Om konton och lösenord, och hur jag håller reda på dem

1. Inledning

Vi handlar, vi engagerar oss på sociala media, vi använder mail och vi spara bilder i molnet – i allt högre grad är vi aktiva på nätet, och detta ifrån olika typer av enheter.

Detta innebär att vi måste vara ”kända” på nätet, eller åtminstone ”igenkända” när vi ansluter oss till alla tjänster vi använder. Användaridentitet, lösenord, …. ***konton***! Hur många måste vi ha, och hur håller vi reda på dem?

Även en modest internetanvändare är säkerligen känd på minst 20 - 30 ställen, och de mer avancerade på betydligt fler. Vi använder webbläsare i datorer och appar på mobila enheter.

Här kommer några rekommendationer om hur du bör hantera din digitala identitet.

2. Ett konto – vad är det

När man är känd hos ett företag/tjänst säger man att man har ett ***konto*** där. Detta är INTE samma sak som ett bankkonto! Det innebär bara att man kan identifiera sig med ett användarnamn och ett lösenord för att komma åt sitt data (köphistorik, bilder, Facebook-inlägg, mm).

Så för att hålla reda på sina konton måste man spara tre parametrar om varje konto:

a) Företag/tjänst/site (där man har sitt konto)
b) Användaridentitet (oftast en mejladress, så att företaget kan nå dig)
c) Lösenord (gärna ett unikt sådant)

Det finns tre olika typer av konton:

1) Distributionslistor
   Företaget känner bara till din mejladress för att kunna skicka ut nyheter, mm. Detta kan knappast kallas ett konto, med det är medtaget för att ge hela bilden.
2) Vanliga konton
   Det är denna typen du har flest av – hos tidningar och mediahus, bredbandsleverantörer, näthandlare, mm. Här anger vi oftast vår vanliga mejladress, och försöker hitta på ett bra lösenord. Men det är väldigt vanligt att vi anger samma lösenord på flera ställen.
3) Plattformskonton
   Det finns tre stora plattformar för slutanvändare inom IT, och de är PC (Microsoft), iPhone/iPad/Mac (Apple) och Android/Chromebook (Google). För att kunna använda dessa behöver vi ett konto för respektive plattform. Vi talar om
   - Google-konto (oftast ett Gmail-konto)
   - Microsoft-konto (oftast ett hotmail/outlook/live-konto)
   - Apple-konto (oftast ett Apple-id = iCloud-konto)

Dessa plattformskonton är ”systemkritiska”, de används för att ge dig tillgång till mejl, data och bilder i molnet, dina appar i mobilen, dina sparade bokmärken i webbläsaren, mm, mm. Det är fatalt om inloggningsdetaljer till dessa konton blir avslöjade. Det är ofta här du ibland måste byta lösenord, kanske för att plattformsleverantören anser att ett intrångsförsök har skett.

3. Att återanvända Användaridentiteter och ”konton”

För distributionslistor och vanliga konton är det naturligt att som Användaridentitet ange en mejladress där vi kan tänka oss att få nyheter, reklam, information om leveranser, mm.

Att återanvända lösenord mellan vanliga konton är vanligt, men inte bra. Försök att hitta på unika lösenord och skriv ned dem! De flesta webbläsare innehåller nu också funktionalitet för att generera lösenord.

Det är inte heller ovanligt att återvända användaridentiteter mellan plattformskonton, t ex så anger man sin Gmail-adress som användaridentitet när man skapar sitt Microsoftkonto. Det fungerar, men det är också en orsak till väldigt mycket problem. Kom ihåg – om du har angivit din Gmail-adress som användaridentitet till både Google och Microsoft, så är det fortfarande två olika konton, med var sitt unikt lösenord! Alltför ofta håller man inte reda på vilket lösenord för Gmail-användaridentiteten som hör ihop med vilket plattformskonto. **Du rekommenderas entydigt** att ha en Gmail-adress för ditt Google-konto, en hotmail.com/live.se/outlook.com-adress för ditt Microsoft-konto och en iCloud.com-adress för ditt AppleID.

