OUCH! | September, 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Oversikt
- Hvordan virker passordhvelv
- Å velge riktig passordhvelv

Passordhvelv

Oversikt

Et av de viktigste grepene for å være sikker på nett, er å bruke unike, sterke passord for hver eneste brukerkonto og app. Dessverre er det nok umulig å huske alle de forskjellige passordene til alle de forskjellige brukerkontoene. Derfor ender enkelte opp med å gjenbruke det samme passordet. Dessverre er det å gjenbruke et passord på flere brukerkontoer farlig, fordi dersom det passordet kommer på avveie, vil det kunne brukes for å få tilgang til alle brukerkontoer hvor du har benyttet det. En enkel løsning er å bruke et passordhvelv, noen ganger også kalt passord-håndteringsprogram. Dette er programmer som lagrer alle passordene dine på en sikker måte, noe som gjør det enkelt å ha forskjellig passord for hver brukerkonto. Passordhvelv gjør dette enkelt, for istedenfor å måtte huske alle passordene, trenger du kun å huske hovedpassordet til passordhvelvet.

Gjesteredaktør

Chris Christenson er informasjonssikkerhetskonsulent basert i California, og har 20 år med erfaring og diverse tekniske sertifiseringer. Han har snakket på mange forskjellige konferanser og har bidratt til mange artikler i industrien. Du kan nå Chris på **@cchristianson** og **https://ismellpackets.com**.

Hvordan virker passordhvelv

Passordhvelv lagrer alle passordene dine i en database, som noen ganger også kalles et hvelv. Passordhvelvet krypterer hvelvets innhold og beskytter det med et passord som kun du vet hva er. Når du har behov for et passord, f.eks. om du skal logge inn på nettbanken eller sjekke e-post, taster du ganske enkelt inn hovedpassordet for å låse opp hvelvet. I mange tilfeller henter passordhvelvet automatisk passordet du har behov for og logger inn for deg på en trygg måte. Dette gjør det enkelt å ha hundrevis av unike, sterke passord, siden du ikke trenger å huske dem.

Noen passordhvelv lagrer hvelvet på PC-en din eller på mobilen, mens andre lagrer det i nettskyen. I tillegg har de fleste passordhvelv funksjonalitet som automatisk synkroniserer innholdet i passordhvelvet på tvers av enheter du har, som du har godkjent at dette skjer på. På denne måten vil endringer du gjør på et passord på laptopen din, automatisk synkroniseres til alle de andre enhetene dine. Uansett hvor databasefilen er lagret, må du ha installert passordhvelv-applikasjonen for å bruke den.

Passordhvelv

Når du først setter opp et passordhvelv, må du manuelt skrive inn eller importere innloggingene og passordene dine. I ettertid vil passordhvelvet kunne oppdage når du registrerer en ny brukerkonto eller endrer passordet på en eksisterende konto, og oppdaterer innholdet i hvelvet deretter. Dette er mulig fordi de fleste passordhvelv fungerer hånd i hånd med nettleseren din. Denne integreringen gjør det mulig for dem å automatisk logge deg inn på nettsider også.

Det er kritisk at hovedpassordet du bruker for å beskytte innholdet i passordhvelvet er sterkt, og vanskelig å gjette for andre. Faktisk anbefaler vi at du bruker en passordsetning som hovedpassord, det er en av de sterkeste formene for passord man kan ha. Om passordhvelvet ditt støtter to-trinns bekreftelse burde du absolutt bruke det. Sist men ikke minst, sørg for at du husker hovedpassordet. Om du glemmer det mister du tilgangen til alle de andre passordene dine.

Passordhvelv er en enkel løsning for å lagre og bruke alle de forskjellig passordene dine på en sikker måte.

Å velge riktig passordhvelv

Det er mange passordhvelv å velge mellom. I Resurser-seksjonen har vi lagt inn en link til en anmeldelse av forskjellige passordhvelv. Når du prøver å finne den som er best for deg, kan du ha følgende i tankene:

- Passordhvelvet burde være enkelt å bruke. Om du synes løsningen er for kompleks til at du forstår den, bør du finne en annen som passer din stil og ekspertise bedre.
- Passordhvelvet burde fungere på alle enheter hvor du har behov for passord. Det burde også være enkelt å holde passordene dine synkronisert på alle enhetene dine.
- Bare bruk godt kjente og pålitelige passordhvelv. Vær på vakt med produkter som ikke har vært tilgjengelig særlig lenge, eller som har lite eller ingen tilbakemeldinger fra bransjen. Cyberkriminelle kan også lage falske passordhvelv for å prøve å stjele informasjonen din. Vær også på vakt ovenfor enhver produsent som hevder å ha utviklet sin egen krypteringsløsning.
- Unngå et hvert passordhvelv som hevder å kunne gjenopprette hovedpassordet for deg. Det betyr at de kjenner til hovedpassordet ditt, hvilket utsetter deg for stor risiko.

Passordhvelv

- Sørg for at løsningen du ender på er en hvor produsenten kontinuerlig fikser på og kommer med oppdateringer til passordhvelvet, og sørg for at du alltid bruker den nyeste versjonen.
- Passordhvelvet burde ha muligheten til å automatisk generere sterke passord for deg, samt vise deg styrkegraden på passordene du har valgt.
- Passordhvelvet burde la deg få lagre annen sensitiv informasjon også, som f.eks. svar på sikkerhetsspørsmål, og informasjon om bank- og kredittkort.

Passordhvelv er en flott måte for å lagre alle passordene dine, og annen sensitiv data, på en sikker måte. Men, siden de beskytter såpass viktig informasjon, må du sørge for at hovedpassordet du bruker er unikt og sterkt, og ikke bare vanskelig for andre å gjette, men enkelt for deg å huske.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

De beste passordhvelvene i 2017:	https://www.pcmag.com/article2/0,2817,2407168,00.asp
Passordsetninger:	https://securingthehuman.sans.org/ouch/2017#april2017
Totrinns pålogging:	https://www.securingthehuman.org/ouch/2015#september2015
Lock Down Your Login:	https://www.lockdownyourlogin.org/
SANS Dagens sikkerhetstips:	https://www.sans.org/tip-of-the-day

Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS