til hvordan du bedre kan sikre bedriften, foreningen eller idrettslaget.**

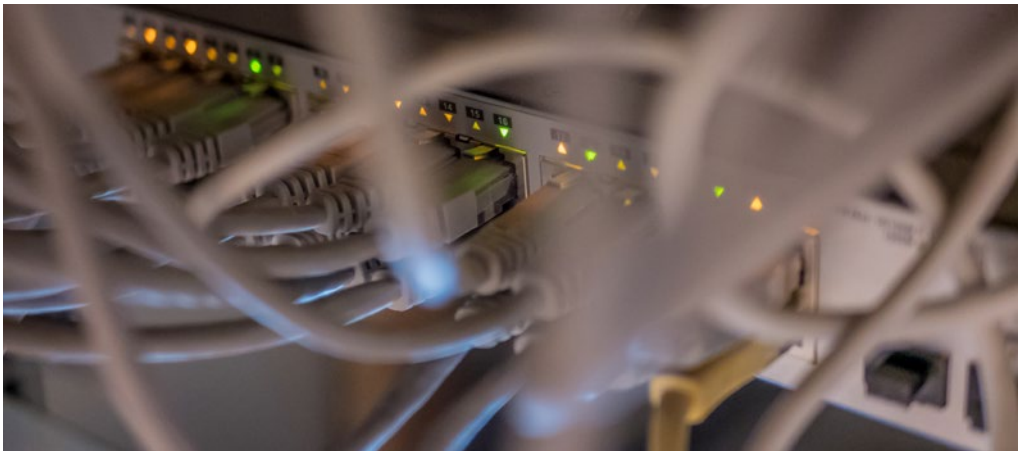
## Hvordan vet de så mye om oss?

Etter å ha valgt seg ut et egnet mål, starter informasjonsinnhentingen for bedragerne.

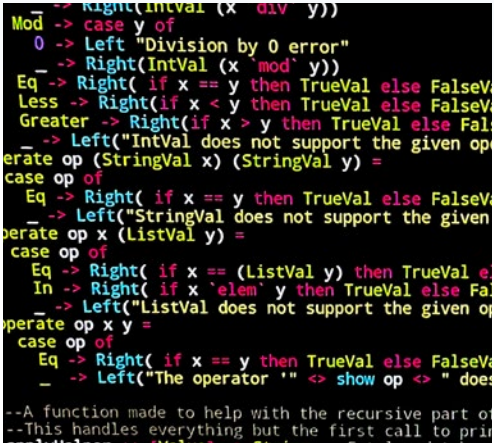
På virksomhetens hjemmeside finner man ofte et galleri over nøkkelpersoner og ledere, deres funksjoner og kontakt-informasjon. Også i sosiale medier og i nettaviser er bedrifter, foreninger og idrettslag ofte eksponert. Et enkelt søk på internettet kan være godt egnet for å innhente nok informasjon om virksomheten for å starte et angrep. Informasjon om oppkjøp, investeringer eller samarbeid er spesielt interessant.

Det er organiserte kriminelle som står bak slike angrep. De vil ofte rette angrepet mot en person forholdsvis høyt opp i organisasjonen. Typisk en regnskaps-sjef eller en CFO. Men alle med betalings-fullmakt i en virksomhet er mulige mål.

Vi har også sett eksempler på at de utnytter e-post-tilgang hos kundeanvarlige for å manipulere andre i virksomheten som kan godkjenne fakturaer eller gjennomføre betalinger.



> I 2020 ble DNBs bedriftskunder forsøkt bedratt for 138 millioner kroner
>
> Kilde: DNB




I løpet av 2020 ble et statlig investeringsfond utsatt for avansert direktørsvindel. Selskapet tapte cirka 100 millioner kroner i angrepet. Tap av store summer kan få veldig store konsekvenser for en virksomhet. I verste fall kan man gå konkurs. Tilgang til en virksomhets e-post er viktig for de kriminelle. Denne tilgangen kan de bruke både til å manipulere informasjon i en faktura, eller de kan kopiere og laste ned innhold som de senere bruker til utpressing.

