Vill du slippa lös från lösenorden?

Lars Andersson
Johan Murray

1.123456
2.123456789
3.Qwerty
4.Password
5.12345
6.12345678
7.111111
8.1234567
9.123123
10.Qwerty123

Det här är dagens minsta textstil

SeniorNet Södermalm

sök här … Ok

Senaste nytt | Om klubben ▼ | Kanelbullen ▼ | Kurser | Dataträffar ▼ | Medlemskap

- Om våra dataträffar
- Kommande träffar
- Referat från tidigare dataträffar

Hem › Dataträffar

Dataträffar

Om våra dataträffar

Ett referat av hela presentationen och bilderna går att ladda ner från i morgon, från https://snso.se/datatraffar/

Välkommen till

SeniorNet Södermalm

Kanelbullen, vårt Internetcafé, finns på Rosenlundsgatan 44A, dit alla seniorer är välkomna. Klicka här för våra öppettider.

Vår devis är "Seniorer lär seniorer IT" och det gör vi med kurser och dataträffar för våra medlemmar.

Medlemmar som önskar särskild hjälp med felsökning eller undervisning kan boka stöd på våra fasta supporttider eller på annan tid efter överenskommelse.

Dagens agenda

Del 1 13:30

- Somliga lever farligt
- Vem är jag på nätet?
- Bra och dåliga e-legitimationer
- Konto – vad är det

Del 2 ca 14:00

- Bra och dåliga lösenord
- Autentisering: 1FA, 2FA, 3FA
- Olika lösningar på problemet

Del 3 ca 14:30

- Demo av lösenordshanterare
- Summering
- Frågor

Del 4 ca 15:00

- Mera frågor
- Avslutning

Somliga lever farligt på Internet

- Lösenord? Konto? Logga in – det gör jag aldrig!

- Varför ska man ha flera, jag kan mitt – tror jag.

- Återställa, vad är det?

Det ger supporten huvudvärk

- De riskerar att bli ID-kapade!
- Som vi skall visa idag – det finns inga genvägar.
  Ni måste hålla reda på era konton och lösenord.
  Det finns hjälpmedel, men ni måste tyvärr ändå begripa vad ni håller på med!

Att vara digital är att vara kluven

Vem är jag analogt?

- Mitt namn
- Min adress
- Mina egenskaper

Vem är jag digitalt?

- Mitt personnummer / alias
- Min telefon / epost
- Googles sökresultat om mig

Bevisa det!

- En identitet
- Ett körkort
- En namnteckning
- Kan förfalskas

Bevisa det!

- Olika identiteter
- Många lösenord / PINkoder
- Biometri
- Många bedrägerier och virus

Finns det några bra e-legitimationer?

BankID & Freja eID+

- Utgår från en analog legitimation
- Legitimerar en identitet med en PINkod
- Samma inloggning på många sajter och appar (BankID har flest)
- Visst bedrägeriskydd med QR-koder
- Knyts till smarta mobiler och kräver vana vid dem
- BankID gäller bara i Sverige

BankID kan användas för digital underskrift av dokument i Kivra

Freja eID+ kan också användas som analog legitimation

Finns det bra lösningar i andra länder?

Juridiken bromsar och länderna vill ha egna system

Estland

Alla invånare får en statlig e-postadress
Kortläsare

Italien

Bostadsadressen anges på kortet
Blipp-bart

Sverige

Används digitalt i kombination med BankID

Hos FB och Google är man också bara EN

Är inte det bra det?

De har inte så hög säkerhet, precis.

- Inloggningen kräver i regel inte något utöver lösenord
- Möjliggör omfattande kunskapsinhämtning om användaren
- Även på andra sajter kan man logga in med FB/Google
  (De får då ta viss del av FB/Googles kunskaper.)
- Läcker detta lösenord öppnar sig en hel värld för bedragarna

På Google och FB är jag ju alltid inloggad!

Ja, du har nog kryssat för "Kom ihåg mig", eller hur?

Låt bli det, när du inte har din egen dator eller mobil!

"Kom ihåg mig" finns på väldigt många sajter

Se till att din dator/mobil självlåser om du använder funktionen.

