



Til ansatte og bedrift:

Alt du trenger å vite om passordbeskyttelse



procano

Innhold:

- Bli en IT-sikker bedrift med riktig Password Manager
- 7 gode tips for å beskytte passordene dine
- Beskytt kontoene dine med totrinnsverifisering
- Oppskriften er klar

Introduksjon IT-sikkerhet

Beskytt passordene dine

Det er mange ting vi gjenbraker i hverdagen. Pass på at passord *ikke* er en av dem.

Bedrifter kan ha hundrevis av kontoer de må ha kontroll på. I tillegg har de ansatte et titalls forskjellige passord å holde styr på selv. Det ville krevd mye dersom vi skulle husket på alle de forskjellige passordene. Gjentatte ganger benytter man ulike kombinasjoner av passordet sitt med "123" på slutten, eller kanskje et av disse tegnene "#!?".

Ofte gjenbraker vi passord fordi det er "enkelt", men det er ikke spesielt sikkert. Hvert år oppstår det mange passordlekkasjer, noe som kan koste små og mellomstore bedrifter mye.

Visste du at en av de største årsakene til passordlekkasjene faktisk er hvordan ansatte behandler, bruker, oppretter og lagrer passordene sine? Her har vi samlet sammen nyttig informasjon sånn at du kan ta vare på kontoene og passordene dine på en enkel og IT-sikker måte.

Team Procano



Password Manager

Bli en IT-sikker bedrift med riktig Password Manager

Vår anbefaling er å komme i gang med en Password Manager. Det finnes både gratis og betalte varianter, så det gjelder å finne den som passer ditt behov best.

En Password Manager lagrer påloggingsinformasjonen din for alle nettstedene du bruker, og hjelper deg med å logge på automatisk. I tillegg vil en god Password Manager kunne lage sikre, tilfeldige passord for deg og huske dem – slik at du slipper!

Dersom passordet ditt er lekket, har hackeren innhentet informasjon om din e-postadresse, ditt brukernavn og/eller en passordkombinasjon, og fått tilgang til plattformen. Dette kan føre til at hackeren kan gjette seg til kombinasjonen på andre plattformer også. Det vil si at dersom du bruker den samme påloggingsinformasjonen overalt, kan en lekkasje på en plattform gi dem tilgang til alle kontoene dine.

En Password Manager krypterer passorddatabasen din med ett hovedpassord, som også er det eneste passordet du må huske på! Password Manager programmene “[Dashlane](#), [Lastpass](#) og [1Password](#)” støtter både privat- og bedriftskontoer, og er derfor anbefalt av IT-eksperterne.

7 gode tips for å beskytte passordene dine:

For deg som enda ikke har kommet i gang med *Password Manager* har vi listet opp noen tips til deg og dine ansatte.

1. Bruk unike passord på alle nettsteder og applikasjoner.
2. Benytt sterke passord; lange, uforutsigbare passord som inneholder bokstaver, tall og symboler.
3. Opprett og oppbevar passordene på en IT-sikker måte.
4. Ha kontroll over tilganger, og ha gode rutiner for on/offboarding av ansatte, innleide ressurser, leverandører og samarbeidspartnere.
5. Bytt passord hver 12. – 15. måned, eller når du får varsel om at det er lekket. Sjekk om passordet ditt er på avveie med vår [passordsjekk](#).
6. Ikke ta unødvendig risiko: tenk zero trust – altså, forvent alltid at passordet ditt er lekket.
7. Til slutt vil vi oppfordre deg til å investere i en Password Manager som passer ditt behov.



Beskytt kontoene dine med totrinnsverifisering

To hengelåser er tryggere enn én.

Totrinnsverifisering betyr ganske enkelt at det kreves to eller flere autentiseringsmetoder for å logge seg inn på en digital plattform. Autentiseringsmetoder for totrinnsverifisering er:

- Noe du *er* – ansiktsgjenkjenning eller fingeravtrykk
- Noe du *vet* – passord, sikkerhetsspørsmål, PIN-kode
- Noe du *har* – kort, kodebrikke eller telefon

Et eksempel er å handle noe over nett. For å få gjennomført kjøpet trenger vi både bankkortet (detaljene) og PIN-kode fra kodebrikke eller bankID. Det samme prinsippet gjelder for digitale passord – jo flere hengelåser, jo mer beskyttet er man.

Totrinnsverifisering er det ekstra sikkerhetsnivået som vil hindre at uvedkommende får tilgang til selskapets, og dine personlige, (sensitive) data, selv om de skulle klare å få tak i passordet ditt.

Husk at det også er en risiko for brudd på bedriftens IT-sikkerhet når du bruker apper og plattformer som privat e-post, Instagram, LinkedIn, Facebook, banken din eller andre plattformer.

Oppskriften er klar

Det finnes flere smarte investeringer man kan foreta for å beskytte passordene til de ansatte. Er du klar for å komme i gang med sikkerheten?

De nye medievanene er her for å bli, og det gjør oss også mer sårbare på nett. Hvert år er det et stort antall kontoer som blir hacket på grunn av passordlekkasjer.

Vi arbeider med selskaper i forskjellige bransjer, og vi vet at alle bedrifter har ulike IT-løsninger og behov. Derfor anbefaler vi i Procano at alle bedrifter tar utgangspunkt i forretningsbehovene sine for å finne den løsningen som passer best for seg.

Vi håper du har fått noen gode tips og forslag til hvordan du kan øke IT-sikkerheten for din bedrift. Om du skulle trenge ekstra hjelp eller veiledning for å komme i gang med sikkerhet, er vi klare for å hjelpe deg!



Morten Halvorsen
Senior Advisor

