

Passordvett

Valg av passord

1. Et passord skal være lett å huske for deg og vanskelig å gjette for andre
2. Benytt ulike passord for ulike tjenester
3. Passordet bør være så langt som mulig
4. Bytt passord med jevne mellomrom eller hvis du tror det er på avveier

Noen eksempler

Lag forskjellige passord på forskjellige tjenester. Bruk gjerne en setning som du assosierer med tjenesten, men helst ikke direkte navnet på tjenesten. Eksempelvis trenger du passord for nettbutikk for bøker. Passordet kan da være en setning knyttet til yndlingsboka eller forfatteren din. Setningen bør ha mellomrom eller andre spesialtegn. Dette gjetter ingen og det er også vanskelig å knekke for hackere. Passord som består av vanlige ord må helst være mer enn 20 tegn. Har du med blank og andre spesialtegn kan det være kortere. Bruk gjerne en sangstrofe eller en annen kort setning.

- «Lisa g1kk til, face» er lett å huske for tilgang til Facebook. Det er for langt til å knekkes, lett å huske for deg og vanskelig å gjette.
- «Lisa g1kk til, regn» er lett å huske for tilgang til regnskapssystemet.

Men, IKKE bruk disse eksemplene. Lag dine egne gode passord som er unike for deg og dine tjenester.

Noen tjenester har regler slik at du har begrensning i antall tegn eller krav til tall eller spesialtegn i passordet. Dette må du da innrette deg etter. Bruk da varianter av huskereglene over.

Hvorfor er gode passord viktig

Bruker-ID og passord gir deg tilgang til spesifikke tjenester eller programmer. Dersom noen har passordet ditt kan de opptre som deg i mange sammenhenger, og dette kan gi mange uheldige konsekvenser.

Programmer laget for å knekke passord blir stadig mer sofistikerte. De følger sinnrike regler og kan ha tilgang til ordlister på mange språk. Det finnes også mye offentlig informasjon om deg som kan misbrukes til å gjette dine passord. Venner eller noen som har kjennskap til deg kan også gjette passordet ditt og misbruke det.

Beskyttelse av passord

Passord er en hemmelighet

- Gi aldri passord eller pin-kode til noen, verken til familiemedlemmer eller til banken.

PC-en kan sladre

- Når du har valgt et godt passord er neste steg å beskytte det. Da er det ikke godt nok å la være å skrive det ned eller fortelle det til noen. Også PC-en må forhindres fra å sladre.

La ikke programmet huske passordet

- PC-en må forhindres fra å sladre. Mange programmer tilbyr seg å huske passordet til neste gang du logger inn. Dessverre er det ulikt hvordan de gjør det, og i verste fall kan passordet lagres i klartekst på PC-en. Benytt derfor aldri denne funksjonen på en fremmed datamaskin.

Logg ut og lukk vinduene

- På PC-er som brukes av flere må du alltid huske å logge ut. Lukk også alle nettleservinduene, da enkelte programmer husker passord selv om du ikke har bedt om det.

Bruk nøkkelkryptering

- Dersom nettleverandøren tilbyr alternative autentiseringssystemer bør du velge Kerberos, challenge/response eller en offentlig nøkkelkryptering.
- Bruker leverandøren bare vanlige passord bør du be dem om å gå over til sikrere løsninger.