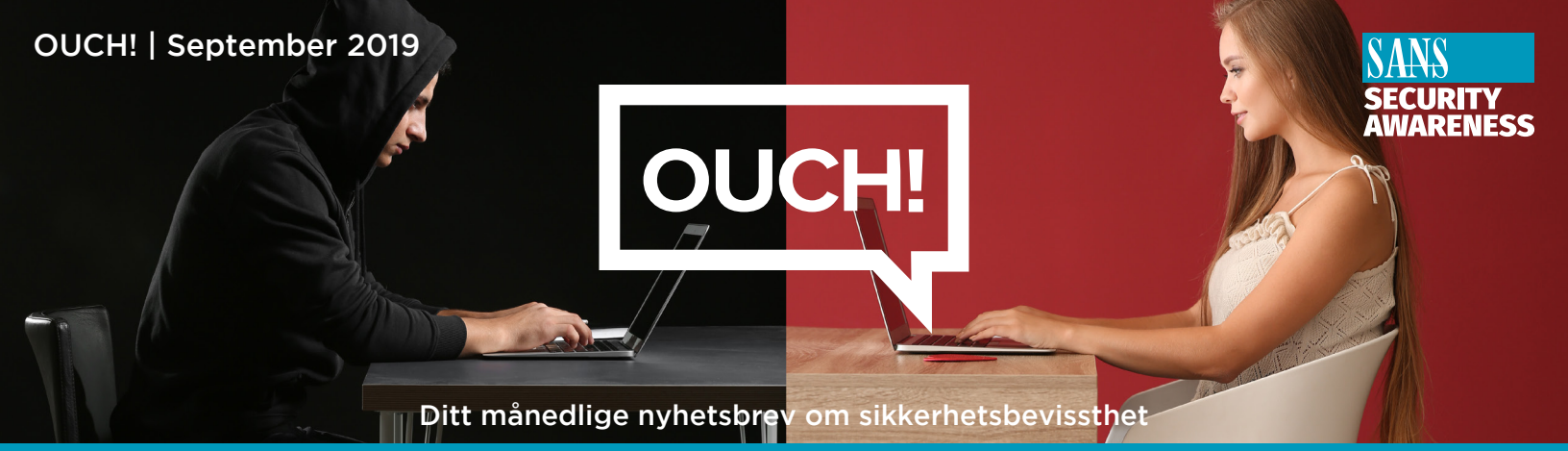
OUCH! | September 2019




Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

# Svindel gjennom sosiale medier

## Oversikt

Mange av oss har mottatt e-poster på jobb eller privat, hvor det fiskes etter personlig informasjon. Dette er e-poster som ser tilsynelatende legitime ut, som for eksempel fra banken, sjefen på jobb eller fra den nettbutikken du bruker mest. Men e-postene kan være et forsøk på å få deg til å gjøre noe du ikke burde, som for eksempel å åpne et vedlegg, oppgi passordet ditt eller overføre penger. Ofte spiller e-postene på følelser som tillit, frykt og fristelse, og så er det gjerne nødvendig å gjøre noe raskt. Utfordringen er at jo flinkere vi blir til å identifisere disse e-postsvindlene, jo flinkere blir de kriminelle til å benytte andre og flere metoder for å nå oss med svindelen.

Forsøk på å svindle oss kan gjøres nesten gjennom alle mulige kommunikasjonskanaler vi bruker, fra Skype, WhatsApp og Slack til Twitter, Facebook, Snapchat, Instagram og til og med ulike spill-applikasjoner. Kommunikasjon gjennom disse kanalene virker ofte mer uformell og tillitsskapende. Dette vet de kriminelle å utnytte. I tillegg til alle de tilgjengelige kommunikasjonskanalene har teknologien gjort det enklere for de kriminelle hvor som helst i verden til å framstå som hvem, eller hva, de ønsker. Det er viktig å huske på at de henvendelser du får ikke nødvendigvis kommer fra de som tilsynelatende står som avsender, eller at avsenderen ikke nødvendigvis er den han/hun påstår å være.

## Hovedpunkter

Her er de vanligste signalene på at henvendelsen du har fått er et forsøk på svindel:

**Frykt;** en melding som tilsynelatende haster, og krever øyeblikkelig handling før noe ubehagelig skjer, som for eksempel at bankkontoen sperres eller politiet kobles inn. Den kriminelle vil at du handler uten å tenke på konsekvensene av det du gjør, du har det travel.

**Press;** krav om å fravike eller ignorere fastsatte prosedyrer på jobb.

**Fristelse;** Tilbud om noe nytt og fantastisk, eller noe som er for godt til å være sant. Nei, du vinner ikke i et lotteri du ikke har kjøpt lodd i.

**Sensitiv informasjon;** en forespørsel om å oppgi sensitiv personlig informasjon, som for eksempel detaljer om bank- eller kredittkort, eller helseopplysninger.

**Tillit, offentlig myndighet;** melding fra offentlige myndigheter som har dårlig språk eller mange skrivefeil. De fleste myndighetsorganer vil ikke benytte sosiale medier for en personlig kommunikasjon med deg. Er du usikker ta kontakt med avsenderen over telefon, med et telefonnummer du finner på nettsiden deres.

**Tillit, person;** melding du mottar fra en venn eller kollega, men språk og ordlyd er ikke slik det vanligvis er. Er du usikker ta kontakt med vedkommende for å få bekreftet at det var de som sendte meldingen. Det er relativt enkelt for kriminelle å lage meldinger hvor de utgir seg for å være noen du kjenner. I enkelte tilfeller kan de ha overtatt brukerkontoen til kollegaen din, og sendt melding til deg derfra. Vær spesielt oppmerksom på tekstmeldinger, Twitter-meldinger eller andre meldinger i kort format. I disse er det ofte vanskelig å kjenne igjen avsender på ordbruk og språk.

Du er det beste forsvar mot slik svindel. Virker en melding eller henvendelse rar eller mistenkelig, er det best å overse den og slette den. Er den fra noen du kjenner kan du ta direkte kontakt med vedkommende over telefon for å få bekreftet at de virkelig sendte meldingen.

## Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

## Gjesteredaktør

***Dr Jessica Barker*** *(@drjessicabarker) er en fremtredende aktør innen det menneskelige aspektet av digital sikkerhet. Hun er direktør/partner i Cygenta, hvor hun kan bruke sin lidenskap for positiv påvirkning av holdninger til digital sikkerhet, adferd og kultur rundt om i verden. Hun er leder for ClubCISO og en populær foredragsholder.*

## Ressurser

| | |
|---|---|
| Sosial manipulering: | https://www.sans.org/u/Uz6 |
| Telefonsvindel: | https://www.sans.org/u/Uzb |
| Stop fiskingen: | https://www.sans.org/u/Uzg |
| Persontilpasset svindel: | https://www.sans.org/u/Uzl |