OUCH!

SANS SECURITY AWARENESS

Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Passord gjort enkelt

Oversikt

Du blir ofte fortalt at passord er nøkkelen til å beskytte brukerkontoene dine (og det stemmer), men du fortelles sjelden hvordan du lager sikre passord, eller hvordan du holder styr på dem. Under går vi gjennom tre enkle steg som gjør det enkelt å lage passord, sikre brukerkontoer, og beskytte fremtiden din.

Passordsetninger

Tiden for vilt komplekse passord er over. De passordene var vanskelige å huske, vanskelige å skrive, og med dagens superraske datamaskiner kan de også være enkle for cyberkriminelle å knekke. Nøkkelen til sterke passord er lengden, jo flere tegn de har jo bedre. Disse kalles passordsetninger, en type passord som består av en kort setning eller en tilfeldig sammensetning av ord. Her er to eksempler:

> ***Tid for sterk kaffe!***
> ***tapt-snegle-kravler-strand***

Begge disse er sterke og har minst 20 tegn i lengde. De er enkle å huske og enkle å skrive, men vanskelige å knekke. Fra tid til annen vil du havne i situasjoner hvor det kreves symboler, tall, store bokstaver og tilsvarende i passordene, og det går fint å legge til det i setningen. Men husk at det er lengden som er det viktigste.

Passordhvelv

Du trenger et unikt passord for hver brukerkonto. Dersom du bruker det samme passordet på flere forskjellige steder utsetter du deg selv for stor risiko. Alt en cyberkriminell trenger å gjøre er å hacke en nettside du bruker, stjele alle passordene, inkludert ditt, for så å bruke passordet ditt til å logge inn på alle de andre brukerkontoene dine som om de var deg. Det skjer mye oftere enn du kanskje har innsett. Om du ikke tror oss kan du sjekke https://haveibeenpwn.com. Der får du se hvilke av nettsidene du bruker som har blitt hacket opp gjennom tidene, og hvor passordet ditt kanskje er på avveie. Så hva bør du gjøre? Bruk et passordhvelv.

Passordhvelv, også kjent som passordhåndteringsprogrammer, eller password managers på engelsk, er et spesielt program som lagrer alle passordene dine trygt i et kryptert hvelv. Du trenger kun å huske ett passord, som er hovedpassordet til passordhvelvet. Passordhvelvet henter automatisk passord når du trenger dem, og logger inn på nettsider og apper for deg. De har også andre

funksjonaliteter, som å lagre svarene på sikkerhetsspørsmål, advare deg når du gjenbruker passord, en generator som lager sterke passord for deg, og mye annet. Mange passordhvelv synkroniserer seg også på tvers av det du måtte bruke av mobiler og PC-er, så uansett hva du bruker har du enkel, sikker tilgang til passordene dine.

Til sist, husk å skrive ned hovedpassordet til passordhvelvet ditt og oppbevar det på et trygt sted hjemme. Noen passordhvelv lar deg til og med skrive ut et gjenopprettingssett. På den måten har du en sikkerhetskopi dersom du skulle glemme hovedpassordet. Eller, dersom du blir syk eller utsatt for en nødssituasjon kan nærmeste pårørende hente ut nødvendig informasjon på dine vegne.

2-trinns bekreftelse

2-trinns bekreftelse (også kjent som totrinns pålogging, tofaktor autentisering og multifaktor autentisering, for å nevne noen) gir deg et ekstra lag med sikkerhet. Med 2-trinns bekreftelse kreves det to ting når du skal logge inn på en ny side: Passordet ditt, og en numerisk kode som genereres på mobilen din, eller som du får tilsendt på mobilen. Dette sørger for at selv om en cyberkriminell får tak i passordet ditt, så kan de fortsatt ikke komme inn på brukerkontoen din. 2-trinns bekreftelse er enkelt å sette opp, og du trenger som regel kun å bruke det én gang, når du logger inn for første gang med en ny enhet. Alltid skru dette på der det er mulig, spesielt for de viktigste kontoene dine, som e-post. Offentlige tjenester er som oftest sikret med BankID, som er en annen form for 2-trinns autentisering. Dersom du bruker et passordhvelv anbefaler vi på det sterkeste at du beskytter det med et sterkt passord, OG 2-trinns bekreftelse.

Det høres kanskje rart ut, men disse tre stegene gjør svært mye for å beskytte jobben din, omdømmet ditt, og den finansielle fremtiden din.

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.

Gjesteredaktør

Justin Henderson *(@SecurityMapper) er medgrunnlegger av H & A Security Solutions, sertifisert SANS-instruktør og forfatter av SANS-kursene for Cyber Defense og SIEM-systemer. Han elsker alt som har med cyberforsvar og gjøre, og har jobbet som konsulent i 15 år.*

Ressurser

Nettvett.no: Sikker pålogging:	https://nettvett.no/sikker-palogging/
Have I Been Pwned:	https://haveibeenpwned.com/
Nettsted om 2-trinns pålogging:	https://twofactorauth.org/
Plakat: You Are a Target:	https://www.sans.org/u/OGi