Lösenord har både fördelar och nackdelar

+ Lösenord är en enkel och billig teknik för sajter och appar, det krävs ingen särskild hårdvara ens för användaren.
+ Funkar i alla sammanhang överallt, för vem som helst
+ Lösenord är lätta att dela med sig av

- Knyts till ett ”konto” (skumt, mer om det strax)
- Många lösenord är alldeles för svaga, dvs lätt att knäcka
- Man måste själv hålla reda på sina olika lösenord och konton

Biometri som alternativ till lösenord

Fungerar alldeles utmärkt för det mesta!

Face ID

Touch ID

vs PIN/Lösenord

Om konton……

- Ett konto är ….. en registrering hos ett företag/myndighet vars tjänster man använder. Det innehåller t ex
  - Personliga uppgifter
  - Köphistorik (t ex Amazon, H&M)
  - Mejl, kontakter, kalender, bilder, moln-disk (t ex Google, Apple, Microsoft)
  - Inlägg, reaktioner (t ex Facebook)
  - Mm, mm

- Varje konto identifieras med
  - En användaridentitet (ofta en mejladress)
  - Ett lösenord (skall vara långt och unikt per konto)
  - Ev. ytterligare attribut för säker inloggning

- Dina konton hos Google/Apple/Microsoft är speciella.

PAUS

Del 2 ca 14:00

- Bra och dåliga lösenord
- Autentisering: 1FA, 2FA, 3FA
- Olika lösningar på problemet

Hur är ett dåligt lösenord?

Lätt att gissa

Kort och krångligt

1.123456
2.123456789
3.Qwerty
4.Password
5.12345
6.12345678
7.111111
8.1234567
9.123123
10.Qwerty123
11. 1q2w3e
12. 1234567890
13. DEFAULT
14. 0
15. Abc123
16. 654321
17. 123321
18. Qwertyuiop
19. Iloveyou
20. 666666

Populärt eller återanvänt

Hur är ett bra lösenord?

Det är **långt**, **unikt** och **svårt att gissa**, men lätt att komma ihåg. Gärna minst 12 tecken. Det behöver inte bytas ideligen.

Bra metoder

- Flera ord som inte hör ihop
- Initialer från en lång mening man kan, t.ex. från en sång eller dikt.
- Ren rappakalja – logga in via glömt-funktionen

Sättet att mäta säkerheten på - autentisering

(Autentisering betyder att intyga äkthet)

Tre viktiga faktorer = 3FA

En egenskap (ÄR)

En ägodel (HAR)

En förmåga (KAN)

Säkerhetsnivåer vid inloggning

- 1-faktor-autentisering
  Lösenord (KAN)
- 2-faktor-autentisering
  Lösenord + SMS-kod eller annan kvittens i mobilen (KAN + HAR)
  BankID/Freja med PIN/Fingeravtryck i mobilen (HAR + KAN/ÄR)
  Bankdosa med PIN (HAR + KAN)
  Så, var rädd om din mobil och din bankdosa!

2-faktorautentisering blir ett allt vanligare krav
för inloggning på webbsidor från en ny dator.
Ett "måste" för FB-, Google-, Microsoft- och Apple-konton!

Lista på sajter som har 2-faktorsautenticering: https://2fa.directory/se/#banking

2-faktor-autentisering (2FA)

- Lars visar ett enkelt exempel – inloggning på Google-kontot

1. Vanlig inloggning med Gmail-adress och lösenord
2. Aktivera 2FA
3. Logga ut
4. Logga in, visa vad som händer på datorn och i mobilen

- Visa exempel på Autentiseringsapp i mobilen, både Google Authenticator och Microsofts motsvarighet

Lösningar på lösenordsproblemet

Din egen

- En papperslapp (metod 1)

