2Secure

LÖSENORDSHANTERING

2Secure

www.2secure.se

Lösenordshantering

Våra liv utspelar sig numera i stor utsträckning online. Vi handlar kläder, böcker och prylar, streamar filmer och musik, skickar e-post, delar bilder och meddelanden i sociala medier, betalar räkningar, ansöker om föräldrapenning, och mycket mer. För allt detta finns onlinetjänster i någon form, och för alla dessa tjänster behöver vi kunna identifiera oss.

För att identifiera oss på en webbsida behöver vi vanligtvis ange ett användarnamn och ett lösenord. I vissa fall har vi en fysisk enhet (t ex en mobiltelefon eller ett bankkort) som kräver en PIN-kod. I mobilen har vi ett BankID där vi måste mata in en verifieringskod. Och så vidare.

Hur många koder, lösenord, säkerhetsfrågor och andra inloggningsuppgifter har du? Några exempel som du kanske känner igen:

Användarkonton och lösenord

- AppleID och iCloud
- Gmail/Google Apps
- Hotmail
- Facebook
- Twitter
- Instagram
- Snapchat
- Internetbanken
- Försäkringskassan
- Hem-/bil-/sjuk-/olycksfallsförsäkringen
- Pensionsbolag
- Livsförsäkring
- Aktiedepå
- Spotify
- Netflix
- Mataffären/Matkassen
- Flygbolag
- Taxibolag
- Bokhandel
- Kläder och skor
- Apoteket
- Online-dating
- Spel och dobbel
- Routern till hemmanätverket

Koder

- Mobiltelefon - lösenkod till enhet, PIN och PUK till SIM-kort
- Surfplatta - lösenkod till enhet, eventuell PIN och PUK till SIM-kort
- Kod till hemlarmet
- WiFi-lösenordet hemma
- Bank- och kreditkort - PIN, CVV-kod, SecureCode/3DSecure för online
- BankID

Och då har vi inte ens pratat om alla användarkonton, lösenord och koder på jobbet. VPN, intranät, HR-portalen, CRM-systemet, andra affärssystem...

Information

Vi har numera dussintals olika konton för tjänsterna vi använder för allehanda syften. "Nyckeln" till varje tjänst är ett användarnamn och ett lösenord. Redan här behöver vi alltså hålla reda på väldigt känslig information.

Användarnamnet är i många fall en e-postadress. Den är kanske inte så känslig för sig, men blir det om någon också tar reda på det tillhörande lösenordet. Lösenorden låser upp våra konton och ger oss, men även andra personer tillgång till det vi har lagt in i respektive tjänst.

Lösenordshantering

Om vi tar listan ovan kopplar vi lite information till varje tjänst. Bedöm själv om du tycker att informationen är känslig eller inte:

Tjänst	**Information**
AppleID och iCloud	namn, postadress, telefonnummer, inköpta appar, kreditkortsuppgifter i iCloud: backuper av telefoner, surfplattor, datorer (bl. a. dokument, adressböcker, bilder, mail)
Gmail/Google Apps, Hotmail	e-post, kalenderuppgifter, adressböcker, todo-listor, kreditkortsuppgifter, anteckningar
Facebook Twitter Instagram Snapchat	kompislistor, bilder, meddelanden (delvis privata som ingen annan ska kunna se), chatt, statusuppdateringar
Försäkringskassan Hem/bil/sjuk/olycksfalls-försäkringen Pensionsbolag Livsförsäkring	personuppgifter (egna och övriga familjen), avtalsnummer, adresser, inkomstuppgifter, finansiell information om privatekonomi
Internetbanken Aktiedepå	mycket finansiell information, personuppgifter, kontouppgifter, bank- och kreditkort, inkomster och utgifter
Spotify Netflix	personuppgifter, spellistor, kreditkortsuppgifter, annan kontoinformation (bl. a. kompislistor)
Flygbolag Taxibolag	personuppgifter, bonusstatus, tidigare och framtida bokningar, planerade resor
Bokhandel Kläder och skor Apoteket	personuppgifter, adress, kreditkortsuppgifter, eventuellt avvikande leveransadresser
Mataffären/Matkassen	matsedel, leveransadress, eventuellt kreditkortsuppgifter
Spel och dobbel	personuppgifter, vinster, saldo, bonusar, eventuellt kreditkortsuppgifter
Online-dating	personuppgifter, kontakthistorik, chattmeddelanden, övriga meddelanden
Routern till hemmanätverket	anslutna datorer, surfplattor, mobiltelefoner, lagringsenheter - potentiellt stora mängder privat information

