OUCH! | April 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Passordsetninger

Bakgrunn

Passord er noe du bruker nesten hver dag, fra å aksessere e-post og nettbanken til å kjøpe varer og aksessere smarttelefonen. Passord er også ett av de svakeste leddene i sikkerheten, hvis noen finner ut passordet ditt kan de stjele identiteten din, overføre penger eller få tak i personlig informasjon om deg. Sterke passord er nødvendig for å beskytte deg selv. I dette nyhetsbrevet vil vi lære deg hvordan du kan lage sterke passord som er lette å huske, for å oppnå dette bruker vi passordsetninger.

Gjesteredaktør

Guy Bruneau er seniorkonsulent hos IPSS Inc., SANS instruktør og ISC handler. Guy holder SANS GSE og har fullført SANS Cyber Guardian programmet. Du kan følge Guy på Twitter (**@GuyBruneau**) og på **handlers.sans.org/gbruneau**.

Passordsetninger

En utfordring med passord er at angripere har utviklet avanserte metoder for å gjette eller "brute force" passordet. De blir også hele tiden bedre på det. Hvis passordet ditt er svakt eller enkelt å gjette, så kan angripere kompromittere passordet. Et viktig steg for å beskytte deg selv er å bruke sterke passord. Jo flere bokstaver passordet ditt har, desto sterkere er det og dermed vanskeligere å knekke for en angriper. Problemet er at lange og komplekse passord kan være vanskelig å huske. Derfor er det anbefalt at du bruker passordsetninger, dette er setninger som er lette å huske, men vanskelige å knekke. Her er et eksempel:

Hvor er kong Julian?

Det som gjør dette passordet sterkt er at det er 20 tegn langt og det bruker små bokstaver, store bokstaver og spesialtegn (mellomrom og tegnsetting regnes som spesialsymboler). Du kan lage passordsetningen enda sterkere hvis du erstatter bokstaver med tall eller symboler, som å erstatte 'a' med '@' eller å erstatte bokstaven 'o' med tallet '0'. Hvis nettsiden eller programmet begrenser antall tegn tillatt, bruk så mange tegn som mulig.

Passordsetninger

Sikker bruk av passordsetninger

Du må også være forsiktig med hvordan du bruker passordsetninger. Det hjelper ikke å bruke en passordsetning hvis en angriper kan stjele eller kopiere det.

Passordsetninger er en av de mest effektive stegene du kan ta for å beskytte din identitet og din informasjon.

1. Sørg for at du bruker forskjellig passordsetning for hver konto eller enhet du har. For eksempel, ikke bruk samme passordsetning for arbeidskonto og bankkonto, som passordet du bruker på andre personlige kontoer, som Facebook, YouTube og Twitter. Dette innebærer at, hvis en av kontoene dine blir kompromittert, så er alle de andre kontoene trygge. Hvis du har for mange passord du må huske på (dette er ganske vanlig), kan du bruke en passordhåndterer; dette er et spesielt program som sikkert lagrer passordene for deg. Passordene kan åpnes via ett hovedpassord, derfor trenger du bare å huske hovedpassordet og passordet til datamaskinen.

2. Aldri del passordet eller strategien du bruker for å lage dem med noen andre, inkludert medarbeidere og venner. Husk at passordet er en hemmelighet, hvis noen andre har tilgang til det er det ikke lenger sikkert. Hvis du ved et uhell deler passordet med noen andre eller hvis du tror passordet har blitt kompromittert, sørg for at du bytter det umiddelbart.

3. Akkurat som med passord, sørg for at du unngår passordsetninger som er lett å gjette eller ofte brukt. Kjente sitater fra filmer, bøker, taler osv. burde ikke brukes som passord.

4. Unngå å bruke offentlige maskiner, som de på hotell eller bibliotek, til å logge inn på sensitive kontoer som arbeidskonto eller nettbanken. Siden hvem som helst kan bruke disse maskinene kan de bli infisert med ondsinnet kode som fanger alle tastetrykkene. Ikke logg inn på sensitive kontoer med mindre du bruker en maskin eller mobil enhet du stoler på.

5. Vær forsiktig med nettsider som bruker sikkerhetsspørsmål. Disse spørsmålene blir brukt hvis du glemmer passordet og trenger å resette det. Problemet er at man kan ofte finne svaret til disse spørsmålene på Internett,

Passordsetninger

eller til og med på Facebook-siden din. Sørg for at svaret du bruker inneholder informasjon som ikke er offentlig tilgjengelig eller at det inneholder informasjon du har funnet på. Noen passordhåndterere kan også hjelpe deg med dette, da flere av disse programmene kan lagre ekstra informasjon.

6. Mange tjenester på nett støtter noe som kalles to-steg verifisering, også kalt to-steg autentisering. Med dette aktivert trenger du mer enn bare passord for å logge på, som for eksempel en kode sent til smarttelefonen. Dette gir betydelig bedre sikkerhet enn bare et passord alene, hvis mulig ta i bruk to-steg verifisering.

7. Mobile enheter krever ofte en PIN før du kan aksessere dem. PIN er bare et annet eksempel på et passord, jo lengre PIN er desto sikrere er det. Mange mobile enheter gir deg også muligheten til å bruke et ekte passord.

8. Til slutt, hvis du ikke lenger bruker kontoen, sørg for at du avslutter, sletter eller deaktiverer den.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos 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 www.norsis.no.

Ressurser

To-steg verifisering:	http://www.securingthehuman.org/ouch/2013#august2013
Passordhåndterere:	http://www.securingthehuman.org/ouch/2013#october2013
Sosial manipulering:	http://www.securingthehuman.org/ouch/2014#november2014
Vanlige sikkerhetsbegrep:	http://www.securingthehuman.org/resources/security-terms
Veiledning om passord:	https://norsis.no/2012/06/passordvett/

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis