4. Lösenordens brister

Varför är det viktigt att ha unika lösenord? Det korta svaret på den frågan är att lösenord har en tendens att läcka. Det långa svaret på den frågan ägnar vi hela detta inledande lösenordskapitel till. I kapitlet visar vi även hur vi kan ta reda på om en e-postadress har funnits med i någon av de senaste årens lösenordsläckor.

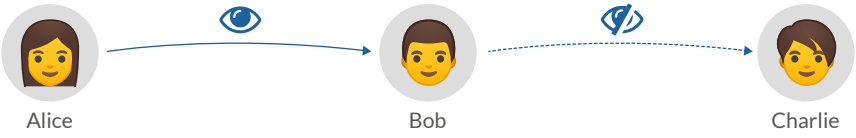
4.1 Lösenord är bäst i brist på alternativ

I dagens uppkopplade värld behöver vi ofta autentisera oss på ett eller annat sätt. Varje gång vi loggar in på en webbplats måste vi berätta vem vi är (användarnamn) och verifiera att vi är personen som vi utger oss för att vara. För att göra detta har vi vanligtvis ett lösenord, det vill säga en teckenkombination som endast vi själva känner till. I teorin är det inget fel med den autentiseringsmetoden, men i praktiken fyller inte lösenord den önskade rollen.

Ett lösenord garanterar inte att vi är personen som vi utger oss för att vara. Det garanterar enbart att vi känner till den berörda användarens hemliga teckenkombination. Den hemligheten kan vi antingen ha fått med gott uppsåt (t.ex. ett frivilligt delat Spotify-lösenord) eller ha lurat till oss (t.ex. genom så kallat **nätfiske** som förklaras längre fram i kapitlet).

Om Bob känner till Alices lösenord märker Spotify ingen skillnad på Alices och Bobs inloggningar.

Vi har svårt att veta om vi är de enda som känner till våra lösenord. Det räcker att vi gör ett litet misstag så kan våra lösenord hamna på avvägar. Om det sker förlorar vi kontrollen helt. Vi kan varken stoppa spridningen eller överblicka omfattningen av den. Ett läckt lösenord kan spridas vind för våg, precis som alla avslöjade hemligheter.



Om Alice berättar sitt lösenord för Bob kan hon inte veta om det sprids vidare.

Till råga på allt måste vi utgå från att även webbplatserna som vi loggar in på kan läcka våra lösenord. Varenda månad rapporteras det om nya webbplatser som läckt våra lösenord till kapare.

Dagens lösning på dessa problem är att aldrig använda samma lösenord på flera webbplatser samt att byta lösenord vid minsta misstanke om lösenordsläcka. Det är det enda sättet vi kan begränsa konsekvenserna av en lösenordsläcka. Utan unika lösenord kan angripare komma åt flera av våra konton så fort vi (eller någon annan) läcker lösenordet till ett av dem.

Utan unika lösenord äventyrar vi hela autentiseringsmetoden. Att ha unika lösenord överallt är dock lättare sagt än gjort, eftersom våra mänskliga hjärnor inte kan komma ihåg massvis av hemliga lösenord. Vi kan säkerligen komma ihåg några stycken, men att komma ihåg uppemot hundratals olika lösenord är inte bara orimligt; det är bokstavligen omänskligt.

Lösenord är dessvärre den bästa väletablerade autentiseringsmetoden som vi har än så länge. I väntan på att en bättre autentiseringsmetod vinner mark får vi därför göra det bästa vi kan av situationen. Det gör vi genom att:

- vara medvetna om lösenordens säkerhetsmässiga svagheter
- prioritera vilka konton som är mest skyddsvärda
- välja starka lösenord som är svåra att knäcka
- dra nytta av verktyg som hjälper oss hantera alla lösenord.

4.2 Så stjäls våra lösenord

Det finns många olika sätt som våra lösenord kan hamna på avvägar. Vissa av dem är mer uppenbara än andra. Ifall vi förvarar våra lösenord på post-it-lappar under tangentbordet kan vi knappast förvånas över att andra känner till dem.

Lösenord hör inte hemma på post-it-lappar under tangentbordet.

Nätfiskeattacker

Ett annat uppenbart sätt är om vi råkar försäga oss, till exempel genom att mejla lösenordet till bedragare. En klassisk nätfiskeattack är den där angripare låtsas kontakta oss från något företags supportavdelning. Angriparna påstår att de ska hjälpa oss med något och att de behöver vårt lösenord för att kunna fixa det (alternativt att vi måste ange vårt lösenord för att styrka vår identitet). Sådana mejl är alltid och utan undantag bedrägeriförsök. Ingen seriös supportavdelning behöver någonsin be om sina kunders lösenord eftersom de har egna administrativa vägar in i samma system.

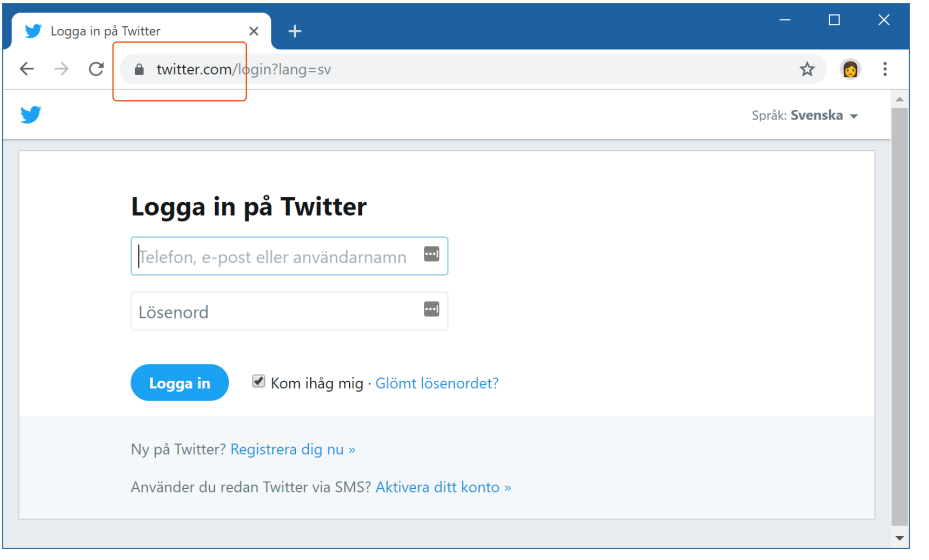
> Varning! Det finns aldrig något skäl att skriva lösenord i mejl. Mejl som vi skickar är lika öppna för nyfikna ögon som vanliga vykort (se *kapitel 19*). Enbart bedragare ber oss mejla lösenord.

Tekniska attacker

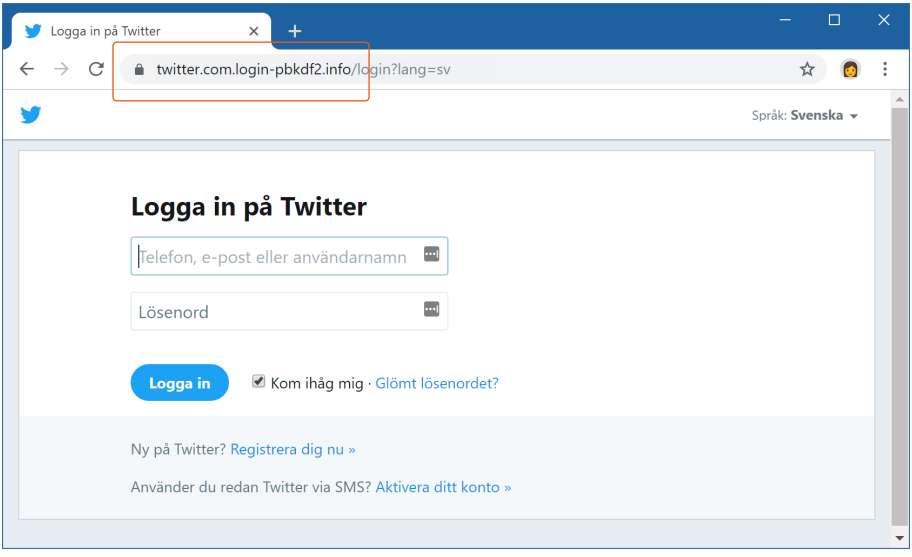
Om vi bortser från de mer uppenbara sätten, så kan angripare även stjäla våra lösenord på teknisk väg. De kan till exempel infektera våra datorer med skadeprogram som snappar upp alla lösenord. De kan också avlyssna nätverkstrafiken så att de ser eventuella lösenord vi anger på webbplatser som inte stöder säkra anslutningar (läs mer om hur vi förhindrar detta i *gröna sektionen*).