*Ta umiddelbart kontakt med egen bank og politiet dersom du frykter at du har blitt utsatt for bedrageri.*

Et angrep starter ofte med en phishing-e-post der de kriminelle sikrer seg brukernavn og passord til en ansatt. Ved å lese e-post over lang tid, får bakmenn unik innsikt i virksomheten.
De vet da nøyaktig hvordan de skal gå frem for å lure noen. For å gjøre terskelen høyere for at de kriminelle skal lykkes med å skaffe seg tilgang til e-post-systemene anbefaler vi to-trinns autentisering ved pålogging til e-postkonto. Da får ikke de kriminelle tilgang hvis de skulle lykkes med å lokke til seg brukernavn og passord. En slik anbefaling gjelder også alle private kontoer man har hvor dette er mulig, som privat e-post og sosiale medier.

Det kan være ulike grunner til at akkurat din virksomhet blir valgt ut. Noen kriminelle jobber målrettet, mens andre jobber mer tilfeldig og sprer angrepet sitt.
Kanskje er det åpen informasjon på nettet om virksomheten som gjør den interessant? Kanskje er de kriminelle inne i e-post-systemet deres og leser all korrespondanse dere har med kundene fordi en ansatt har vært utsatt for phishing.
Når undersøkte virksomheten deres sist påloggingsloggene til Office 365 for å se etter ukjente innlogginger?

**Hvordan kommer de i kontakt med oss?**
I mange tilfeller er det en av disse metodene som blir brukt:
1) Kompromittering av e-post (BEC)
2) Sosial manipulasjon
3) Passord-angrep
3) Utnyttelse av sårbarhet

**Kompromittering av e-post** (BEC - Business Email Compromise) Kriminelle som skal lure virksomheten vil som hovedregel bruke e-postkanalen.
De vil da skaffe seg informasjon og bruke denne informasjonen til å manipulere ansatte i organisasjonen til å gjennomføre en betaling. Dette kan de gjøre ved å sende en falsk faktura, eller endre et kontonummer på en eksisterende faktura.

Federal Bereau of Investigation (FBI) oppgir at BEC er det mest brukte verktøyet for bedragerier mot virksomheter, og det er den metoden som gir absolutt størst utbytte for de kriminelle.
De kriminelle som gjennomfører slik kriminalitet er godt organiserte, har god kompetanse og god kapasitet.
Virksomheter må derfor ta dette på alvor og ha gode betalingsrutiner og gode sikkerhetskontroller. Vi anbefaler at man ved inngåelse av en større kontrakt avtaler å bruke en annen kommunikasjonskanal enn e-post til å kontrollere at betalings-informasjonen er riktig. Ved større betalinger kan man også gjennomføre en testtransaksjon.

Det finnes tre måter å gjennomføre en kompromittering på. Kriminelle kan forfalske e-postadresser til å ligne på adresser tilknyttet en virksomhet, de kan bruke phishing for å skaffe seg tilgang til en e-postkonto, eller de kan sende en programvare som installeres på e-post-serveren slik at de får tilgang til all e-post hos virksomheten.

Med denne tilgangen kan de lære seg hvordan virksomheten opererer, lære seg språket mm. Deretter bruker de sosial manipulasjon som gjør at de får overført penger til en konto de selv kontrollerer.
Vi kjenner til at enkelte kriminelle grupper har spesialisert seg på forskjellig bransjer slik at de kjenner faguttrykk og andre faktorer typisk for bransjen.


På denne måten kan de skape stor grad av troverdighet i sine angrep.

**Sosial manipulasjon** er en viktig del ved gjennomføring av alle bedragerier. Når de

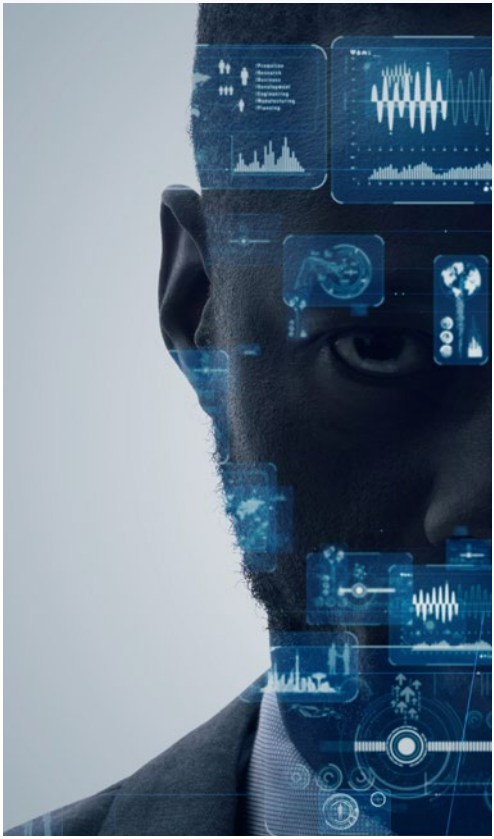
> **Hele 13 prosent av norske virksomheter har opplevd såkalt direktørsvindel. Men det fryktes store mørketall**
> Kilde: Politiet

kriminelle skal lure noen i en virksomhet, bruker de tilgangen de har skaffet seg til en e-postkonto (BEC) i virksomheten som ledd i bedrageriet. Typisk vil de sende en melding om endret betalingsinformasjon, eller de kan endre en faktura. De kan sende en falsk faktura, eller i enkelte tilfeller kun en e-post med beskjed om å betale.

Det viktigste du kan gjøre for å avdekke falske e-poster er å vurdere om innholdet fremstår normalt, eller om det er noe som skurrer. Hvis du lurer på om kollegaen din eller andre faktisk har sendt e-posten, ring eller send en melding for å få bekreftelse. Det er viktig at flere personer kontrollerer innholdet i en faktura, slik at dere er sikre på at det er riktig.

**Passord-angrep** går ut på å tilegne seg tilgang med enten lekkende passord, svake passord eller at man lurer/stjeler til seg passord fra offeret ved hjelp av en phishing-e-post.
Mange ulike merkevarer misbrukes til phishing. Når det gjelder phishing mot virksomheter har det i stor grad blitt brukt forfalskede e-poster som gir seg ut for å være fra Microsoft og oppgradering

*Når de kriminelle har stjålet brukernavn og passord har de tilgang til å lese all e-post på denne kontoen.* ●●●



av Office 365-konto. Når de kriminelle har stjålet brukernavn og passord har de tilgang til å lese all e-post på denne kontoen. De kan sende og slette e-post og de kan sette opp faste regler - for eksempel kan de videresende all e-post til en konto de selv kontrollerer.
To-trinns autentisering og One Time Password (OTP) vil komplisere et slikt angrep. Selv om det finnes veier rundt,

kan dette føre til at de kriminelle ikke får tilgang til e-post eller at de velger et mål som er enklere å kompromittere.

**Utnyttelse av sårbarhet.** De kriminelle kan bruke eksisterende feil eller sårbarheter som er kjent, men som ikke er rettet.
Det vil være enklere å utnytte en kjent sårbarhet enn å bruke tid på å finne egne veier inn.
Dette fordi hacking krever både kompetanse og ressurser ikke alle kriminelle har.

