OUCH! | Oktober 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Passordhåndterere

Oversikt

Et av de viktigste grepene du kan ta for å beskytte deg selv på nettet, er å bruke et sterkt, unikt passord for hver eneste brukerkonto. Dessverre er det slik at de fleste av oss har alt for mange brukerkontoer til å huske alle passordene. En enkel løsning er å bruke en passordhåndterer, også kalt passordhvelv. Slike programmer er designet for å lagre innloggingsinformasjonen din på en sikker måte. I tillegg kan de gjøre det mye enklere for deg å logge deg inn på nettsider, mobil-apper, og annen programvare.

Gjesteredaktør

Lenny Zeltser fokuserer på å beskytte kunders IT-operasjoner ved NCR Corp, og trener opp sikkerhetsprofesjonelle ved SANS Instituttet. Lenny er aktiv på Twitter som **@lennyzeltser**, og publiserer artikler på **zeltser.com**.

Hvordan en passordhåndterer fungerer

En passordhåndterer fungerer som en digital safe; den lagrer brukernavn, passord, og annen sensitiv informasjon på en sikker måte. Når en nettside krever at du logger inn på brukerkontoen din, kan passordhåndtereren automatisk hente passordet ditt og logge deg inn på nettsiden på en sikker måte. Dette gjør det enkelt å ha hundrevis av unike, sterke passord, siden du ikke trenger å huske dem.

Passordhåndterere lagrer informasjonen din i en database, noen ganger kalt et hvelv. Passordhåndtereren krypterer hvelvets innhold, og beskytter det med et hoved-passord som bare du kjenner til. Når du har behov for å få tak i innloggingsinformasjon, for eksempel til en nettbank eller epostkonto, behøver du bare å taste hoved-passordet inn i passordhåndtereren for å låse opp hvelvet.

Noen passordhåndterere lagrer hvelvet ditt på din lokale maskin eller smart-telefon, mens andre lagrer det på et nettsted som vedlikeholdes av firmaet som lagde passordhåndtereren. I tillegg har de fleste passordhåndterere mulighet til å automatisk synkronisere hvelvets innhold med andre enheter som du har autorisert. På denne måten blir det slik at når du endrer et passord fra laptopen din, blir endringene automatisk synkronisert til telefonen din, nettbrettet ditt, og eventuelle andre datamaskiner du bruker. Uansett om hvelvet er lagret på nettet eller på en maskin, må du installere den aktuelle passordhåndtereren på alle datamaskiner og enheter du akter å bruke den på.

Passordhåndterere

Når du tar i bruk en passordhåndterer for første gang, må du skrive inn eller importere all innloggingsinformasjonen din manuelt. Etter dette kan passordhåndtereren automatisk oppdage når du oppretter en ny brukerkonto på nettet, eller endrer passordet på en eksisterende brukerkonto, og oppdatere hvelvet deretter. Dette er mulig fordi de fleste passordhåndterere fungerer hånd i hånd med nettleseren din. På grunn av dette kan du også logge inn på nettsider hvor du har brukerkontoer automatisk.

Passordhåndterere er en enkel metode for å lagre å bruke alle de forskjellige passordene dine på en sikker måte.

Passordhåndterere er designer for å lagre dine sensitive data på en sikker måte. Det er imidlertid svært viktig at hoved-passordet du bruker for å beskytte innholdet i hvelvet er sterkt, og veldig vanskelig for andre å gjette. Vi anbefaler faktisk at du bruker en hel setning som hoved-passord, som er en av de sterkeste passord-typene som finnes. Hvis passordhåndtereren din støtter totrinns pålogging, bruk det for hoved-passordet. Til slutt må du være helt sikker på at du ikke bruker hoved-passordet med noe annet system eller noen annen brukerkonto. På denne måten blir det slik at selv om hackere får tak i hvelvet ditt, vil de ikke klare å gjette passordet som gir dem tilgang til innholdet. Til slutt må du passe på at du kan huske hoved-passordet. Hvis du glemmer det, mister du også tilgangen til alle de andre passordene dine.

Å velge en passordhåndterer

Det er mange passordhåndterere å velge mellom, både gratis og kommersielle. Når du skal velge den som er best for deg, må du tenke over følgende:

- Bekreft at passordhåndtereren vil fungere på alle systemer og mobile enheter hvor du vil ha behov for tilgang til hvelvet ditt. Det burde også være enkelt å holde hvelvets innhold synkronisert på de forskjellige enhetene.
- Bruk bare godt kjente og pålitelige passordhåndterere. Vær på vakt rundt produkter som ikke har vært tilgjengelig særlig lenge, og har liten grad av tilbakemeldinger fra forbrukerne. Akkurat som med falske antivirusprogrammer, kan kriminelle lage falske passordhåndterere for å stjele informasjonen din.
- Det burde være enkelt for deg å bruke passordhåndtereren din. Hvis løsningen er for kompleks til at den er forståelig, finn et alternativ som passer deg bedre.
- Vær sikker på at passordhåndtereren du velger får oppdateringer og patcher jevnlig, og vær sikker på at du alltid har den nyeste versjonen.

Passordhåndterere

- Passordhåndtereren burde gjøre det lett for deg å velge sterke passord for de forskjellige brukerkontoene dine, inkludert muligheten til å generere sterke passord for deg, og vise deg styrkegraden på passord du har valgt.
- Passordhåndtereren burde kunne la deg lagre andre sensitive data, slik som svar på sikkerhetsspørsmål, kredittkort-nummer, og lignende.
- Vær på vakt mot passordhåndterere som bruker lite kjente krypteringsmetoder, istedenfor å kryptere hvelvet ditt med metoder som holder industristandard. Hvis leverandøren hevder å ha utviklet sine egne krypteringsløsninger, burde du velge en annen leverandør.
- Unngå enhver passordhåndterer som hevder å kunne gjenopprette hoved-passordet ditt for deg. Det betyr at de har lagret hoved-passordet ditt i klartekst, noe som innebærer mye mer risiko for deg.

Passordhåndterere er en sterk løsning for å lagre alle passord og sensitiv data på en sikker måte. Men siden de beskytter mye viktig informasjon, er det like viktig at du bruker et hoved-passord som er vanskelig å gjette for angripere, og 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 http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på https://norsis.no.

Ressurser

Passordsetninger:	http://www.securingthehuman.org/ouch/2015#april2015
Totrinns pålogging:	https://www.securingthehuman.org/ouch/2015#september2015
Topp fem passordhåndterere:	http://lifehacker.com/5529133/five-best-password-managers
SANS Dagens sikkerhetstips:	http://www.sans.org/tip_of_the_day.php

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Oversatt av: Mats Authen