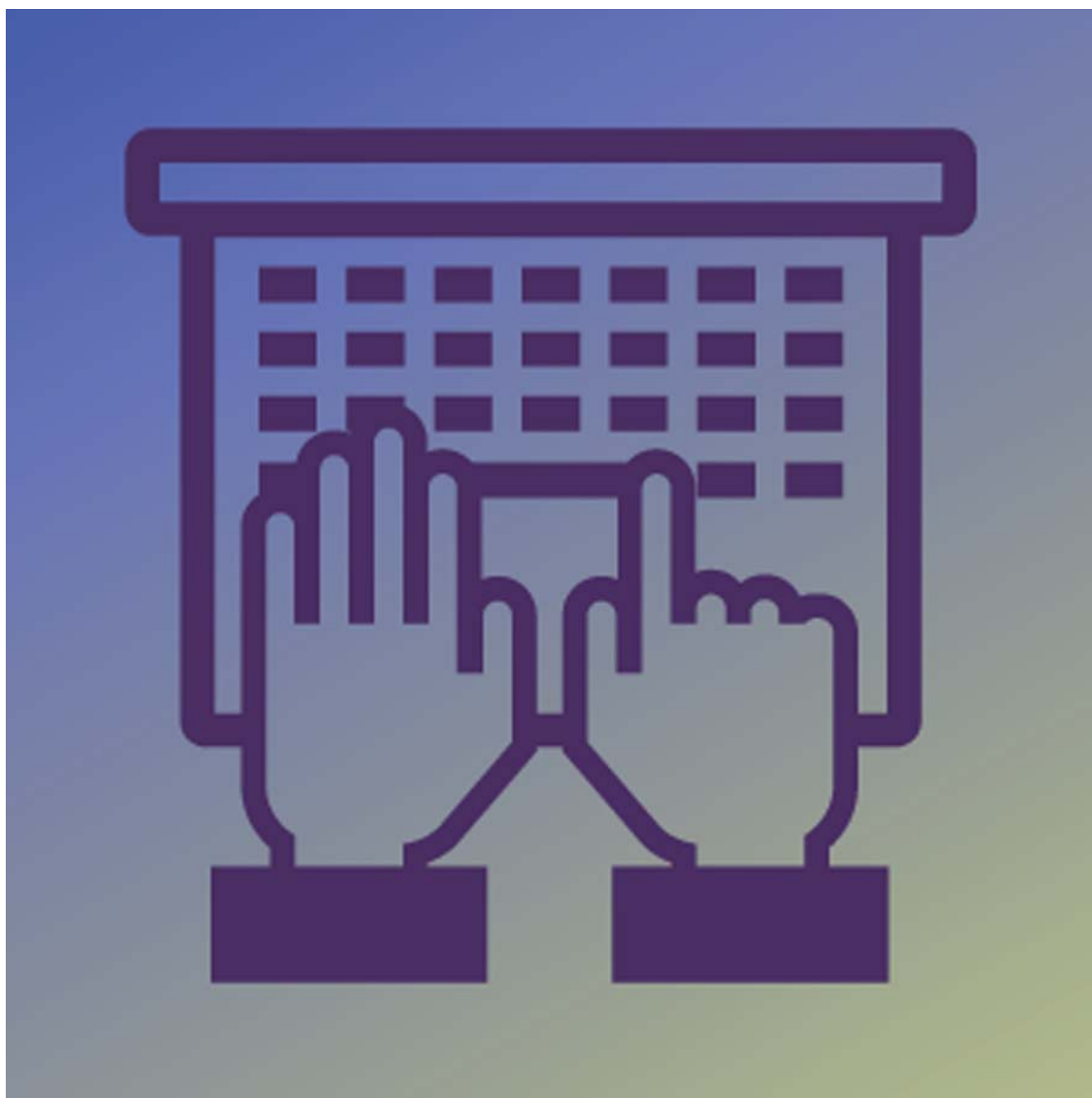


# Lösenord för alla



Statistik, råd och rekommendationer för bättre säkerhet



Version 1.0

Anne-Marie Eklund Löwinder

Texten skyddas enligt lag om upphovsrätt och tillhandahålls med licensen Creative Commons. Erkännande 2.5 Sverige, vars licensvillkor återfinns på <http://creativecommons.org/>, för närvarande på sidan <http://creativecommons.org/licenses/by/2.5/se/legalcode>.

Vid bearbetning av verket ska IIS logotyper och IIS grafiska element avlägsnas från den bearbetade versionen. De skyddas enligt lag och omfattas inte av Creative Commons licensen enligt ovan.

Författare: Anne-Marie Eklund Löwinder

IIS (Internetstiftelsen i Sverige) är en oberoende allmännyttig organisation som ansvarar för internets svenska toppdomän .se och verkar för en positiv utveckling av internet i Sverige.

Organisationsnummer: 802405-0190

# Innehållsförteckning

01. Förord.....	5
02. Sammanfattning.....	6
03. Svenskarna och deras lösenordsvanor.....	9
03.1 Analys av enkätresultaten .....	9
04. Lösenordens tio i topp-lista.....	25
05. Lösenordens historia .....	27
05.1 Så började det.....	27
06. Lösenordens anatomi.....	28
06.1 Varför statiska lösenord är vanligare än dynamiska.....	28
06.2 Dåliga lösenord .....	29
06.3 Riktigt dåliga lösenord .....	31
07. Konsekvenser av lösenordsläckor.....	33
07.1 Vad har hänt.....	33
07.2 Hur används de läckta lösenorden?.....	36
08. Så hackas lösenord och lösenfraser .....	37
08.1 Bristande skydd av lösenord .....	37
08.2 Olika sätt att komma över användares lösenord.....	39
08.3 Kvalificerade gissningar on-line eller off-line .....	40
08.4 Råstyrkemetoden (brute force attack).....	40
08.5 Ordlistemetoden (dictionary attack).....	41
09. Råd och rekommendationer.....	42
09.1 Längden har betydelse .....	42
09.2 Komplex och ovanligt.....	42
09.3 Lösenord i nivåer.....	42
09.4 Byt inte ett bra lösenord – om du inte måste .....	43
09.5 Är ditt lösenord röjt? .....	44
09.6 Lösenfraser .....	44
09.7 Lösenordsgeneratorer på nätet.....	45
09.8 Lösenordshanterare .....	45
09.9 Spara lösenord i webbläsare .....	47
09.10 Engångslösenord och tvåfaktorsautentisering.....	47
09.11 Vad händer med mina konton och lösenord när jag dör?.....	48

010. Tips om effektivare försvarssystem för systemägare, systemutvecklare och systemadministratörer.....	50
011. Fakta om undersökningen .....	53

## 01. Förord

Gång efter annan uppmärksammas vi med stora, svarta rubriker på hur lösenordsdatabaser kommit på vift, hur någon fått sin identitet på nätet kapad eller hur dåliga vi är på att konstruera säkra, unika lösenord som ger oss en rimlig grad av skydd på nätet. Säkerhetsexperterna river sitt hår över användarnas ignorans och fantasilöshet.

Åtskilliga artiklar har skrivits om vad som är ett bra nätbeteende, i synnerhet när det gäller valet av lösenord, men få tar det på allvar, varken användare eller utvecklare av tjänster. Visst, de allra flesta känner till att det bästa lösenordet är slumpartade kombinationer med versaler, gemener och specialtecken, med ett minimiantal tecken och så vidare. Men vi lever inte som vi lär.

Hur osäkra lösenord i allmänhet än är kommer användningen av dem inte att försvinna inom någon överskådlig framtid. Varje år behöver vi hantera fler och varje år blir verktygen att knäcka lösenord bättre. Vi behöver ha en strategi.

Med den här rapporten vill IIS bidra med kunskap om hur svenskarna använder lösenord, förklara riskerna och konsekvenserna av att få sina lösenord knäckta, hur det går till, vad vi svenskar känner till om lösenord och vad vi gör åt saken. Och inte minst, vad vi borde göra.

Jag vill framföra ett särskilt varmt tack till Per Thorsheim, säkerhetsrådgivare från God Praksis AS i Norge som har lagt både tid och engagemang på att granska sakinnehållet och bidragit till viktiga förbättringar. Ett varmt tack riktar jag också till min kollega Pamela Davidsson som i egenskap av Excel-virtuos och statistiker hjälpt mig att lyfta fram kärnan i undersökningsresultatet som snygga grafer.

Anne-Marie Eklund Löwinder, CISO, IIS

## 02. Sammanfattning

Den finske forskaren och säkerhetsexperten Mikko Hyppönen från F-Secure sa på en konferens en gång (fritt översatt): Behöver du ett bra lösenord? Välj något som du absolut inte kan komma ihåg. Skriv inte ner det någonstans.

Att behöva hålla reda på mängder av lösenord är en del av vår tids gissel. Så hur gör svenskarna för att komma ihåg sina? IIS har genomfört en undersökning och ställt en rad frågor kring lösenord och lösenordsanvändning till drygt 1000 svenskar.

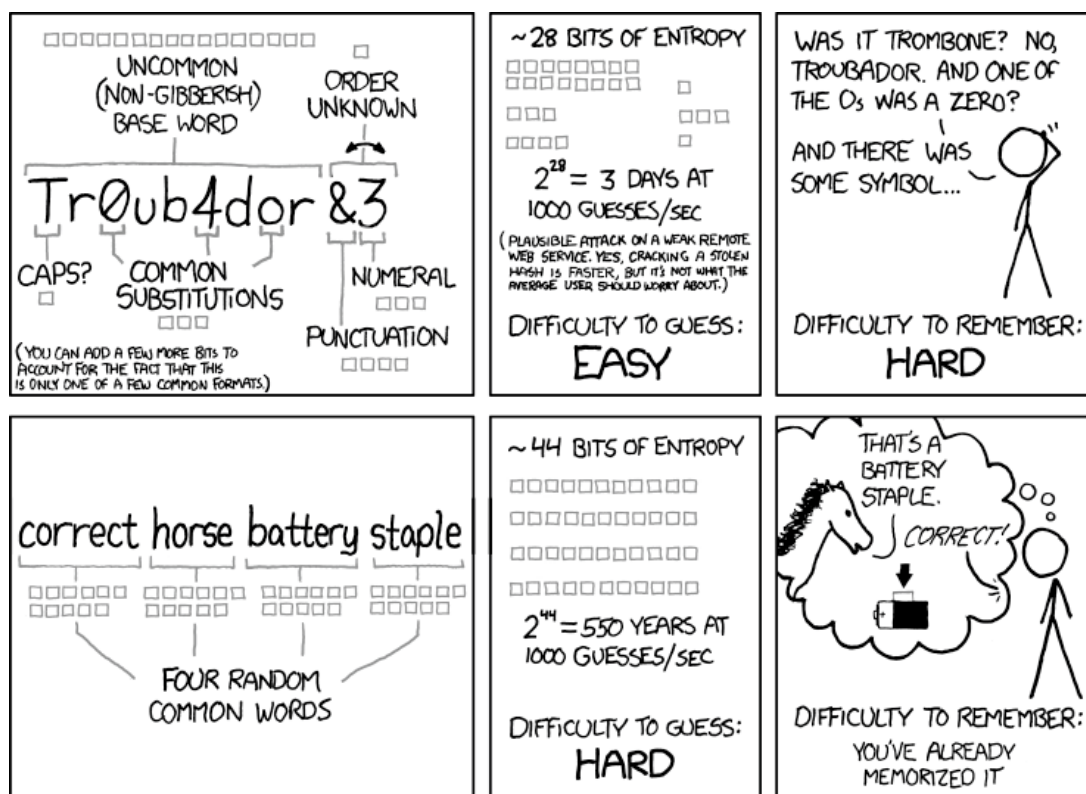
Vi lever idag i ett samhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas. På individnivå betyder det att arbetsliv och privatliv lätt flyter samman och att vi hanterar stora mängder av information varje dag, en del känsligare än annat. Medvetna användare har alltid framhållits som en viktig del i säkerhetsarbetet, och där är utbildning en hörnsten. Ändå visar undersökningen att utbildning saknas i stor utsträckning.

Av de tillfrågade anger en dryg tredjedel att de alltid använder starkare lösenord till tjänster som de anser behöver skyddas extra mycket, en knapp tredjedel gör det oftast, vissa bara ibland och några gör det inte alls. Så trots att man vet vad man ska göra väljer man att ignorera det, förmodligen av bekvämlighetsskäl. Oroväckande många användare är dessutom beredda att ta stora risker genom att återanvända samma lösenord på flera olika ställen.

Det finns olika skolor kring hur man konstruerar starka lösenord. Grundprincipen är att lösenordet ska vara ganska långt. Post- och telestyrelsen föreslår minst tolv tecken. I sammanhang där information hanteras som är mycket känslig och där den som kan vara intresserad av att knäcka lösenord förmodligen har gott om pengar och/eller mycket datorkraft kan det vara värt att överväga ett betydligt längre lösenord och om möjligt använda flera olika faktorer. Var man landar bör vara resultatet av en riskbedömning.

Många hävdar att det är ett måste med en teckensoppa som innebär en kombination av stora och små bokstäver, siffror och specialtecken som #%&?+. Andra förespråkar långa fraser sammansatta av vanliga ord. Om man använder den senare varianten blir längden mycket viktigare. Ju längre fras desto svårare för en angripare att prova sig fram, även om lösenfrasen är lätt för dig att komma ihåg.

Undvik alla fraser som är väl kända och sannolikt spridda globalt, som bibelcitater, filmcitater ur de största kassasuccéerna, citat ur den klassiska litteraturen och liknande. Då är det bättre med en helt egen transkription av något uttryck på tornedalssvenska eller östgötska, en fras ur din svenske lokallyrikers alster eller en svensk barnsång från seklets början, eller varför inte bara en helt absurd mening. Per Thorsheims råd är att välja fraser som väcker positiva känslor, som man blir glad av att skriva in. Det underlättar för användaren att komma ihåg sina fraser.



<https://xkcd.com/936/>

I vissa sammanhang är den möjliga längden på lösenorden begränsad. Om du exempelvis bara kan använda 8-10 tecken är en teckensoppa nödvändig för att uppnå någorlunda säkerhet. Med så korta lösenord är namn och ord ur ordlistor direkt olämpliga att använda. Program som används för att knäcka lösenord testas ofta igenom ordlistor på olika språk. Att ta ett känt ord och byta några tecken – LinkedIn omgjort till 1!nked!n – är för lätt att lista ut.

I vilken mån tecken kan upprepas eller inte är en stridsfråga. Vissa hävdar att inget lösenord bör upprepa samma tecken mer än tre gånger medan andra och däribland vi anser att något i stil med Kuf#####s är ytterligt svårt att knäcka. Ibland finns det dock tekniska begränsningar som gör att det inte går att använda samma tecken flera gånger.

Lösenorden bör aldrig sparas någonstans digitalt i klartext. Den som skriver upp sina lösenord på papper bör betrakta dokumentet som en värdehandling. Hur förvarar man 100 000 kronor? Knappast liggande löst på skrivbordet.

Det finns program för lösenordshantering, kontrollera gärna recensioner<sup>1</sup> av de som gjort det, sök efter rapporterade sårbarheter och se framför allt till att inte

<sup>1</sup> <http://uk.pcmag.com/password-managers-products/4296/guide/the-best-password-managers-of-2016>

glömma ditt lösenord dit. Gör du det måste du börja om från början. Det finns inget annat sätt.

Använd helst inte online-baserade lösenordsgeneratorer, du vet oftast inte vem som ligger bakom och vilken kvalitet tjänsten har. Ladda ner en lösenordsgenerator som du använder lokalt<sup>2</sup>. Lösenordshanterare har inbyggda lösenordsgeneratorer där man väljer parametrar som typ av tecken, antal tecken och så vidare. Vi rekommenderar starkt användning av lösenordshanterare.

Lösenord till e-postkonton är förmodligen det viktigaste du har, och de bör alltid vara unika och riktigt starka. En angripare som får tag i dem kan gå in och beställa nya lösenord i ditt namn på andra sajter och får därmed tillgång till alla dina tjänster, kan byta lösenorden och ta över din nätidentitet.

Om du varit glömsk är det många webbsajter som via en knapptryckning skickar ut nya lösenord till den e-postadress du angett. Ändra alltid omedelbart det nya lösenordet till något som du själv valt om det har skickats i klartext. Om någon snappat upp din e-post får den personen annars tillgång till sajten lösenordet gäller för.

Även om vi i grunden talar emot regelbundna och täta byten av lösenord innebär det inte att du aldrig ska byta. Framför allt som vi ser av undersökningen att användare i regel använder för korta och för enkla lösenord som man dessutom återanvänder på flera ställen och dessutom ibland lånar ut. Byt ibland, och omgående om du misstänker att lösenordet blivit röjt. Se också till att dina lösenord motsvarar kraven på starka lösenord. Om det finns regler på jobbet som tvingar fram byten måste de givetvis följas, även om det enligt vår uppfattning är en mindre bra regel.

Lämna inte ut ditt lösenord till någon annan om du inte har goda skäl. Ta som regel att alltid ignorera mejl som ber dig skicka lösenord eller som innehåller länkar där du ombeds logga in. Det är klassiska metoder för att lura av folk deras användaridentiteter och lösenord (så kallat nätfiske).

Ett idealiskt lösenord är lätt att komma ihåg för användaren och svårt att lista ut för alla andra. Samma lösenord ska aldrig återanvändas på flera tjänster med inloggning eller på olika apparater. Hitta en metod för att skapa lösenord som är smidig och fungerar för just dig.

Cormac Herley från Microsoft research har uttryckt det mycket enkelt: Så länge ditt lösenord inte finns med bland de vanligaste 10 000 eller så, är du relativt säker från ordlisteattacker.

Den generella principen kring säkerhet är att den är precis så hög som obekvämligheten. Vill du ha en säker miljö så blir det lite mer obekvämt. För egen del kan jag leva med det, jag har sett alltför många exempel på konsekvenser av för låg säkerhet, men många, kanske de allra flesta, orkar inte göra rätt. I grunden finns det kanske inte heller något rätt eller fel, bara en bedömning av vilka risker man är beredd att ta.

