

Passord: slik lager du et som er godt



5 gode råd for å lage gode passord:

- Passordet bør inneholde minst 8 tegn
- Du bør bruke både små og store bokstaver, tall og gjerne spesialtegn
- Passordet bør ikke være et ord som står i en ordbok
- Ikke bruk stedsnavn, eget navn, sekvenser av bokstaver eller repetisjon av tegn
- Lag gode huskereglar, og ta gjerne utgangspunkt i hele setninger

5 gode råd for bruk av passord:

- Passordet skal være vanskelig å gjette...
- ... men enkelt å huske
- Ikke oppgi passordet ditt til andre, og ikke skriv det ned
- Bytt passord med jevne mellomrom
- Ikke bruk samme passord over alt

I. Gode passord hindrer misbruk

Uvedkommende som får tak i passordet ditt, kan bruke dette til å skaffe seg informasjon om deg, og tilgang til dine personlige tjenester. Det er derfor viktig å lage gode passord som kun du kjenner til, for å hindre at andre kan utgi seg for å være deg. I tillegg til å være hemmelig, må passordet være så komplisert at andre ikke kan gjette det. Samtidig må det være så enkelt at du selv greier å huske det. Du må også huske at det å lage kompliserte passord for hver eneste tjeneste som krever pålogging, kan føre til at det blir veldig mange passord å holde styr på.

For å slippe unna med færre passord, kan det være lurt å dele tjenestene dine inn i kategorier etter hvor kritiske de er. Da kan du for eksempel bruke ett passord for hver kategori.

Uvedkommende som avslører passordet ditt, kan bruke dette for å skaffe seg tilgang til de tjenestene som krever at du logger på med passordet. Motivet kan være å få innsyn i informasjon om deg, få tilgang til dine filer, eller å misbruke e-postkontoen din for masseutsendelse av e-post. Et annet motiv for å skaffe seg tilgang til din brukerkonto, kan være for å bryte seg inn i systemet til den organisasjonen du er tilknyttet.

Gode passord er altså viktig for å forhindre at uvedkommende får tilgang til dine personlige tjenester og informasjon, men er også minst like viktig for å beskytte organisasjonen mot mer alvorlige innbrudd.

2. Hvordan lage gode passord?

Gode passord skal helst bruke så stor del av tegnsettet som mulig, og inneholde både store og små bokstaver, tall og spesialtegn hvis dette er tillatt. Passord bør ha en viss lengde, og ikke inneholde kjente ord, navn, datoer eller lignende. Helst skal det se ut som et sett av vilkårlige tegn.

Et godt passord skal være vanskelig for andre å gjette, men likevel lett for deg å huske. Å oppfylle disse to kriteriene samtidig, og i tillegg oppfylle kravene som organisasjonen din stiller, kan virke vanskelig. Det lar seg imidlertid gjøre, det krever bare at du bruker litt tid på å lage passordet ditt.

2.1. Lag passord som er vanskelige å gjette

For at passordet ditt skal være vanskelig å gjette, bør det helst inneholde en blanding av store og små bokstaver, tall og spesialtegn. Om du kommer til å bruke passordet på ulike systemer og tastaturer, tenk over at eventuelle spesialtegn må aksepteres alle steder. Sørg også for at passordet ditt inneholder flest mulig ulike tegn, og ikke bare de vanligste tegnene.

Et passord blir vanskeligere å gjette jo flere tegn det inneholder. Gode passord skal derfor være så lange som mulig, helst åtte tegn eller mer. Med nok maskinkraft og tid kan ethvert passord avsløres dersom en angriper får lov til å prøve nok ganger. En angriper kan også ha flaks og gjette passordet ganske fort, spesielt hvis det er et dårlig passord.

En som ønsker å avsløre passordet ditt prøver først passord basert på enkle ord og personlige assosiasjoner. Prøv derfor å unngå dette i dine passord.

Passordet ditt bør ikke inneholde følgende:

- Ord som står i ordbøker, leksika og lignende, uansett språk. Også deler av slike ord, slike ord baklengs, slike ord med vanlige feilstavinger og erstatninger.
Eks: "daVinci", "ttakepa", "Mercedes".
- Navn og stedsnavn, titler på bøker, sanger, filmer og lignende, eller navn fra slike.
Eks: "honolulu", "pippi", "HarryPotter", "returnofthejedi".
- Informasjon knyttet til deg eller noen som står deg nær. Typisk navn, brukernavn, initialer, adresse, telefonnummer, fødselsdato, personnummer og lignende.
Også deler av slik informasjon.
Eks: "annetteg", "ag1982", "abelsgate5".
- Sekvenser av bokstaver eller tall, stigende eller synkende.
Eks: "123456", "vutsrqpo".
- Bokstavrekker fra tastaturet.
Eks: "qwerty", "mnbvcxz".
- Repetisjon av samme tegn mange ganger.
Eks: "7777777", "vvmmm".
- Repetisjon av samme mønster.
Eks: "agagag", "OL94OL94".
- Ord hvor alle symboler er erstattet med tall som ligner.
Eks: "see you later" blir til "CUL8R", "oslo" blir til "0\$10".
Å erstatte bokstaver på denne måten er imidlertid et godt virkemiddel kombinert med variasjon, feilstaving og lignende.

2.2. ... men som du likevel klarer å huske

Problemet med lange og komplekse passord, er at vi gjerne sliter med å huske dem. Men det finnes råd. Når du skal lage gode passord, kan det være lurt å lage noen enkle huskereglar:

Ta utgangspunkt i noe du lett klarer å huske, for eksempel en setning. Erstatt så ordene i setningen med en blanding av store og små bokstaver, tall og gjerne også spesialtegn. Slik kan du lage passord som for andre ser ut som en tilfeldig rekke av tegn og tall, men som du klarer å huske.

En måte å gjøre dette på, er å bytte ut hvert ord i en setning med en bestemt bokstav fra det aktuelle ordet, typisk første bokstav. For å gjøre passordet litt mer komplekst kan du deretter erstatte noen av bokstavene med tall og tegn som ligner. Du kan også legge inn feilstavinger og bytte om på bokstaver. Passord laget med utgangspunkt i én eller flere setninger er lettere å lære utenat enn tilfeldige passord, men er så og si like gode.

Du kan også lage passord som består av flere ord, en såkalt passordfrase. Mange vil synes det er lettere å huske en setning enn et passord, derfor kan passordfraser være særlig aktuelt for de minste barna. Og siden passordfraser gjerne inneholder mange tegn, blir de vanskelige å gjette. I tillegg er det i setninger naturlig å bruke tegnsetting og spesialtegn, som også kan bidra til å øke styrken til et passord. Dersom mellomrom er tillatt, kan du skille ordene med mellomrom. Alternativt kan du la ordene henge sammen uten mellomrom, eller skille dem med andre tegn.

3. Ta vare på passordet ditt

Når du har brukt tid på å lage et godt passord, bør du også bruke litt tid på å lære det utenat.

3.1. Øv deg på passordet

Øv deg på å skrive passordet ditt noen ganger, så du er sikker på at du husker det til neste gang. Dersom du må oppgi passordet jevnlig, vil det fort sette seg i fingrene. Da vil du skrive passordet nokså fort, og risikoen for at noen kan se passordet over skuldrene dine, blir ganske liten.

3.2. Ikke skriv ned passordet

Om du bruker passordet sjelden og i begynnelsen sliter med å huske det, kan du notere et hint eller to som gjør at du klarer å resonnerer deg frem til passordet. Må du skrive ned passordet, må du alltid sørge for å skjule det i en kode. Skriv aldri ned selve passordet!

3.3. Oppgi aldri passordet

Oppgi aldri passordet ditt til andre. Dette gjelder ikke bare venner, familie eller kjæreste, men også it-personellet i din organisasjon. Ved brukerstøtte må du sørge for at du skriver inn passordet selv.

3.4. Unngå usikre maskiner

Unngå i så stor grad det er mulig å skrive inn passordet ditt på usikre maskiner, for eksempel på internettkafeer, biblioteker og flyplasser. Forsikre deg om at ingen ser deg over skuldrene når du skriver inn passord, og ikke la nettlesere og programmer huske passordet ditt på delte maskiner. Noen programmer som tilbyr å huske passord for deg, lagrer passordet ditt i klartekst på maskinen. Det betyr at uvedkommende kan få tilgang til det når du har logget ut. Vær også forsiktig med hvor du oppgir passordet ditt.

4. Bytt passord en gang i blant

Ingenting varer evig, heller ikke gode passord. Uansett hvor godt du beskytter passordet ditt, bør det byttes med jevne mellomrom. Særlig viktig er det at du umiddelbart bytter passord om du har grunn til å mistenke at noen har fått kjennskap til det. Sørg for at du vet hvor og hvordan du bytter passord ved de systemene og tjenestene du bruker.

Når du bytter passord, bør du ta deg tid til å lage et helt nytt et, ikke gjenbruk passord du har brukt tidligere. Du bør heller ikke gjenbruke deler av gamle passord ved at du kun bytter ut et par tegn eller stokker om på rekkefølgen.

Vær oppmerksom på at det som var et godt passord for noen år siden ikke nødvendigvis er et godt passord i dag. Når datamaskiner får stadig større maskinkraft, blir det stadig mindre tidkrevende å knekke passord. Unngå derfor korte passord på mindre enn åtte tegn.

5. Ikke bruk samme passord overalt

Mange velger å bruke samme passord overalt, fordi dette er mye enklere enn å holde styr på forskjellige passord for forskjellige tjenester. Vi fraråder imidlertid sterkt å gjenbruke passord ukritisk ved alle tjenester, siden sikkerheten rundt ulike typer tjenester varierer veldig.

