Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA NUMMER…

Lösenordsfraser

Bakgrund

Lösenord är något du använder nästan varje dag, från att komma åt din e-post och bank på nätet, för att köpa varor eller logga in på din smartphone. Men lösenorden är också en av dina svagaste punkter, om någon lär sig ditt lösenord kan de stjäla din identitet, överföra dina pengar eller få tillgång till personuppgifter. Starka lösenord är avgörande för att skydda dig själv. I detta nyhetsbrev får du lära dig att skapa starka lösenord som är lätta att komma ihåg genom att använda en typ av lösenord som kallas lösenordsfraser.

Gästredaktör

Guy Bruneau är en senior säkerhetskonsult med IPSS Inc., en SANS instruktör och ISC handledare. Guy har SANS GSE och avslutade SANS Cyber Guardian programmet. Du kan följa Guy på Twitter **@GuyBruneau** och **handlers.sans.org/gbruneau**.

Lösenordsfraser

Utmaningen vi alla står inför är att cyber angripare har utvecklat sofistikerade metoder för att gissa, eller använda “brute force” för att knäcka lösenord, och de är ständigt bli bättre på det. Detta innebär att de kan äventyra dina lösenord om de är svaga eller lätt att gissa. Ett viktigt steg för att skydda dig själv är att använda starka lösenord. Ju fler tecken lösenordet har, desto starkare är det och desto svårare för en angripare att gissa. Men länge och komplexa lösenord kan vara svåra att komma ihåg. Så istället rekommenderar vi att du använder lösenordsfraser, dessa är enkla fraser eller meningar som är lätta att komma ihåg, men svårt att hacka. Här är ett exempel.

Var är kung Julian?

Vad som gör detta lösenord så starkt är inte bara att det är 21 tecken lång, men det använder versaler och symboler (kom ihåg, mellanslag och skiljetecken är symboler). Du kan göra din lösenordsfras ännu starkare om du byter bokstäver med siffror eller symboler, såsom byte av bokstaven “a” med “@” symbolen eller bokstaven “o” med siffran noll. Om en webbplats eller ett program begränsar antalet tecken som du kan använda i ett lösenord, använd maximalt antal tillåtna tecken.

Lösenordsfraser

Använd lösenordsfraser säkert

Du måste också vara försiktig med hur du använder lösenordsfraser. Användning av lösenordsfraser kommer inte att hjälpa om skurkarna lätt kan stjäla eller kopiera den.

Att använda lösenordsfraser är en av de mest effektiva åtgärder du kan vidta för att skydda din identitet och information.

1. Se till att använda en annan lösenordsfras för varje konto eller enhet du har. Använd till exempel aldrig samma lösenord för ditt arbete eller bankkonto som du använder för dina personliga konton, som Facebook, YouTube eller Twitter. På detta sätt, om ett av dina konton blir hackat, är de andra kontona fortfarande säkra. Om du har för många lösenfraser att komma ihåg (vilket är mycket vanligt), överväg att använda en lösenordshanterare. Detta är ett speciellt program som säkert lagrar alla dina lösenordsfraser för dig. På så sätt är de enda lösenfraser du behöver komma ihåg de till datorn och lösenordshanteraren.

2. Dela aldrig en lösenordsfras eller din strategi för att skapa dem med någon annan, inklusive medarbetare. Kom ihåg att en lösenfras är en hemlighet; om någon annan känner till ditt lösenord är det inte längre säkert. Om du råkar dela lösenordsfras med någon annan, eller tror att din lösenordsfras kan ha äventyrats eller stulits, se till att ändra det omedelbart.

3. Precis som lösenord, undvik lätta att gissa eller ofta använda lösenordsfraser. Till exempel, frasen “fyra tjog och sju år sedan” är inte en bra lösenordsfras eftersom det är så välkänd.

4. Använd inte offentliga datorer, såsom de på hotell eller bibliotek, för att logga in till ditt arbete eller bankkonto. Eftersom vem som helst kan använda dessa datorer, kan de vara infekterade med skadlig kod som fångar alla dina tangenttryckningar. Endast logga in på ditt arbete eller bankkonton på betrodda datorer eller mobila enheter.

5. Var försiktig med webbplatser som kräver att du svara personliga frågor. Dessa frågor används om du glömmer ditt lösenord och måste återställa det. Problemet är svaren på dessa frågor kan ofta hittas på Internet, eller till och med på din Facebook-sida. Se till om du svarar på personliga frågor att du endast använder information som inte är allmänt tillgänglig eller fiktiv information som du har gjort upp. Lösenordhanterare kan hjälpa till med detta eftersom många tillåter att du lagrar denna ytterligare information.

Lösenordsfraser

6. Många online-konton erbjuder något som kallas tvåfaktorsautentisering, även känd som tvåstegsverifiering. Det är där du behöver mer än bara din lösenordsfras för att logga in, till exempel en kod som skickas till din smartphone. Detta alternativ är mycket säkrare än bara ett lösenord av sig själv. När det är möjligt, alltid använda dessa starkare metoder autentisering.

7. Mobila enheter kräver ofta en PIN-kod för att skydda tillgången till dem. Kom ihåg en PIN är inget annat än ett annat lösenord. Ju längre din PIN-kod är, desto säkrare är det. På många mobila enheter kan du ändra din PIN-kod till en faktisk lösenordsfras.

8. Slutligen, om du inte längre använder ett konto, se till att stänga, ta bort eller inaktivera det.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhetsbranchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

Tvåstegsverifiering:	http://www.securingthehuman.org/ouch/2013#august2013
Lösenordshanterare:	http://www.securingthehuman.org/ouch/2013#october2013
Social Ingenjörskonst:	http://www.securingthehuman.org/ouch/2014#november2014
Vanliga Säkerhets Termer:	http://www.securingthehuman.org/resources/security-terms

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson