OUCH! | April 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Passordsetninger
- Sikker bruk av passordsetninger
- Ressurser

Passordsetninger

Bakgrunn

Passord er noe vi bruker daglig, fra e-post og nettbank, til kjøp av varer eller bruk av smarttelefon. Passord er imidlertid også et av dine svakeste punkt; dersom noen får vite eller klarer å gjette passordet ditt kan de få tilgang til dine brukerkontoer som om de var deg, og potensielt overføre penger, lese konfidensielle e-poster, eller stjele identiteten din. Det er derfor sterke passord er essensielle for å kunne beskytte seg selv. Passord kan imidlertid være forvirrende, og vanskelige å huske og skrive. I dette nyhetsbrevet kan du lære deg hvordan du lager sterke passord som er enkle å både huske og skrive- kjent som passordsetninger.

Gjesteredaktør

My-Ngoc Nguyen (uttales Me-Nop Wynn) er en sertifisert SANS-instruktør, og CEO/Principal Consultant for Secured IT Solutions. Hun bringer med seg ekspertise med toppsertifisering og mer enn 14 år med utvikling, modning, og styring av cybersikkerhetsprogrammer for diverse industrier og sektorer. Twitter: **@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Passordsetninger

Utfordringen vi står ovenfor er at angripere i cyberdomenet har utviklet sofistikerte og effektive metoder for å brute-force (automatisk gjetning) av passord. Dette betyr at folk med onde hensikter kan kompromittere passordene dine hvis de er svake og enkle å gjette. Ett viktig steg for å beskytte deg selv, er ved å bruke sterke passord. Dette ble typisk gjort ved å lage komplekse passord, men disse kan bli vanskelig å huske, forvirrende og vanskelig å stave. Istedenfor anbefaler vi at du bruker passordsetninger, en serie av forskjellige ord eller en setning. Jo flere tegn passordsetningene dine har, desto sterkere er de. Fordelen er at disse er mye enklere å huske og skrive, men fremdeles vanskelige for cyberangripere å hacke. Her er to forskjellige eksempler.

Oppretthold-Enkel-Fengsling
Tid for te kl 12:34

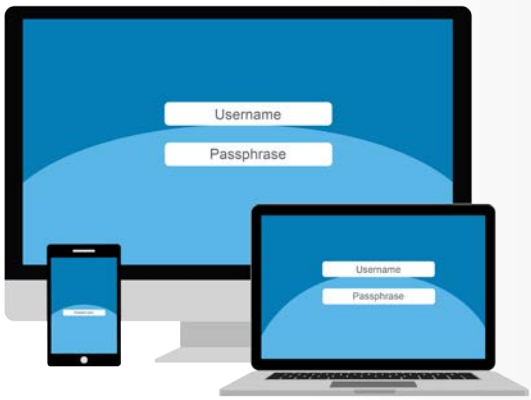
Disse passordsetningene er sterke ikke bare fordi at de er lange, men de bruker store forbokstaver og symboler (husk, mellomrom og punktum er symboler). Samtidig er passordsetningene enkle å huske og skrive. Du kan lage passordsetningene dine enda sterkere hvis du vil, ved å erstatte bokstaver med sifre eller symboler, som for eksempel erstatte bokstaven 'a' med et '@' symbol, eller bokstaven 'o' med tallet null. Dersom et nettsted eller et program har begrenset med antall

Passordsetninger

med tegn du kan bruke i et passord, så bruk det maksimale antallet av tegn som er tillatt.

Sikker bruk av passordsetninger

Du må også være forsiktig med hvordan du bruker passordsetninger. Det å bruke passordsetninger hjelper ikke hvis folk med onde hensikter enkelt kan stjele eller kopiere dem.



Passordsetninger er en enklere metode for å lage og huske sterke passord.

1. Bruk forskjellige passordsetninger for alle brukerkontoer og enheter du har. Bruk for eksempel aldri samme passordsetning for jobb eller bank som du bruker til personlige ting som Facebook, YouTube eller Twitter. Selv om en av brukerkontoene dine skulle komme til å bli hacket, vil de andre da forbli trygge. Dersom du har for mange passordsetninger til at du kan huske alle (hvilket er veldig vanlig), burde du vurdere å bruke et passord-håndteringsprogram. Dette er et spesielt type program som lagrer alle passordsetningene for deg på en sikker måte. Dermed er de eneste passordsetningene du trenger å huske de som er til datamaskin og mobile enheter, samt til passord-håndteringsprogrammet selv.
2. Del aldri passordsetninger, eller strategien du bruker for å lage dem med noen, hverken kolleger, sjef, venner eller andre. Husk at en passordsetning er en hemmelighet, dersom noen andre kjenner til den er den ikke lenger sikker. Dersom du deler en passordsetning med noen ved et uhell, eller mistenker at den kan ha blitt kompromittert eller stjålet, må du endre den så fort som mulig. Det eneste unntaket er dersom du er nødt til å dele en personlig passordsetning med et pålitelig familiemedlem i en nødsituasjon. En mulig tilnærming er å skrive ned personlige passordsetninger (sørg for at de ikke er jobbrelatert), og lagre dem på et sikkert sted, og fortell hvor dette er kun til familiemedlemmer du stoler veldig på. Dermed kan dine nærmeste hjelpe deg med tilgang til dine kritiske kontoer dersom noe skulle skje.
3. Ikke bruk offentlige datamaskiner, slik som de du finner på hoteller eller kafeer til å logge inn på brukerkontoene dine. Siden hvem som helst kan bruke disse datamaskinene, kan de være infisert med virus, og fanger kanskje opp alt som skrives på dem. Logg deg kun inn på brukerkontoer på pålitelige datamaskiner eller pålitelige mobile enheter.
4. Vær forsiktig med nettsider som ber deg om å svare på personlige spørsmål. Disse spørsmålene brukes om du glemmer passordsetningen din og trenger å tilbakestille den. Problemet er at svarene på disse spørsmålene ofte kan finnes på nettet, for eksempel på Facebook-siden din. Sørg for at du kun bruker informasjon som ikke er offentlig tilgjengelig, eller bruk fiktiv informasjon som du har funnet på dersom du må legge inn slike svar. Klarer du ikke å huske alle disse

Passordsetninger

sikkerhetsspørsmålene og svarene? Velg deg et tema, for eksempel en filmfigur, og baser svarene på den figuren. En annen mulighet er nok engang å bruke et passord-håndteringsprogram. De fleste av dem gjør det mulig for deg å også lagre tilleggsinformasjon som sikkerhetsspørsmål på en sikker måte.

5. Mange nettsider og tjenester som må logges inn på tilbyr noe kalt to-trinns bekreftelse, også kjent som to-trinns pålogging. Da trenger du mer enn bare passordsetningen for å logge inn, for eksempel en engangskode som sendes til smarttelefonen din. Dette alternativet er langt sikrere enn kun passordsetningen i seg selv. Bruk alltid denne forbedrede sikkerhetsmekanismen for innlogging når det er tilgjengelig.
6. Mobile enheter krever ofte en påloggingskode, eller et mønster for å beskytte tilgangen til dem. Husk at dette ikke er noe mer enn et annet passord. Jo lengre denne koden er, jo sikrere er den. Mange mobile enheter lar deg også bruke fullstendige passordsetninger istedenfor, eller biometrisk innlogging, som for eksempel scanning av fingeravtrykket ditt.
7. Dersom du har en brukerkonto du ikke lenger bruker, burde du deaktivere, slette eller stenge den.

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

Passordhåndterere:	https://securingthehuman.sans.org/ouch/2015#october2015
Totrinns pålogging:	https://securingthehuman.sans.org/ouch/2015#september2015
Lock Down Your Login:	https://lockdownyourlogin.com
SANS SEC301 - 5-dagers kurs i grunnleggende cybersikkerhet:	https://sans.org/sec301

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