Ytterligare en metod som angripare använder är så kallade **MITM-attacker** (Man In The Middle-attacker). I en sådan attack luras vi in på en fejkad version av en riktig webbsida. Den fejkade webbsidan drivs av angriparna och sparar alla autentiseringsuppgifter vi anger. Angriparna skickar i sin tur vidare autentiseringsuppgifterna till den riktiga webbsidan, så att vi inte märker att något är fel.

Se exempelvis följande två webbsidor. Den ena är Twitters riktiga inloggningssida. Den andra är en klonad version av densamma. Webbsidorna ser identiska ut och den enda skillnaden vi kan se är att adresserna i adressfälten skiljer sig.



Twitters riktiga inloggningssida (lägg märke till adressen).



En lösenordskapande version av Twitters inloggningssida (lägg märke till adressen).

4.3 Webbplatser läcker våra lösenord

Det är inte bara vi som kan råka avslöja våra lösenord. Webbplatserna som vi loggar in på kan också bli attackerade och läcka dem.

En av de allvarligaste lösenordsläckorna i modern tid råkade mjukvaruföretaget Adobe ut för 2013 (Adobe är företaget bakom bland annat PDF-formatet och bildredigeringsappen Photoshop). De blev attackerade och läckte information från 152 miljoner användarkonton (varav 400 000 tillhörde svenskar[2])! Användarnas lösenord var visserligen maskerade[3], men de låg tillsammans med läsbara lösenordsledtrådar! Många av lösenordsledtrådarna var så uppenbara att de avslöjade lösenorden direkt. Ifall flera användare hade valt samma lösenord kunde angriparna också kombinera de olika användarnas lösenordsledtrådar för att ännu enklare lista ut de rätta lösenorden (detta hade inte varit möjligt om lösenorden maskerats på ett korrekt vis).

2. Reinfeldts lösenord läckte ut (SVT, 2013). Nyhetsartikel publicerad 2013-11-09, hämtad 2018-07-28. https://nikka.systems/ref-110

3. Ordet ”maskerade” syftar på att lösenorden inte lagrades i klartext. Adobe lagrade matematiska värden (så kallade hash-summor) som representerade lösenorden.

Adobe-läckan visar med all tydlighet vikten av att ha unika lösenord på alla webbplatser. Även om vi som användare är noga med hur vi hanterar våra lösenord, kan vi inte vara säkra på hur webbplatserna hanterar dem. Här följer en lista över stora webbplatser som har läckt användarnas lösenord under de senaste åren (se haveibeenpwned.com för fler exempel).