---

<sup>2</sup> <http://pwgen-win.sourceforge.net/>



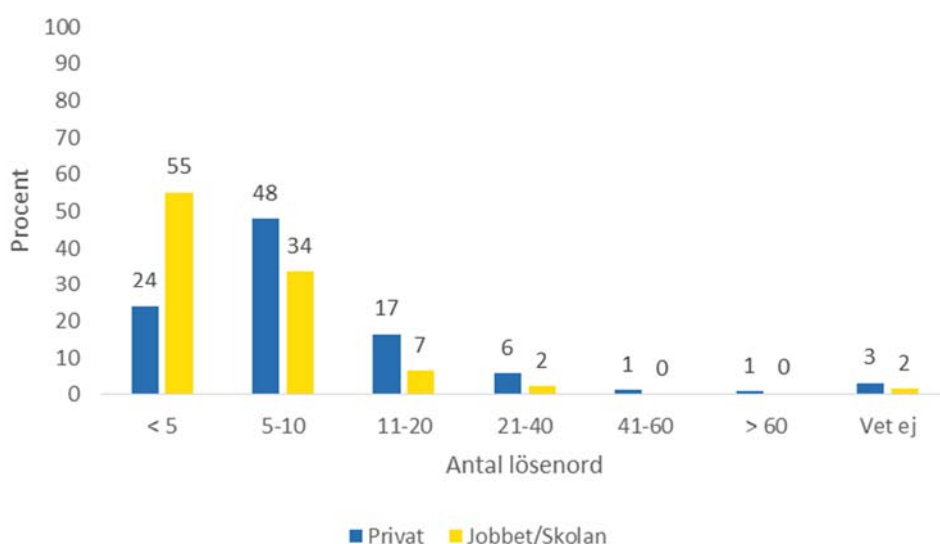
## 03. Svenskarna och deras lösenordsvanor

IIS har ställt en rad frågor (se formuläret) som är relaterade till lösenord på olika sätt, i det inledande avsnittet redovisas svaren med en kort analys. I den andra delen av rapporten går vi igenom historia, lösenordens anatomi, några inträffade incidenter och vilka risker som följer av att slarva med lösenord. I den tredje delen går vi in på råd och rekommendationer om åtgärder för att undvika att någon hackar ditt lösenord och tar kontrollen över dina konton på internet. Ett avsnitt tar också upp vad man bör tänka på som systemägare eller systemutvecklare. Läsaren kan själv ta del av insamlad data så att den som vill kan göra analyser och dra egna slutsatser.

### 03.1 Analys av enkätresultaten

Det är relativt säkert att påstå att lösenord är ett centralt fenomen i vår internetvardag. De allra flesta har upp till 10 lösenord att hålla reda på.

#### 03.1.1 Hur många lösenord måste du hålla reda på?



Figur 1. Antal lösenord att hantera

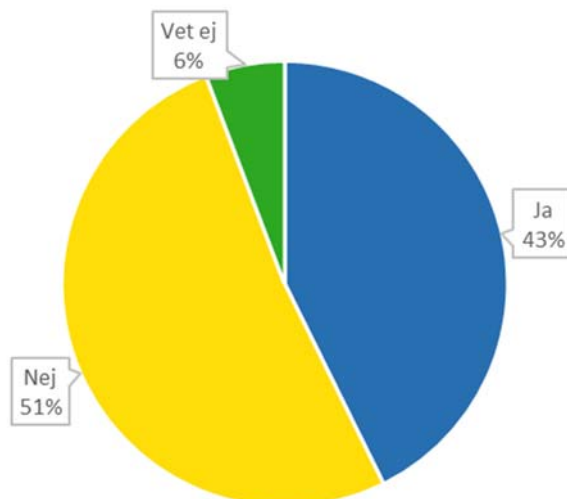
Mer än hälften av de tillfrågade behöver inte hålla reda på mer än upp till 5 lösenord på jobbet. Privat är det betydligt fler lösenord att hålla reda på för användarna.

Personer inom IT- och kommunikationsbranschen har fler lösenord att hålla reda på än verksamma inom andra branscher. Det är också den bransch där man har de längsta lösenorden och använder lösenordshanterare i större utsträckning än andra. Det är föga överraskande i sig. Inom IT- och kommunikationsbranschen får vi anta att man använder IT-stöd i stor utsträckning och därmed också är mer IT-kunniga.

Flest lösenord måste du hålla reda på om du ligger i åldersspannet mellan 26 och 55 år.

### 03.1.2 Har du fått utbildning/information om hur man skapar lösenord?

Av undersökningens resultaten förefaller det som att det brister i information kring hur man skapar lösenord.

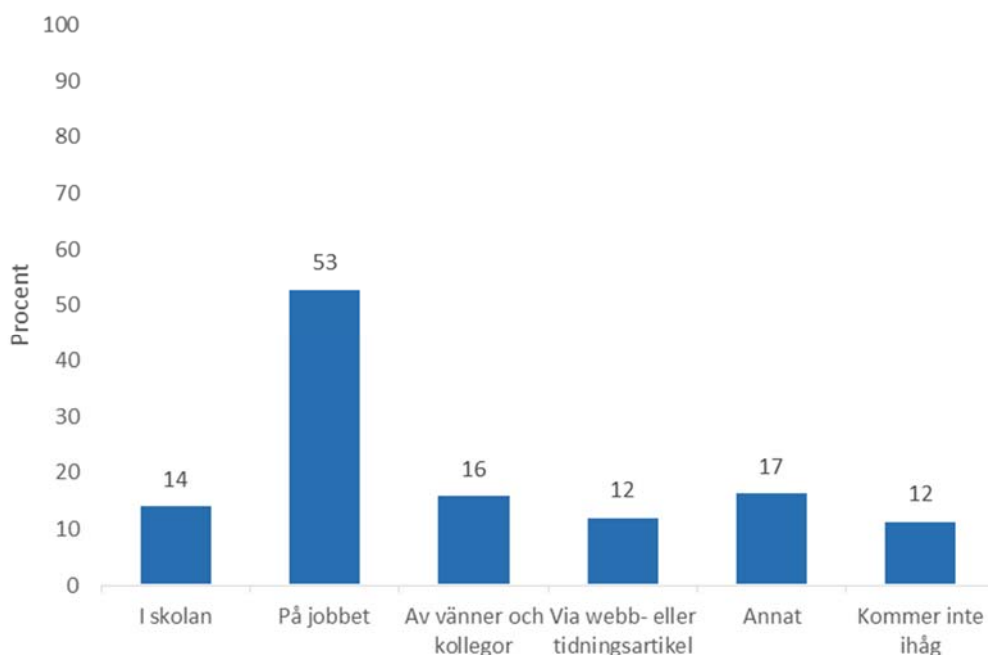


Figur 2. Fått utbildning/information om hur man skapar lösenord

Knappt hälften uppger att de har fått utbildning eller information om hur man skapar lösenord, drygt hälften att de inte har fått sådan utbildning. Sex procent kan inte säga om de har fått det. Detta är både överraskande och väldigt oroväckande siffror. Den typen av kunskap behöver användare få så tidigt som möjligt, redan på dagis, och det behövs regelbundna påminnelser.

Undersökningen visar inte på några större skillnader mellan könen, mer än att det verkar vara vanligare att män får utbildning om hur man skapar lösenord (47 procent) än kvinnor (38 procent).

Vi lever idag i ett samhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas. På individnivå betyder det ofta att arbetsliv och privatliv lätt flyter samman och att vi hanterar stora mängder av information varje dag, en del av den känsligare än annat. Medvetna användare har alltid framhållits som en viktig del i säkerhetsarbetet, och där är utbildning en hörnsten.

**03.1.3 Var har du fått utbildning/information om hur man skapar lösenord?**

Figur 3. Var har du fått utbildning/information om hur man skapar lösenord

Jobbet verkar vara en viktig källa till information om hur man skapar lösenord, däremot utgör skolan en blygsam andel som källa till kunskap inom detta område.

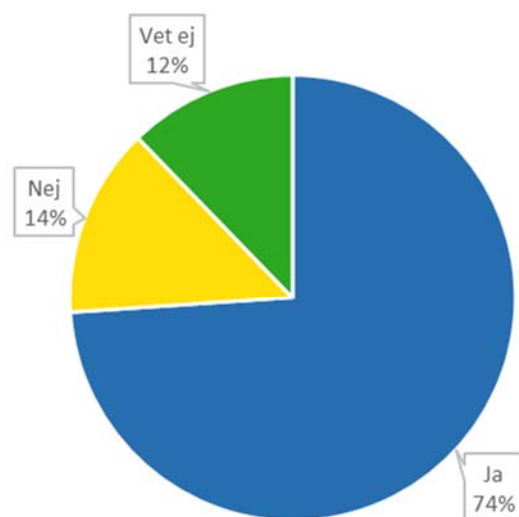
De allra flesta som säger sig ha fått utbildning eller information om hur man skapar lösenord har alltså fått det via jobbet. Andra har fått sådan utbildning eller information av vänner och kollegor, i skolan samt via webb- eller tidningsartiklar. Vi ser här ännu tydligare hur liten andel som har fått utbildning och information i skolan, endast 14 procent. 13 procent har fått det på något annat sätt och 9 procent kommer inte ihåg hur de fått det.

Säkerhetsmedvetandet måste komma in så tidigt som möjligt i internetanvändares beteende. Att det inte är en större andel som får utbildning eller information i skolan eller ännu tidigare är både beklagligt och oroväckande.

**03.1.4 Känner du att du har tillräcklig kunskap för att skapa ett starkt lösenord?**

Begreppet starkt lösenord förekommer ganska ofta när vi pratar om informationssäkerhet. Starkt innebär i det här fallet lösenord som är minst 9-14 tecken långa och innehåller både små och stora bokstäver, siffror samt specialtecken. Ett längre lösenord är bättre, och ett mycket längre lösenord är mycket bättre. Varje tecken ökar säkerheten flerfaldigt.

Utbildning eller inte så verkar de tillfrågade ha stort självförtroende när det gäller nivån på den egna kunskapen.



Figur 4. Har tillräcklig kunskap för att skapa starka lösenord

Frågan om man har tillräcklig kunskap för att skapa ett starkt lösenord besvaras med ett rungande "Ja", bara 14 procent besvarar frågan nekande och 12 procent vet inte om de har tillräcklig kunskap.

I den här frågan lämnas även möjligheten att med egna ord beskriva vad som anses vara ett starkt lösenord. Det är uppenbart att frågan om lösenord engagerar, av 1 005 svarande har drygt 800 personer eller ungefär 80 procent delat med sig någon form av beskrivning av vad de betraktar som starka lösenord.

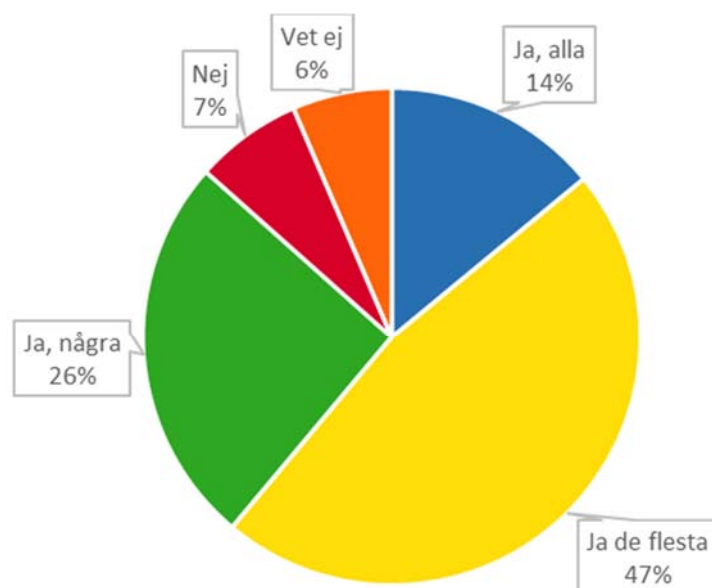
Cirka 28 procent eller 284 personer anger att en blandning av stora och små bokstäver samt siffror är viktiga ingredienser för att skapa ett starkt lösenord, ytterligare 35 procent eller 351 personer lägger specialtecken till listan.

En annan faktor som också har slagit igenom är att ett lösenord inte ska ha några kopplingar till dig som person, 169 personer lyfter fram det som ett särskilt krav. Långt, slumpmässigt, att det inte är riktiga ord, allt återfinns bland svaren.

Det verkar alltså inte råda någon större brist på kunskap om hur säkra lösenord skapas. Några delar med sig av exempel, och andra delar av sig av sina personliga recept. Endast 2 procent (22 personer) lyfter fram det här med unikt per sajt eller tjänst som en viktig egenskap.

### 03.1.5 Motsvarar dina lösenord kraven på starka lösenord?

De som besvarat enkäten vet alltså vilka egenskaper som förknippas med starka lösenord. Trots det är det relativt många som inte tillämpar principen fullt ut, men hälften uppger ändå att de har starka lösenord på de flesta sajter.

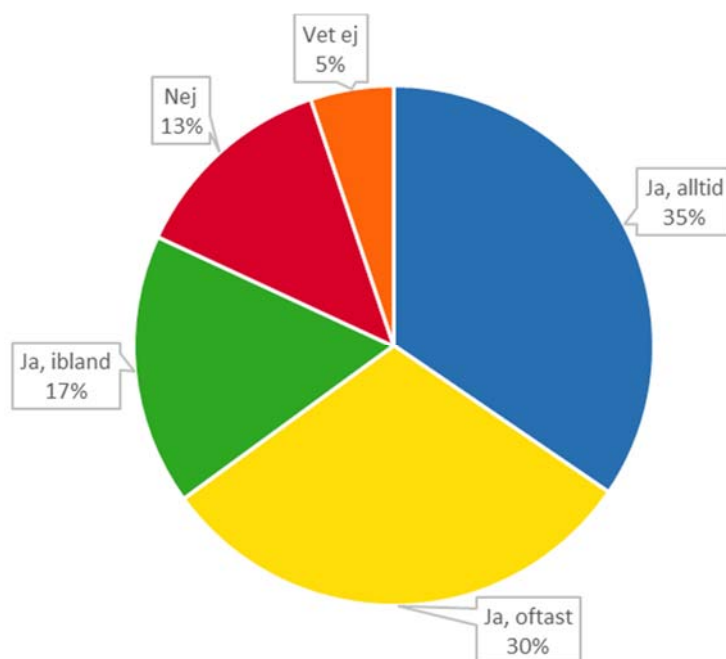


Figur 5. Använder lösenord som motsvarar kraven på starka lösenord

Av de svarande är det en del som påstår att de har starka lösenord överallt, knappt hälften anger att de har det på de flesta ställen, en fjärdedel har det på några ställen. En mindre andel anger att de inte har lösenord som motsvarar kraven på starka lösenord.

### 03.1.6 Använder du starkare lösenord till tjänster som du anser behöver skyddas extra mycket?

Det är trots allt så att all information inte är lika skyddsvärd eller att samma höga säkerhetsnivå krävs överallt.



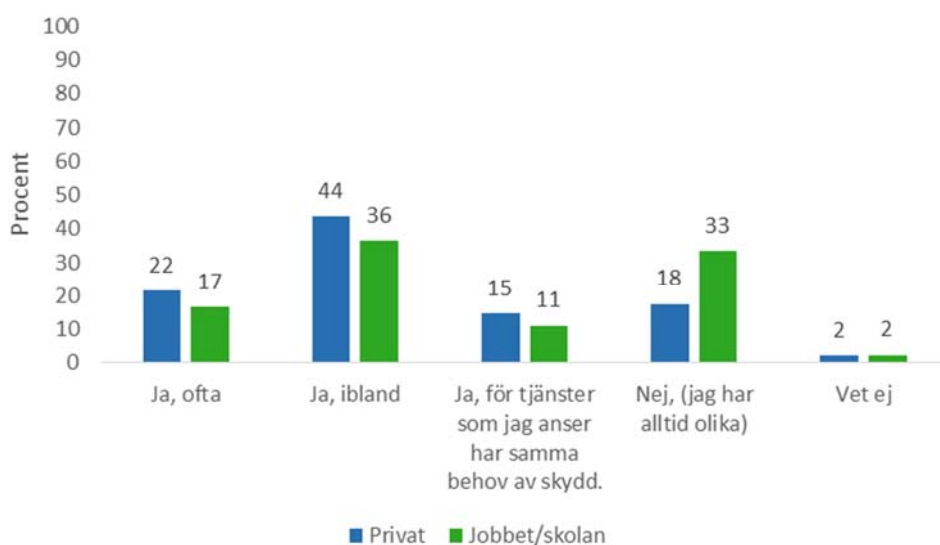
Figur 6. Använder starkare lösenord till viktiga tjänster

Det är därför inte så överraskande då att man inte tillämpar principen med starka lösenord överallt, men där det behövs borde det vara en regel.

Det verkar alltså inte vara självklart för de svarande. Av de tillfrågade anger en dryg tredjedel att de alltid använder starkare lösenord till tjänster som de anser behöver skyddas extra mycket, en knapp tredjedel gör det oftast, vissa bara ibland och några gör det inte alls. Det är uppenbart att här finns stora brister.

### 03.1.7 Återanvänder du samma lösenord på flera ställen för privat bruk respektive jobbet/skolan?

Frågan om användarna återanvänder lösenord ställs utifrån två olika förutsättningar, om man gör det för privat bruk eller om man gör det på jobbet eller i skolan. Svaren fördelade sig enligt följande diagram.



