Real Time Phishing

Eksempel hvor Skatteetaten misbrukes

Husk – virker det for godt til å være sant er det som oftest det!

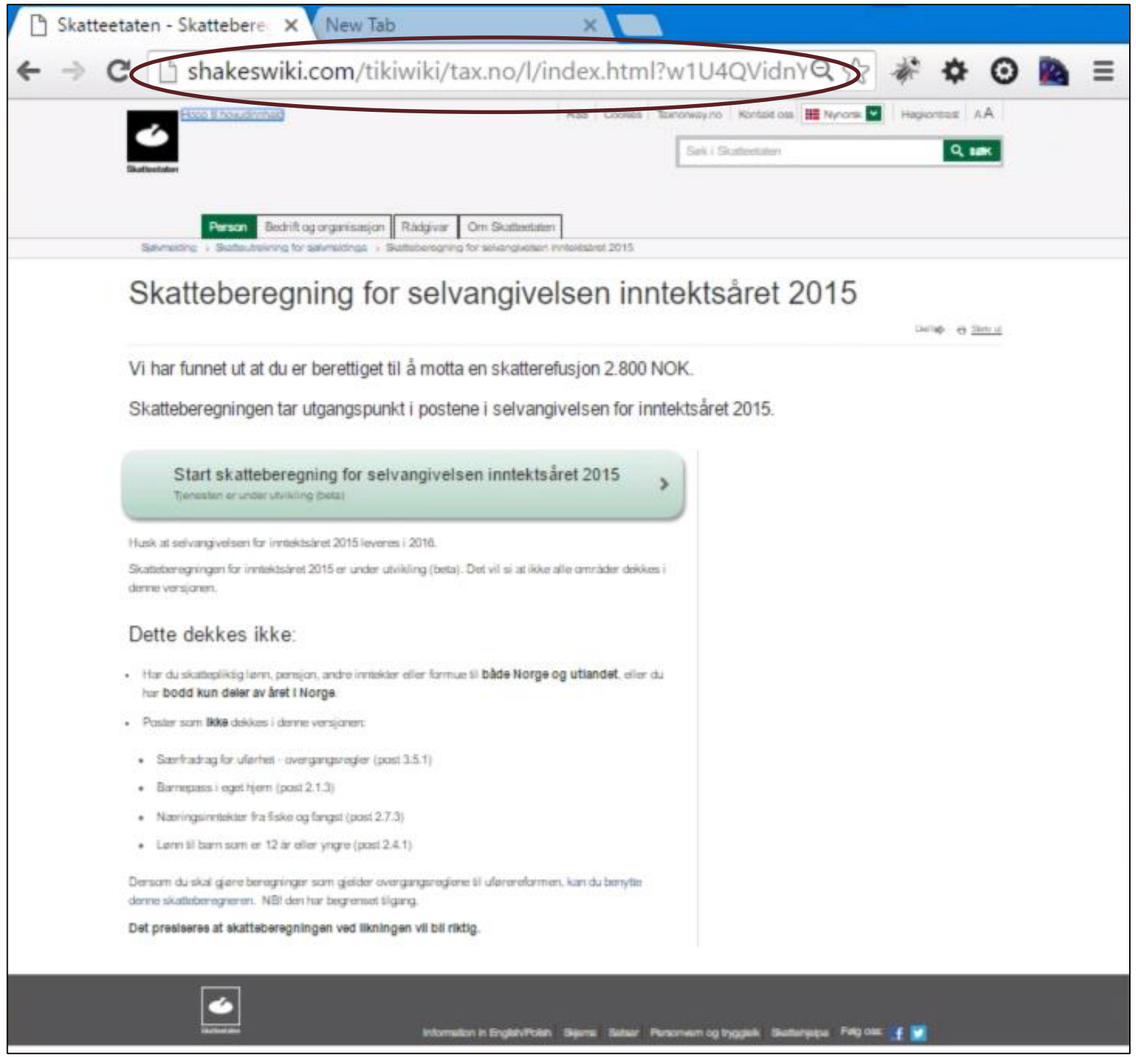
Fra: Skatteetaten [mailto:skatteetaten@skatt.no]
Sendt: 30. august 2016 17:42
Til:
Emne: Betaling mottatt 2.800 NOK

Kjære kunde,

Vi har funnet ut at du er berettiget til å motta en skatterefusjon 2.800 NOK.
Klikk her for å motta.

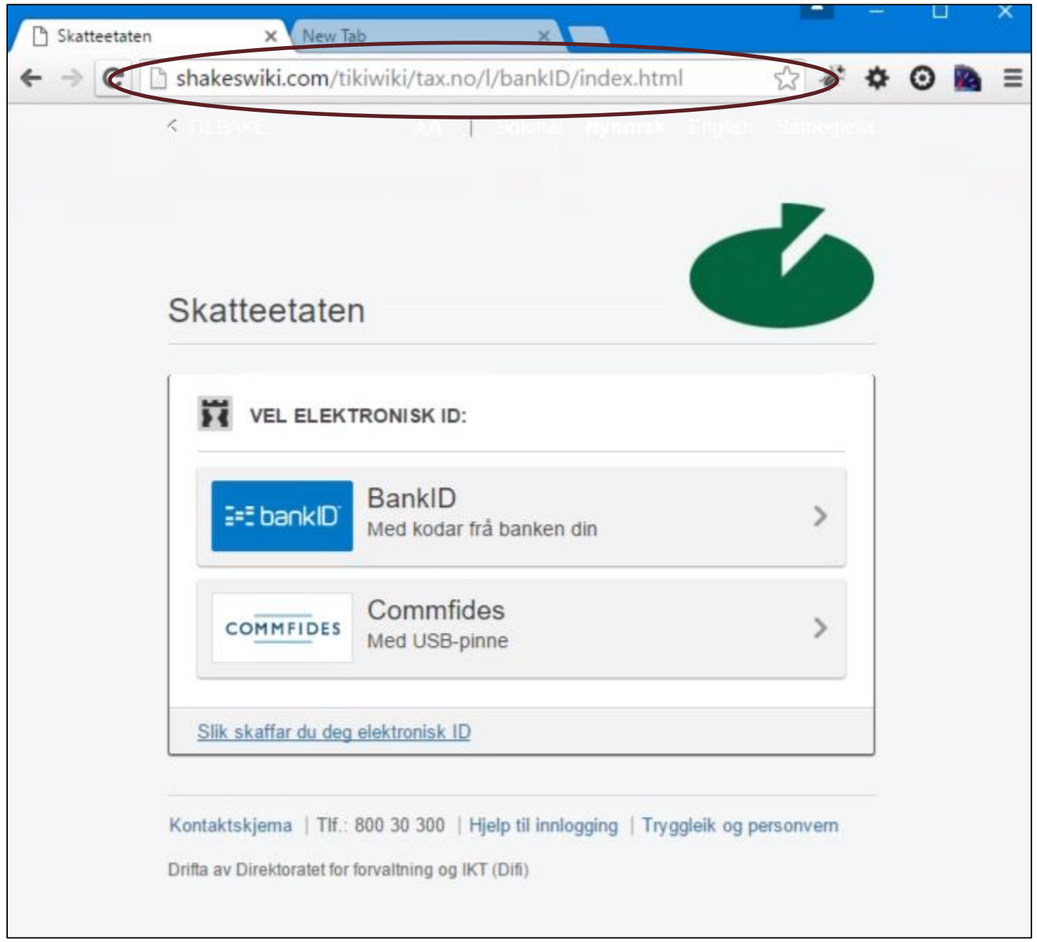
- Formålet med phishing e-post er å lure brukeren til å oppgi kontoinformasjon slik at svindlerne kan benytte informasjonen til bedrageri senere
- E-postene kommer ofte fra en avsender brukeren anser som trygg, som i eksemplet over hvor avsender er Skatteetaten
- Formålet er å få brukeren til å klikke på lenken og gi fra seg informasjon i de kommende feltene

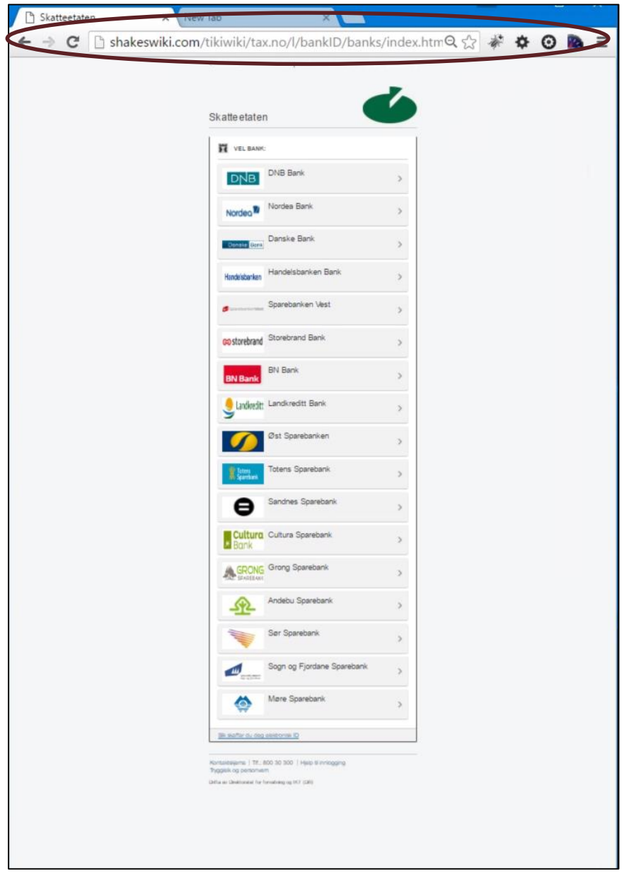
Aurskog Sparebank
– stor nok for folk flest