Företag (tjänst)	Beskrivning	Läckta konton	År
Adobe	Mjukvaruföretag	152 miljoner	2013
Ashley Madison	Dejtingsida	31 miljoner	2015
Badoo	Dejtingsida	112 miljoner	2013
Bitly	Webbverktyg	9 miljoner	2014
Brazzers	Porrsida	1 miljon	2013
Disqus	Kommentarsfunktion	18 miljoner	2012
Dropbox	Molnlagringstjänst	69 miljoner	2012
Forbes	Nyhetssida	1 miljon	2014
Imgur	Bilddelningssida	2 miljoner	2013
Kickstarter	Finansieringssida	5 miljoner	2014
Last FM	Radiosida	37 miljoner	2012
Linkedin	Socialt nätverk	165 miljoner	2012
Myspace	Socialt nätverk	359 miljoner	2008
Patreon	Finansieringssida	2 miljoner	2015
Youporn	Porrsida	1 miljon	2012

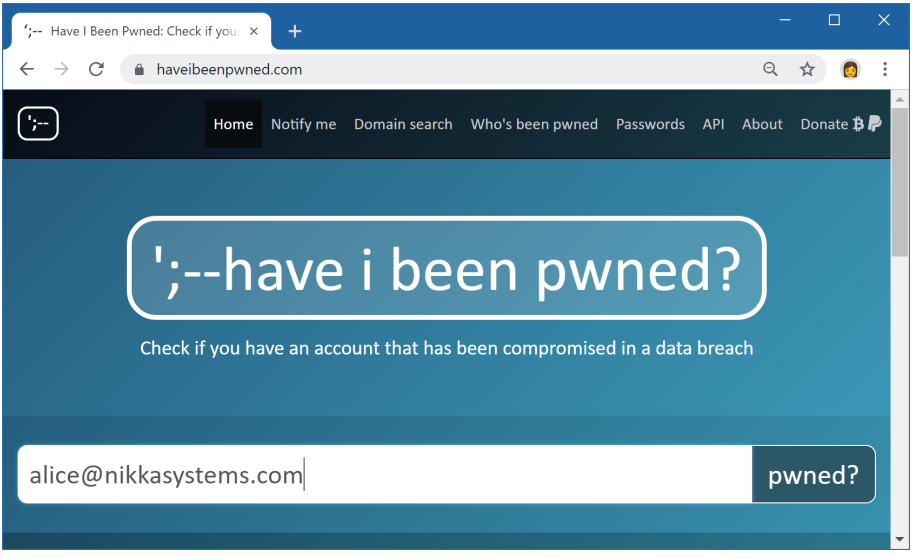
Källa: haveibeenpwned.com

Ur ett svenskt perspektiv är det även värt att nämna forumen Flashback och Sweclockers som läckte användarnamn och lösenord 2015.

4.4 Have I Been Pwned?

Säkerhetsforskaren Troy Hunt driver webbplatsen ”Have I Been Pwned?”. Där finns det en databas med över fem miljarder kapade konton. Besökarna kan söka

efter sina egna e-postadresser för att se om de har funnits med i någon eller några av läckorna som Troy Hunt har tagit del av.



På Have I Been Pwned? kan du se ifall din e-postadress finns med i kända lösenordsläckor.

Gå till haveibeenpwned.com och sök efter din e-postadress (Troy Hunts sida är helt legitim att använda och du riskerar inte att få skräppost av att ange din e-postadress där). Ifall din e-postadress finns med i någon av läckorna bör du säkerställa att du har bytt lösenord efter att läckan inträffade. Om du har använt samma lösenord på fler ställen bör du även byta lösenord där.

> Obs! Det är helt naturligt att din e-postadress finns med i en eller flera av läckorna. Det betyder inte att angriparna har kommit åt dina konton. Seriösa webbplatser lagrar lösenorden maskerade, vilket gör det svårt för angriparna att lista ut vilka de rätta lösenorden är. Så länge du har bytt lösenord efter att läckan inträffade är allt i sin ordning.

På samma webbplats kan du även ange din e-postadress för att få en notis ifall den dyker upp i framtida lösenordsläckor. Tjänsten är gratis att använda och finansieras genom donationer.

> Tips! Pwned är slang för att ”ha blivit ägd”, det vill säga att ha förlorat kontrollen över sitt eget konto.