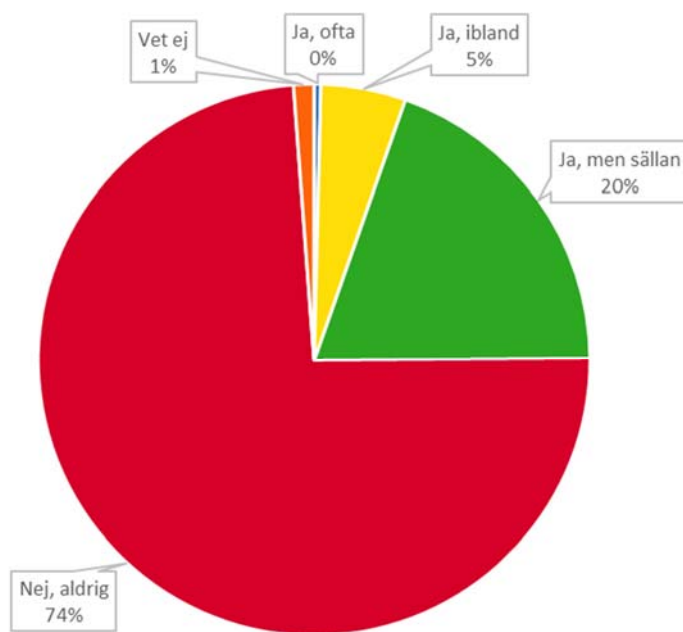
Figur 7. Återanvänder du samma lösenord på flera ställen för privat bruk respektive jobbet/skolan

Här skiljer sig svaren något, och man förefaller mindre försiktig med återanvändning av lösenord privat än på jobbet. En dryg femtedel av de tillfrågade återanvänder ofta samma lösenord för privat bruk medan 17 procent gör det på jobbet. Andelen som bara återanvänder lösenord ibland är 44 respektive 36 procent, alltså igen, fler som gör det privat än på jobbet. 18 procent har alltid olika lösenord privat, medan motsvarande för jobbet/skolan är 33 procent. Många företag har regler för användare som förbjuder återanvändning utanför jobbet av lösenord som används i företagets system. Det är omöjligt att kontrollera efterlevnaden av en sådan regel, och eftersom man inte kan följa upp ett krav på att inte återanvända lösenord i jobbet för privata sammanhang är det klokare att formulera det som en mycket stark rekommendation med en tydlig förklaring av varför det är viktigt.

Senare i rapporten återkommer vi till varför det är viktigare att ha unika lösenord än både långa och komplexa.

### 03.1.8 Brukar du dela med dig av dina lösenord till andra?

Lösenord är en värdehandling och ska helst inte delas med andra om det inte krävs av olika anledningar och spårbarheten kan garanteras på något annat sätt. Det är en av informationssäkerhetens grundprinciper. Om din inloggning inte är unik kan du komma att bli misstänkt i de fall något dåligt har inträffat genom att någon missbrukat ditt förtroende.

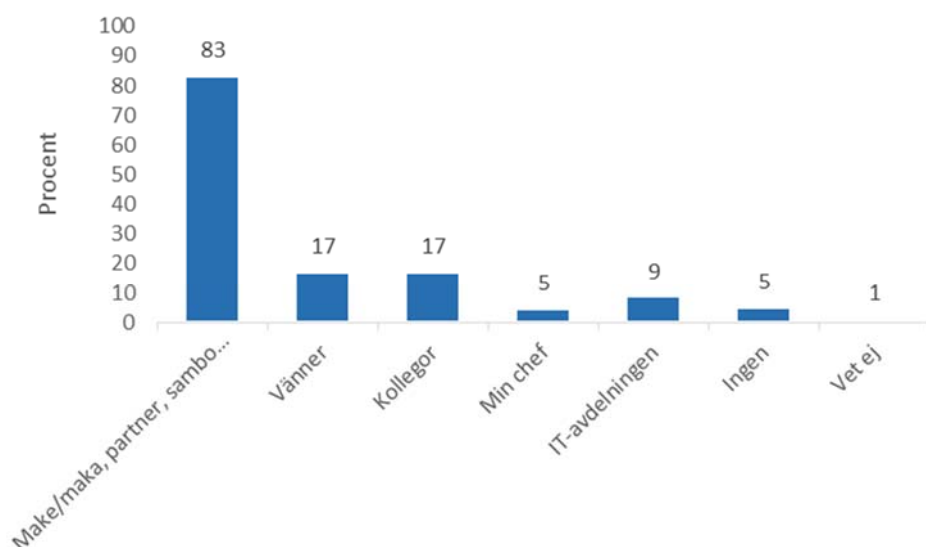


Figur 8. Delar med sig av lösenord till andra

Det är väldigt positivt att majoriteten anger att de aldrig delar med sig av lösenord till andra, en femtedel säger dock att de gör det, men gör det sällan, ett fåtal anger att de gör det ibland, men inte någon av de tillfrågade anger att de gör det ofta. Vår rekommendation är att inte dela lösenord med andra utan att ha ett riktigt gott skäl. Vi tror dock att de som svarat på frågan inte har tagit med pin-koder till kredit- eller betalkort, pin-koder till smarttelefoner eller surfplattor i kalkylen. Där finns det anledning att tro att många delar med sig till barn och respektive för att gå och handla med kreditkort, spela spel på telefonen eller plattan med mera.

### 03.1.9 Till vem delar du med dig av dina lösenord?

Antalet dataintrång ökar för varje år. Om det inte beror på faktiska hackerattacker där lösenord eller lösenordsdatabaser läckt ut beror det på att man har delat med sig av lösenord till någon annan. En kategori är före detta partners som vill förstöra för sina ex. Det sker relativt ofta att personer som tidigare haft en relation och där den har avbrutits missbrukat den andra partens lösenord för att hämnas eller göra skada. Det är oerhört viktigt att byta lösenord när man byter partner eller vän om man inte vill utsätta sig för risken att bli smutskastad på nätet. Byt alltid lösenord när du byter partner. Bästis är för alltid kan snabbt vända till svurna fiender.



Figur 9. Till vem delar man med sig av lösenord?

Föga förvånande alltså, de som delar med sig av sina lösenord gör det oftast till make/maka, partner, sambo eller motsvarande. Vänner och kollegor verkar också kunna få förtroendet att ta del av lösenord. Några anger att de delar med sig av lösenord till chefen och – kanske mer överraskande – till IT-avdelningen. Ingen verkar dela med sig av sina lösenord till banken, polisen, leverantörer eller till vem som helst.

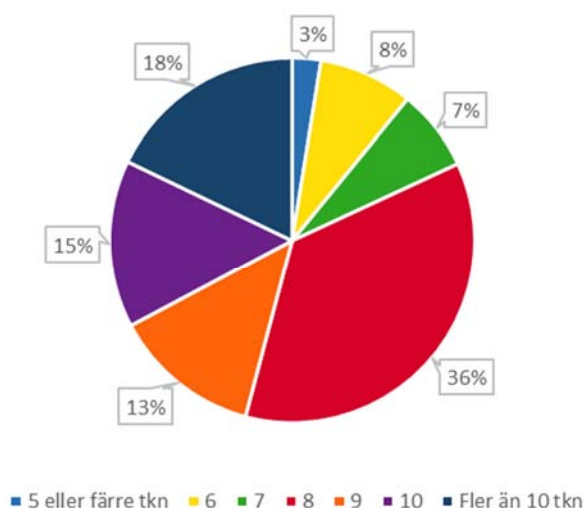
Män och kvinnor är lika benägna (eller obenägna) att dela med sig av sina lösenord, men av de som faktiskt gör det är det vanligare bland männen att de delar med sig till sina vänner och bland kvinnorna att dela med sina kollegor.

#### 03.1.10 Hur många tecken brukar du använda i dina lösenord?

Detta är en intressant fråga eftersom möjligheten till variation ökar med antalet tecken, samtidigt som möjligheten att knäcka ett lösenord minskar signifikant med varje tecken som läggs till.

Det är glädjande att kunna konstatera att nästan hälften väljer att ha lösenord som är längre än 8 tecken. Samtidigt är det alltså drygt hälften som har lösenord som är 8 tecken eller kortare vilket radikalt ökar risken för att få dem röjda. Den som använder kortare lösenord än 8 tecken bör allvarligt överväga att ändra sin strategi och byta till längre lösenord.



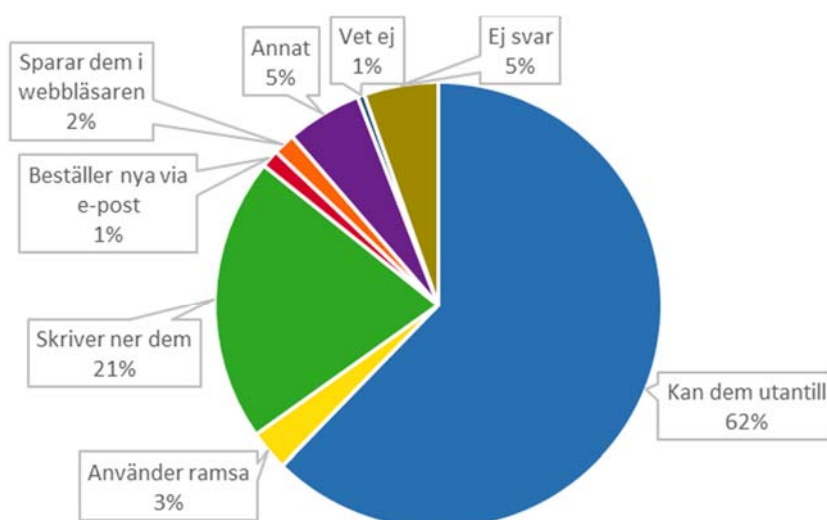


Figur 10. Antal tecken som brukar användas i lösenord

Här kan vi även urskilja en viss skillnad mellan könen. En större andel män (21 procent) använder längre lösenord med fler än 10 tecken medan motsvarande andel för kvinnorna är 12 procent. Förklaringen kan stå att finna i att det är fler män (12 procent) än kvinnor (5 procent) bland de svarande som kommer från IT- och kommunikationsbranschen, och vi har redan konstaterat att det är i den gruppen man har de längsta lösenorden.

### 03.1.11 Hur gör du oftast för att komma ihåg dina lösenord?

Vi vet alla att detta är en del av vår tids gissel, att behöva hålla reda på mängder av lösenord och koder. Så hur gör svenskarna för att komma ihåg sina?

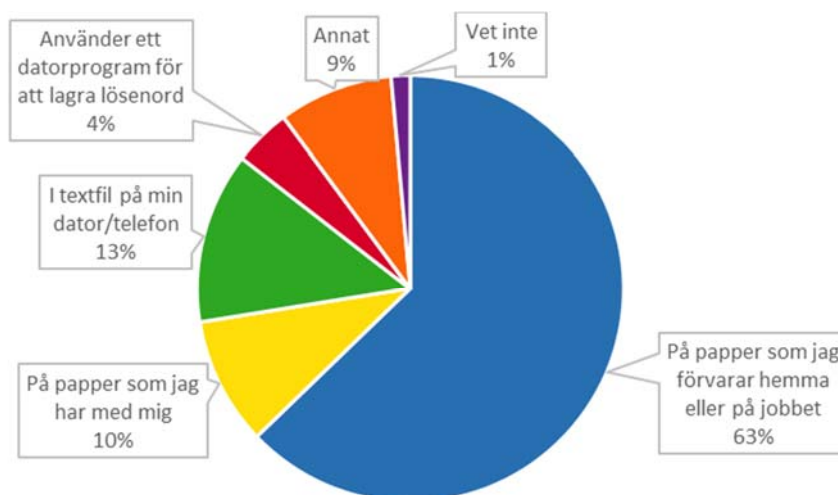


Figur 11. Metod för att hantera lösenord

Färre än väntat beställer nya via e-post. Uppenbarligen är vi svenskar duktiga på att lära oss utantill men påfallande många skriver ner sina lösenord.

### 03.1.12 Om du skriver ner dina lösenord, hur sparar du dem?

Det här med att skriva ner sina lösenord är inte någon dålig idé, bara man förvarar informationen på ett säkert sätt, som den värdehandling den faktiskt är. Allra bäst är det att använda en lösenordshanterare som stöd.

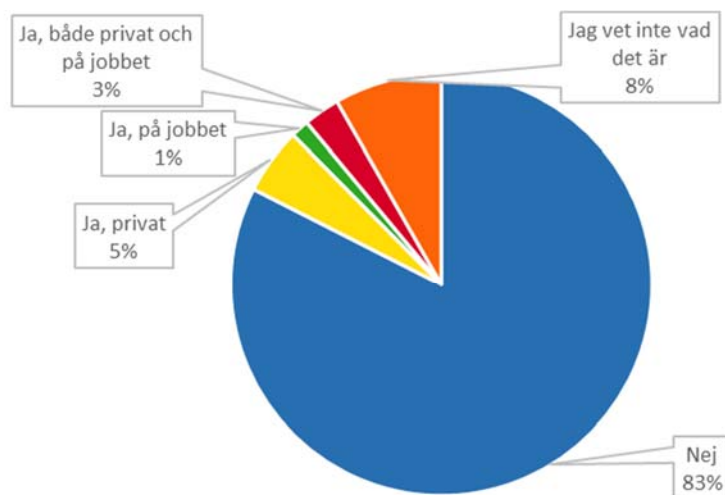


Figur 12. Hur sparas nedskrivna lösenord

Av de tillfrågade svarade omkring en femtedel att de skriver ner sina lösenord för att komma ihåg dem, och på frågan om hur de sparas är det vanligaste svaret att man har dem på papper som förvaras hemma eller på jobbet. En tiondel bär pappret med lösenord med sig och ungefär lika många lagrar lösenorden i en textfil på sin dator eller telefon. Endast ett fåtal anger att de använder ett datorprogram för att lagra lösenord, en så kallad lösenordshanterare.

### 03.1.13 Använder du en lösenordshanterare?

Vi konstaterade redan i förra frågan att mycket få använder ett datorprogram för att lagra lösenord, fyra av fem gör det inte. Hur ser det ut bland de som faktiskt använder ett program som stöd för lösenordshanteringen?

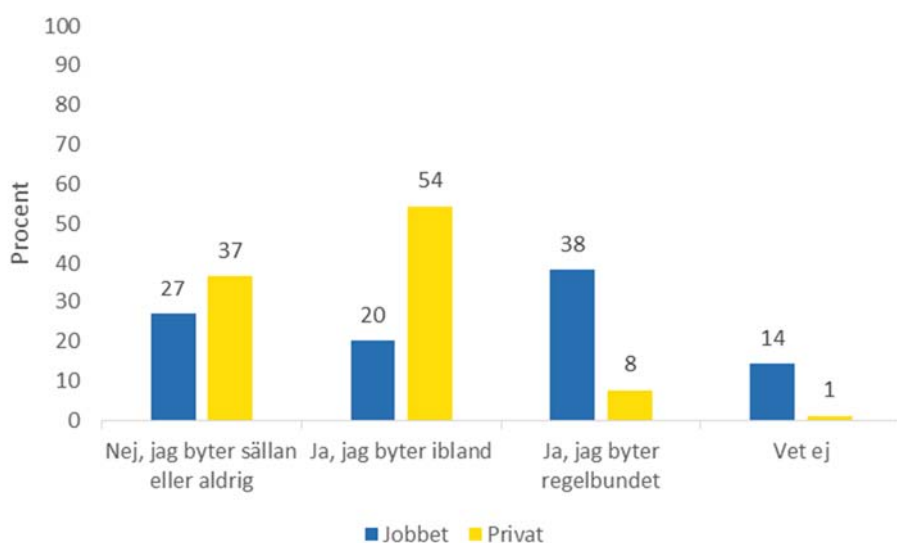


Figur 13. Använder lösenordshanterare

Fem procent anger att de använder lösenordshanterare privat och ännu färre använder en lösenordshanterare på jobbet (1 procent). Ett fåtal procent använder lösenordshanterare både privat och på jobbet. Åtta procent av de tillfrågade har svarat att de inte vet vad en lösenordshanterare är. Vi rekommenderar starkt att man använder en lösenordshanterare både privat och på jobbet. Med en sådan behöver användaren bara komma ihåg ett enda lösenord, och får bra stöd för att generera starka och slumpmässigt valda lösenord.

#### 03.1.14 Brukar du byta lösenord för privat bruk och på jobbet

Det finns en väldigt seglivad tradition inom lösenordshantering som säger att man ska byta lösenord både ofta och regelbundet, en regel som rapportförfattaren och många med henne har försökt komma ifrån under det senaste decenniet.



Figur 14. Byter lösenord regelbundet

När vi tittar på hur vanligt det är att man byter lösenord för privat bruk så är det en dryg tredjedel som sällan eller aldrig byter medan drygt hälften byter ibland och några få byter regelbundet.

Om vi ställer samma fråga när det gäller lösenord på jobbet är bilden en annan. Där är det en dryg fjärdedel som säger att de sällan eller aldrig byter, en femtedel byter ibland medan hela 38 procent byter regelbundet.

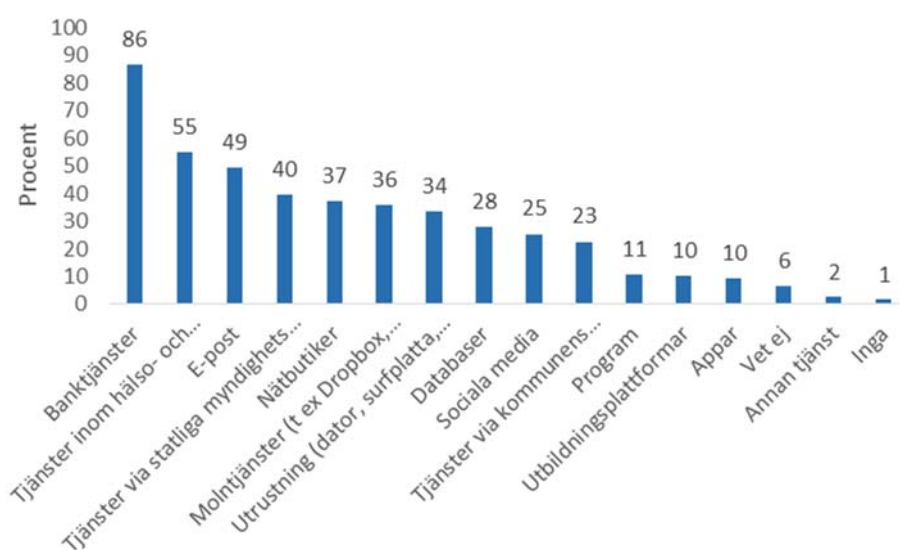
De tillfrågade har haft möjlighet att med egna ord berätta om anledningen till att man byter lösenord dels privat, dels på jobbet/skolan. Det som är slående är att skälen som anges för att byta lösenord privat i första hand är att man vill höja säkerheten och minska riskerna för intrång och läckage eller att man har glömt bort sitt lösenord och därför måste byta till ett nytt, medan det absolut dominerande skälet att byta på jobbet/skolan är att man tvingas till det av regler och system.