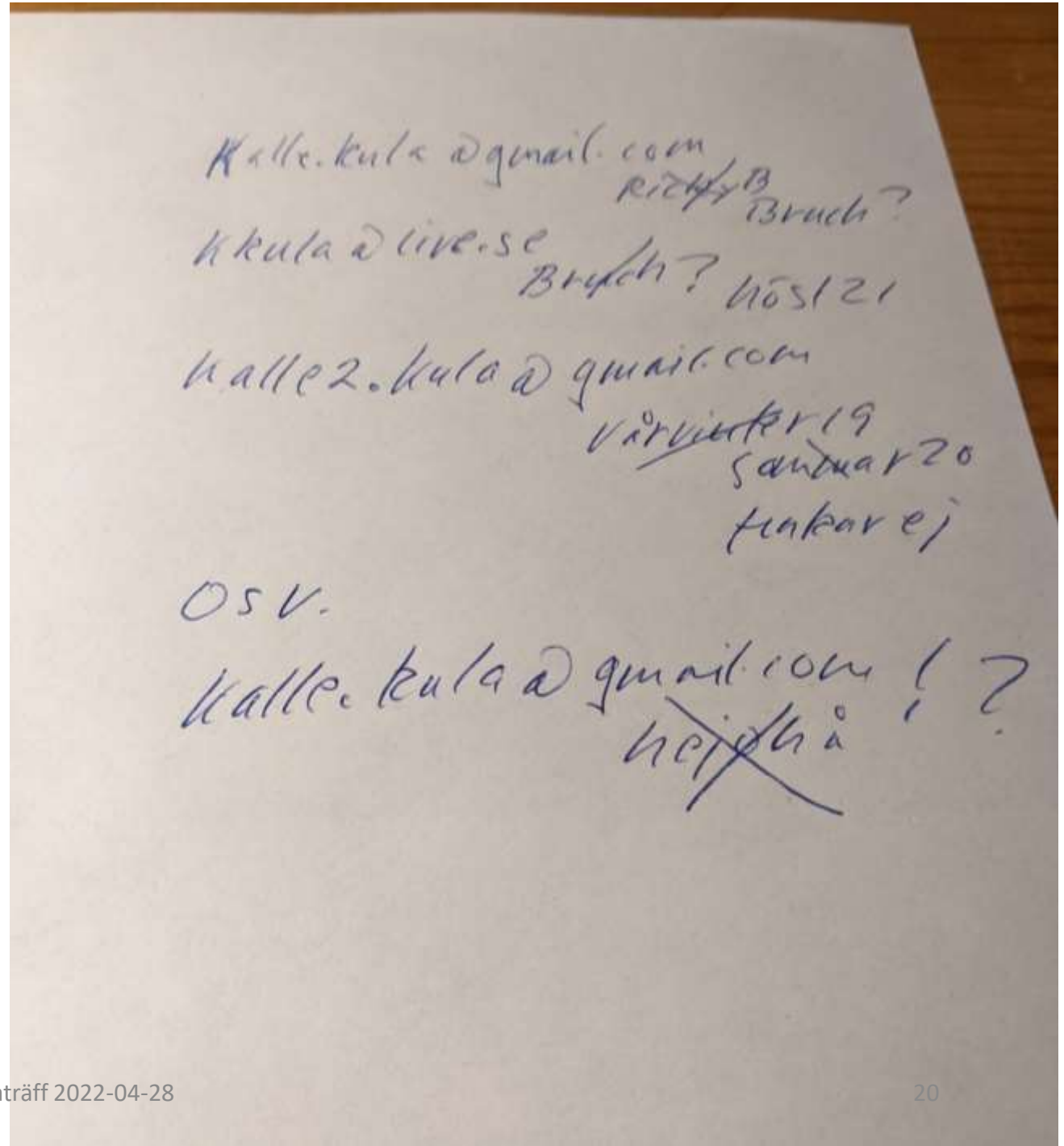
Industrins lösenordshanterare – fyra typer

- Inbyggda i operativsystemet (som Apples Nyckelring)
- Komplement till Antivirus
  (Norton, Avira, Total AV, Bitdefender, m.fl.)
- Inbyggda i Webbläsare (Chrome, Edge, Firefox) (metod 2)
- Separata (mmåånnggaa) (metod 3)

Metod 1 – på papper

Ett dåligt exempel.

Känns det igen?



