



POLITIET

Nyhetsbrev fra næringslivskontakten **Nordland politidistrikt**

I denne utgaven:

- ✓ Nettrelaterte bedragerier mot søkere i forbindelse med rekruttering.



De siste månedene har politiet i flere politidistrikter mottatt anmeldelser knyttet til nettrelaterte bedragerier mot søkere til stillinger hos ulike arbeidsgivere. Her følger en beskrivelse av hvordan bedrageriene gjennomføres, hva man selv skal gjøre hvis man blir utsatt for dette, og hva arbeidsgivere bør gjøre for å verne seg mot dette.

Nettrelaterte bedrageri mot søkere i forbindelse med rekruttering

Framgangsmåte

Lederen med ansvar for rekrutteringsprosessen lures ved phishing (digital snoking hvor det fiskes etter passord eller kredittkortnummer) til å gi fra seg påloggingsinformasjon til rekrutteringssystemet.

Svindleren/gjerningspersonen benytter deretter tilgangen til:

1. Gjerningspersonen henter ut personinformasjon om søkerne.
2. Gjerningspersonen forbereder et phishingangrep mot de aktuelle søkerne.
3. Gjerningspersonen sender phishing-SMS. I meldingen inviteres søkeren til intervju, og bes om å bekrefte intervjuet ved å følge en lenke.

Dersom den som mottar phishing-SMS følger lenken tas de med til en side som ligner rekrutteringssystemet til den bedriften hvor de har søkt jobb. De bes deretter om å bekrefte sin identitet med BankID.

Dersom de legger inn data i BankID-vinduet (som er falskt), leses informasjonen av gjerningspersonen, og brukes til å logge på søkerens konto/bank uten at søkeren ser dette.

Søkeren får en bekreftelses-SMS med tidspunktet for intervjuet, som da kommer fra gjerningspersonen og ikke fra bedriften hvor de har søkt jobb.

Når søkeren oppdager at penger er borte er de allerede overført til en

kryptovekslingstjeneste, eller tjeneste for overføring til utlandet.

Hvordan sikre egne verdier?

Fornærmede må kontakte banken snarest mulig og forklare hva som har skjedd. Enten med hjelp av egen bank, eller på egenhånd snarest kontakte mottakerbank/eier av kontoen pengene er overført til – hvis mulig.

Politiet oppfordre alle til å anmelde dersom de blir utsatt for slik svindel. Ta vare på aktuelle melding(er)/SMS slik at dette kan dokumenteres, samt dokumentasjon på eventuell bankoverførsel.

Forebyggende tiltak for de som skal rekruttere nye medarbeidere

Orienter i stillingsannonsen om at dere aldri ber om BankID-informasjon i søknadsprosessen.

Eier av rekrutteringssystemet som er benyttet i våre saker jobber også med sikkerhetstiltak for å begrense mulighetene framover. Men det finnes mange ulike systemer, og det vil ta til å gjøre alle kjent med denne typen bedrageri.

Politiets hovedstrategi

Politiets hovedstrategi er å forebygge kriminalitet. I tillegg til at næringslivet og offentlige etater selv gjør nødvendige tiltak, er politiet helt avhengig av et godt samarbeid og god informasjonsutveksling for å lykkes.

Kontaktinformasjon politiet i Nordland politidistrikt

Næringslivskontakt: Håvard Fjærli

Mailadresse: havard.fjarli@politiet.no

Mobiltelefon: 918 83 382