Det förefaller som om skälen att byta lösenord för privat bruk är mer förankrade i en riskbedömning och ett behov som användaren själv har kommit fram till, medan motsvarande för jobbet är regelstyrt och att man där egentligen inte reflekterar kring varför man byter.

Att regelmässigt tvingas byta lösenord är ett problem som leder till att användare väljer alltför enkla lösenord.

### 03.1.15 Vilka tjänster anser du behöver extra starka lösenord?

Vi tittade på vad man anser vara tjänster som behöver extra starka lösenord både generellt och ur ett branschperspektiv. De kategorier som kunde väljas var banktjänster, tjänster inom hälso- och sjukvården, e-post, tjänster via statlig myndighets webbplats, nätbutiker, molntjänster (till exempel Dropbox, Googledocs, iCloud, utrustning (dator, surfplatta, telefon), databaser, sociala media, tjänster via kommunens webbplats, program, utbildningsplattformar, appar, annan tjänst eller ingen. Alternativet vet ej kunde också anges.



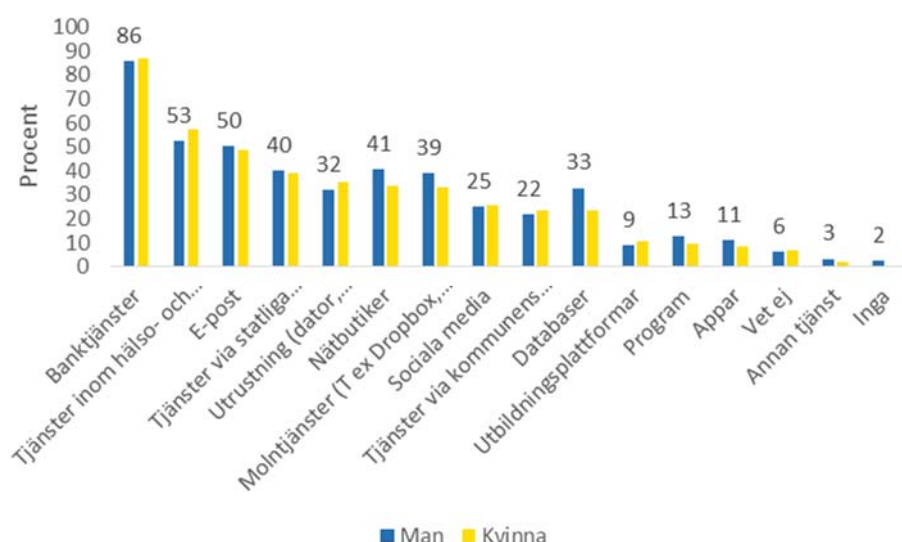
Figur 15. Tjänster som behöver extra starka lösenord

Det finns alltid information som har varierande skyddsvärde och ibland är det kanske till och med onödigt att ta till starka och komplexa lösenord om det inte är någon särskilt känslig information som behöver skyddas. När vi ställer frågan om vilka tjänster som anses behöva extra starka lösenord är svaren inte oväntade. I topp ligger banktjänster och tjänster inom hälso- och sjukvården medan program, appar och utbildningsplattformar inte anses vara tjänster som kräver extra starka lösenord. Fördelningen framgår av diagrammet ovan.

Det är fascinerande hur framgångsrika bankerna har varit i att övertyga sina kunder om att bankkonton är det absolut mest skyddsvärda man har. Vår uppfattning är dock att bankerna oftast hjälper kunden att få tillbaka pengarna vid eventuella bedrägerier (om man inte varit gravt oaktsam), medan komprometterande fotografier eller videofilmer som läcker och sprids i sociala media med stor sannolikhet skulle skapa större problem för en individ, och i princip är omöjliga att få bort.

När vi granskar svaren med utgångspunkt från vilken bransch de tillfrågade angett att de tillhör konstaterar vi att finanssektorn sticker ut en smula åt det mer negativa hållet. Där använder man exempelvis inte starkare lösenord till tjänster man anser behöver skyddas extra mycket. Dessutom är det vanligare att personer i finansbranschen återanvänder lösenord, framför allt privat, men även på jobbet. De är också mer benägna att dela med sig av lösenord i den branschen än inom någon av de andra, i synnerhet till kollegor.

Vi kan dock inte dra för stora slutsatser kring svaren från finansbranschen eftersom gruppen är relativt liten. Men det kan trots allt finnas ett visst mått av sanning bakom och det väcker en viss nyfikenhet hur det faktiskt ser ut. Men för en sådan analys behöver vi göra en mer omfattande undersökning.

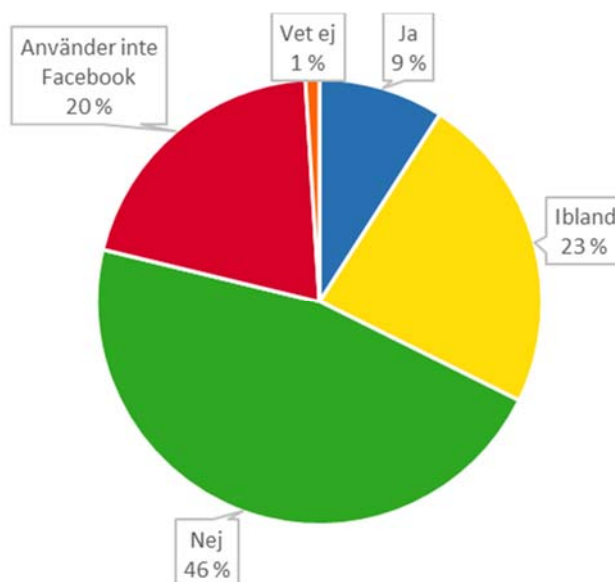


Figur 16. Mäns och kvinnors uppfattning om vilka tjänster som behöver extra starka lösenord

Tittar vi på mäns och kvinnors uppfattning om vad man anser vara tjänster som behöver extra starka lösenord så går det inte att se några större skillnader mellan könen.

### 03.1.16 Brukar du använda din inloggning till Facebook för att logga in på andra tjänster?

Idag erbjuder flera tjänster inom bland annat sociala media möjlighet att via dem få inloggning till andra tjänster. Vi ställde frågan om man brukar använda Facebook för att logga in på andra tjänster.



Figur 17. Använder Facebook för inloggning i andra tjänster

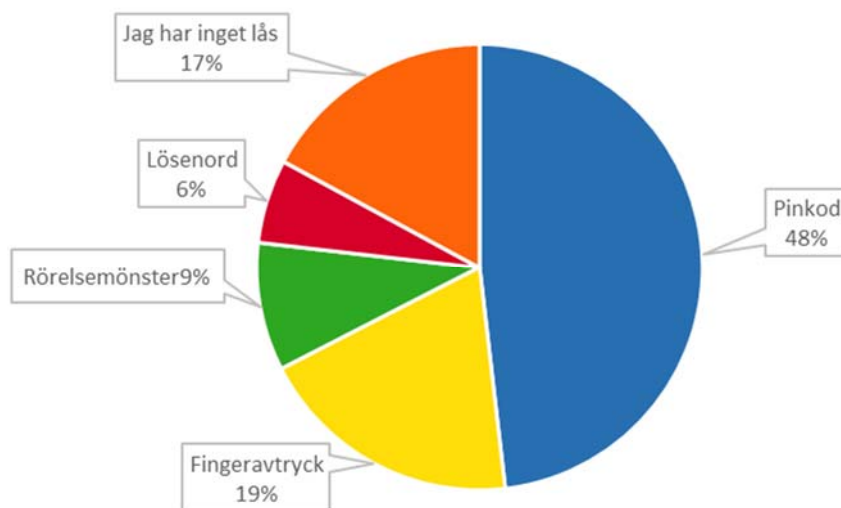
Av de tillfrågade svarar nära hälften nej. Nio procent anger att de använder möjligheten och ungefär en fjärdedel gör det ibland. En femtedel av de tillfrågade har inget konto på Facebook. Av det drar vi slutsatsen att det trots allt är rätt många som använder sig av möjligheten.

Det går alltså att använda sitt Facebook-konto för inloggning på andra webbplatser och applikationer som erbjuds av en tredje part. Dessa använder Facebooks plattform och måste därmed följa de riktlinjer som gäller. Det är dock viktigt att kontrollera att det öppnas ett separat fönster i webbläsaren när man klickar på inloggningsknappen, och att webbadressen för det fönstret innehåller rätt domän så att det är en giltig Facebook-sida och inte ett försök till nätfiske.

Metoden kan i vissa fall vara att föredra då vi de facto ser att många företag, stora som små, brister i hanteringen av inloggningsuppgifter. Samtidigt innebär det att information om vilka tjänster du loggar in på och använder samlas hos en och samma aktör.

### 03.1.17 Hur låser du upp din mobil?

Väldigt många använder idag sin smarttelefon som plattform för att komma åt det mesta som till exempel bankkonton, sociala media och andra mer eller mindre känsliga tjänster för spel och underhållning. Mobilen har kommit att bli en plats där man förvarar känslig information, utan att reflektera över vilka konsekvenserna blir om någon skulle komma över den. Det finns olika metoder som kan användas för att låsa och låsa upp mobilen.



Figur 18. Metod för att låsa upp mobil

Hela 17 procent anger att de inte har något lås alls på mobilen. Så stor andel som 13 procent av de som på en tidigare fråga svarade att de skriver ner sina lösenord anger att de använder en textfil på mobilen för att spara dem. Det innebär att mobilen innehåller en hel del känslig information som är värd att skydda.

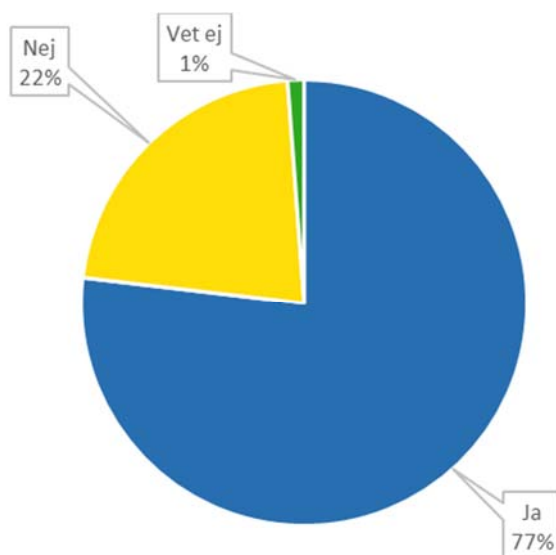
Den dominerande metoden för att låsa upp mobilen är pinkod som används av nästan hälften av de tillfrågade. Fingeravtryck och rörelsemönster är det relativt få som använder, lösenord ännu färre. Vi ställde inte någon fråga om hur många tecken som används för pinkoder. Teoretiskt finns det 10 000 möjliga kombinationer för fyra siffror vilket såvitt vi vet är det vanligaste i dagsläget. Forskning visar dock att det är färre än 100 av dessa 10 000 kombinationer som används regelmässigt. Människor är, kan vi återigen konstatera, inte bra på att göra slumpmässiga val. Vid en enkel rundfråga bland unga högskoleelever visade det sig att medan tjejer gärna väljer sitt födelseår som pinkod väljer killar mer nördiga saker som 1337.<sup>3</sup>

### 03.1.18 Använder du mobilt bank-ID?

Mobilt bank-ID är en tjänst som har vunnit mark under de senaste åren. Ju mer tjänsten används, desto mer beroende blir vi användare av den, och desto känsligare blir den givetvis för eventuella avbrott och attacker. Ofta erbjuds inte heller något alternativ hos de tjänster som använder mobilt bank-ID som inloggningsmetod. Det kan innebära att mobilt bank-ID närmar sig en nivå där den utgör en så kallad felkritisk systemdel (single-point-of-failure), om vi inte

<sup>3</sup> <https://en.wikipedia.org/wiki/Leet>

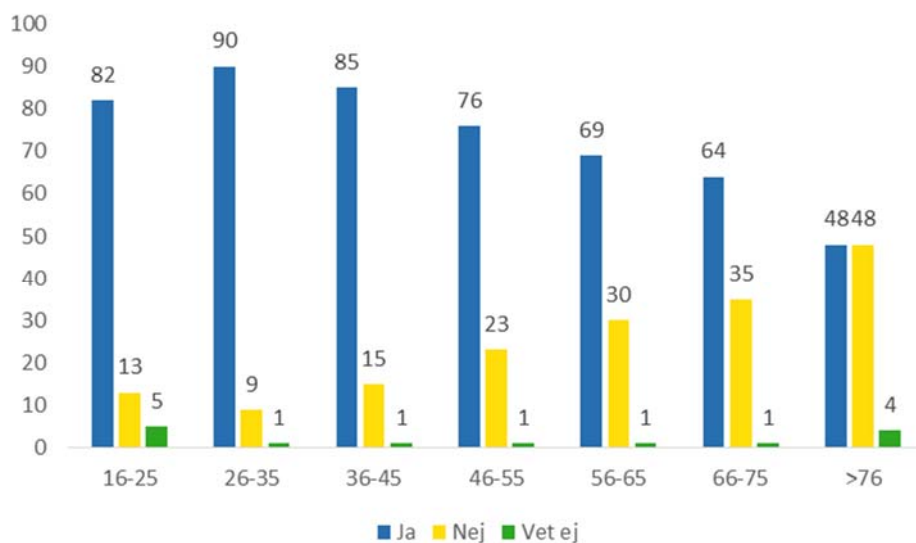
redan är där. Kännetecknande för en sådan systemdel är att den utgör en del av ett it-system som måste fungera för att systemet som helhet, eller särskilt viktiga funktioner i systemet, ska fungera. Om den svaga punkten havererar fungerar inte systemet eller så går det inte att använda på något meningsfullt sätt. Det innebär att konsekvenserna blir omfattande om någon sorts haveri skulle inträffa med mobilt bank-ID.



Figur 19. Använder mobilt bank-ID

På frågan om man använder mobilt bank-ID svarar majoriteten jakande. Endast 22 procent anger att de inte gör det.

Ser vi på åldersfördelningen bland användare av mobilt bank-ID framgår att det är vanligare bland yngre, flest användare finns i åldrarna 26-45 år.



Figur 20. Åldersfördelning hos användare av mobilt bank-ID



## 04. Lösenordens tio i topp-lista

Genom att lösenordsdatabaser läcker med jämna mellanrum går det också att analysera vilka som är de vanligaste lösenorden. Man måste förundras över den bristande fantasi och variationsrikedom som normalanvändaren uppvisar.

Varje år genomförs olika undersökningar, bland annat en av ett företag som heter SplashData som sätter ihop en topplista över de vanligaste lösenorden som läckt på internet det gångna året. I allmänhet är det lösenord som hackare har lyckats hitta och publicerat.

Att databaser med användaruppgifter läcker publikt är vardagsmat och det handlar inte bara om små sajter med bristande säkerhetstänkande, det är också vanligt att riktigt stora aktörer har dataläckage där användaruppgifter läcker, inklusive namn, e-postadresser, lösenord och kreditkortsnummer. Några exempel är Adobe, LinkedIn, Sony<sup>4</sup>.

De tio absolut vanligaste lösenorden 2012-2015 är enligt SplashData:

År				
Position	2012	2013	2014	2015
1	password	password	123456	123456
2	123456	123456	password	password
3	12345678	12345678	12345	12345678
4	abc123	abc123	12345678	qwerty
5	qwerty	qwerty	qwerty	12345
6	monkey	monkey	123456789	123456789
7	letmein	letmein	1234	football
8	dragon	dragon	baseball	1234
9	111111	111111	dragon	1234567
10	baseball	baseball	football	baseball

Figur 21. Vanligast förekommande lösenorden 2012-2015

Som synes har det inte ändrat sig nämnvärt över fyraårsperioden och skulle förmodligen se likadant ut även om vi gick ännu längre tillbaka i tiden. Eftersom internet är globalt och många tjänster internationella går det inte att urskilja svenska användare ur de läckta databaserna på något enkelt sätt. Däremot finns det databaser med användaruppgifter som har läckt från svenskspråkiga sajter med tjänster som vänder sig till en svensk publik.

<sup>4</sup> [Http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)

Nedan listas de 25 vanligaste lösenorden bland svenska användare och hur många konton som använde respektive lösenord (med reservation för att demografin hos användarna av de tjänster varifrån de läckt kan misstänkas vara något snedvriden - mest yngre män).

Lösenord	Antal konton som använder
123456	3 478
12345	1 878
knulla	756
qwerty	702
666666	689
hejsan	587
stilet	521
123456789	503
12345678	455
password	437
mamma	388
volvo	387
sommar	361
hejhej	325
niklas	316
bajskorv	315
gnaget	314
artto	300
kungen	300
kalle	297
sverige	291
general	287
kalleanka	285
kuken	274
123123	258
cocacola	249

Figur 22. Vanligaste lösenorden bland svenska användare

Vi kan alltså konstatera att svenska användare tyvärr inte verkar vara det minsta bättre än andra nationaliteter på att välja lösenord. Sorgligt men sant. 123456, password och qwerty, alla finns med. Vi ser inget avvikande mönster i jämförelse med den "globala" tio i topp-listan, med undantag för exempelvis de svenska sex- och könsorden. Som kurios i sammanhanget tror vi att lösenordet general har uppstått ur den svenska snustraditionen. General är trots allt Sveriges mest sålda snus.