..men hellre så här

Företag/tjänst/ konto	Webbadress, app	Användaridentitet	Lösenord	Ändringslogg
Google	Google.se, Gmail	Kalle.x.gson@gmail.com	Knivamornäsnus2	Upplagt 2017
- ”” -			mattaräfsgräset738	Ändrat 220412
Blocket	Blocket.se, Blocket	Kalle.x.gson@gmail.com	Kulstyving109	Upplagt 211016
Microsoft	Outlook.com min PC	kalle1949@hotmail.com	Hopplabaklänges PIN=0120	Upplagt 2019

Att tänka på:

1. Göm papperslappen på ett bra ställe!
2. Håll reda på hos vilket företag/tjänst som kontot gäller!!
3. I många (men inte alla) fall är det vettigt att ha samma användaridentitet = din mejladress.
   Men det innebär INTE att lösenordet skall vara samma.
4. De flesta klarar sig på mindre än 20 konton, så det är ingen oöverstiglig uppgift

Hur fungerar lösenordshanterare?

- Ett krypterat valv för förvaring av lösenord mm
- Man låser upp det med ett huvudlösenord,
  som man måste komma ihåg och som ska vara starkt.
- Man bör *inte ha lösenordet till sin e-post* i valvet
  (ifall man råkar glömma bort huvudlösenordet).

- Hanteraren kan (oftast) fylla i rätt lösenord vid alla inloggningar.
- Hanterare brukar kunna skapa nya starka lösenord,
  så man slipper hitta på dem själv.

- Valvet finns som regel i själva datorn/mobilen
- Har man flera enheter så kan man vilja att valvet synkroniseras i krypterad form mellan dessa.

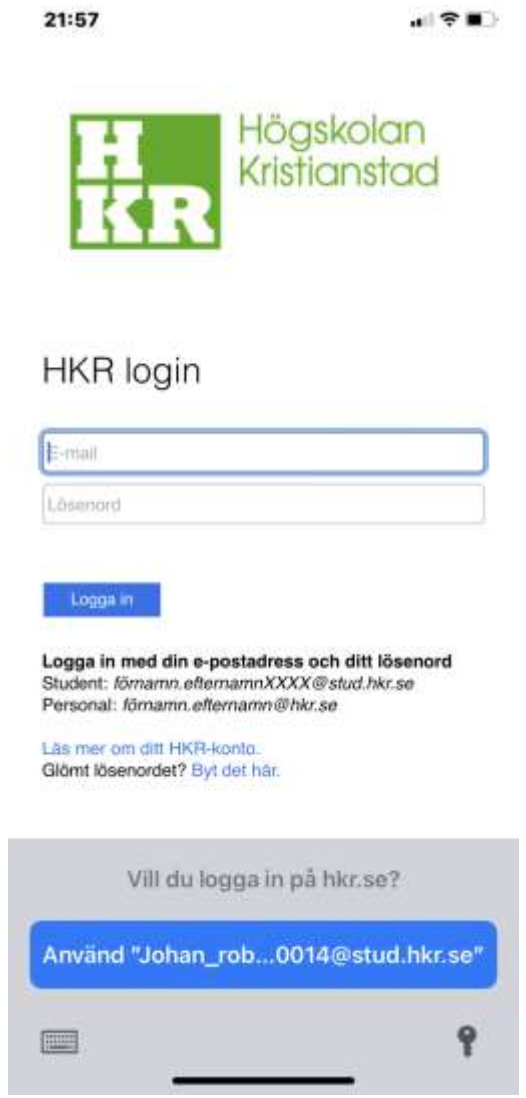
PAUS

Del 3 ca 14:30

- Demo av lösenordshanterare
- Summering
- Frågor

Apples nyckelring

- Sparar lösenord och konto
- Inbyggd i Mac, iPhone och iPad
- Synkroniserar mellan enheterna
- Går att ha i Windows också
- Lösenord kan sändas till någon annans nyckelring via AirDrop



Antivirustillverkarnas lösenordshanterare

- Särskilda appar och webbläsar-tillägg,

  utöver övrig mjukvara som ingår i AV-paketet.
- Man behöver ha ett konto hos Antivirustillverkaren.
- Synkroniserar informationen mellan de enheter man har

  valt att ansluta till kontot.

