POLITIET

Vest Politidistrikt

Nettrelaterte bedragerier mot søkere i forbindelse med rekruttering

Juni 2021

De siste månedene har politiet i flere distrikter 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.

Sør-Øst politidistrikt melder om følgende modus i sine saker:

- 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.
- Aktøren henter personinformasjon om søkerne.
- Aktøren forbereder et phishingangrep mot de aktuelle søkerne.
- Aktøren sender phishing-SMS. I meldingen inviteres søkeren til intervju, og bes om å bekrefte intervjuet ved å følge en lenke.
- Dersom de følger lenken tas de til en side som ligner rekrutteringssystemet sin side, hvor de bes om å bekrefte med BankID.
- Dersom de legger inn data i BankID-vinduet (som er falskt), leses informasjonen av aktøren og brukes til å logge på søkerens konto/bank uten at søkeren ser dette.
- Deretter får de en bekreftelses-SMS med tidspunktet for intervjuet.
- Søkeren oppdager at penger er borte. Pengene er gjerne overført til en kryptovekslingstjeneste eller tjeneste for overføring til utlandet.

Politiets hovedstrategi:

Vest politidistrikt har ikke registrert informasjon om lignende fenomen. Vi ønsker å formidle ut informasjon i forkant slik at vi sammen kan forebygge sannsynlighet for lignende uønskede hendelser i Vest politidistrikt.

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.

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.
- Oppfordre til å anmelde forholdet, ta vare på aktuelle melding(er)/SMS slik at dette kan dokumenteres, samt dokumentasjon på eventuell bankoverførsel.
- Lurer du på hvordan du skal sikre skjermbilder eller har behov for råd og veiledning? Ta kontakt med Politiets nettpatrulje Vest (politivest) på Messenger eller Instagram Direct. De svarer vanligvis innen 1 døgn.

For næringslivet og offentlig forvaltning:

- Orienter i stillingsannonsen om at de 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 systemer, og det vil ta tid å gjøre alle kjent med denne typen bedrageri.

MVH politiet i Vest

Næringslivskontakt: sonja.lund@politiet.no

Digitalt politiarbeid: Rune.Kenneth.Bauge@politiet.no

For innspill og kontakt i andre politidistrikter finnes oversikt over de forskjellige næringslivskontaktene i lenken nedenfor. Tilsvarende for landets nettpatruljer

https://www.politiet.no/kontakt-oss/naringslivskontakter/

https://www.politiet.no/rad/trygg-nettbruk/politiets-nettpatrulje/