## 05. Lösenordens historia

Behovet av att reglera tillgång till information, informationstjänster och informationssystem har alltid funnits, men behovet har ökat de senaste decennierna i takt med ökade möjligheter till kommunikation över internet. Behovet av åtkomstskydd varierar beroende på vilken information som hanteras, men generellt gäller att information sällan är så betydelselös att den inte behöver någon typ av skydd.

### 05.1 Så började det

1961 introducerade MIT (Massachusetts Institute of Technology) lösenord så att flera personer kunde använda ett delat datorsystem. Varje användare behövde ett individuellt lösenord för att få åtkomst till systemet och tiden som användaren var aktiv registrerades.

Alla lösenord lagrades i systemet och säkerheten byggde på att ett allt större antal medarbetare som deltog i delandet av samma system förstod vad det hela gick ut på, att skydda information från obehörig åtkomst. Begreppet åtkomstskydd var fött.

1962 klurade en forskare på MIT ut hur han kunde skriva ut lösenordslistan med syftet att kunna logga in som en annan användare och därmed få tillgång till systemen mer än de fyra timmar som var standardtilldelningen. Och den första hackaren var född.

1970 utvecklades det som kallas för hashning med vars hjälp systemet översätter ett lösenord till ett numeriskt värde som innebär att lösenordet krypteras och alltså inte lagras i systemet i klartext. Dagens system använder fortfarande kryptering av lösenord i kombination med salt, ett slumpmässigt tillägg till ett lösenord som gör det svårare för en angripare att lista ut det riktiga lösenordet (läs mer om det i avsnitt 6, Lösenordens anatomi).

## 06. Lösenordens anatomi

Ett lösenord är en teckensträng som anges vid identifiering av användare, ofta i samband med inloggning. I lösenordssammanhang skiljer man på versaler och gemener på så sätt att en och samma semantiska sträng kan representera två unika lösenord. Password123 och password123 är två lösenord som är unika för de flesta operativsystem och applikationer. Ett antal användare skulle förmodligen säga att det är samma lösenord om de fick frågan.

Ett lösenord kan vara skapat av användaren själv, av systemet eller en kombination av båda. Karaktären på lösenorden är ofta en kompromiss mellan att vara användarvänliga (möjliga att komma ihåg) och tillräckligt säkra (svåra för någon annan att gissa).

Det finns två typer av lösenord, statiska och dynamiska. Statika lösenord kan användas flera gånger och dynamiska lösenord är lösenord som bara kan användas en gång och därefter är förbrukade.

Vanligen skapas en kryptografisk kontrollsumma, en hash, av lösenordet som förvaras på den server som kontrollerar lösenordet då en användare loggar in. Så länge filen med krypterade lösenord (lösenordshashar) är skyddad kan serverprogramvaran begränsa antalet gissningar per tidsenhet, till exempel tre försök på tre sekunder, det vill säga ungefär hundratusen gissningar per dygn.

Om en angripare däremot kommer över en fil med krypterade lösenord offline och kan bearbeta den på en egen dator kan hundratals miljarder gissningar per sekund göras, beroende på vilken algoritm som använts för att kryptera lösenordet, vilka datorresurser angriparen förfogar över med mera. En ofta använd algoritm för att skapa krypterade lösenord är SHA1, en algoritm som vi idag vet är mycket svag och enkel att knäcka. Osaltade SHA1 lösenord är en barnlek att knäcka med en vanlig persondator och ett kraftigt grafikkort av den typ som är vanligt för att spela dataspel. Ofta används därför också så kallat *salt* för att tvinga angriparen att pröva lösenorden skilt för varje användare.

Ett salt är ett slumpmässigt tillägg till ett lösenord som gör det svårare för en angripare att lista ut det riktiga lösenordet. Saltet tilldelas varje användare unikt och ligger dolt i användarens profil. När användaren väljer lösenord skapar systemet först en kontrollsumma av lösenordet (matematik). Saltet adderas och systemet beräknar en ny kontrollsumma som blir det krypterade lösenord som sparas i databasen. Varje gång användaren loggar in genomför systemet samma beräkning av lösenordet som användaren matar in och kontrollerar att det överensstämmer med det som finns lagrat i databasen.

Eftersom lösenorden inte uttryckligen finns i databasen, utan bara bildar kontrollsummor så blir de obrukbara och värdelösa vid en eventuell stöld.

### 06.1 Varför statiska lösenord är vanligare än dynamiska

Statika lösenord är det ojämförligt billigaste och enklaste sättet att identifiera användare. Trots teknikutvecklingen och allt mer komplexa system är det fortfarande statiska lösenord som i de allra flesta fall är standardlösningen för att

kontrollera åtkomst till information och tjänster. Kanske är det inte så svårt att förstå, det kräver ingen extrautrustning och är lätt att implementera. Därför har det varit svårt att konkurrera med andra och säkrare lösningar. Statiska lösenord är inte heller automatiskt dåligt, det är sättet vi använder dem på som har brister.

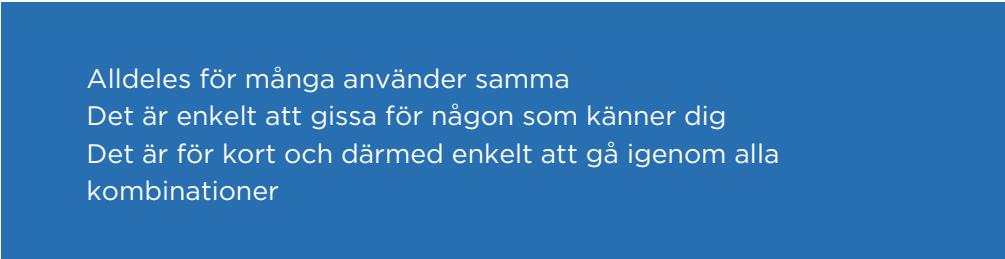
Det skydd ett lösenord erbjuder behöver inte heller alltid vara säkert bara för att lösenordet är starkt, det kan ibland kringgås. Datorer och mobila terminaler innebär speciella utmaningar som möjligheten till avlyssning av trafik, loggning av tangenttryckningar och även återställningsfunktioner som ibland kan användas för att komma runt kravet att ange ett lösenord. Sårbarheter i programvaror kan också användas för att komma runt lösenord.

## 06.2 Dåliga lösenord

Dåliga lösenord är inte bara dåliga, de är också de vanligaste lösenorden. Varför just dessa är de vanligaste beror på att de är lätta att skriva och lätta att komma ihåg. Det är mänskligt att försöka göra det lätt för sig, människor är av naturen ganska lata. Dessvärre går enkelhet och säkerhet inte alltid ihop, något som är särskilt sant när det gäller lösenord.

Vi blir fler och fler användare som använder fler och fler tjänster på fler och fler enheter. Även hackarverktygen blir fler och mer sofistikerade för varje år. Det enda som inte följer trenden och blir bättre med tiden är kvaliteten på lösenorden.

Enkelt uttryckt, ett dåligt lösenord kännetecknas av att de har ett eller flera av följande karakteristika:



Alldeles för många använder samma  
Det är enkelt att gissa för någon som känner dig  
Det är för kort och därmed enkelt att gå igenom alla  
kombinationer

### 06.2.1 Användargenererade lösenord och lösenfraser

Ett lösenord eller en lösenfras som en användare själv hittar på är i allmänhet sämre än ett som genereras automatiskt av en process i en dator.

När säkerhetsexperter pratar om styrkan hos lösenord nämner de ofta entropi, vilket enkelt uttryckt representerar antalet slumpmässiga gissningar som krävs för att lista ut och knäcka ett lösenord. Ju högre entropi, desto bättre.

Entropi är alltså ett mått på styrkan i lösenordsgenereringen och brukar uttryckas i antal bitar. Ett lösenord med 8 tecken som väljs ut bland en teckentabell med 83 tillgängliga tecken har en entropi på 51 bitar, medan det om längden ökas till 10 tecken har en entropi på 63 bitar, alltså 12 bitar mer.

Anta att du har en tabell med alla tillgängliga tecken (stora och små bokstäver, siffror och specialtecken innebär med det latinska alfabetet 96 unika tecken):

Antal tecken (bas 96 tecken)	Möjliga kombinationer
2	9 216
3	884 736
4	85 miljoner
5	8 miljarder
6	782 miljarder
7	75 triljoner
8	7,2 kvadriljoner

Figur 23. Möjliga kombinationer av lösenord

Anta sedan att du väljer 8 tecken, slumpmässigt från listan, då har du 7,2 kvadriljoner kombinationer att välja bland. Antalet kombinationer kan förstås komma att begränsas av ytterligare restriktioner som till exempel att ett tecken inte får förekomma mer än en gång.

Vissa personer föredrar lösenfraser och menar att dessa både är svårare att knäcka och samtidigt lättare att komma ihåg. Med lösenfraser blir längden viktigare för att åstadkomma högre säkerhet i form av högre slumpmässighet. I fallet med lösenfraser är det viktigt att utgå från en relativt stor ordlista.

Att vissa ord är korta och andra är långa, några är pluralformer eller vissa är mer lockande än andra, har i det här fallet ingen som helst inverkan på entropin.

Entropi är alltså en egenskap hos genereringsprocessen, och medan en automatisk maskinell genereringsprocess inte lägger någon som helst vikt vare sig vid längden på eller tjusningen hos ett specifikt ord har det visat sig att vi människor helt enkelt är dåliga på slumpmässighet och att användargenererade lösenord och lösenfraser därför i allmänhet ger lägre säkerhet än de automatiskt genererade. Även om den genomsnittliga mänskliga användaren försöker använda hjärnan tenderar de att välja vissa ord oftare än andra.

På internet finns en tjänst som hjälper användaren att välja slumpmässiga ord för lösenfraser med användning av en vanlig tärning, Diceware.<sup>5</sup> Tjänsten bygger på en ordlista som tagits fram och som tar hänsyn till språk, förekomsten av dubbeltydiga ord och synonymer med mera. Listan finns publicerad på sajten, och varje ord i listan representeras med ett femsiffrigt nummer. Alla siffror i numret är mellan ett och sex vilket skapar en möjlighet att välja ett ord för lösenfrasen utifrån fem slagningar med en tärning, eller en slagning med fem tärningar. Proceduren upprepas för varje ord till dess att man har det antal ord man önskar. Diceware har publicerat ordlistor på en rad olika språk; katalanska, danska, nederländska, esperanto, finska, franska, tyska, italienska, japanska, maori, norska, polska, ryska, spanska, svenska och turkiska.

<sup>5</sup> <http://world.std.com/~reinhold/diceware.html>

## 06.3 Riktigt dåliga lösenord

Vissa kombinationer är särskilt dåliga att välja som lösenord om man använder dem var och en för sig. En kombination av flera dåliga varianter kan ändå bli ett bra lösenord. Nedan följer några exempel på särskilt dåliga val. Medan vissa lämpar sig för riktade attacker är andra mer lämpliga för slumpmässiga attacker.

### 06.3.1 Tangentbordskombinationer

En del tycker att de är listiga när de använder tangentbordskombinationer som lösenord, som till exempel querty, qazwsx, asdfgh, 1qaz2wsx. Ni ser mönstret? Det är dåliga lösenord, och något bland det första en angripare provar när det ska gissas lösenord.

### 06.3.2 Ord och begrepp i lexikon

Ord och begrepp som finns i lexikon, varumärken, geografiska namn är dåliga lösenord. Jordgubbar, Volvo, Stockholm går alltså bort. Den typen av lösenord är särskilt sårbara eftersom de finns de verktyg som används för ordboksattacker som provar alla ord som förekommer i större språkgrupper.

### 06.3.3 Personnamn och smeknamn

Personnamn och smeknamn som har anknytning till din egen person, dina fritidsintressen är inte heller lämpliga som lösenord som till exempel Zlatan10 (för den som gillar fotboll), skidkungen (för den som ägnar sig åt skidåkning), roadrunner (för den som gillar att springa långt), Superman (för den som gillar superhjältar), Shakespeare (för den som gillar klassisk litteratur) och så vidare. I princip **allt** kultur- och sportrelaterat är dåliga lösenord om det inte är väldigt lokalt och på ett mindre vanligt språk.

### 06.3.4 Namn på husdjur, barn och partner

Namn på egna husdjur ska man också välja bort som lösenord, liksom barnens namn, partners, film-, musik-, idrotts- eller andra typer av namn på kändisar likaså.

### 06.3.5 Svordomar och sex

Svordomar och sexrelaterade ord är också relativt vanliga och därmed lätta att försöka sig på att prova när man ska gissa lösenord. Hur kittlande det än är att skriva något snuskigt på tangentbordet varje gång man loggar in är det bättre att låta bli.

### 06.3.6 Minnesvärda datum

Speciellt minnesvärda personliga eller internationellt välkända datum är dåliga lösenord som din egen bröllopsdag, födelsedag, när andra världskriget började eller tog slut, nineeleven et cetera.

### 06.3.7 Teckensubstitution

Eftersom en del webbsajter med tiden krävt större variation än bara bokstäver när någon ska välja lösenord så har en del användare försökt lösa det genom att använda substitution av vissa tecken så att exempelvis O=0, L=1, A=4, S=5, G=6, T=7. Det beteendet är numera så vanligt förekommande och så allmänt känt att det till och med finns inbyggt i knäckningsverktygen att prova sådana kombinationer. Det bidrar alltså inte särskilt mycket till att öka säkerheten.

### **06.3.8 Standardlösenord**

Lösenord kan betraktas som säkra bara om de hålls hemliga och inte delas med någon. Ofta finns det standardlösenord som är satta från början på till exempel hemmaroutrar och andra tekniska apparater. Dessa är väl kända och publiceras ofta på öppna forum. Därför är det en viktig regel att byta standardlösenord så fort man tar någonting i bruk, även om det inte kommer någon automatisk uppmaning om att göra det.

Standardlösenord sätts ofta till password, admin, welcome, letmein eller guest. Därför bör du inte heller välja något av dessa som ditt personliga lösenord. De tillhör utan tvekan bland de första som en angripare kommer att försöka med när de ska gissa lösenord.

### **06.3.9 Övriga mindre lämpliga val**

Använd aldrig nuvarande eller tidigare telefonnummer, organisationsnummer, personnummer, registreringsskyltar med mera.

Lösenord som är relaterade till tjänsten du vill logga in på är också relativt sett mindre bra, hoppa därför över Facebook111, InstaGram, photoshOp, TwittrFlatrr, Adobe.pdf....



## 07. Konsekvenser av lösenordsläckor

Mängder av lösenordsdatabaser, mer eller mindre väl skyddade, har läckt genom åren. Spelar det någon roll? Hur används de? I det här avsnittet redovisar vi några av de mest kända fallen.

### 07.1 Vad har hänt

Samma sak har upprepats otaliga gånger och med ibland enorma informationsläckage inom och utanför Sveriges gränser.<sup>6</sup> Lösenordsdatabaser läcker ut, det sköljer en våg av artiklar, synpunkter, råd och rekommendationer över användarna. Efter varje händelse pratar hela Sverige it-säkerhet under några dagar. Användarna ruskar dock relativt snabbt av sig obehaget och går vidare. Med samma dåliga lösenord och vanor som tidigare. Här följer några stora exempel på lösenordsläckor och konsekvenserna av dessa händelser.

#### 07.1.1 Bloggtoppen med flera

År 2011 hackades sajten Bloggtoppen.se (tillsammans med 57 andra svenska sajter) och runt 180 000 konton (uppgifterna varierar något) med inloggningsuppgifter och lösenord kom på vift. I vissa fall har även personnummer publicerats.

Den första datafilen med lösenord publicerades den 15 augusti på Twitter. Uppgifterna kom alltså från ett stort antal sajter förutom bloggtoppen.se, allt från musiksidan emusic.se till släktforsarsajten genealogi.se.

De drabbade var i allra flesta fall helt vanliga privatpersoner, men också riksdagsmän och andra politiker fick sina kontouppgifter röjda. Uppgifterna från det hacket användes bland annat för att hacka sig in på en känd politikers Twitterkonto och posta uppmärksammade uttalanden.

Därefter följde gratisbio.se med över 200 000 medlemmars okrypterade lösenord som lades ut på nätet. Via både Twitter och Flashback spreds länkar med kändisars, journalister och riksdagsledamöters mejladresser och lösenord. En stor skillnad jämfört med Bloggtoppen.se var att lösenorden inte var krypterade utan lagrade i klartext i databasen.

#### 07.1.2 Rockyou

2010 knäcktes lösenordsdatabasen till en stor tjänst vid namn Rockyou. En databas med 32 miljoner lösenord läckte. Eftersom lösenorden var lagrade i klartext behövde ingen anstränga sig för att räkna ut vilket lösenord en viss användare hade. I det här fallet spelar det ingen roll hur duktig du som användare är på att skapa starka lösenord. Om tjänsten inte förmår att skydda dina användaruppgifter, inklusive lösenord, på ett adekvat sätt så läcker ditt starka lösenord. En sådan databas är en guldgruva och en ovärderlig tillgång för hackare som försöker hitta nya metoder att knäcka lösenord i framtiden.

---

<sup>6</sup> <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

### 07.1.3 Sony Playstation

I april 2011 drabbades Sony Playstation av ett intrång. Någonstans mellan 70 miljoner och 100 miljoner konton omfattades, främst onlinespelare med Playstation. Avslöjandet av att det skett ett intrång började med att Sonys Playstation Network (PSN) stängdes och efter en vecka spekulerades det vilt bland användare kring orsaken till det långdragna avbrottet. Till sist tillkännagav Sony att alla användarkonton i PSN och tjänsten Qriocity potentiellt läckt ut någon gång mellan den 17-19 april. Enligt Sonys egen bedömning kom inkräktaren över uppgifter som namn, adress, land, e-postadress, födelsedatum, inloggningsuppgifter till PSH och Qriocity och PSN online ID (handle). Sony kunde inte heller utesluta att kortuppgifter läckt ut. Ytterligare information såsom köphistorik, säkerhetsfråga och -svar (vid glömt lösenord) kunde också ha fallit i orätta händer. Sony tvingades att stänga av den delen av verksamheten i ungefär en månad. Den bristande säkerheten och företagets långsamma agerande kritiserades mycket hårt, bland annat av den amerikanska kongressen.

