Lösenord

De flesta av oss är ganska dåliga på att hantera våra lösenord. Men genom några enkla åtgärder kan du minimera risken för att någon ska komma över dem – och därmed också ditt digitala liv.

I takt med att vi lever en allt större del av våra liv på nätet, och gör oss beroende av program och tjänster, ökar antalet lösenord vi måste hålla koll på.

Du kanske redan har en strategi? Brukar du använda ”123456”? Dotterns namn tillsammans med födelseår? Eller är du en av dem som ser till att du kan memorera ett långt lösenord som du sedan använder till alla dina inloggningar?

Sluta! Exemplen du just läst är precis sådana som ökar risken för att någon ska kunna räkna ut ditt lösenord.

Lösenordsregler

När det gäller lösenord finns ett par enkla regler att förhålla sig till. Följer du dem minskar du avsevärt risken för att någon ska komma över ditt lösenord. För helt säker kan man aldrig vara, det handlar om att minimera faran.

Använd unika lösenord

Viktigast av allt är att du har unika lösenord. Alltså att du inte använder samma till alla dina inloggningar, utan har ett specifikt för varje tjänst.

Man ser ofta olämpliga lösenord som ”123456” eller ”password”.

Att databaser med lösenord hackas är dessvärre vanligare än många tror. Internationella företag som Adobe, Sony och Facebook är bara några av dem som drabbats av hackerattacker som inneburit att användaruppgifter läckt ut. Har du då samma lösenord till flera olika tjänster ökar risken för att flera konton blir kapade, eftersom den som kommit över ditt lösenord kan testa det på många tjänster.

Undvik vanliga lösenord

Förutom att ha unika lösenord ska du undvika vanliga lösenord. Använd inte enstaka ord, såsom personnamn, platser eller tangentbordskombinationer som "qwerty" (bokstäver i raden överst på tangentbordet). Detsamma gäller kända citat. Allt är exempel på så kallat "vanligt förekommande lösenord", vilket innebär att de inte är säkra.

Listor över vanligt förekommande lösenord sprids ofta på nätet och används vid så kallade *ordlisteattacker*, där angriparen systematiskt testar tänkbara lösenord för att komma över ditt konto. Så länge ditt lösenord inte finns med bland de vanligaste 10 000, är du relativt säker från ordlisteattacker. Ett starkt lösenord är ett som ingen annan har tänkt på.

Långa lösenord

Du ska också skapa långa lösenord. En metod som angripare kan använda för att knäcka lösenord kallas ”brute force” och innebär att de använder program som är skapade för att gå igenom olika kombinationer av bokstäver, siffror och specialtecken. Vid en sån attack kommer lösenordet till slut att knäckas, men ju längre lösenord du har desto längre tid tar det.

Grundrekommendationen är att lösenordet ska innehålla *minst tolv tecken*, men det får gärna vara ännu längre. Lägger du även in specialtecken ökar säkerheten ytterligare.

Lösenordstecken
Använd både stora och små bokstäver, minst en siffra och minst ett tecken i dina lösenord.

Använd fraser
Ett bra sätt för att skapa långa lösenord är att använda lösenordsfraser, alltså kombinationer av ord. En lösenordsfras är betydligt lättare att komma ihåg än en lång följd av olika slumpmässiga bokstäver, siffror och specialtecken.

En lösenordfras bör innehålla över fyra ord för att bli lång nog och orden ska vara slumpvis utvalda. Vanliga uttryck eller sammanhängande fraser minskar säkerheten drastiskt.

Väljer du fyra slumpvisa ord från SAOL (Svenska akademins ordlista) och sätter i hop dem i en fras finns hela 252 047 376 000 000 000 000 olika lösenordskombinationer.

Var inte personlig
Använd aldrig lösenord som kan kopplas till dig som person. Barn, födelseår och namn på föräldrar är alla exempel på lösenord med en förhöjd risk att knäckas.

Tänk också på att olika tjänster är olika viktiga att skydda. Det absolut viktigaste är din *e-post*. Det är via mejlkontot vi kan byta lösenord på olika tjänster eller begära ett nytt om vi har glömt bort det ursprungliga. Kapar någon ditt mejlkonto kan de byta ut lösenord på alla dina tjänster och faktiskt låsa dig ute från hela din digitala identitet.

Viktigast efter mejlkontot är dina *sociala medier*. Skulle någon ta över dina sociala medier gör de snabbt skada, antingen genom att personen försöker lura dina vänner på pengar eller genom att använda ditt konto för att misskreditera dig eller förstöra dina sociala relationer.