Ganska ofta erbjuds du möjligheten ”Logga in med ditt Google- eller Facebook-konto”. Det är något helt annat. Om du tackar ja till detta erbjuder du alltså företaget att fråga Google/Facebook om det är OK att du loggar in, och du ber Google/Facebook att hålla reda på till vilka företag du en gång har medgivit detta. Det förutsätter att du redan är inloggad mot Google/Facebook när du försöker logga in på det första företaget. Bekvämt, inte osäkrare än att ha en egen inloggning, men du etablerar beroenden och kopplingar som du kanske inte vill ha i framtiden.

4. Hjälp för att komma ihåg lösenord

Hur ska vi då hålla reda på våra konton och det som hör till dem? Här beskrivs de alternativ som är vanligast:

a) Vi kan använda penna och papper. Det är enklast och vi begriper vad vi håller på med. Glöm inte att alla tre kontoparametrarna måste skrivas ned, och framför allt, göm papperet på ett bra ställe, och kom ihåg var!!

b) Vi kan skriva ned samma saker på en fil och spara på datorn. Om du använder en modern version av Word kan du sätta ett lösenord på filen och kryptera den. Om datorn kraschar, eller om du glömmer lösenordet, ja då är dina sparade lösenord borta. Ta en backup på filen!

c) Våra vanligaste webbläsare blir allt duktigare på att både generera och spara lösenord, och att automatiskt fylla i dina parametrar när du kommer till en inloggningssida. Bekvämt, men om datorn kommer i orätta händer så kan den obehörige komma in på dina konton. Och om du skall logga in i en app i din mobil så har du ingen glädje av att webbläsaren känner till ditt lösenord. Om du använder flera olika webbläsare så har du inte heller alltid tillgång till dina sparade lösenord. Men, om du använder enbart en webbläsare, och inte behöver lösenorden i dina mobilappar, ja då är detta ett alternativ. Men, kom ihåg att
   - slå på ”synk” i webbläsaren så att lösenorden sparas i molnet och du därmed klarar en datorkrasch
   - skydda inloggning till datorn med krångligt lösenord, fingeravtryck, ansiktsigenkänning eller något liknande

d) Det finns speciella lösenordshanterare. Några är gratis, andra kostar pengar. Oftast måste du ange ett master-lösenord för att använda den, och de klarar inloggning både i appar och via webbläsare. Bättre än webbläsarfunktionen alltså, men också lite svårare att hantera. Man ska vara en ganska van mobil/dator-användare för att fullt ut ha glädje av en lösenordshanterare.

Ingen lösning är alltså självklart enklast och bäst. Men, för den ovane användaren är rekommendationen att börja med att skriva ned sina konton med parametrar på ett papper, och sedan ha en bra rutin för att hålla detta papper uppdaterat och säkert förvarat! Så här skulle ditt lösenordspapper kunna se ut:

Företag/tjänst	**www-adress/app**	**Användarid**	**Lösenord**
Telia	www.telia.se	Förnamn.efternamn@telia.com	aQwe/&
Microsoft	Min PC www.outlook.com	Kalle123@hotmail.com	Xyz123; PIN=2578
Blocket	Blocket.se	Förnamn.efternamn@telia.com	Block2010#
Google	Min mobil + Gmail www.google.se	Förnamn.x.efternamn@google.com	5702ert Tvåstegsverifiering

5. Till sist

Håll ordning på dina lösenord och konton! Det är allvar! Den absolut vanligaste orsaken till problem för normalanvändaren är bortglömda lösenord och missuppfattningen att ”konto, vad är det? Det har jag inte!”.

Plattformskonton är extra viktiga. Använd sådana, med unika användaridentiteter, och se till att vara inloggad med dem på dina enheter. Det går fortfarande att köra Windows utan ett Microsoft-konto, men det blir allt svårare, och du får flera fördelar (gratis molnlagringsutrymme, mail, synk av inställningar mellan olika enheter) om du använder ett.

Inför tvåstegsverifiering på dina plattformskonton! De är så viktiga, och konsekvenserna av illegala intrång så allvarliga, så det får inte ske. Tvåstegsverifiering innebär att det inte räcker med att känna till ditt lösenord. Den som loggar in måste dessutom identifiera sig på ytterligare ett unikt sätt – genom en kod som skickas till din mobil, genom att trycka OK i en app som sedan tidigare är certifierad av just dig, osv. Hur man gör för att aktivera tvåstegsverifiering? Sök på ”Google/Microsoft/Apple tvåstegsverifiering” så hittar du flera beskrivningar.

Lars Andersson

SeniorNet Södermalm
September 2020