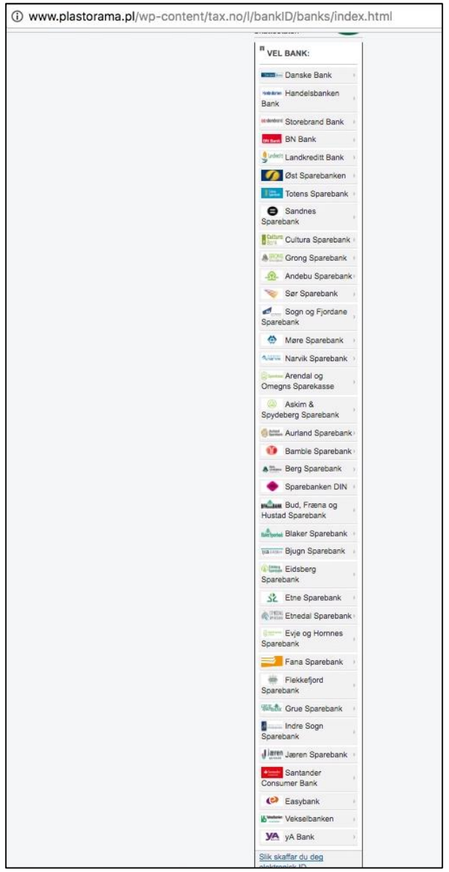


- Dersom brukeren klikker på lenken i e-posten kommer brukeren videre til en side som ser ut til å være Skatteetaten
  - **Men,** sjekk alltid nettadressen (URL)
  - I eksemplet ser man enkelt at det ikke er skatteetaten.no man er inne på
- Formålet til svindlerne er at brukeren skal klikke seg videre inn for å starte skatteberegningen for 2015

Aurskog Sparebank
– stor nok for folk flest

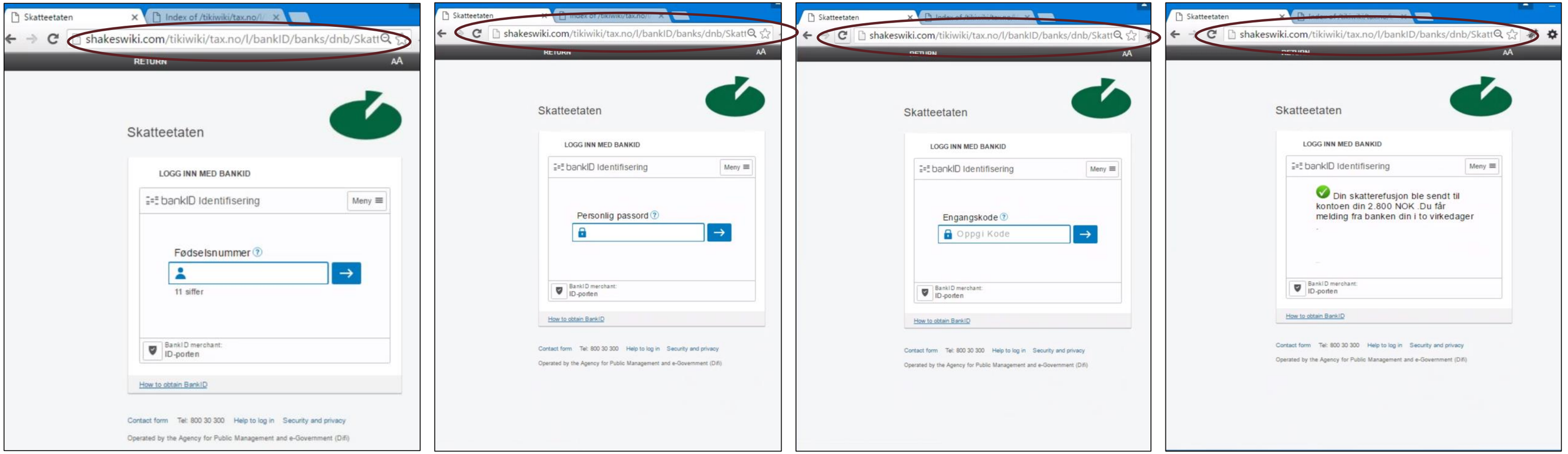






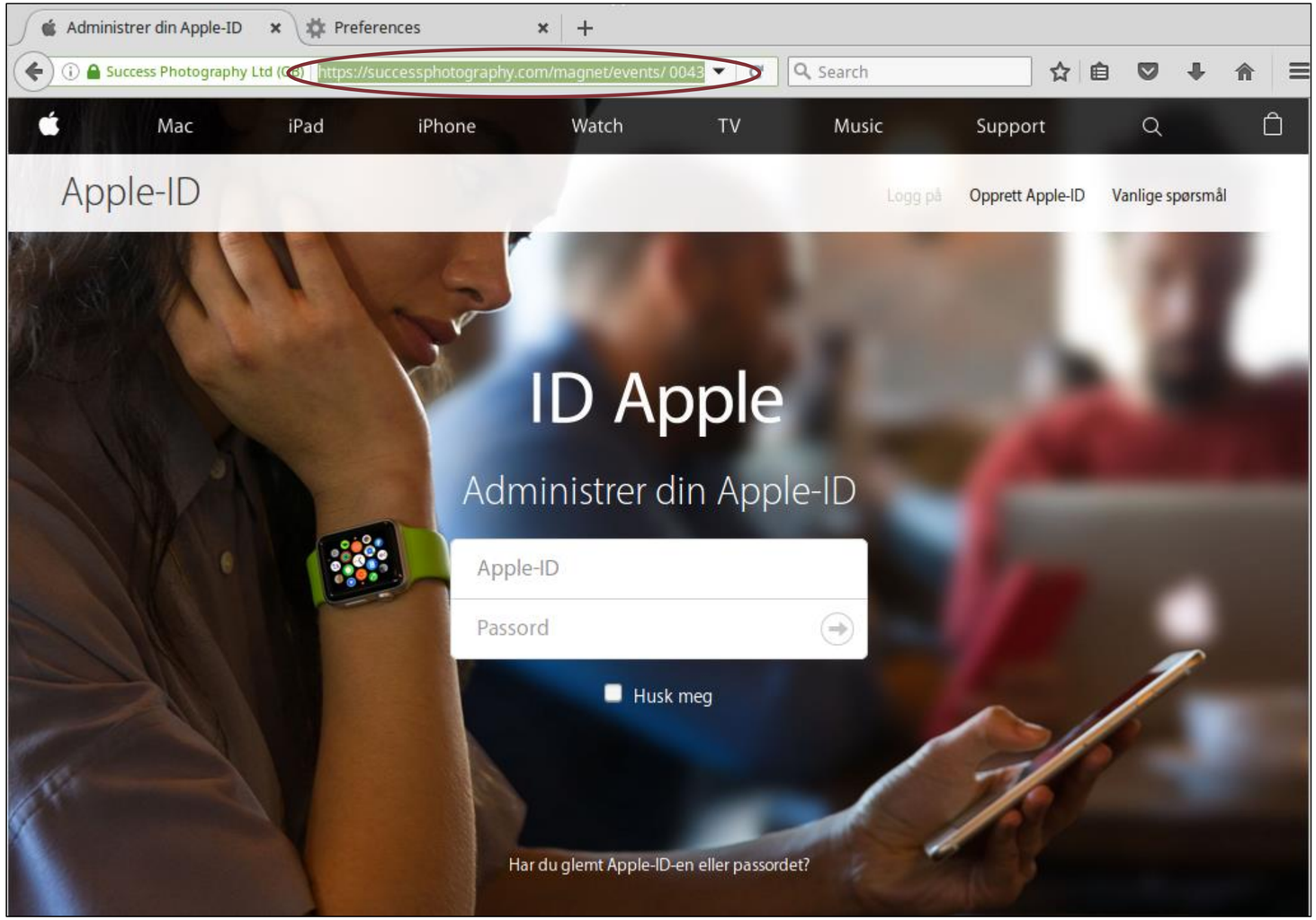
- Nå kommer brukeren inn på BankID pålogging
- I eksemplet må brukeren finne banken sin i en liste for å kunne logge seg på med BankID – dette valget får man aldri ved ordinær BankID-pålogging
- Nettadressen (URL) er fremdeles til en ukjent side