5.1. Usikre tjenester gir usikre passord

Husk at passordet ditt aldri er sikrere enn den minst sikre tjenesten du har registrert det ved. Selv om du har et komplekst og i utgangspunktet godt passord i nettbanken, er det ikke lenger et godt passord om du også benytter det for pålogging til et tilfeldig diskusjonsforum på nettet. Om noen lykkes i å fange opp passordet ditt når du logger på for å poste et innlegg i diskusjonsforumet, vil de samtidig få passordet ditt til nettbanken.

Det ideelle ville være aldri å gjenbruke samme passord på flere tjenester. Bruker du bare et fåtall tjenester, bør dette være mulig. Virkeligheten er imidlertid at mange har en lang rekke tjenester å forholde seg til, og da sier det seg selv at det er nærmest umulig å lage og huske nye, gode passord for hver tjeneste.

5.2. Kategoriser tjenester og passord

For å slippe unna med færre passord kan det være lurt å kategorisere tjenestene dine etter hvor kritiske de er, og å bruke ett passord for hver kategori. For eksempel kan du ha ett passord for alle tjenester du bruker på skole eller jobb, et annet til nettbanken, et tredje for andre tjenester som har kredittkortopplysninger, og et fjerde til alt annet.

Gjør du det på denne måten vil du slippe unna med færre passord. Pass bare på at du ikke bruker samme passord i flere kategorier.

6. Eksempel på gode passord

På de neste sidene følger noen eksempler på hvordan du kan gå frem for å lage passord som ser komplekse ut for andre, men som du selv lett kan klare å huske. Ikke gjenbruk disse eksemplene i dine egne passord, men la deg gjerne inspirere av fremgangsmåten.

Flere av eksemplene antar at spesialtegn og norske sært tegn er tillatt. Dersom dette ikke er tilfelle ved din organisasjon, må du naturligvis la være å bruke slike tegn.

Eks 1:

Tar utgangspunkt i et ord: **"skomakergata"**

Erstatter noen av bokstavene med tall og tegn som ligner. Et mulig resultat av en slik erstatning er "sk0m@kerg@ta@". Vi anbefaler imidlertid litt mindre forutsigbarhet i utbyggingen. Du kan gjerne erstatte en del av bokstavene med tall og tegn som ligner, men uten å være fullt så konsekvent. Resultatet blir et langt og godt passord, som består av store og små bokstaver, tall og tegn. Selv om det ser komplekst ut, kan du med litt trening fint huske det:

Passord: "\$K0m@kRgA7a"

Eks 2:

Lager et ord som ikke finnes i noen ordbok og som ikke er personlig relatert: **"mobiltreneren"**
Dette er et ord uten mening, satt sammen av to tilfeldige ord. Ordet er greit å huske, men andre vil ha problemer med å gjette det. Ved å bytte ut stavelsen "tre" med tallet "3", "bil" med den store bokstaven "B" og endingen "en" med en stor "N" får du et godt passord som består av store og små bokstaver samt tall.

Passord: "moB3nerN"

Eks 3:

Tar utgangspunkt i to ord: **"jalapeñopepper" og "pepperkaker"**

Lager ut i fra disse ordene et helt nytt ord; "jalapeñokaker". Ordet står neppe i noen ordbok, men er likevel et ord du kan klare å huske. Det er fullt mulig å lage et godt passord ut av dette ved å bytte ut noen av bokstavene med tall og store bokstaver, og ved å legge inn en feilstaving. Du kan for eksempel feilstave "jalapeño" som "hallapenjo", erstatte "o" med "0" og bytte ut "er" med "R". Man står da igjen med et langt og godt passord:

Passord: "hallapenj0kakR"

Eks 4:

Lager en setning som er lett å huske: **"alt jeg ønsker meg er tre pannekaker med sukker"**
Ved å ta første bokstav fra hvert ord får du "ajøme3pms". For å gjøre passordet litt mer komplekst kan bokstaven "p" for pannekaker gjøres stor, siden pannekaker jo er så godt. Og så kan "j" erstattes med et utropstegn, da utropstegnet minner om en "j" som står opp ned. Vi får da et godt passord som inneholder store og små bokstaver, tall og spesialtegn:

Passord: a!øme3Pms"

Eks 5:

Tar utgangspunkt i en linje fra en sang: **"money for nothin' and your chicks for free"**
Tar forbokstaven fra hvert ord også her. I tillegg kan "money" erstattes med et dollartegn, og "for" med tallet fire andre gang det inntreffer. I tillegg kan "chicks" få stor forbokstav. Man står da igjen med et godt passord:

Passord: "\$fnayC4f"

Eks 6:

Lager en setning, en såkalt passordfrase: **"vernebriller er en finfin ting"**
Kunne valgt å la setningen stå slik, eventuelt å skrive setningen uten mellomrom og få passordet "vernebrillererenfinfinting". Velger i stedet å separere ordene med understrek slik at passordet blir som følger:

Passord: "vernebriller_er_en_finfin_ting"

UNINETT ABC

Abelsgt. 5
7465 Trondheim
Tlf: 73 55 79 00

www.uninettabc.no