Lösenord

1 Målgrupp

Alla användare som har datorer anslutna till Umeå universitets datornät.

2 Viktigt att tänka på

Lösenordet är strängt personligt och skall hanteras därefter.

- Avslöja eller lämna aldrig ut dina lösenord till någon annan.
- Ha ett starkt lösenord - ju krångligare och längre desto bättre.
- Använd aldrig samma lösenord på flera olika ställen.
- Skydda lösenordet väl. Använd en digital lösenordshanterare eftersom det är omöjligt att hålla alla lösenord i huvudet numera.
- Skicka inte lösenord via e-post eller annan osäker förbindelse.
- Byt lösenord direkt om du misstänker att någon känner till det.

3 Allmänt

Syftet med detta dokument är att beskriva hur man som anställd ska förfara vid hantering av lösenord och hur man ska gå tillväga för att skapa ett starkt lösenord.

Ett lösenord är en del i processen för att identifiera dig som användare mot olika IT-system och datorresurser. Detta för att försäkra sig om att våra IT-system och datorresurser endast används av de som är behöriga att göra det. Lösenorden och din användaridentitet ger dig inte bara åtkomst till applikationer utan styr också ofta vilken behörighetsnivå du har, d.v.s. vilka olika funktioner och resurser du har tillgång till. Ett lösenord som ger åtkomst till en ekonomiapplikation och som kommer på avvägar, innebär en större risk för skada än ett lösenord som endast styr en prenumeration på ett elektroniskt nyhetsbrev.

Ett lösenord som kommer på avvägar kan inte bara ställa till med problem för den enskilde användarens data utan kan också komma att exponera känslig information i de universitetsövergripande systemen. Exempel på vad den som fått lösenordet i sin ägo kan göra:

- Skicka e-post i en avsändares namn.
- Logga in på system och läsa/ändra information (epost, Box, OneDrive).
- Utföra ekonomiska transaktioner (boka resor, beställa varor).
- Installera programvara som ställer till skada på systemet.

- Lagra filer med illegalt material på hårddisken.
- Göra intrångsförsök på andra maskiner.
- Få tillgång till konfidentiell information.

I vilket fall så kan både den enskilde individen och Umeå universitet komma att lida stor skada.

I vissa fall är angivandet av ett lösenord bara en del av processen för att identifiera sig. Förutom att du känner till ett korrekt lösenord ska du kanske också inneha ett digitalt avläsbart media som ett kort (exempelvis ett bankkort med en magnetremsa eller chip) eller ett BankID. Eftersom att detta ger en inloggning i flera steg där du måste känna till alla steg kan ofta själva lösenordet vara enklare i dessa fall.

Ett sätt att komma över lösenord är att avlyssna ett nät eller en maskin och på så sätt plocka upp användarnamn och lösenord direkt i klartext. Idag är oftast lösenord krypterade men om du är osäker på den förbindelse du använder så använd inte applikationer som skickar lösenord i klartext. Ett exempel på ett protokoll som skickar sina lösenord i klartext är HTTP. Du ska inte skicka lösenord via e-post. Dels för att lösenordet skickas i klartext, men också för att man inte kan garantera att brevet hamnar hos rätt mottagare. Undantag kan förekomma, det har då föregåtts av en riskanalys.

4 Policy

Alla användare av Umeå universitets IT-resurser har ett ansvar att iaktta de åtgärder som krävs för att skapa och förvara lösenord på ett säkert sätt.

Lösenord ska aldrig lämnas ut till obehörig person.

Misstänker du att ditt lösenord har kommit på avvägar så kontakta omedelbart den systemansvarige och se till att ditt lösenord byts direkt.

För system och applikationer som har definierat egna regler för hur ett lösenord ska konstrueras och hanteras, gäller det systemets regler.

5 Regler

Lösenord ska förvaras på ett säkert ställe. Lösenord ska inte sparas i klartext på din dator. Rekommendationen är att du använder en digital lösenordshanterare. Kom ihåg att ta backup på lösenordsdatabasen.