### 07.1.4 LinkedIn

Ett av de allra största fallen med läckta lösenord inträffade 2012 hos LinkedIn. En del av de läckta lösenorden knäcktes och listor publicerades, närmare bestämt 6,4 miljoner krypterade lösenord, men det var fortfarande bara en bråkdel. I maj 2016 publicerades plötsligt nya listor, den här gången med 177,5 miljoner krypterade lösenord tillhörande 164,4 miljoner unika användare, en siffra som visade sig nästan helt överensstämma med antalet användare hos LinkedIn i andra kvartalet 2012.

### 07.1.5 MySpace

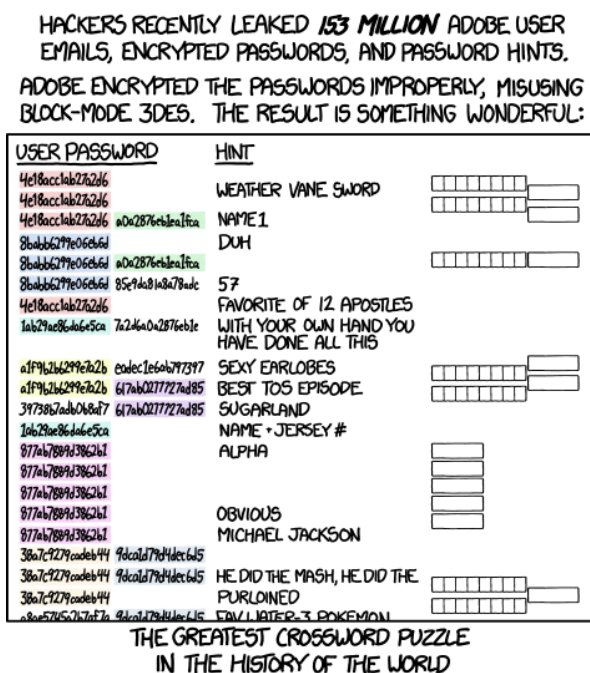
11 juni 2013 hackades MySpace. Den totala datamängden bestod av 360 213 024 poster. Varje post kan innehålla en e-postadress, ett användarnamn, ett lösenord och i vissa fall ett andra lösenord som används som ledtråd när användaren glömt sitt primära lösenord.

Lösenorden lagrades krypterat med algoritmen SHA1 och utan salt. Saltning gör som vi beskrivit tidigare dekryptering av lösenord exponentiellt mycket svårare när det handlar om ett stort antal lösenord som i det här fallet. Den metod MySpace använde för att lagra lösenord är inte vad internetstandard rekommenderar och ger en mycket svag kryptering, vissa skulle säga att det är inte är någon kryptering alls. När databasen analyserades av experter på området upptäckte man att mycket få lösenord var längre än 10 tecken och nästan inga innehöll någon stor bokstav, vilket gör det mycket lättare för människor att dekryptera.

Dessutom indikerade mängden konton med lösenordet "homelesspa" att detta verkade genereras automatiskt. Med tanke på det stora antalet lösenord med en etta i slutet misstänkte experter också att MySpace vid något tillfälle börjat kräva både siffror och bokstäver.

Nu kan man ju tycka att drygt 360 miljoner läckta lösenord (MySpace) är värre än 178 miljoner (LinkedIn). Men faktum är att incidenten med lösenord som läckte från MySpace (vilka relativt nyligen var till salu någonstans på "darkweb") hanterades bättre än incidenten hos LinkedIn. MySpace informerade snabbt alla användare om vad som hade hänt för att ge dem möjlighet att byta. Dessutom

hade alla lösenord som lagrades i databasen blivit modifierade innan de krypterades. Modifieringen innebar att systemet gjorde om alla lösenord automatiskt till endast små bokstäver om 10 tecken, oavsett vad användaren matat in och innan de krypterades. En operation som gör det helt omöjligt att bakvägen försöka gissa vad det ursprungliga lösenordet var. Systemet kan emellertid alltid verifiera användaren genom att upprepa samma metod när användaren matar in sitt lösenord genom att genomföra samma steg igen och jämföra resultatet, vilket alltså är det som finns lagrat i systemet i krypterad form.



<https://xkcd.com/1286/>

### 07.1.6 Ashley Madison

I juli 2015 stal en grupp som kallade sig "The Impact Team" användardatabasen till en flitigt använd kommersiell dejtingsajt. Rykten sa att tjänsten var lämplig för att skapa utomäktenskapliga förbindelser. Hackergruppen kopierade all information om sajten användare och hotade att publicera användarnamn och annan personlig information om tjänsten inte omedelbart stängdes. Denna attack skiljde sig alltså från de vanliga "tjäna pengar snabbt". Vid två tillfällen, den 18 respektive den 20 augusti läckte gruppen mer än 25 gigabyte information, inklusive detaljer om användare. Tack vare tjänstens hållning att aldrig gallra eller ta bort personlig information som riktiga namn, hemadresser, sökhistorik och kreditkortstransaktioner, var det många användare som var oroliga för att bli förnedrade offentligt.

Att bli utskämd och förnedrad offentligt och oroa sig för hur man ska hantera det faktum att ens partner, chef eller nära släkting kan bli uppmärksam på att man använt en sådan sajt kan leda till personliga tragedier.<sup>7</sup> Även om det kanske är att betrakta som en av de mer extrema konsekvenserna av ett angrepp finns det ett antal personer som tagit sitt eget liv som konsekvens av Ashley Madison-läckan.

<sup>7</sup> <http://fusion.net/story/242502/ashley-madison-hack-aftermath/>

## 07.2 Hur används de läckta lösenorden?

Oavsett hur angriparen kommer över dina användaruppgifter kommer de att göra sitt bästa för att använda dem för sina egna ändamål, som exempelvis identitetsstöld, desinformation och bedrägerier.

När lösenord knäcks lär sig angripare mer om hur lösenord skapas och hur användare tänker, vilket leder till ännu mer kunskap som kan användas för att knäcka fler lösenord i framtiden.

Det är inte heller bara lösenord som är intressanta. Alla teckensträngar genererade av en mänsklig hand, exempelvis användarnamn och e-postadresser, är potentiellt intressanta. Val av användaridentitet och e-postadress skiljer sig inte nämnvärt från val av lösenord.

## 08. Så hackas lösenord och lösenfraser

Att hacka lösenord innebär att man försöker gissa eller komma åt lösenord antingen från lagringsplatsen eller vid överföring. Det används antingen för obehörig åtkomst eller vid penetrationstester där det är en viktig komponent för att kontrollera säkerhetsnivån i en applikation eller ett system.

Det vanligaste sättet för hackare att komma över användares lösenord är att hitta svagheter på sajter för att ta sig in och stjäla databaser med lösenord.

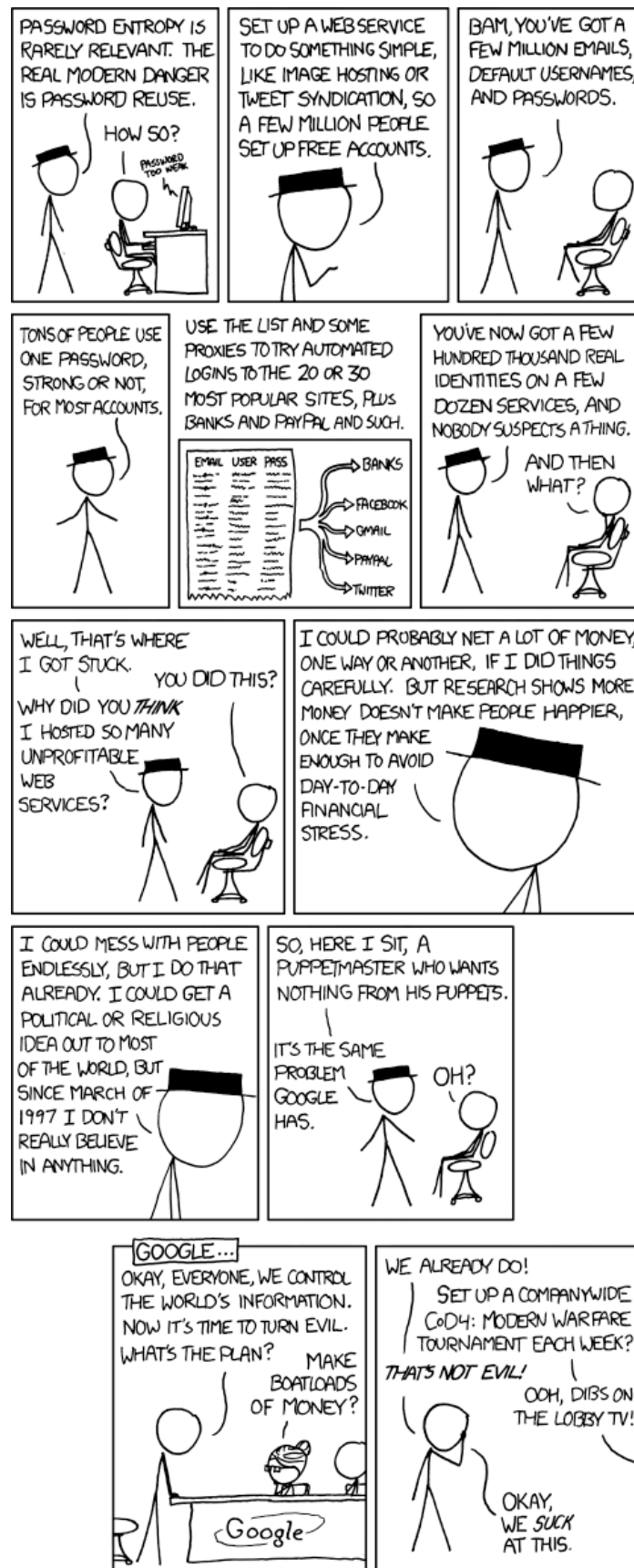
### 08.1 Bristande skydd av lösenord

När en användare registrerar sig på sajter som Facebook, Twitter, Instagram, olika forum, mejlkonton med mera ska lösenorden lagras krypterade vilket betyder att lösenordet inte finns tillgängligt i klartext.

Enkelt beskrivet innebär det att varje lösenord omvandlas till en kontrollsumma. Lösenordet "Sommar" blir till exempel "81dc9bdb52d04dc20036dbd8313ed055" i krypterad form om man använder en viss algoritm för att beräkna kontrollsumman. Om systemet som gör omvandlingen använder en svag algoritm för att beräkna kontrollsummor kan hackarna köra dem genom särskilda knäckverktyg och få fram lösenordet i klartext.

Eftersom användarnamn och e-postadresser oftast används som användaridentitet och oftast sparas i klartext är det en enkel match att ta sig in på andra sajter där du använder samma inloggningsuppgifter och i värsta fall även samma lösenord.

De stulna lösenordsdatabaserna läggs dessutom ofta ut på forum som är publikt tillgängliga för vem som helst eller säljs vidare till mindre nogräknade individer.



<https://xkcd.com/792/>

## 08.2 Olika sätt att komma över användares lösenord

En angripare bryr sig inte om hur de får tag på information vare sig det är genom att bryta sig in i system, stjäla en bärbar dator från en parkerad bil, eller kika över någons axel på en skärm. Nedan följer några vanliga sätt att komma över användares lösenord.

### 08.2.1 Axelsurfning

Ett sätt att komma över en användares lösenord är att helt enkelt kika över axeln på när lösenordet matas in. Via bärbara datorer, surfplattor eller smarttelefoner sitter vi idag var som helst och gör vad som helst. Det är enkelt för någon i omgivningen att snappa upp vad som skrivs. Därför ska man vara väldigt försiktig och se till att ha ryggen fri eller skärmen skyddad med ett sekretessfilter.

### 08.2.2 Social ingenjörskonst

Social ingenjörskonst är konsten att komma över känslig eller hemlig information genom att manipulera behöriga användare. Angriparen utnyttjar människors naturliga vilja att lita på andra snarare än att utnyttja tekniska säkerhetsbrister. Detta har kommit att bli en allt vanligare metod. Normalt följer angriparen ett antal steg.

1. Informationsinsamling – Det finns en mängd olika tekniker som används av angriparen för att samla in känslig information om sitt/sina mål. När informationen väl är samlad kan den användas för att bygga en relation, antingen med målet eller med någon som är viktig för att attacken ska bli framgångsrik. Information som kan samlas in är bland annat födelsedatum, intressen, familj, kontaktlistor, organisationskartor.
2. Utveckla en relation. En angripare kommer först försöka bli vän med målet och bygga upp ett förtroende mellan sig själv och målet som utnyttjas senare.
3. Exploatering. När målet väl litar på angriparen kan han eller hon manipuleras att lämna ifrån sig känslig information som exempelvis lösenord.
4. Genomförande – När målet för attacken väl har genomfört det som angriparen ville är attackcykeln komplett och angreppet ett faktum.

Tyvärr finns det inte något enkelt sätt att förhindra den här typen av attacker. Det gäller att vara medveten om att det sker och att man inte ska lita på vem som helst utan vidare. Ett visst mått av misstänksamhet anbefalls. Var särskilt försiktig med att lämna ut information som exempelvis:

- Användarnamn
- Lösenord
- Personnummer
- PIN-koder
- Servernamn
- Systeminformation
- Kreditkortsnummer
- Känslig information i allmänhet

Så sent som i juli 2016 varnade Pensionsmyndigheten för att vissa sparare kan ha drabbats av så kallade bankid-kupper där användare förmåtts att frivilligt lämna ifrån sig inloggningsuppgifter via telefon eller mejl, något man **aldrig** ska göra utan en extra kontroll av vem det är man lämnar uppgifterna till.

### 08.2.3 Keylogger

En keylogger är ett stycke skadlig kod som registrerar tangenttryckningar som du skriver in på ett tangentbord. Det kan också vara en hårdvara som placeras mellan tangentbordet och datorn. Keyloggers kan komma in i miljön genom att du installerar något annat, till exempel ett spel eller annan programvara, där keylogger-programmet installeras samtidigt utan att du märker något. Syftet är oftast att stjäla viktig information från en datoranvändare, som till exempel lösenord.

En keylogger sparar all information till en loggfil, eller skickar den direkt till angriparen via mejl. Att upptäcka om man har fått en keylogger i sin dator är viktigt för att skydda känslig information från att falla i händerna på någon obehörig. Det gör man genom att titta på anslutningarna för att se om någon har planterat en hårdvarubaserad keylogger och genom att använda program för att upptäcka skadlig kod, antivirus och antispyware-program.

## 08.3 Kvalificerade gissningar on-line eller off-line

För att knäcka ett lösenord med kvalificerade gissningar måste varje gissning kunna testas. Det kan man göra på lite olika sätt.

Det går att skicka en gissning till inloggningsfunktionen, till exempel inloggningen till någons Facebook-konto, alltså on-line. Metoden tar oftast lång tid och risken för upptäckt är överhängande om systemet har åtminstone ett minimum av övervakning och funktioner som låsning av konton efter ett visst antal försök.

Alternativet är att ha tillgång till lösenordsdatabasen för att direkt kunna testa mot den utan att vara uppkopplad mot den aktuella sajten (off-line). Även om lösenorden lagras krypterade har angriparen gott om tid att försöka gissa sig fram till ett korrekt lösenord, framför allt i andra tjänster än den som har hackats. Sannolikheten att användaren har återanvänt samma lösenord på andra platser är stor.

För att mäta styrkan i ett valt lösenord går det att använda olika typer av verktyg som tillhandahålls av olika tjänster på internet, exempelvis Dropbox. Lösenordshanterare brukar också erbjuda en sådan mätare, som med färger från rött, via orange och gult till grönt indikerar när ett lösenord kan anses vara tillräckligt starkt.

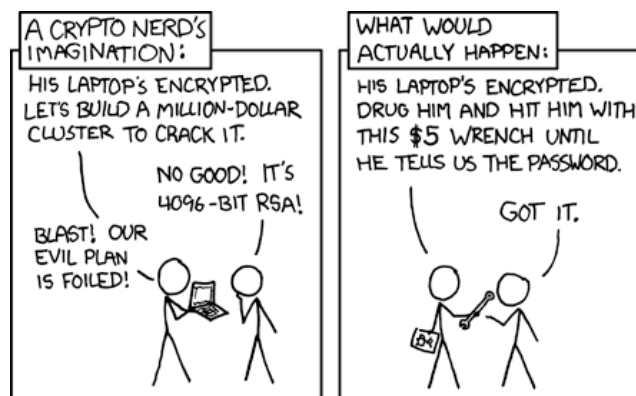
## 08.4 Råstyrkemetoden (brute force attack)

Råstyrkemetoden innebär att angriparen låter ett program gå igenom alla möjliga teckenkombinationer för att hitta ett lösenord. Den metoden garanterar att lösenordet kan hittas, men det kan ta väldigt lång tid, beroende på tillgången till datorkraft, samt komplexiteten och längden hos lösenordet i fråga.



## 08.5 Ordlistemetoden (dictionary attack)

Ordlistemetoden innebär att angriparen använder en ordlista med de vanligast förekommande lösenorden och låter dessa vara gissningarna. Eftersom många användare återanvänder sina lösenord på flera platser behöver angriparen inte ha tillgång till lösenordsdatabasen för just den sajt man är intresserad av att attackera. Det räcker med att användaren har återanvänt lösenordet i någon av de tjänster som redan har knäckts och vars lösenordsdatabaser finns publicerade på en mängd platser på nätet. Det är en effektiv metod eftersom det ger ett relativt sett färre antal gissningar än råstyrkemetoden. Om lösenordet inte finns med i ordlistan kommer man dock aldrig att kunna knäcka det på detta vis.