Aurskog Sparebank
– stor nok for folk flest

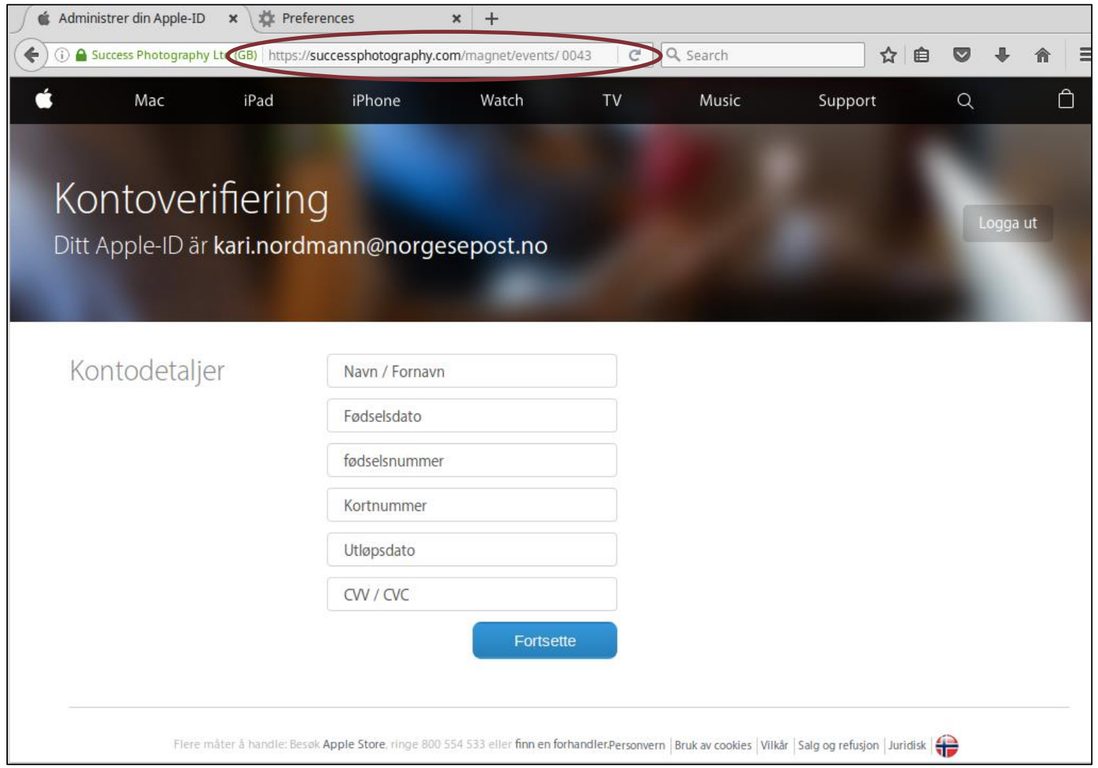


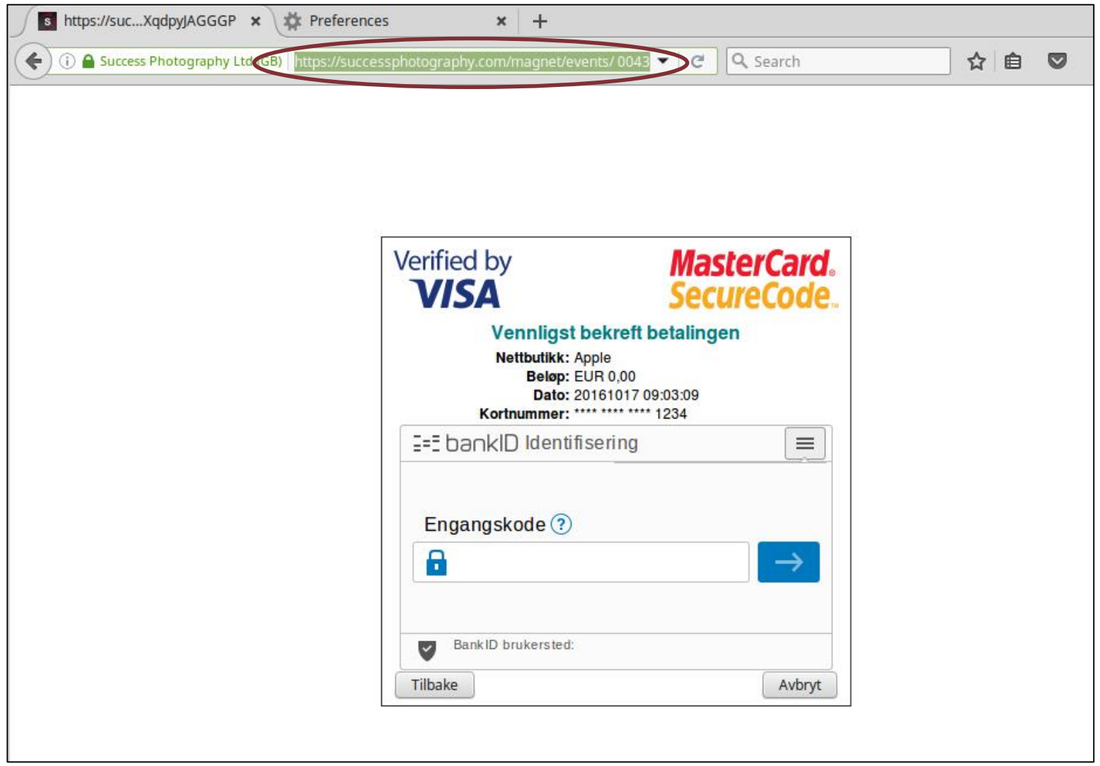
- Nå kommer brukeren videre til inntasting av informasjon i BankID-påloggingen; fødselsnummer, personlig passord og engangskode
- Når dataen er tastet inn har svindlerne full kontroll over kontoinformasjon og kan svindle brukeren
- Den fiktive bekreftelsen til slutt har ingenting å si
- Igjen, sjekk nettadressen (URL) som er et tydelig bevis på at sidene er falske

Aurskog Sparebank
– stor nok for folk flest



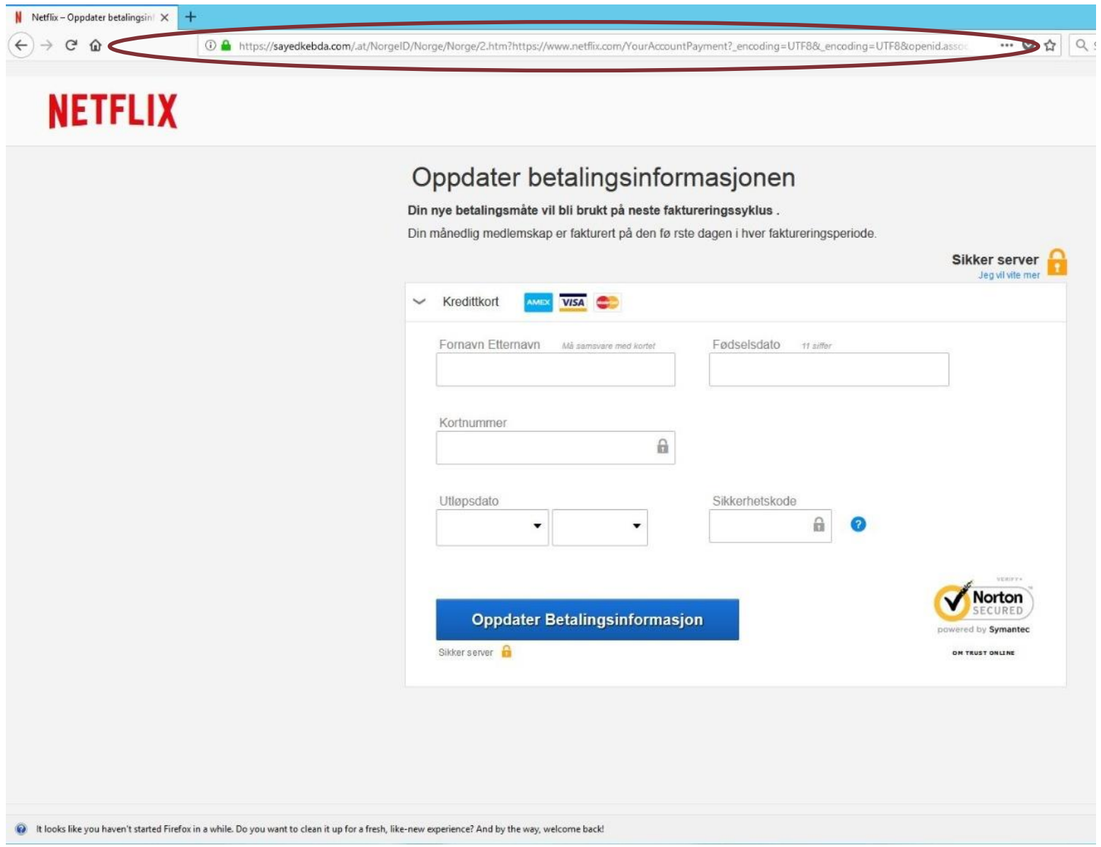
- En annen aktør som ofte blir misbrukt i phishing- og svindelforsøk er Apple
- Her har brukeren fått e-post fra «Apple» med beskjed om å oppdatere Apple-ID og brukeren kommer så videre til en falsk side
- At siden er falsk er enkelt å se av nettadressen (URL)

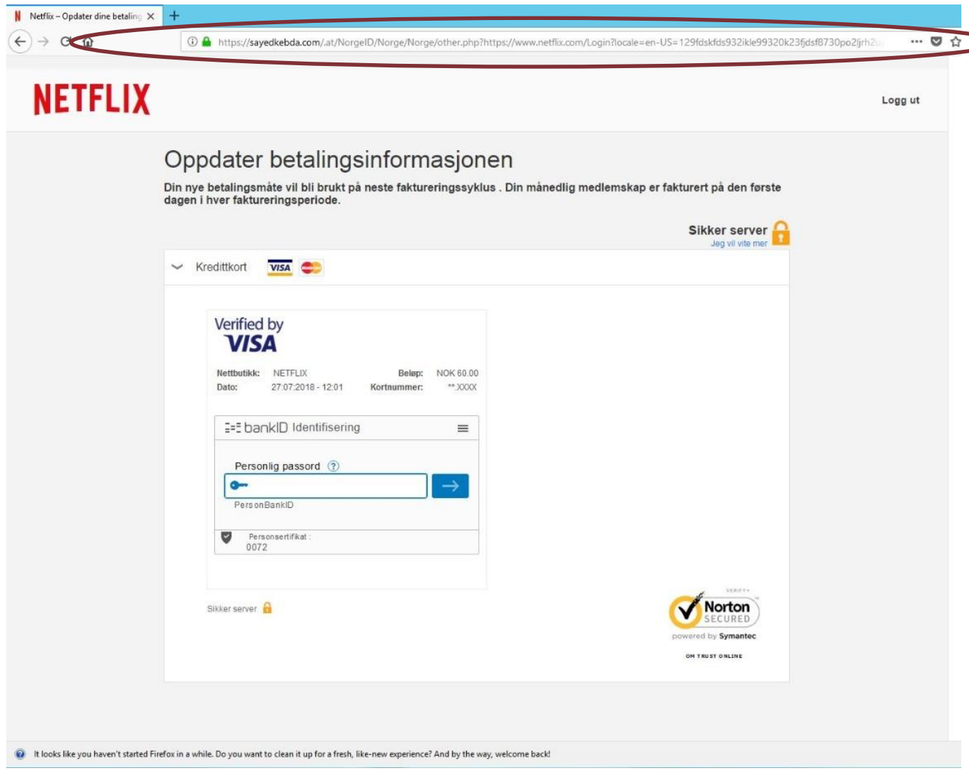




- Brukeren får deretter beskjed om å taste inn kontodetaljene sine
- Og kommer så videre til BankID pålogging
- Når all dataen er tastet inn har svindleren full kontroll på kontoen til brukeren
- Nok en gang kan man av nettadressen (URL) se at siden er falsk

Aurskog Sparebank
– stor nok for folk flest



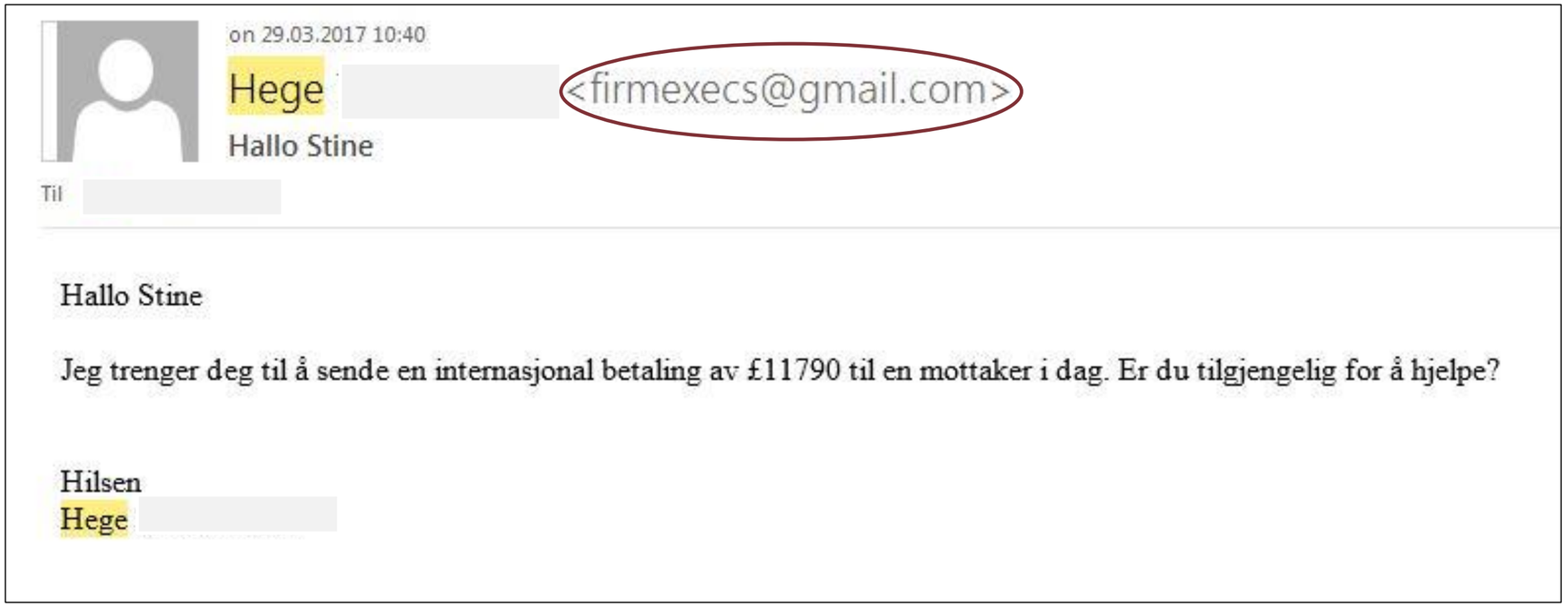


- Den samme fremgangsmåten har også blitt brukt med Netflix som er en kjent merkevare
- Brukeren får beskjed om å oppdatere betalingsinformasjon og må legge inn kort- og BankID detaljer
- Når dataene er lagt inn har svindleren full kontroll på betalingsinformasjonen
- Nok en gang kan vi av nettadressen (URL) se at siden er falsk

Aurskog Sparebank
– stor nok for folk flest

Pengeoverføringer/CEO-fraud

Populær svindelmetode i større bedrifter hvor man forsøker å lure ansatte til å overføre større beløp



