



POLITIET

Datakriminalitet og bedrageri Unngå å bli svindlernes neste offer

Kyrre Lindanger
Næringslivskontakt, Sør-Vest politidistrikt

Stort omfang

Datakriminalitet begås først og fremst for økonomisk vinning, for å skade maskinvare eller digitale tjenester eller for å skaffe sensitiv informasjon.



Dataangrep mot kritisk infrastruktur

Tre kategorier:


- Datainnbrudd
- Løsepengevirus
- Tjenestenektangrep



Hvordan forebygge?

- Fortell de ansatte at deres bedrift kan bli utsatt for forsøk på bedrageri
- Gå gjennom rutiner for god digital hygiene på e-post
- Gå gjennom rutinene for gjennomføring av transaksjoner med de ansatte
- Bruk alltid to-trinns autorisering av en faktura.
- Ser fakturaen ekte ut?



- 
- Bruk virusprogram og brannmur.
 - Lag sikkerhetskopier og hold programvaren oppdatert.
 - WiFi: Bytt alltid standardpassordet du har fått oppgitt for ruterens.
 - Gå gjennom tillatelsene til appene dine, slett dem du ikke bruker.
 - Velg sterke og unike passord for e-post og kontoer på sosiale medier.
 - Gå gjennom personverninnstillingene for kontoene på sosiale medier.
 - Ikke klikk på lenker i e-poster.
 - Sjekk om nettadressen eller e-postadressen er til å stole på.
 - Sjekk alle lenker ved å holde musepekeren over lenken.
 - Sjekk språket og rettskrivingen.
 - Ikke oppgi sensitive personopplysninger

- Se etter det grønne ikonet med en hengelås helt til venstre i nettleserens adressefelt.
- Høres det for godt ut til å være sant? Da er det som regel det.
- Du må ikke besvare e-post på sekundet.
- Synes du noe skurrer? Ta deg tid til å lese en gang til.





POLITIET

For mer informasjon:

www.nsm.no

www.nsr-org.no

www.nettvett.no/korona