Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Gör lösenord enkelt

Inledning

Du får ofta höra att dina lösenord är nyckeln till att skydda dina konton (vilket är sant!), men sällan får du ett enkelt sätt att säkert skapa och hantera alla dina lösenord. Nedan beskriver vi tre enkla steg för att förenkla hanteringen av lösenord och konton för att skydda din framtid.

Lösenordsfraser

Dagarna med galna och komplexa lösenord är över. Dessa lösenord är svåra att komma ihåg, svåra att skriva, och med dagens supersnabba datorer kan det vara lätt för en cyberangripare att knäcka. Nyckeln till bra lösenord är att göra dem långa, ju fler tecken du har desto bättre. Dessa kallas lösenordsfraser, en typ av starkt lösenord som använder en kort mening eller slumpmässiga ord. Här är två exempel

Tid för starkt kaffe!
borttappad-snigel-krälar-strand

Båda lösenorden är starka med över tjugo tecken, lätta att komma ihåg och enkla att skriva men svåra att knäcka. Du kommer att träffa på webbplatser eller situationer som kräver att du lägger till symboler, siffror eller versaler till ditt lösenord, vilket är bra. Men kom ihåg att det är längden som är viktigast.

Lösenordshanterare

Du behöver ett unikt lösenord för varje konto. Om du återanvänder samma lösenord för flera konton sätter du dig i stor fara. Allt en cyberangripare behöver göra är att hacka en webbplats du använder, stjäla alla lösenord inklusive ditt, sedan använda ditt lösenord för att logga in som dig på alla dina andra konton. Det händer mycket oftare än du tror. Tror du inte det är sant? Kolla in webbplatsen www.haveibeenpwned.com för att se vilka webbplatser du använder som hackats och om dina lösenord potentiellt har kompromitterats. Så vad ska du göra? Använd en lösenordshanterare.

Dessa är speciella datorprogram som säkert lagrar alla dina lösenord i ett krypterad valv. Du behöver bara komma ihåg ett lösenord, det till lösenordshanteraren. Lösenordshanteraren hämtar dina lösenord och loggar in dig automatiskt på webbplatser när det behövs. De har också andra funktioner som att lagra dina svar på hemliga frågor, varna dig när du återanvänder lösenord,

lösenordsgenerator som säkerställer att du använder starka lösenord och många andra funktioner. De flesta lösenordshanterare synkroniseras också säkert med nästan vilken dator eller enhet som helst, så oavsett vilket system du använder har du enkel och säker tillgång till alla dina lösenord.

Slutligen, var noga med att skriva ner lösenordet till din lösenordshanterare och lagra det på ett säkert ställe hemma. Vissa lösenordshanterare kan även skapa en återställningskopia. Så om du glömmer lösenordet till lösenordshanteraren har du en säkerhetskopia. Eller om du blir sjuk eller befinner dig i en nödsituation, kan din partner eller betrodd familjemedlem hämta informationen åt dig.

Tvåstegs verifiering

Tvåstegs verifiering (ofta kallad tvåfaktorautentisering eller multifaktorautentisering) lägger till ytterligare ett säkerhetslager. Det kräver att du har minst två saker när du loggar in på dina konton, ditt lösenord och en numerisk kod som genereras av eller skickas till din telefon. Denna process säkerställer att även om en cyberangripare har ditt lösenord kan de fortfarande inte komma åt dina konton. Tvåstegsverifiering är enkelt att aktivera och du behöver vanligtvis bara använda den en gång när du loggar in från en ny dator eller enhet. Aktivera detta där det är möjligt, särskilt för dina viktigaste konton, t.ex. bank- eller pensionskonton eller till din e-post. Om du använder en lösenordshanterare rekommenderar vi starkt att du skyddar den med ett starkt lösenords OCH tvåstegsverifiering.

Det kan låta dumt, men du kommer långt med hjälp av dessa tre enkla steg för att skydda ditt jobb, rykte och ekonomiska framtid.

Gästredaktör

Justin Henderson *(@SecurityMapper) är en av grundare till H & A Security Solutions, en Certifierad SANS Institute Instruktör och författare till SANS Cyber Defense och SIEM-kurser. Han älskar cyberförsvar och har varit konsult i femton år.*

Källor

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https://pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi