POLITIET

Norwegian Police

Informasjon fra Oslo politidistrikt

Fra: Næringslivskontakt/politiinspektør Christina Rooth Oslo politidistrikt Dato: 12.08.21

Målrettet passordangrep - «Spear phishing»

Politiet har registrert flere henvendelser fra målrettede passordangrep mot jobbsøkere, og nå sist mot hybelleietakere. I forbindelse med studiestart og at flere studenter er på utkikk etter en plass å bo finner Oslo politidistrikt det nødvendig å varsle om at flere unge personer er blitt bedratt, og forsøkt bedratt, via nettsiden hybel.no.

Modus

Gjerningspersoner benytter åpent tilgjengelig informasjon på jobbsøker-portaler, og nå sist på hybel.no, til å sende ut målrettede passordangrep mot jobbsøkere eller leietakere.

Jobbsøkerne eller leietakerne mottar en forfalsket (spoofet) SMS eller e-post der avsender utgir seg for å være fra rekruteringsportalen eller fra hybel.no.

I meldingen fra gjerningspersonen blir du bedt om å gå inn på en lenke for å avtale time til intervju eller til visning. For å gjøre dette må du ifølge svindlerne først legitimere deg med BankID. Dette er en phishing-side som kontrolleres av gjerningspersonene.

BankID-påloggingsinformasjonen som gjerningspersonene tilegner seg brukes til å gjennomføre datainnbrudd i nettbanken. Pengene blir deretter sendt ut fra bankkontoer og ut til ulike betalingsformidlingstjenester, kryptovalutabørser eller kontonummer.

Gjerningspersonene

Kyniske gjerningspersoner som bevisst utnytter de legitime ønskene om å få en jobb eller leilighet/bolig for å stjele penger fra denne målgruppen.

De fornærmede

Dette rammer studenter, jobbsøkere og andre som blir frastjålet penger fra sine bankkontoer.

Politiets rolle og hovedstrategi

Politiets hovedstrategi er å forebygge kriminalitet. Politiet skal dele av sin informasjon for å sette den enkelte i stand til å beskytte sine egne verdier.

Forebyggende tiltak

- Du kan ikke alltid stole på navnet eller telefonnummeret i avsenderfeltet på telefonen da dette lett kan forfalskes
- Les avsenderadresse i e-post nøye for å se om e-posten faktisk kommer fra domenet til den legitime aktøren

OSLO POLITIDISTRIKT
Post: Postboks 2093 Vika, 0125 Oslo / (+47) 22 66 90 50
post.oslo@politiet.no / www.politiet.no / 961 398 142

- Sjekk lenkene du får tilsendt nøye da gjerningspersonene kan ha opprettet et annet domene som ligner på den legitime aktøren
- Unngå å klikke på lenker du får tilsendt på SMS og e-post. Gå heller via den offisielle kanalen eller via nettsiden du normalt benytter
- STOPP – TENK – SJEKK: Ta deg tid og sjekk henvendelsen nøye

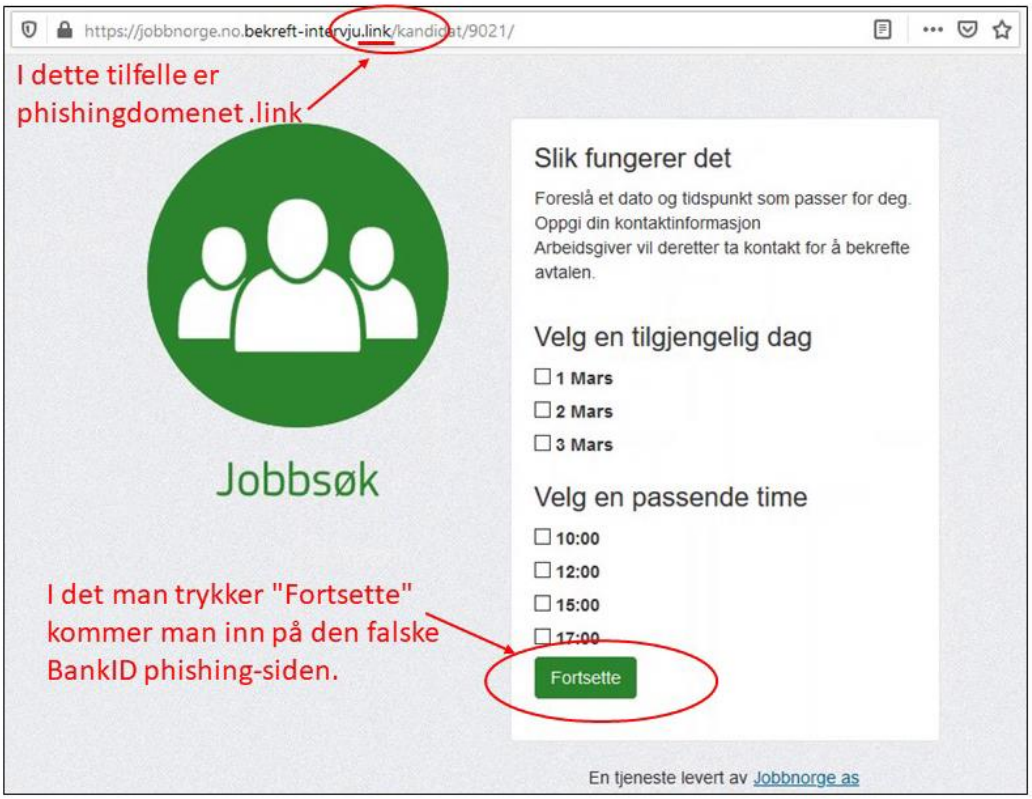
Merk
Noe av grunnen til flere lar seg lure, er at det er et målrettet angrepet mot enkeltperson. Vi er alle mer mottakelige til å trykke på en lenke fra "hybel.no" dersom vi selv har annonsert at vi er på utkikk etter å leie hybel på deres portal. Tilsvarende gjelder dersom du får tilbud om intervju til en jobb når du har annonsert at du er jobbsøkende.

Kontakt egen bank snarest dersom du har blitt bedratt, eller kontakt mottakerbank/eier av kontoen pengene er overført til – hvis mulig.

Ved en eventuell anmeldelse så ta vare på aktuelle meldinger/SMS slik at dette kan dokumenteres, samt dokumentasjon på eventuell bankoverførsel.

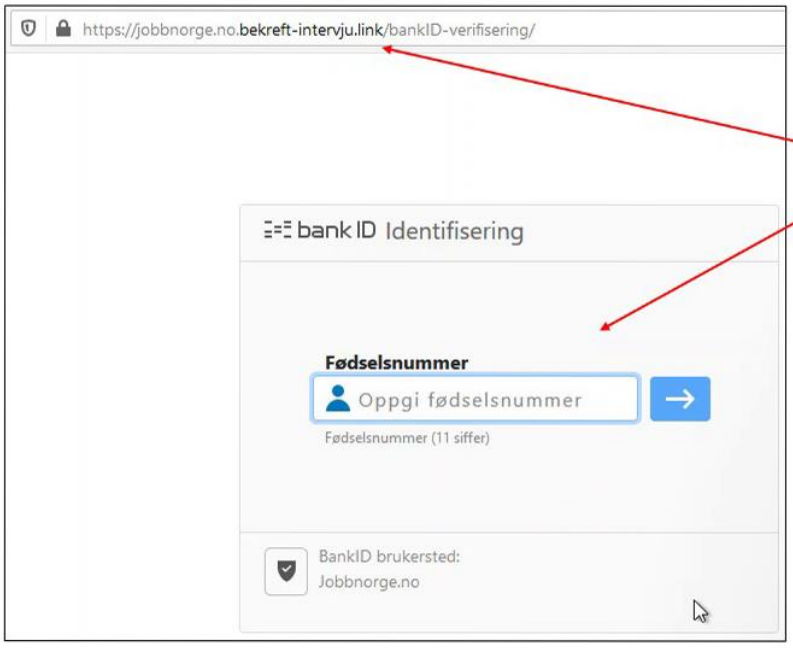
Kontakt
Politiet tlf. 02800 eller https://tips.politiet.no/web/

Nedenfor følger noen bilder som viser hvordan slike bedragerier utføres:



Merk at det ikke er mulig å velge BankID for mobil, men kun vanlig BankID med engangskode.

Vær ekstra på vakt dersom dette er tilfelle, da det er lettere for svindlere å misbruke vanlig BankID med engangskode i forbindelse med målrettet passordangrep (spear phishing).



Dette er en falsk BankID påloggingsside (phishing side)