Lösenordshantering

Återigen har vi inte ens belyst alla jobbsystem. Dessa innehåller vanligtvis också en del känslig information, från företagshemligheter till finansiella rapporter, personuppgifter och kundinformation.

Och allt detta ska alltså skyddas av lösenord. Lösenord som helst ska vara enkla att komma ihåg, men svåra att gissa för andra personer och datorer. Dessutom ska de vara minst 10 tecken långa, innehålla stora och små bokstäver, siffror, specialtecken, ändras var 90:e dag, inte upprepas och inte heller återanvändas någon annanstans.

Utmaningar

Tyvärr är vi människor inte vidare bra på det där med lösenord vi själv har hittat på. Några exempel:

- "Sommar2018!" uppfyller alla krav enligt ovan men är ett för övrigt alldeles för enkelt lösenord eftersom det är lätt att gissa. Ordet "Sommar" förekommer i en ordbok, 2018 pekar på årtalet då lösenordet skapades, och "!" är det vanligaste specialtecknet.
- "AIKÄrBäst2Lax9" faller under kategorin "laget jag hejar på" + "ett år då laget tog guld". Att ersätta "2009" med "2Lax9" förbättrar inte lösenordet avsevärt eftersom guldfirandet stod just under detta motto, vilket är lätt att ta reda på.
- "4maz0n_p4ssw0rd" ser på pappret ok ut men är det inte. System som är specialiserade på att knäcka lösenord har det inbyggt som grundrutin att ersätta vissa bokstäver med siffror. Dessutom består lösenordet av två ord som förekommer i ordböcker eller innehåller ett produktnamn.

Återanvändning

Om vi tror att vi har hittat ett bra lösenord, så använder vi det på många olika webbsidor. "jocke_är_en_best_hv71" blir plötsligt "huvudnyckeln" till Gmail, Twitter, AppleID och 2-3 andra konton. Detta kan medföra en olycklig dominoeffekt: råkar en av dessa tjänster ut för ett intrång där lösenord kommer på avvägar är alla andra konton med samma lösenord i riskzonen.

Mönster

Kanske har vi tänkt till lite mer och hittat ett mönster för att sätta ihop säkra lösenord för många tjänster. Lösenordet till Gmail blir då kanske "gmail_jocke_är_bäst!", det för Facebook "facebook_jocke_är_bäst!", osv.

Datorer har faktiskt lite större svårigheter med sådana mönster eftersom det handlar om längre lösenord som tar längre tid att knäcka. Däremot är dem ganska lätta att gissa för människor eftersom mönstret blir synligt väldigt snabbt - särskilt om "gmail" används på Gmail osv.

Säkerhetsfrågor

Lösenord är inte alltid lätta att komma ihåg exakt för oss själva. Var det ett stort eller litet ä i "AIKÄrBäst"? Var det en 0, ett o eller ett O i "p4ssw0rd"?

Lösenordshantering

Till slut hamnar man på länken "Glömt lösenord" och ska då mata in 1-4 svar på säkerhetsfrågor som i sin tur ofta är lätta att ta reda på, eller rentav användarovänliga för att de kan tolkas på olika sätt:

- mammas flicknamn kan man leta fram via Google, släktforskningssidor och folkbokföringen
- samma med staden där man föddes
- namnet på favoritläraren i grundskolan - tog jag den från 3:an eller 9:an? Tog jag förnamnet, hela namnet, bara efternamnet?
- första bilen jag ägde - skrev jag in märket, typ, färg, motorstorlek, något annat?

Säkerhetsfrågor kan faktiskt sänka säkerheten för ett användarkonto eftersom de kan innehålla lättillgänglig information som möjliggör obehöriga personer att skaffa sig tillgång kontot.