Tvåfaktorsautentisering kan användas på de tjänster som är viktigast att skydda. Den möjligheten finns på vissa webbplatser. Det innebär att det utöver ditt lösenord behövs ytterligare en kod eller annan faktor för att logga in.

Komma ihåg alla lösenord
Man brukar säga att om man kan komma ihåg lösenordet är det inget bra lösenord. Det finns dock smarta lösningar för att komma ihåg även krångliga lösenord.

När du ska skapa ett lösenord kan du först tänka dig en mening och sedan ta första bokstaven i varje ord samt lägga till ett tecken och en siffra. Om du t.ex. tänker ”Jag ska ta kaffe-paus klockan 12.30” kan lösenordet bli *Jstk-pk12.30!*

Ett annat sätt kan vara att i stället för att skriva minkattmisse skriva MinKattMISSE eller MinKattMisse. Lägg gärna till en siffra och ett tecken t.ex. *minKATT2%vit*.

Du kan också använda en *lösenordshanterare*. Det är ett program som både lagrar och hjälper dig att skapa säkra lösenord. När dina lösenord väl är sparade i hanteraren får du också hjälp att logga in på dina tjänster. I teorin behöver du alltså bara komma ihåg lösenordet till lösenordshanteraren. Ett sådant program är t.ex. *Lastpass* som finns för såväl dator som mobil/surfplatta. En rekommendation är dock att inte använda lösenordshanterare för de allra viktigaste lösenorden, t.ex. lösenordet för BankID.

För den som inte vill arbeta med en databaserad lösenordshanterare rekommenderar jag att skaffa en skrivbok med alfabetiskt register och där skriva in alla användarkonton och lösenord så att de är lätta att hitta vid behov. Ta gärna med den boken när du söker hjälp på PC/IT-hjälpen, men placera den annars på ett säkert ställe och inte intill datorn.

Internetstiftelsens råd inför lösenordshantering

• **Dela inte lösenord med någon annan** – Du vet aldrig om den andra personen hanterar ditt lösenord på ett säkert sätt. Dessutom kan din relation till personer förändras och då kan lösenordet användas för att göra dig skada.

• **Lösenordshanterare är att föredra** – Om du inte vill använda lösenordshanterare och i stället skriver ner dina lösenord på papper, låt det inte ligga framme utan förvara det som den värdehandling det är. Och kom ihåg: Det är inte bra att ha lösenord antecknat i klartext i en textfil på datorn eller mobilen.

• **Spara inte lösenord i webbläsaren** – Om någon använder din dator kan personen se alla dina lösenord.

• **Byt bara lösenord om du tror att det har blivit röjt –** Med ständiga lösenordsbyten ökar risken att man väljer lösenord som är lätta att komma ihåg, vilket för det mesta är samma sak som ett svagt lösenord.

• **Att logga in på olika tjänster via Facebook innebär en ökad risk** – Det är visserligen enkelt, men om någon kommer över ditt Facebook-konto kommer den personen också över möjligheten att logga in på alla de tjänster som du loggar in på via Facebook.

• **Undvik lösenordsgeneratorer** – På nätet finns sajter som erbjuder just sådana, men det är ofta oklart vem som driver dem och om de genererade lösenorden sparas.

• **Byt lösenord om du blir bestulen på en enhet** – Blir du av med din mobil, dator eller platta byt alla dina lösenord omgående!

• **Lämna aldrig ifrån dig koder –** Ditt mobila BankId, ditt bank- och kreditkort eller koden till din bankdosa är personliga. Banken skulle aldrig kontakta dig för att fråga om koder eller kortnummer eftersom deras system är byggda så att de kommer åt ditt konto ändå.

• **Logga aldrig in på en tjänst via någon annans enhet** – Det gäller både dina vänners datorer och mobiltelefoner eller till exempel om du besöker internetcaféer när du är ute och reser. Lånade enheter kan autospara dina lösenord och vara infekterade med skadlig kod.

Om du skulle vilja fördjupa dig ytterligare i begreppet lösenord så finns här exempel på några länkar:

https://internetstiftelsen.se/docs/Rapport_Losenord_for_alla.pdf

https://internetkunskap.se/article/5be2d5445c9ba10dc853bb0f/ar-det-inte-dags-att-bry-dig-lite-mer-om-dina-losenord

https://www.kjell.com/se/kunskap/hur-funkar-det/dator/dator-och-datasakerhet/sakra-losenord?ds_rl=1263038&ds_rl=1263038&gclid=CjwKCAjwt-L2BRA_EiwAacX32YSygn5YvKF314lw0vT-rQTHxnfGDnAM7ZLSBOj5ccrjmyFBRrLkpRoC0WsQAvD_BwE&gclsrc=aw.ds