



17. februar 2021

Varsel til fylker, kommuner, helsesektor og DSB

## **Vaksine-svindel er en trussel man må forberede seg på**

Vaksinasjon mot Covid-19 er noe store deler av befolkningen er opptatt av og venter på. Samtidig vet vi at svindel og spredning av skadevare er utbredt i andre land, og at dette også rammer Norge for tiden.

Informasjon fra myndighetene må derfor være på en form som gjør det vanskelig for kriminelle å utnytte situasjonen.

Basert på erfaring forventer NSM ved Nasjonalt Cybersikkerhetssenter (NCSC) at svindelforsøkene vil øke i omfang i tiden fremover.

**Ulike kommunikasjonskanaler benyttes av svindlere for å nå frem til ofrene.** Det er observert svindel via telefonoppringninger, tekstmeldinger, eposter, meldinger via sosiale medier, osv.

### **Svindlernes metoder vil variere:**

- Mange av svindlerne vil trolig tilby tidlig vaksinasjon mot forhåndsbetaling, kanskje forklart med at pasienten må selv dekke en «egenandel». Vi har sett tilfeller der innbyggere fikk telefonoppringning som tilsynelatende var fra et privat medisinsk senter eller en kommune, med tilbud om snarlig vaksinasjon, mot forhåndsbetaling.
- Man må også regne med svindelforsøk som har til hensikt å lure inn skadevare på privat eller arbeidsgivers datautstyr, for eksempel løsepengevirus.
- Det kan dreie seg om mer «tradisjonelle» motiver som å tilegne seg bankkontonumre, kredittkortnumre, personalia, helseopplysninger (allergier, sykdommer, mm). Slike opplysninger kan brukes i svindel eller for utpressing av offeret senere.

**Det er potensielt en rekke konsekvenser hvis man blir lurt.** Blant annet kan helseinstitusjoner måtte håndtere oppmøte av pasienter som er overbevist om at de har gyldig timebestilling og gyldig kvittering på betalt «egenandel». I en krevende tid kan dette skape uheldige situasjoner.

**Det er utfordringer med myndighetenes budskap.** Det sentrale i budskapet i dag er at «du vil bli kontaktet når det er din tur for vaksine». Et slikt budskap mangler presisjon om *hvem* som tar kontakt og

*hvordan* det blir tatt kontakt. Dette er en form for budskap som antagelig er hensiktsmessig helsefaglig, men som er godt egnet til å bli misbrukt av svindlere. Et budskap fra myndighetene med for mange ukjente faktorer kan øke svindlernes muligheter.

#### **NSMs anbefalinger:**

**Kommuner og helsemyndigheter anbefales å spisse og standardisere budskapet.** Dette kan bidra til at innbyggerne blir trygge på at reelle innkallinger faktisk kommer fra kommunen samt at de falske innkallingene blir korrekt oppfattet som svindel. Følgende kan vurderes for å spisse budskapet:

1. Tydeliggjør *hvem* er det som vil ta kontakt med pasienten. Er det kommunene, FHI, helsedirektoratet, helsedepartementet, fastlegen, private legetjenester eller andre? Hvem vil aldri ta kontakt? Dette er nok ikke opplagt for alle innbyggere.
2. Det bør tydeliggjøres *hvilken kanal* (epost, telefonoppringning, SMS, mm) som innbyggerne kan forvente å bli kontaktet på, og hvilke kanaler vil *ikke* benyttes (for eksempel neppe via sosiale medier).
3. *Hvordan* vil beskjeden være utformet? F.eks. bruk av lenker i offentlig informasjon bør unngås.
4. Det bør understrekes at det aldri vil være krav om (forhånds)betaling for å få vaksine tidligere.

Man kan vurdere å ha et tilsvarende spisset og standardisert budskap mht. sykdoms-testing, som også er utsatt for svindelforsøk.

For å redusere sårbarheter (ikke minst mot skadevare) og øke virksomheters IT-sikkerhet anbefaler vi alle virksomheter om å følge de tiltak som er beskrevet i «NSMs Grunnprinsipper for IKT-sikkerhet», samt å be ansatte være oppmerksomme ved bruk av både privat og arbeidsgivers datautstyr.