<https://xkcd.com/538/>

## 09. Råd och rekommendationer

Nu har du lärt er allt om vad som kännetecknar dåliga lösenord. Vad kännetecknar då ett starkt lösenord?

Enkelt uttryckt är regel nummer ett – ett starkt lösenord är ett unikt lösenord.

Lösenord ska vara:

Långa  
Komplexa  
Ovanliga

Ingen annan i hela världen ska ha valt samma lösenord.

### 09.1 Längden har betydelse

En generell regel är att lösenord kortare än 10 tecken (och en del skulle till och med gå längre än så) är svaga eftersom en angripare vid en uttömmande sökning (brute force) eller ordlisteattack (dictionary) kan testa många miljarder kombinationer och knäcka kortare lösenord på inte alltför lång tid.

Fler tecken med variation i ett lösenord eller många ord i en lösenfras bidrar till att skapa mer entropi (se avsnitt 06.2.1) vilket alltså gör det svårare att gissa. I allmänhet gäller också att ju längre lösenord eller lösenfras desto mindre sannolikt att någon annan använder samma.

### 09.2 Komplext och ovanligt

Enbart längden gör inte ett lösenord med 10 tecken eller fler säkert. När du ska skapa ett lösenord, använd en mening som är positiv för dig och som du kan komma ihåg. En användare som har användarvänlighet som högsta prioritet väljer oftast ett mindre säkert lösenord vilket skapar risker.

En av fördelarna med långa, komplexa och ovanliga lösenord är att de flesta andra har sämre lösenord och därmed utgör enklare måltavlor än du. Var kreativ.

### 09.3 Lösenord i nivåer

Det finns de som förespråkar lösenord i nivåer. Trots allt är inte all information lika viktig och skyddsvärd och samma höga säkerhetsnivå krävs därmed inte överallt. Det kan vara en lämplig modell att ha några olika nivåer för val av lösenord. Det är exempelvis en särskilt passande modell för den användare som har hundratals konton på olika sajter som ska memoreras eller i vart fall finnas tillgängliga när de behövs.

Det kan vara acceptabelt att använda samma lösenord för den lägsta nivån, medan det aldrig är acceptabelt att använda dåliga lösenord på särskilt skyddsvärda tjänster.

De tjänster som medför åtkomst till känslig information eller särskilt skyddsvärda system behöver alltid ha särskilt hög säkerhet på lösenorden. Exempel på sådana tjänster är lösenord till jobbet, e-postkonton, hälso- och sjukvårdsinformation.

Till sajter med lägre krav på säkerhet räknas sådana där användaren måste logga in för att kunna läsa artiklar, ladda ner material, titta på bilder eller vad det nu kan vara. Alltså mindre viktiga sajter som någon envisats med att skydda med inloggning, ofta för att de ska få din e-postadress för att kunna nå dig med utskick i exempelvis marknadsföringssyfte. Där kan det kanske vara acceptabelt att använda samma lösenord på flera olika tjänster. Ett bättre alternativ för den typen av sajter är att inte ens försöka komma ihåg lösenorden. Använd funktionen "Glömt lösenordet" i stället och begär ut ett nytt varje gång.

## 09.4 Byt inte ett bra lösenord – om du inte måste

Det finns en seglivad tradition inom lösenordshantering som säger att man ska byta lösenord både ofta och regelbundet. Detta är vansinne.

I en stor verksamhet blir hundratals lösenord bortglömda varje dag och måste bytas ut med mer eller mindre säkra rutiner. Hanteringen av användarnas lösenord är med andra ord jobbig, dyr och mycket osäker.

I många verksamheter tvingas användarna att byta lösenord med 30, 60 eller 90 dagars mellanrum. Byten ger inga som helst fördelar eftersom stulna lösenord i allmänhet utnyttjas relativt omgående. Tvingande och täta byten av lösenord bidrar till att många användare inte uppfattar lösenorden som speciellt känsliga och både delar med sig av och återanvänder dem.

Den enda gången man verkligen måste byta lösenord är om man misstänker att det har blivit röjt eller om det har framkommit metoder som gör att de lösenord man använder försvagats (behöver fler tecken eller mer entropi) och det inträffar inte så ofta.

Regelbundna lösenordsbyten är ett vanligt krav i många säkerhetsriktlinjer. Det finns ingen tydlig historik som beskriver när och varför kravet kom till. En teori är att kravet föddes någon gång på den tiden då man fortfarande använde hålkort. För att processa hålkorten på ett konto måste användaren ha ett lösenord. Oftast fick inte användaren själv processa sina hålkort utan var tvingad att lämna över lösenordet till en systemoperatör. En annan teori är den som vi presenterar i avsnitt 5, att lösenord användes för att reglera tillgång till processorkraft. På den tiden var det befogat att tvingas byta ibland. Idag är situationen en annan. Varje användare har sin egen dator, smarttelefon eller surfplatta, med sina egna applikationer, loggar själv in på sina konton på nätet och så vidare.

Debatten om nyttan med obligatoriska lösenordsbyten har förts under åtminstone ett decennium. På senare tid har det också framkommit forskning som stödjer tesen att obligatoriska lösenordsbyten inte är så bra som man tidigare trott, ibland till och med kontraproduktivt.<sup>8</sup> Användare som tvingas byta lösenord

---

<sup>8</sup> <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>

ofta är mer benägna att välja svagare lösenord och byter dem sedan visserligen regelbundet men ofta på ett sätt som är förutsägbart och gör det lätt att gissa.

Tänk på saken. Problemet med regelbundna byten är att man inte alls tar hänsyn till omaklet det innebär att tvingas byta ett lösenord utan egentlig anledning mer än att en viss tid förflutit, ofta när det är väldigt opassande. Därför blir det många gånger ett lösenord som tillkommer i all hast och valet görs med utgångspunkt från att användaren inte ska glömma det meddetsamma eftersom denne förmodligen satt mitt uppe i någonting annat. Resultatet blir ett lösenord som förmodligen är alltför enkelt att gissa eftersom det inte fanns tid att tänka efter.

I vissa fall tvingar lösenordsregler oss att använda lösenord som inte går att komma ihåg eftersom de ska vara så långa och så komplexa som möjligt. Den regeln kanske fungerar om vi bara har ett fåtal lösenord att hålla reda på, men knappast för de dussintals lösenord som många av oss använder i våra liv på internet. Dessutom är vi väldigt dåliga på att göra slumpmässiga val. Längre fraser visar sig också ofta vara obetydligt bättre än vanliga traditionella lösenord.<sup>9</sup>

Och som sagt, som om det inte vore nog insisterar de flesta lösenordsregler på att vi måste byta dem. Ofta. Och regelbundet. Och att vi inte får använda något av de  $n$  senaste, där  $n$  kan vara ett värde på 10, 20 eller kanske ännu mer. När vi tvingas att byta ofta och regelbundet är risken överhängande att det nya lösenordet är väldigt likt det gamla. En angripare kan oftast räkna ut det nya lösenordet om denne har något av de gamla.

## 09.5 Är ditt lösenord röjt?

Det är inte alltid uppenbart om ett lösenord blivit röjt. Det behöver inte alltid vara användaren som har brustit i sin hantering, det kan vara så att det är en sajt som inte skyddar användarnas lösenord tillräckligt och fått sin databas publicerad på nätet. Vi har beskrivit ett flertal sådana händelser i avsnitt 7.1. Med tanke på hur ofta det inträffar, inte minst hos stora och välkända sajter, kan man som internetanvändare ha anledning att vara orolig.

Det finns en tjänst på nätet där man snabbt kan avgöra om något konto har hackats eller blivit "pwned" som det heter genom något intrång. Man hittar funktionen på <https://haveibeenpwned.com>, en tjänst tillgänglig för en bredare allmänhet som behöver ha möjlighet att kontrollera om deras lösenord blivit röjda och måste bytas, och där man kan hålla sig uppdaterad om de senaste händelserna. På sajten erbjuds också möjlighet att kontrollera alla e-postadresser knutna till en viss domän förutsatt att man kan verifiera att man har kontroll över domänen i fråga. Det är ett verktyg som blir mer användbart ju fler användare man har i en verksamhet.

## 09.6 Lösenfraser

Som vi nämnde tidigare förespråkar en del användningen av lösenfraser framför lösenord. En lösenfras är helt enkelt en mening eller en rad med ord som väljs

---

<sup>9</sup> <http://arstechnica.com/business/2012/03/passphrases-only-marginally-more-secure-than-passwords-because-of-poor-choices/>

slumpmässigt på ett eller annat sätt. Eftersom man här frångår kravet på komplexitet blir längden desto viktigare.

## 09.7 Lösenordsgeneratorer på nätet

För den som behöver hjälp att generera starka lösenord finns det tjänster på nätet som kan användas för att slumpa fram lösenord. Lösenord som genereras via tjänster på nätet ska genereras och sändas till användarens webbläsare via en krypterad förbindelse och får inte lagras hos tjänsten.

God praxis inom informationssäkerhet är dock att aldrig låta generera dina viktigaste lösenord via online-tjänster. Den typen av lösenord kan möjligen användas för wifi-kryptering eller för det där slaskkontot man har för viss typ av e-post, men bör inte användas för att generera lösenord för inloggning på konton där känslig information hanteras, som det primära e-postkontot, pengar, personuppgifter, affärshemligheter et cetera.

En svårighet med den typen av verktyg är att veta om man kan lita på den som har skapat verktyget och att de har ett högt säkerhetstänkande.

## 09.8 Lösenordshanterare

Det finns flera bra verktyg där användare lokalt både kan generera och lagra lösenord för olika tjänster. De fungerar alla på ungefär samma sätt. Allt användaren behöver göra själv är att skapa och komma ihåg ett unikt och säkert huvudlösenord för att låsa upp och komma åt databasen med länkar till konton, användaridentiteter och lösenord. Några exempel på sådana verktyg:

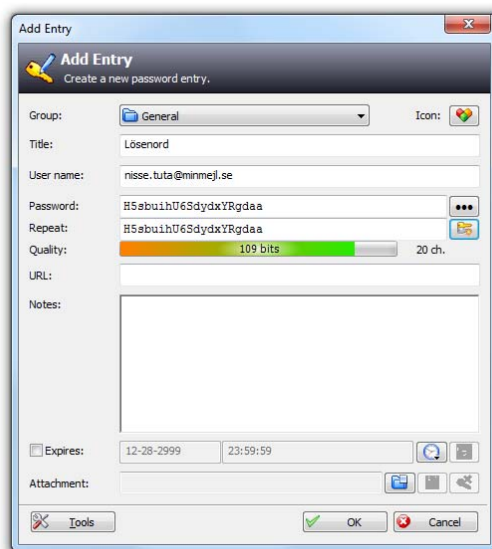
- Password Safe - öppen källkod som är gratis att ladda ner och enkel att använda.
- Keepass - öppen källkod, även den gratis att ladda ner och enkel att använda.
- 1Password - kommersiell produkt som har motsvarande funktioner och kan köpas för flera olika plattformar och enheter.

Vi visar med ett exempel från Keepass hur det kan se ut.



Figur 24. Lösenordshanterare med lösenordsgenerator

Här ställer man in önskvärda parametrar och genererar ett slumpmässigt valt lösenord.



Figur 25. Verktöget indikerar styrkan på lösenordet och det går till exempel att ange ett bäst föredatum

Alla genererade lösenord samlas i en databas och varje post kan kategoriseras under olika grupper som privat, internet, ekonomi, nätverk eller vad du vill med en egen ikon för varje grupp.

Det finns många fler funktioner och det finns många fler verktyg, både gratis och kommersiella produkter. Dessa granskas och recenseras regelbundet i fackpressen.<sup>10</sup> Välj ett verktyg som har goda vitsord och som passar för dina behov.

## 09.9 Spara lösenord i webbläsare

Webbläsare erbjuder en funktion för att spara lösenord som syftar till att underlätta för användare som för det mesta sitter vid en och samma apparat. Då behöver inte lösenordet anges varje gång man loggar in på en sajt.

Funktionen är dock förknippad med vissa svagheter. För exempelvis Firefox och Chrome är lösenorden inte att betrakta som hemliga. De lagras i klientprogrammet och går att se i klartext. Även i Internet Explorer sparas lösenorden, men de går inte att visa på samma enkla sätt och därför finns kanske inte samma behov av att skydda dem extra.

Att funktionen finns är förstås både bra och dåligt. Det är bra för dig som har glömt ett lösenord och vill få hjälp att komma ihåg, men dåligt om du är rädd att andra ska snoka på din dator, platta eller mobil. Dessutom, den gången du inte använder din vanliga dator så har du ändå ingen chans att komma åt lösenordet.

Därför är det alltid bättre att använda en lösenordshanterare som är gjord för ändamålet och som går att komma åt via olika plattformar.

## 09.10 Engångslösenord och tvåfaktorsautentisering

Även om du använder starka lösenord har en angripare fortfarande ganska stora möjligheter att komma över inloggningsuppgifter. Det är här som engångslösenord och tvåfaktorsautentisering kommer in i bilden. Förenklat beskrivet bygger tvåfaktorsautentisering på en kombination av någonting som användaren kan, ett lösenord, och något som användaren har, ett fysiskt föremål som till exempel en dosa eller en smart mobil.

När en användare vill logga in på en tjänst använder denne först sitt statiska lösenord som vanligt. Nästa steg är att ange ett dynamiskt engångslösenord som genererats i dosan eller mobiltelefonen. Först efter att engångslösenordet har angetts får användaren tillgång till det aktuella kontot. Engångslösenord är tillfälliga och kan inte återanvändas.

Det finns ett antal mobilappar som fungerar som inloggningsenheter för autentisering och som bygger på internationella standarder. Två av de allra vanligaste är förmodligen Google Authenticator respektive Facebook.

### 09.10.1 Google Authenticator

Google Authenticator finns för iPhone, Android och Blackberry och möjligheten är stor att en användare redan använder metoden för att logga in till sitt Gmail-konto eller Google Apps via tvåfaktorsautentisering. Google Authenticator ger

---

<sup>10</sup> <http://uk.pcmag.com/password-managers-products/4296/guide/the-best-password-managers-of-2016>

tillgång till flera populära tredjepartstjänster som till exempel Lastpass (lösenordshanterare), Dropbox (lagring av information) och Wordpress (publiceringsverktyg för webb). Appen genererar helt fristående de engångslösenord som används för inloggning.

Eftersom tiden används som en faktor när slumptalet för att framställa engångskoden genereras har den en begränsad giltighetstid. I det här fallet har användaren 30 sekunder på sig att använda koden. Den korta tiden är positivt ur säkerhetssynpunkt eftersom den tillgängliga tiden oftast är för kort för att någon ska hinna ta sig i ett system och göra skada.

### **09.10.2 Facebook**

Även i Facebook kan man använda ett engångslösenord för att logga in på sitt konto om man inte vill ange sitt riktiga lösenord (om du till exempel befinner dig på ett bibliotek eller ett internetcafé). Först måste du förvissa dig om att din mobiloperatör stödjer funktionen och till vilket nummer du ska sms:a för att få ett engångslösenord skickat till dig.

När ditt mobilnummer är kopplat till ditt Facebook-konto svarar de med ett unikt temporärt lösenord som är 6 tecken långt. När du får din kod anger du den i fältet Lösenord På Facebooks inloggningssida.

## **09.11 Vad händer med mina konton och lösenord när jag dör?**

Vi använder oss allt oftare av sociala tjänster där vi delar med oss av våra liv vare sig det gäller glädje eller sorg, i vått och torrt. Ibland händer det att någon vi följer eller känner går bort på riktigt. Vad händer med konton och lösenord efter döden?

Även om Facebook kanske inte ligger högst på prioriteringslistan över saker som måste tas om hand när någon dör så kan det vara bra att veta vad som går att göra. Det är inte säkert att de efterlevande ens vet vilka olika konton eller tjänster som den avlidne använt sig av. Via begravningsbyråer kan anhöriga få hjälp med att stänga av konton på internet på samma sätt som med försäkringar och andra abonnemang.

Det går också att vända sig direkt till tjänsten. Olika tjänster har lite olika lösningar, men i huvudsak innebär det att du måste kunna styrka din rätt att företräda dödsboet och bevisa att användaren i fråga har avlidit.

Facebook erbjuder två olika varianter för hantering av konton och användarprofiler efter avlidna. Antingen kan man skapa en minnessida, eller så kan kontot tas bort. För att en användares Facebookprofil ska bli en minnessida vill Facebook att man skickar in någon form av dödsbevis.

Effekten av att stänga ett konto blir att all information raderas och ingen kan längre se sidan. Det går inte heller att återskapa informationen. Instagram fungerar på samma sätt.

En användare kan också utse en efterlevande kontaktperson att kunna få tillgång till kontot. Det är användaren som själv utser vem det är. Den personen kommer



kunna redigera delar av sidan, ändra profilbild, lägga upp nya inlägg och svara på nya vänförfrågningar. Den som ska vara efterlevande kontaktperson måste vara minst 18 år.

När det gäller Google-konton kan användaren själv bestämma vad som ska hända med informationen vid dödsfall, vem som ska få tillgång till den och efter hur lång tid efter att det blivit inaktivt (3-12 månader). De anhöriga kan även här välja att ta bort ett konto, men då krävs dödsattest och att den som skickar in begäran om stängning företräder dödsboet.

Twitter-konton som varit inaktiva en längre tid stängs av automatiskt, men anhöriga kan också välja att stänga av det. För det krävs dödsattest, id-handling som styrker den anhöriges identitet samt information om den som dött.

Via Efterhjälpen kan man få hjälp att stänga alla möjliga typer av konton, även konton på sociala media som Facebook eller dejtingsajter. Efterhjälpen sparar i dagsläget inget innehåll, konton stängs bara. Dödsboet eller de anhöriga måste lämna en fullmakt för att de ska kunna hjälpa till.