Datorns skärmsläckare ska ha ett lösenord inlagt så att datorn låses automatiskt när den inte används.

Använd inte samma lösenord för flera olika typer av applikationer och datorsystem. Försök gruppera dina lösenord i olika grupper efter vilken typ av datorsystem, där de starkaste lösenorden är förbehållna känsliga system och applikationer (som administrativa system), ned till mindre känsliga applikationer (som prenumerationer på nyhetsbrev).

Var uppmärksam varje gång du ombeds att ange ditt användarnamn och lösenord. Ser det ut

som det brukar? Brukar jag mata in användarnamn och lösenord här?

Många applikationer idag ger möjligheten att spara lösenordet så att man inte behöver ange detta varje gång man ska logga in. Var sparsam med att använda denna funktion.

Skicka inte lösenord i klartext via e-post.

Att välja ett lösenord:

- Utgå ifrån någonting som är lätt att komma ihåg men svårt att gissa.
- Ett starkt lösenord ska vara minst 8 tecken långt.
  Undantag: För system och applikationer som har lösenord som består av mindre än 8 tecken eller på annat sätt avviker från reglerna i detta dokument gäller det systemets regler.
- Blanda stora och små bokstäver, samt specialtecken och siffror. Lösenordet bör innehålla minst 1 versal, 1 specialtecken och 1 siffra.
- Använd inte blanktecken.
- Använd olika lösenord för olika typer av tillämpningar.

Eller använd något hjälpmedel som skapar ett helt slumpmässigt lösenord utifrån reglerna ovan.

Detta är några exempel på hur man kan konstruera ett bra lösenord. Använd dock inte exakt de som visas i exemplen nedan!

- Gör om ett ord eller mening så att det innehåller "konstiga" tecken.
    - Utgå ifrån en barnvisa.
      Exempel: Alla fåglar kom i ett ren...
      Lösenord: @11aFRen
    - Utgå ifrån en rad i en dikt.
      Exempel: Ja visst gör det ont när knoppar brister.
      Lösenord: J_vgd0nkB
    - Utgå ifrån en mat-/efterrätt.
      Exempel: Glass med chokladsås
      Lösenord: g!mchs@s
- Använd inte vanliga ord (svenska eller utländska, personnamn, förkortningar, initialer, orter, hobbies etc.).
- Undvik naturliga omskrivningar av ord (t.ex. 7eleven, seven11 etc).
- Använd inte en tangentbordssekvens (t.ex. asdfghjkl, 1234567890).
- Använd inte korta ord, enstaka tecken, telefonnummer eller födelsedatum.
- Använd inte ord där det enda man har gjort är att byta ut en bokstav till en siffra (t.ex. 0 istället för O).

Byt lösenord:

- Enligt de instruktioner som finns för varje system. Om det är möjligt bör lösenord bytas var 6:e månad.
- Om du har berättat det för någon (oavsett vem det än är!) eller har haft det synligt någonstans.
- Om du har loggat in okrypterat ifrån något annat ställe än ifrån Umeå universitets campus.
- Om du har ett lösenord som inte följer kraven som ställs för ett visst system.

6 Definitioner

Starka lösenord: Ett lösenord som inte enkelt kan härledas utifrån namn på medlemmar i familjen, husdjur, bilmärken etc. Ej heller kan lösenordet enkelt tas fram med hjälp av något automatiserat verktyg som jämför de lagrade krypterade lösenorden med riktiga ord från olika databaser (finns på flera olika språk, även namn/förkortningar/orter/m.m.). Man kan även vända och vrida på orden från ordlistan, lägga till siffror, byta till versaler och annat för att till slut få fram en matchning. Chansen att på detta sätt knäcka ett lösenord är mindre ju mer komplicerat och mer olikt vanligt språk lösenordet är.

7 Revisionshistoria

Fastställt 206-11-23/ Maria Edblom Tauson