**Hva kan du gjøre som virksomhet?**

- Benytt alltid to-trinns verifisering på all e-post og ikke bruk like passord flere steder. Sørg for god e-postsikkerhet også teknisk. Om du ikke har egen IT-avdeling, sett krav til leverandøren.
- Dersom du blir forespurt endringer fra normal rutine, eksempelvis endring av kontonummer, ikke endre betalingsdetaljer på bakgrunn av e-postdialog.
- Avklar betalingsopplysningene via andre kanaler, helst en kryptert meldingstjeneste. Hvilken kanal man bruker for å kontrollere betalingsopplysninger bør avtales tidlig, gjerne ved kontraktinngåelse. Husk at selv om din virksomhet har god e-postsikkerhet, så kan dialogen være kompromittert hos den du prater med.
- Vær varsom med hvilken informasjon man legger ut på nettsider om både virksomheten og ansatte.
- Ta umiddelbar kontakt med egen bank og politiet dersom du har blitt utsatt for bedrageri. Kartlegg på forhånd hvordan og til hvem man kan gjør en slik hastehenvendelse, også utenfor bankens ordinære åpningstid.
- Hvis de kriminelle har fått tilgang til e-postsystemene, kan de sette opp automatiske regler. Ta gjennomgang av e-postregler jevnlig da disse ikke slettes når man bytter passord.
- Vurder å gjennomføre en testtransaksjon på et lite beløp hvis du skal sende til nytt kontonummer for å sikre deg om at dette kommer frem til riktig konto.
- Ha en god sikkerhetskultur. Snakk om sikkerhet fra ledelsen og ned og gjør ansatte oppmerksomme på at de kan utgjøre en rolle i kartlegging av virksomheten. Kommuniser at kontroll av informasjon settes pris på og at det ikke er tegn på mistillit.
- Informerte ansatte er verdifullt, men virksomheter er enda bedre rustet dersom de aktivt trener på håndtering av ulike bedragerimetoder. Hold virksomheten oppdatert på ulike bedragerimetoder og øv med de ansatte i mottiltak.
- Oppgrader applikasjoner og operativsystem. Oppdateringer kan være viktig for å tette sikkerhetshull. Registrer gjerne kjente maskiner og IP-adresser i systemet og blokker for annen bruk av nettet. ***NB!*** *Husk å informere eventuelle ferievikarer om hvordan kriminelle opererer og om viktige rutiner da de kriminelle gjerne slår til i ferietiden.*

> **Vi har foreløpig ikke sett datainnbrudd i faktura/ direktørbedragerier hvor virksomheten har benyttet to-trinns autentisering.**
>
> Kilde: Oslo politidistrikt

**Hva kan du gjøre som ansatt?**

- Følg alle sikkerhetsrutiner for betalinger og innkjøp. Ikke hopp over trinn, og ikke gi etter for press eller stress utenfra.
- Sjekk alltid e-postadresser nøye for å sikre at det ikke er en falsk adresse. Har virksomheten mulighet til å benytte en annen kanal enn e-post, bruk den.
- Er du i tvil om en bestemt forespørsel, rådfør deg med en erfaren kollega. God kontroll er ikke et uttrykk for mistillit. Spør heller en kollega en gang for mye enn en gang for lite. Og sett pris på om en kollega kontrollerer informasjonen de har fått fra deg.
- Åpne aldri mistenkelige lenker eller vedlegg du har fått på e-post. Ikke bruk jobb-pc til privat e-post.
- Begrens hva som deles, og vær bevisst ved bruk av sosiale medier. Bruk to-trinns autentisering også på private kontoer.
- Unngå å dele informasjon om hvordan virksomheten er organisert og hvilke sikkerhetstiltak og rutiner dere har.

***NB!*** *Informer IT-avdelingen og/eller sikkerhetsavdelingen om du mottar en mistenkelig e-post eller telefon-oppringning.*

Næringslivskontakt/politiinspektør i Oslo politidistrikt, Christina T. Rooth

Leder for bedrageribekjempelse i DNB, Terje Fjeldvær

Sikkerhetsekspert i Telenor Norge, Thorbjørn Busch

POLITIET telenor DNB

## Kontakt:

**Ved behov for øyeblikkelig hjelp ring 112**
Andre henvendelser ring **02800**
Informasjon til politiet: **https://tips.politiet.no/web/**

**DNB:**
Kundeservice **915 04800**

**Telenor:**
Kundeservice **915 09000**

## Andre relevante sider:

Les mer om digital sikkerhet på:
**https://www.telenor.no/sikkerhet/trygg-bedrift/**

For webinarserie og sakseksempler se:
**Hvordan unngå bedrageri? | Scene (dnb.no)**
eller se DNBs sider om økonomisk kriminalitet:
**Økonomisk kriminalitet - DNB**