Tjänsten Aftercloud sparar bilder och filmer från olika forum. De hjälper också till att stänga konton i sociala medier. Aftercloud kan ta ut och spara innehåll i Facebook, Instagram, Twitter och LinkedIn. Det finns en gräns för hur lång tid tillbaka det går att komma åt innehåll. En tumregel är ett år tillbaka. För att tjänsten ska kunna avropas krävs att någon av de anhöriga är vän med den avlidne på Facebook.

Innehållet kan läggas på en minnessida eller laddas ner av de anhöriga. För att de ska kunna spåra den avlidne krävs intyg på att personen dött samt ytterligare uppgifter om personen. En del begravningsbyråer samarbetar med tjänsten.

Det bästa är kanske att lägga både lösenord och testamente i ett bankfack eller deponera det hos någon man har stort förtroende för. Skriv ner hur konton ska hanteras, om de ska stängas eller vara kvar, om det ska bli en minnessida på Facebook och om någon ska skriva en sista hälsning till vänner och bekanta. Om man vill att någon i familjen eller nära vän ska ta hand om bloggtexter, bilder, musik och konton i sociala medier krävs ett testamente eftersom det handlar om immaterialrätt. Ett testamente måste finnas i fysisk form, skrivas under av den som testamenterar och ett vittne. Digitala testamenten är inte juridiskt bindande men kan ändå vara rådgivande för de efterlevande.

## 010. Tips om effektivare försvarssystem för systemägare, systemutvecklare och systemadministratörer

Det vore definitivt bättre om de som ansvarar för system och tjänster (systemägare, systemutvecklare och systemadministratörer) tänkte lite mer på alternativa, mer effektiva försvarssystem som går att implementera på serversidan för att upptäcka och förhindra obehörig användning av konton.

Den som vill konstruera en egen lösenordshantering för en sajt ska se till att det finns stöd för olika teckenuppsättningar i lösenord, både när det gäller språk och specialtecken. Den som köper kommersiella produkter och programvaror ska ställa krav på en modern lösenordshantering och att det inte finns några begränsningar i val av tecken, upprepning av tecken och vara frikostiga med hur många tecken som maximalt får ingå i ett lösenord. Någon sorts gräns för hur många tecken ett lösenord kan bestå av är förmodligen nödvändig. Det har uppmärksammats lösningar där överbelastningsattacker skulle kunna skapas i form av felaktiga inloggningar med långa lösenord utan övre gräns.<sup>11</sup> Säg att en angripare matar in 20 megabyte långa, påhittade, lösenord som ska köras genom en hashfunktion för att verifieras. Med ett par sådana felaktiga inloggningsförsök per sekund blir sajten snart överbelastad om det inte införs någon annan typ av begränsningar. Exempel på sådana andra begränsningar är att tvinga användaren att passera en captcha<sup>12</sup> efter tre misslyckade försök.

Här kommer några fler tips till tjänsteägare och systemutvecklare.

**Tips 1:** Byt alltid förinställda lösenord för administration och fjärråtkomst som följer med produkten från leverantören, särskilt på routrar, trådlösa accesspunkter och brandväggar. De är i allmänhet välkända bland angriparna. Genomför regelbundna skanningar för att leta efter förinställda lösenord som har missats.

**Tips 2:** Det finns systemövervakningsverktyg som presenterar information om senaste inloggningsförsök så användarna själva kan följa upp felaktiga inloggningsförsök som de själva inte har gjort. Om det inte är användaren som försökt logga in är det ett tecken på att någon har försökt få åtkomst till dennes konto och användaren ska enkelt kunna rapportera detta vidare för undersökning. Sådana initiativ bidrar sannolikt till att upprätthålla en högre säkerhetsnivå och är framför allt mycket enklare att hantera för användaren.

**Tips 3:** Hjälp användaren att skapa bra lösenord. Studier av användargenererade lösenord har visat att det leder till osäkert beteende. Det innebär till exempel att de väljer för enkla lösenord, återanvänder lösenord på flera platser och använder enkla ersättningsalgoritmer som att byta ut bokstaven "o" mot en nolla, bokstaven "s" mot en femma och så vidare. Sådana strategier är välkända för angriparna och de använder dem för att förfina sina metoder att knäcka lösenord. System med användargenererade lösenord innehåller ofta ett stort antal svaga lösenord som snabbt röjs vid en uttömmande sökning.

---

<sup>11</sup> <http://www.tomsguide.com/us/django-long-password-security,news-17557.html>

<sup>12</sup> <https://en.wikipedia.org/wiki/CAPTCHA>

Utbilda användare och uppmana dem att alltid ha unika lösenord och **aldrig** använda samma lösenord på flera platser.

Se till att svartlista de vanligaste lösenorden i systemen. Dessa finns bland annat på 10 i topp-listor som presenteras varje år, den listan ändrar sig inte mycket över tiden. Gör det tekniskt omöjligt att använda lösenord som förekommer på den listan upp till en viss position och styr användaren med tekniska kontroller mot bättre val. Överväg att presentera styrkan med en lösenordsstyrkemätare. Det har visat sig vara en effektiv metod för att få användare att göra säkrare val av lösenord.

**Tips 4:** Lagra **aldrig** lösenord i klartext. Krypterade och saltade lösenord är en funktion som gör om klartext till en kontrollsumma. En angripare som får åtkomst till en krypterad lösenordsdatabas får inte direkt tag på lösenorden i klartext. De kan fortfarande använda sig av uttömmande sökning och regnbågstabeller (tabeller för att bakvägen räkna ut ett lösenord från en kontrollsumma) för att utvinna lösenord från stulna databaser, särskilt om de har tillgång till databasen off-line. Då kan de göra hur många försök som helst.

Använd **alltid** en krypterad förbindelse mellan användarens klient och den server där användaren förväntas lämna ifrån sig information som användaridentitet, lösenord och andra känsliga uppgifter.

Använd bara lösenord där det verkligen behövs. Använd de tekniska lösningar som finns för att minska bördan för användaren. Tillåt användaren att både generera och spara lösenord på ett säkert sätt. Det finns flera lösenordshanterare som löser problemet.

Undvik att använda webbläsarens inbyggda funktion för att automatiskt spara lösenorden direkt i programmet. Även om det varierar något mellan olika webbläsare är bedömningen att det är betydligt mindre säkert än en lösenordshanterare, framför allt därför att lösenorden oftast inte skyddas av något annat än datorns inloggning.

**Tips 5:** Låt användaren vara med och påverka valet. Maskingenererade lösenord har sina begränsningar, ibland blir de omöjliga att använda även om de representerar en hög andel slumpmässighet. Välj en metod som producerar lösenord som är enklare att komma ihåg. Erbjud användaren möjlighet att välja mellan några olika förslag så brukar de kunna hitta något de gillar.

Inför en teknisk kontroll som innebär att användaren blir utelåst efter ett visst antal misslyckade inloggningsförsök.

Eftersom många användare misslyckas med inloggning på grund av att de har Caps lock aktiverat lägger exempelvis Facebook automatiskt in ett omvänt lösenord i sin databas som de accepterar för inloggning. Om en användares lösenord är Mina Skulor Har Ingen Smak skulle även mINa sKULOR hAR iNGEN sMAK fungera lika bra, trots att det de facto är två unika lösenord.

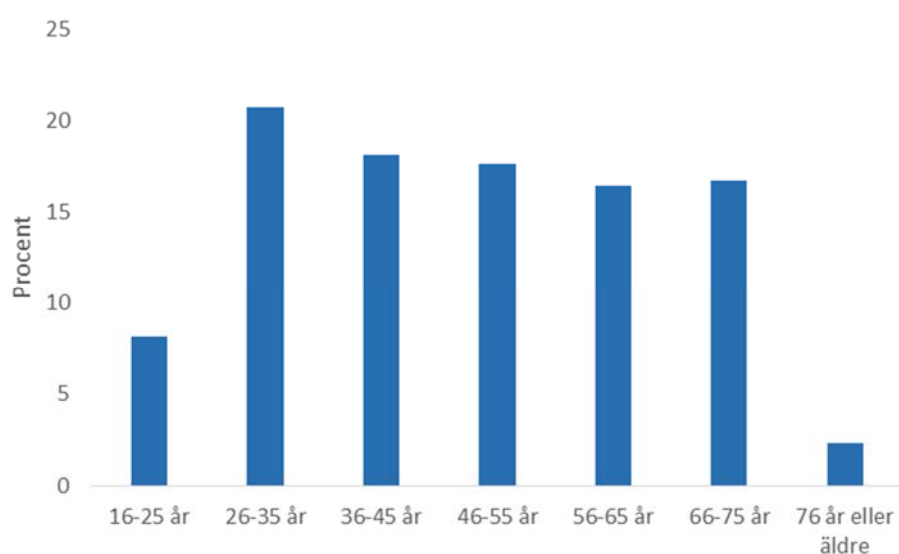
**Tips 6:** För fjärråtkomst och administratörskonton ska det alltid ställas högre krav på säkerhet. Administratörsbehörighet utgör ett rejält hot mot hela miljön om lösenordet till kontot skulle bli röjt och är därför särskilt attraktiva för en

angripare. Administratörskonton ska bara användas för sådant som kräver administratörsbehörighet. Varje användare ska ha ett konto som inte har administratörsrättigheter. En systemadministratör ska också ha ett normalt användarkonto som ska användas för sådant som inte är privilegierade uppgifter. För fjärråtkomst via VPN till e-post och andra interna system ska det krävas ytterligare en faktor förutom ett lösenord. Vid outsourcing och åtkomst från tredjepart ska det finnas tydliga instruktioner vad som krävs av dem för att få åtkomst till system och information i er organisation och hur de ska skydda sina inloggningsuppgifter. Det kan även regleras i avtal.

## 011. Fakta om undersökningen

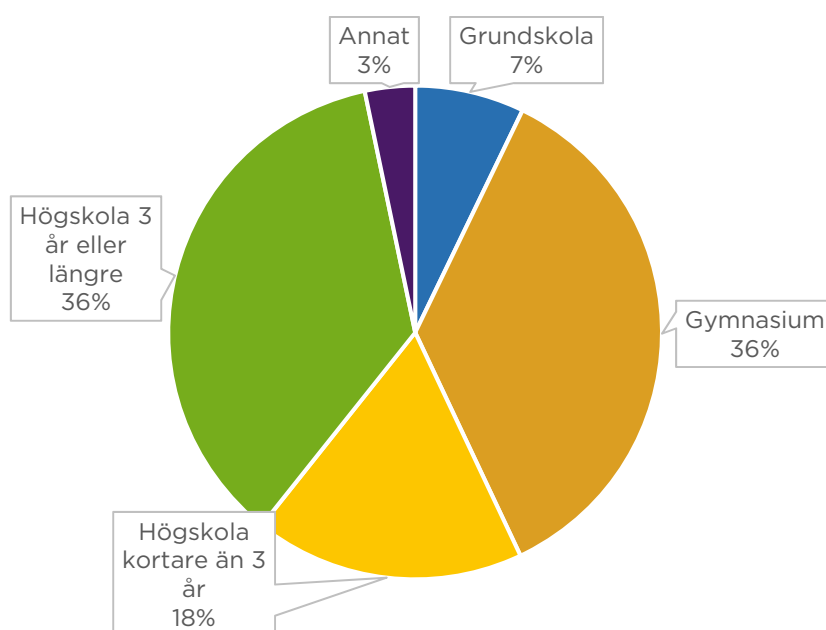
För att ta reda på mer om svenskarnas lösenordsvanor genomförde vi en enkät bland drygt 5 000 slumpmässigt utvalda svenska internetanvändare från hela landet som ingår i en webbpanel. Enkäten finns tillgänglig på sajten. Av de tillfrågade svarade 1 005 personer, vilket innebär en svarsfrekvens på 19,25 procent. Det är relativt lågt, men inom det härad som brukar gälla för webbpaneler. Det står den fritt som själv vill laborera med den insamlade datamängden att göra det. Rådata ligger tillgängligt på sajten.

De 1 005 svarande fördelade sig på 48 procent män respektive 51 procent kvinnor (avrundning gör att det inte blir 100), i åldrarna från 16 till 76 år eller äldre. Åldersfördelningen i procent följer av nedanstående figur.



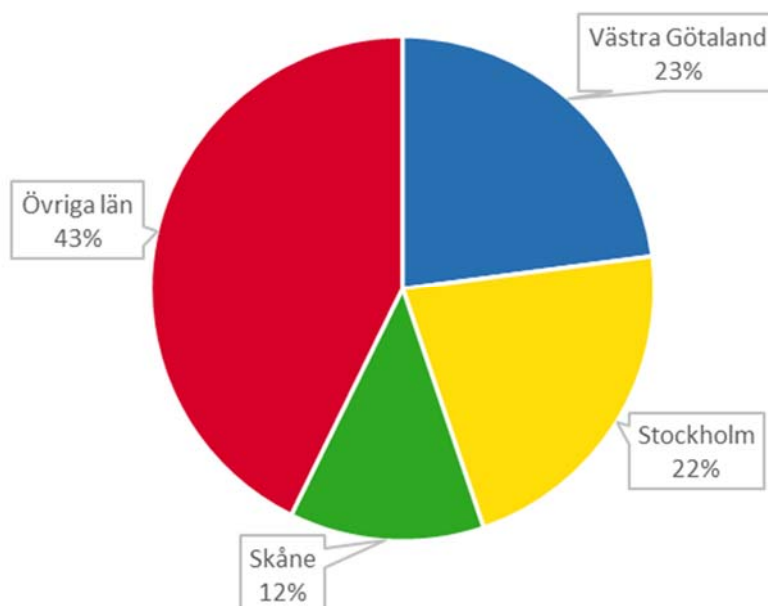
Figur 26. Åldersfördelning

De som svarade på enkäten fördelade sig på utbildningsnivå enligt grafen nedan:



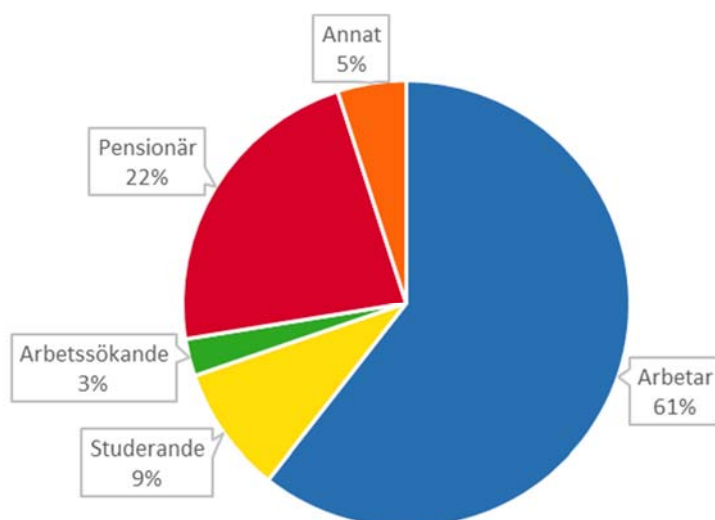
Figur 27. Utbildningsnivå

De svarande har i allmänhet relativt hög utbildning, mer än hälften har någon form av högscoleutbildning.



Figur 28. Hemvist

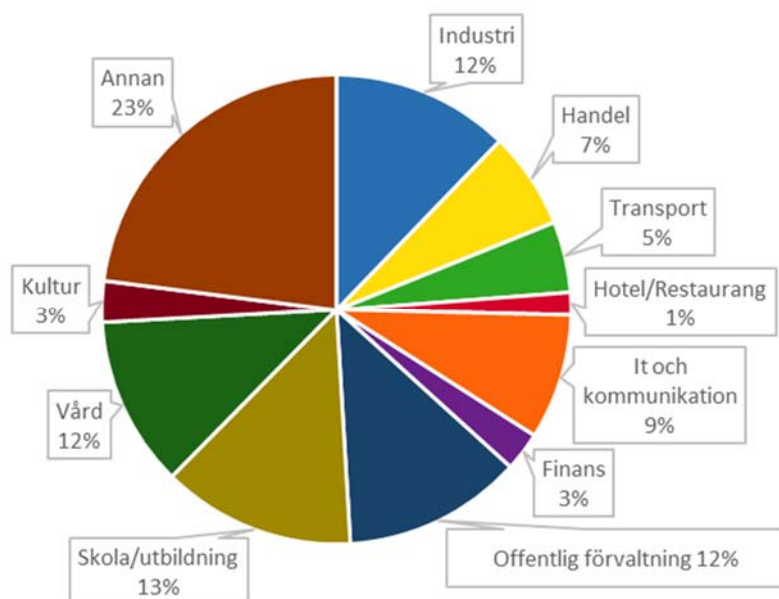
De svarande bor främst i storstadsregionerna, det vill säga i Stockholm, Västra Götaland län och Skåne. De övriga fördelar sig i princip jämt över de återstående länen (mellan 1-4 procent).



Figur 29. Sysselsättning

En majoritet av de svarande arbetar. Resten är pensionärer, studerande eller arbetssökande. 5 procent anger att de gör något annat.

De som angett att de arbetar eller studerar finns inom följande branscher:



Figur 30. Branschfördelning

Vi har alltså relativt få svar från branscherna hotell och restaurang, finans samt kultur.

## **Lösenord för alla - Statistik, råd och rekommendationer för bättre säkerhet**

I denna rapport belyses lösenord och svenskarnas lösenordsvanor.

- Resultat av en undersökning om svenskarnas lösenordsvanor
- Lösenordens tio-i-topp lista
- Lösenordens historia och anatomi
- Konsekvenser av lösenordsläckor
- Hur lösenord hackas
- Råd och rekommendationer



Internetstiftelsen i Sverige  
Box 7399, 103 91 Stockholm  
Telefon 08-452 35 00  
[www.iis.se](http://www.iis.se) [info@iis.se](mailto:info@iis.se)