Att spara lösenord i webbläsaren – metod 2

- Ingen extra mjukvara, men kolla inställningar!
- Synk i webbläsare mellan datorer måste vara påslagen
  - Då synkroniseras väldigt mycket annat också,
  - Farligt på andras datorer.

- Krypteringen är lika hård som de övrigas.
- Lösenordsförslagen blir inte jätte-jätte-säkra (bara säkra)
- Huvudnyckel till valvet :
  - Samma som till e-posten, eller separat
- Någon kan logga in i smyg om dator eller mobil är olåst

- **Ett gott val.**

Demo metod 2

- Följande demo sker i **Microsoft Edge**.
  Google Chrome fungerar ungefär likadant

- Microsoft/Edge stöder Windows (med Edge & Chrome), iOS och Android.
- I mobila enheter används appen Microsoft Authenticator.
- Visa var man slår Av/På lösenordshantering i Inställningar
- Visa följande steg:
  - Skapa konto, autogenerera (starkt) lösenord
  - Logga in
  - Ändra lösenord
- Så lätt är det att se dina sparade lösenord i webbläsaren

- Vad händer i mobilen? I en App eller webbläsare?
  - ”auto-fyll”

Separata lösenordshanterare

- Installeras och arbetar på samma sätt som AV-varianterna gör.
- Standardfunktionerna får man oftast gratis

- Vill man ha något bättre så behöver man betala. Det kan handla om
  - att kunna dela lösenord med andra som har samma lösenordshanterare
  - att få hjälp med att byta lösenord på sina konton
  - att få förslag på jätte-långa jätte-krångliga lösenord
  - att få bevakat om ens konton drabbas av lösenordsläckor
  - att kunna ladda upp dokument till ett väl krypterat moln

- Några separata lösenordshanterare erbjuder full funktionalitet gratis, men man får i stället betala om man har många lösenord.

Några populära lösenordshanterare…enligt PCMag

Att använda en lösenordshanterare – metod 3

- Jag visar ungefär samma scenarios som tidigare (med Edge), men nu med Bitwarden, ett kostnadsfritt alternativ som får bra kritik.

- Bitwarden består av
  - Webbläsaretillägg
  - App för Android och iOS
  - Applikation för Windows / MacOS

- Naturligtvis har jag 2FA även för Bitwarden

Till sist, några tips om lösenordshanterare

- Det är aldrig helt ”idiotsäkert”, ibland inträffar situationer då det inte fungerar
  - Inmatningsfält är ej ”taggade” som lösenordsfält
  - Du glömmer att klicka på ”uppdatera lösenord”
  - En ”inmatningsprompt” täcker inmatningsfältet och du ser inte vad du skriver
  - Det kan bli ”pilligt”, ibland får du gå in i lösenordshanteraren och kopiera informationen därifrån
- Skydda din dator, ingen (människa eller virus) får komma in i den!

..forts …

- ”Lär dig krypa innan du försöker gå eller springa”
  - Lär dig först hantera lösenord på papper innan du går vidare till metod 2 eller 3
  - Det ska vara nyfikenhet eller antalet lösenord som gör att du går vidare från pappersmetoden, inte förhoppningen att allt blir automatiskt och att du slipper bry dig
  - Pröva gärna i liten skala först. Lösenordshantering i webbläsaren (metod 2) är kostnadsfri och ”good enough”, börja med den

Summering

- Vi kommer alltid att behöva identifiera oss digitalt
- Landsomfattande e-legitimationer är bra
- Identifieringen sker med något man ÄR, HAR och/eller KAN
- Se till att inte förlora det du HAR
- Lösenord behöver vara långa, unika och svåra att gissa
- Organisera dina lösenord på papper, till att börja med
- Webbläsarnas inbyggda lösenordshanterare är ett gott val
- Möjligheten att dela lösenord med anhöriga är viktig

Frågor

Kommande dataträffar

VT22-D04 Bra appar att använda i Stockholm
2020-05-13 kl 13:30 – 15:30 i Svärdet och på Zoom

VT22-D05 Om foto- och videobehandling i mobilen
2022-05-20 kl 13:30 – 15:30 i Svärdet och på Zoom

Kontakta oss gärna på: datatraffar@snso.se

Slut för idag!

Tack för idag!