on 29.03.2017 10:40

Hege <firmexecs@gmail.com>

Hallo Stine

Til

Hallo Stine

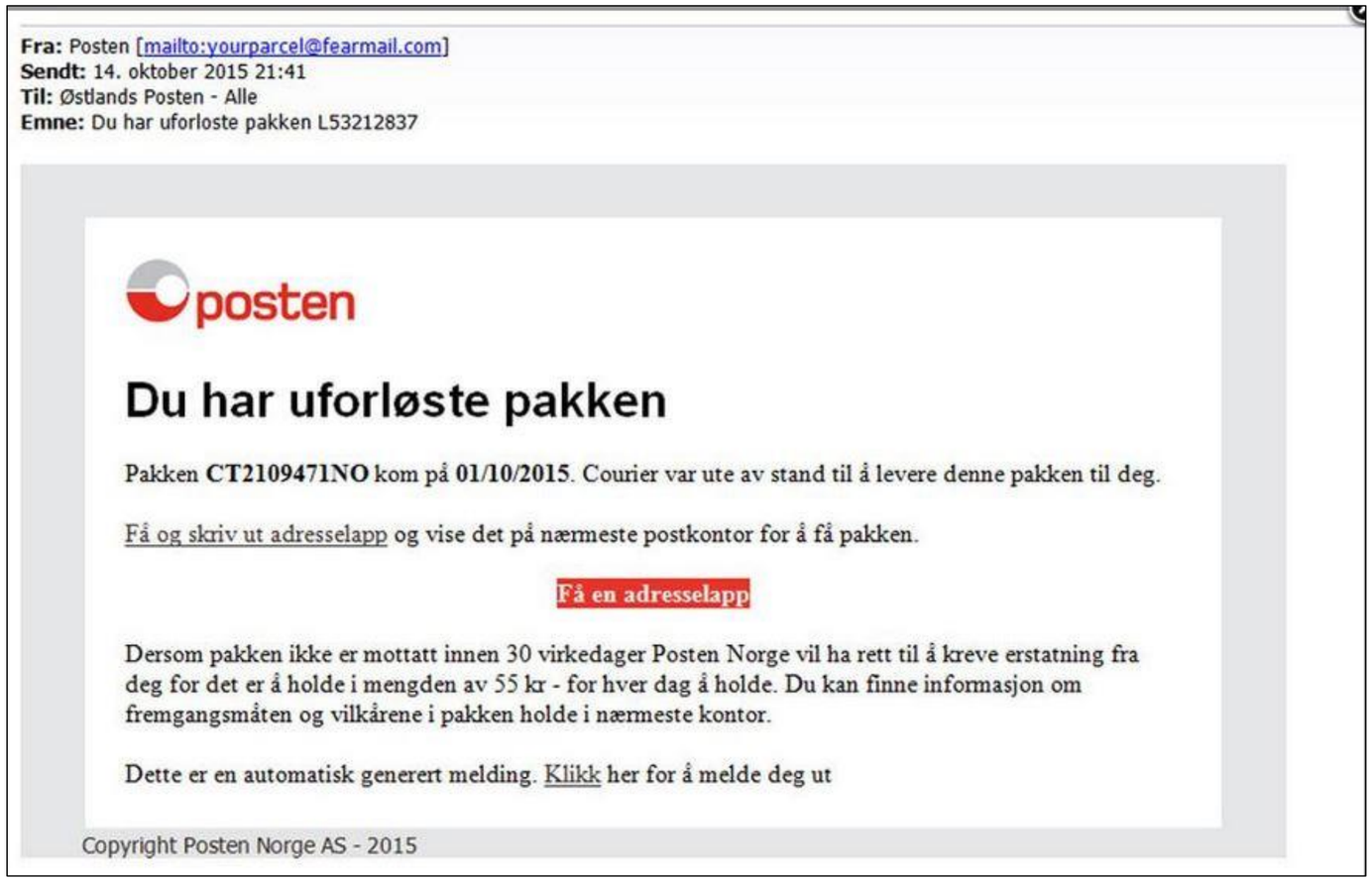
Jeg trenger deg til å sende en internasjonal betaling av £11790 til en mottaker i dag. Er du tilgjengelig for å hjelpe?

Hilsen
Hege

- CEO-fraud er en bedragerimetode hvor svindlerne sender e-post til bedrifter med formål at ansatte skal overføre større beløp, gjerne til utlandet, i sjefen sitt fravær
- Man bør være spesielt oppmerksom på denne type e-poster og gjøre flere undersøkelser for å avklare om sjefen faktisk har sendt e-posten til den ansatte
- Ofte kan man av e-postadressen se at e-posten er falsk, men vær obs – det er ikke alltid man kan se det før man forsøker å svare på e-posten og da ser at det står en annen adresse i «til-feltet»

Infisert PC

Falske e-poster kan inneholde skadevare som infiserer PC dersom man klikker på lenker



Fra: Posten [mailto:yourparcel@fearmail.com]
Sendt: 14. oktober 2015 21:41
Til: Østlands Posten - Alle
Emne: Du har uforloste pakken L53212837

posten

Du har uforløste pakken

Pakken **CT2109471NO** kom på **01/10/2015**. Courier var ute av stand til å levere denne pakken til deg.

Få og skriv ut adresselapp og vise det på nærmeste postkontor for å få pakken.

Få en adresselapp

Dersom pakken ikke er mottatt innen 30 virkedager Posten Norge vil ha rett til å kreve erstatning fra deg for det er å holde i mengden av 55 kr - for hver dag å holde. Du kan finne informasjon om fremgangsmåten og vilkårene i pakken holde i nærmeste kontor.

Dette er en automatisk generert melding. Klikk her for å melde deg ut

Copyright Posten Norge AS - 2015

- Posten er en aktør som dessverre også blir brukt i svindelforsøk
- I eksemplet ser vi en e-post som inneholder lenke til en side som laster ned skadevare til brukerens pc uten at brukeren merker det
- Skadevaren skal senere kunne brukes til å ta kontroll over pc, til å identifisere når brukeren forsøker å logge inn i nettbanken og stjele påloggingsinformasjon etc.
- Vær svært obs før du klikker på lenger i e-poster
- Sjekk avsender adressen på e-posten nøye
- Hold musen over lenken, men ikke klikk, for å se hvilken adresse som ligger bak lenken

"Fra: Telenor Support
Sendt: Tuesday, September 20, 2016 6:39 PM
Emne: Din Telenor er ubetalt, dette er en paminnelse

Kjære kunde,

Vi vil informerer deg at din faktura på kr. 765.77 har forfall den 27 August 2016. For å sjekke fakturaen, vær vennlig at laste ned og åpne fakturaen fra Telenor fakturaservice. I tilfelle du ikke betaler fakturaen i rette tid blir din mobil abonnement sperret og ytterligere gebyrer vil påløpe. Har du ytterligere spørsmål ta kontakt med vår kundesenter. Med vennlig hilsen. Telenor kundeservice."

- Vær også oppmerksom på e-poster som inneholder vedlegg
- Vedleggene kan også inneholde skadevare som lastes ned til brukerens pc
- Dersom skadevare har blitt installert så må pc'en i de aller fleste tilfeller formateres for å bli kvitt noen typer skadevare

Aurskog Sparebank
– stor nok for folk flest