CYBERSIKKERHET FOR
ALLE

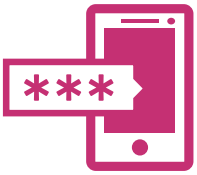
NETTVETT-REGLENE

NorSIS

NorSIS

NETTVETTREGLENE

1. FØLG RÅDENE FOR SIKKER PÅLOGGING



- Aktiver totrinnsbekreftelse for alle brukerkontoer på nett der det er mulig.
- Lag unike passord for alle brukerkontoer. Ta gjerne utgangspunkt i en sang og legg til noe unikt for hver tjeneste.
- Skriv gjerne passordene ned på et papir som du lagrer på et trygt sted. De passordene du bruker ofte bør du memorere.
- Bruk en passordmanager om du er komfortabel med det.

2. HOLD OPERATIVSYSTEM OG PROGRAMMER OPPDATERT

- Sørg for at operativsystemet på alle dine enheter som datamaskin, mobil og nettbrett alltid er oppdatert.
- Sørg for at installerte programmer og apper også er oppdaterte.
- Slå på automatiske oppdateringer der dette er mulig.

3. TA SIKKERHETSKOPI

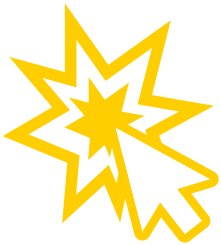
- Sørg for at du tar jevnlig sikkerhetskopi av de viktigste filene dine. Husk at dette må gjøres for alle enhetene dine.
- Bruk gjerne en lagringsenhet som kan være tilkoblet datamaskinen eller mobilen ofte og som støtter automatisk kopiering. Dette kan gjerne være en skytjeneste.
- Bruk også gjerne en ekstern harddisk, som du kopierer manuelt til med jevne mellomrom og som du oppbevarer adskilt fra datamaskinene din, på et trygt sted.

NorSIS

4. BRUK BRANNMUR OG ANTIVIRUS

- De fleste operativsystemer har dette innebygd, men man må selv forsikre seg om at det er skrudd på.

5. TENK FØR DU KLIKKER



- Svært mye av svindel og virus når oss gjennom e-post. Ta deg tid til å tenke gjennom følgende:

  a. Har jeg forventet denne e-posten?

  b. Stemmer avsenderadressen?

  c. Ser selve meldingen troverdig ut?

  d. Ser lenker og vedlegg trygge ut?

- Klikk aldri på lenker i e-post og sms for å legge inn personopplysninger på siden du kommer til. Gå heller inn på virksomhetens nettside.
- Spiller innholdet i meldingen på følelser som tillit, frykt eller fristelser, samtidig som den prøver å få deg til å gjøre noe, så er dette kjente tegn på svindelforsøk.

6. TENK OVER HVA DU DELER

- Vurder hvordan du fremstiller deg selv på ulike sosiale medier.
- Vær bevisst på hva slags personlig informasjon du publiserer.
- Forvent at alle kan se informasjonen du deler, både om jobb og privatliv.
- Ikke legg ut bilder av, eller informasjon om, venner eller kolleger uten tillatelse.

NorSIS

7. TA ANSVAR – VÆR ÅPEN OM HENDELSER

- Alle kan bli lurt. Fortell de rundt deg om trusler og farer du har opplevd. Åpenhet sprer kunnskap og trygghet, uten å spre frykt. Åpenhet gjør det mindre skamfullt å være et offer for kriminalitet på nett.
- Rapporter sikkerhetsbrudd, hendelser og trusler du opplever på arbeidsplassen til nærmeste leder eller IT-ansvarlig.
- Å anmelde datakriminalitet er svært viktig for at politiet skal kunne bekjempe denne type kriminalitet.

8. VÆR EN VENN PÅ NETT

- Vær kritisk og sørg for at du kan stå for det du legger ut! Publiser kun ting du ville sagt ansikt til ansikt.
- Opplever du at noen oppfører seg dårlig mot deg på nett? Ikke svar. Blokkér og rapporter!
- Hvis du blir trakassert, uthengt, ekskludert eller liknende på nett, ta vare på bevis, for eksempel ved å ta skjermbilde
- Trusler og trakassering, på nett eller i annen form, er brudd på norsk lov, og bør anmeldes til politiet.
- Oppdager du at noen utsettes for mobbing, vær en venn, ta ansvar og si ifra.

9. UNNGÅ Å FALLE FOR FRISTELSER

- Noe virker for godt til å være sant – da er det gjerne det!
- Du mottar tilbud på produkter som er tilnærmet eller helt gratis mot at du oppgir personlig informasjon.
- Du mottar e-poster som oppgir at du har vunnet store pengebeløp eller at du har fått «tilbakeført» et pengebeløp du i utgangspunktet ikke kjenner til.