Risker

Vi har alltså följande situation:

- många användarkonton
- mycket känslig information som är kopplad till dessa konton
- lösenord som inte utgör ett tillräckligt bra skydd för konton

Detta medför ett antal risker för oss om obehöriga får tillgång till våra användarkonton:

- ID-stöld, följd av bedrägerier
- finansiella förluster
- informationsläckage - pinsamheter, men även information om andra än oss (barn, släktingar, vänner)
- trakasserier, stalking, hot
- utpressning
- Informationsförlust (bilder på barnen, dokument och deras backuper)

Åtgärder

Tittar vi på avsnitten ovan har vi en otroligt svår utmaning framför oss. Det gäller att memorera en massa svåra lösenord, hålla dem i rätt kontext (vilket lösenord till vilken tjänst?), komma ihåg korrekt stavning, och så vidare.

Eller så väljer vi att bara glömma alla lösenord - förutom det till vår lösenordshanterare.

Lösenordshanterare

En lösenordshanterare är en säker databas för användarnamn och lösenord. Förenklat uttryckt är det ett notisblock där man skriver ner alla sina användarnamn och lösenord till alla olika tjänster man har. För att skydda lösenorden har notisblocket ett hölje som inte går att bryta (databasen är krypterad), och ett kraftigt lås med en unik nyckel (huvudlösenordet till databasen). Det går med andra ord bara att öppna blocket med rätt nyckel.

Det finns en uppsjö av sådana lösningar på marknaden, i alla olika former och prisklasser. Vi tar en närmare titt på fem populära och framför allt erkänt säkra lösningar. Tabellen nedan jämför ett axplock av deras funktioner.

Lösenordshantering

	1Password	Password Safe	SafeInCloud	KeePass	Lastpass
Desktop OS	Mac OS X, Windows	Mac OS X, Windows, Linux	Mac OS X, Windows	Mac OS X, Windows, Linux, etc.	Mac OS X, Windows, Linux
Mobilt OS	iOS, Android	iOS, Android, Windows Phone, Symbian, etc. (utvecklade av tredje part)	iOS, Android	iOS, Android, Windows Phone etc. (utvecklade av tredje part)	iOS, Android, Windows Phone, Firefox OS
Tillägg Webbläsare	Internet Explorer, Firefox, Chrome, Safari, Opera	X	Firefox, Chrome, Safari, Opera, Yandex	X	Internet Explorer, Firefox, Chrome, Safari, Opera
Synk mellan enheter	√	√ via tredjeparts-tjänst, t ex Dropbox	√ valfritt	√ via tredjeparts-tjänst, t ex Dropbox	√ kräver Premium-konto
Databas i molntjänst	√(utvecklarens egen tjänst)	√ via tredjeparts-tjänst	√ (eget val, t ex Dropbox, Google Drive, OneDrive)	√ via tredjeparts-tjänst	√
Lösenordsgenerator	√	√	√	√	√
Policy för generering av lösenord	√	√	√	√	√
Påminnelse för lösenordsbyte	X	√ via policy	X	√	√
Lösenordsanalys (starkt/svagt etc)	√ (per lösenord eller på hela databasen)	X	√ (per lösenord, varnar för återanvändning av lösenord)	√	√
Stark autentisering (se även avsnittet nedan)	√ erbjuder generering av engångslösnord i applikationen X applikationen själv inte skyddad av stark autentisering	√ via tillägg (t ex för YubiKey)	X	√ via tillägg, både i applikationen och till applikationen	√ till applikationen, kräver Premium-konto

