BEIARN
kommune

Økt bruk av hjemmekontor gir nye åpninger for nettkriminalitet. Slik sikrer du deg som ansatt i Beiarn kommune

Nå som vi er oppfordret til å jobbe fra hjemmekontor er vi ekstra sårbare for nettkriminalitet. Mange av oss er ute på nytt digitalt farvann – og svindlerne står klar til å lokke oss ut blant skjærene i sjøen.

Større ansvar på den enkelte

Når du arbeider fra hjemmekontor er du i en situasjon hvor du plutselig får et mye større ansvar for bedriftens nettsikkerhet.

Det er hver og en av oss som må ta ansvar for å sikre hjemmenettet, for å oppdatere operativsystemer og sikkerhetsprogramvare, og å sørge for at vi bruker sikre løsninger for kommunikasjon og fjernjobbing. Derfor er det viktig å følge bedriftens IT-retningslinjer og alltid å ha nettsikkerhet i bakhodet.
Oppkobling av datamaskin på hjemmekontor bør skjer i samarbeid med IKT i kommunen.
Ta kontakt for bistand via telefon eller via e-post It-support@beiarn.kommune.no

Generelle sikkerhetsregler for bruk av hjemmekontor

- De samme sikkerhetskrav gjelder for bruk av hjemmekontor-PC som for all annen bruk av IKT i Beiarn Kommune.
- Det er en forutsetning at familiemedlemmer ikke gis tilgang til bruk av Beiarn kommunens datautstyr eller IT-løsninger. Husk at arbeidsrelaterte telefoner i utgangspunktet er av konfidensiell karakter ovenfor dine familiemedlemmer og på denne bakgrunn SKAL skjermes for disse.
- Dataskjermer skal plasseres slik at innsyn for uvedkommende hindres. Datamaskin settes i hvilemodus når du som ansatt forlater arbeidsplassen.

BEIARN
kommune

1. Vær kjempeskeptisk til uventede meldinger, telefoner eller e-poster

Dette er kanskje det aller viktigste å huske på. Får du en henvendelse som ber deg gjøre *noe som helst* – det være seg å klikke på en lenke, logge inn et sted, åpne et vedlegg eller oppgi en eller annen form for informasjon – må du stoppe opp og tenke. Spør deg selv: hvem er det egentlig som spør? Hva er det de er ute etter? Er det en mulighet for at de forsøker å manipulere meg til å gjøre noe?

2. Bare stol på informasjon fra verifiserte kilder

For å skille seriøse fra useriøse henvendelser er det viktig å ha oversikt over *hvem* som skal kontakte deg – og via hvilke kanaler. Gjelder det ting som har med jobb å gjøre, er det kanskje nærmeste leder eller en arbeidskollega.
Still deg enkle spørsmål som; I hvilken kanal skal det deles viktig informasjon? Hvem er det som er kontaktperson for IT, avsender fra Servicetorget eller annet? Hvordan skal en mail internt fra en kollega eller leder i kommunen se ut?

Tenk deg om to ganger før du klikker på en lenke i en melding du mottar på mail eller SMS (se eget tips om lenker under).

3. Dobbeltsjekk at senderen er den de utgir seg for å være

Det er lett for nettkriminelle å gi seg ut for å være noen andre, både via telefon og e-post. En av den vanligste formen dette tar er såkalt «Microsoft-svindel» , men mange er også mer utspekulerte enn som så.
Om du får en henvendelse som krever aktivitet fra din side, bør du derfor alltid ta en avsjekk med den påståtte avsenderen via en annen kanal. Det koster ingenting å bruke noen ekstra minutter på å sende en SMS eller ta en telefon og spørre «sendte du meg nettopp en mail?».

4. Bekreft linker før du klikker

Blir du tilsendt en lenke via e-post: hold musepekeren over lenken – uten å klikke – så vil få opp nettadressen det *faktisk* linkes til. Dette er viktig, da det er utrolig enkelt å lage en hyperlink som sender deg til en helt annen nettadresse enn det det ser ut som.
Her kan vi for eksempel skrive: «Hold deg oppdatert om retningslinjer for å hindre virusspredning på folkehelseinstituttets nettsider: fhi.no. Trykker du på denne lenken, sendes du i dette tilfellet faktisk ikke til fhi.no, men til UNICEFs kampanjeside om korona-viruset. Hadde dette vært et forsøk på svindel, kunne det i stedet ha vært en lenke som hadde sendt deg til en nettside med skadelig programvare.
Når det gjelder lenker via SMS, anbefales det å at du sikre deg ved å kopiere nettadressen fra meldingen framfor å trykke direkte på linken.

BEIARN
kommune

5. Tenk deg om før du åpner vedlegg

Vedlegg er en av de enkleste måtene å snike inn virus og skadelig programvare på maskinen eller mobilen din. Om du mottar en e-post du ikke eksplisitt forventer å få, er det derfor ekstra viktig at du dobbeltsjekker hvem avsenderen er (se over) før du åpner et eventuelt vedlegg.

6. Ikke oppgi sensitiv informasjon eller personopplysninger på e-post eller telefon

Hva er sensitiv informasjon? Som regel er det snakk om ting som brukernavn, passord, kredittkortinformasjon, personnummer og så videre.

Husk også at du gjennom din jobb håndterer en rekke personopplysninger som ikke må sendes via digitale kanaler. Her gjelder naturligvis de samme reglene som når du arbeider fra kontoret, men det er vedr å være spesielt oppmerksom på dette ved bruk av hjemmekontor.

Regelen, uten unntak, er å aldri dele sensitiv informasjon og personopplysninger via e-post, SMS, telefon eller chattetjenester. *Punktum.*