Lösenordshantering

Backupmöjlighet	√ automatiska backuper på Mac och Windows i egen backup-mapp. Vid behov kan filer flyttas till USB eller annat ställe. vid endast mobil användning (iOS) krävs manuell backup till iTunes	√ automatisk säkerhetskopiering i samma eller annan mapp (kan konfigureras) databas = fil som kan kopieras till annat ställe för backup (hårddisk, USB, molntjänst)	√ fil i molntjänst som kan sparas ned på hårddisk eller USB	√ automatisk säkerhetskopiering i samma eller annan mapp (kan konfigureras) databas = fil som kan kopieras till annat ställe för backup (hårddisk, USB, molntjänst)	√
Övriga funktioner	Watchtower, övervakningstjänst för webbsidor som drabbats av intrång Säkra notiser och dokument Stöd för olika kategorier av känslig data, t ex kreditkort, PIN-koder	AutoType-funktion för automatisk öppning av rätt webbsida + inloggning Jämförelse och synkronisering av flera databas-filer med varandra	inloggning via fingeravtryck släsare (iOS, Android) Automatisk ifyllning av inloggningsuppgifter för webbsidor i Chrome för Android (kräver autentisering)	kan köras från USB-minne utan installation många tillägg för anpassning av lösningen "Secure Desktop"-funktion för att förhindra utläsning av lösenord via trojaner Integration med ett stort antal administrations-tjänster (t ex RDP, SSH) via tillägg - bra för IT-administratörer. Autotype-funktion, kan lagra anteckningar och filer krypterat.	Stöd för fingeravtryck släsare i mobila enheter säker lösenordsdelning med andra personer
Öppen källkod	X	√	X	√	X
Pris	Från 50$ (Mac/Windows); mobila appar gratis	gratis	gratis (basversion + Desktop); 5$/50 kr (Pro Features iOS och Android)	gratis	gratis (Free) 12$/år (Premium, krävs för synk mellan enheter)
Webbsida	https://agilebits.com/onepassword	http://passwordsafe.sourceforge.net/	https://www.safe-in-cloud.com/en/	http://keepass.info/	https://lastpass.com
Kommentar	väldigt användarvänlig, mångsidig, lätt att använda på flera enheter	enkelt att använda, kan användas helt "offline" för väldigt känslig data	snabbt att komma igång med, smidigt över ett antal enheter och plattformar	kraftfull och extremt flexibel, men kräver viss inlärning och konfiguration	snabbt att komma igång med,

Lösenordshantering

Ur ett säkerhetsperspektiv rekommenderar 2Secure samtliga lösningar ovan. Det är alltså upp till dig att välja den lösning som passar dina behov bäst.

Huvudlösenordet

Lösenordshanterare eliminerar behovet att komma ihåg något lösenord så nära som helt. Det återstår dock ett man måste välja ett säkert huvudlösenord till hanteraren, annars riskerar man att bli av med samtliga lösenord på samma gång. Vår rekommendation är att ha minst 18 tecken, t ex 3-4 ord som inte står i något meningsfull samband till varandra.

Säkerhetsfrågor

Längre upp nämndes säkerhetsfrågor som en potentiell risk eftersom de vanligtvis kräver att man matar in information som är lätt att ta reda på. Enklast är i detta fall att automatgenerera även svaren på säkerhetsfrågorna, och lägga dem som anteckning eller säker notis i lösenordshanteraren.

Stark autentisering

I företag blir det allt vanligare att man behöver använda sig av stark autentisering för att komma åt företagets information - vare sig det handlar om en VPN-uppkoppling, e-post, eller molntjänster. Lösningar som används i sådana sammanhang kan vara:

- SMS-koder
- Google Authenticator-app i mobiltelefonen
- ett RSA-token
- smarta kort (särskilt hos myndigheter).

Men även i privata sammanhang används stark autentisering redan ganska flitigt, t ex:

- certifikat i datorn och/eller mobilen (BankID och mobilt BankID är i princip sådana certifikattjänster)
- bankdosa
- e-legitimation
- SecureCode/3DSecure (även om det egentligen bara handlar om ett till lösenord).

Många tjänster som är listade ovan erbjuder numera möjligheten att slå på stark autentisering, vanligtvis via SMS eller Google Authenticator. Vi rekommenderar dig starkt att använda funktionen. Den erbjuder ditt konto skydd även om hela tjänsten skulle bli hackad.

Ett sista tips

Svara aldrig på mail, SMS eller chattmeddelanden som ber dig om lösenord, kreditkortsdata, eller annan känslig information. I 99 av 100 fall handlar det om försök att få informationen för att begå bedrägliga handlingar med den, så kallad phishing. Dina lösenord är dina. Det finns förstås extrema undantagsfall, men dem lämnar vi utanför detta dokument.