SENIORERNA Leksand

IT-Café 17/11 – Tema: IT säkerhet på nätet.

Vad ska man tänka på och göra för att skydda sig med anledning av den lösenordsläcka som man berättat om i tidningar och på TV?

- https://www.tv4play.se/klipp/4ebe065a0ced37c0bd91/video-rekordstor-losenordslacka-sa-skyddar-du-dig-fran-hackare

Här är vad du bör tänka på och göra:

1. Byt lösenord – särskilt där du återanvänder dem

Om du använder samma eller liknande lösenord på flera tjänster ska du **omedelbart byta dem**, särskilt på:

- e-post
- sociala medier
- banktjänster
- andra viktiga konton

2. Aktivera tvåfaktorsautentisering (2FA)

Detta är ett av de effektivaste skydden. Även om ett lösenord läcks behövs en extra kod från mobil/app.

3. Kontrollera om dina uppgifter finns med i läckan

Du kan använda betrodda sidor som: https://internetkunskap.se/

- Svensk polis eller myndigheters rekommenderade verktyg vid stora incidenter

(Använd bara välkända och säkra tjänster.)

4. Var extra uppmärksam på phishing

Efter stora läckor brukar bedragare skicka falska mejl/SMS:

- Klicka inte på länkar i oväntade meddelanden.
- Logga in via tjänstens officiella webbplats, inte via en länk i ett mejl.

5. Använd långa, unika lösenord

Gärna en lösenordshanterare som kan skapa och spara starka lösenord åt dig.

6. Byt ut säkerhetsfrågor vid behov

Om läckan omfattar t.ex. gamla svar på säkerhetsfrågor, ändra dem också.

7. Kontrollera viktiga kontoinställningar

- Se om det finns okända inloggningar eller enheter.
- Stäng av eller ta bort dem du inte känner igen.

8. Följ med i information från myndigheter och tjänsteleverantörer

Om det rör en specifik läcka brukar de tjänster som drabbats skicka instruktioner om vad man ska göra.

Här är en checklista för vad du bör göra när medier rapporterat om en stor lösenordsläcka — även om du inte vet exakt vilka tjänster som drabbats:

---

1. Byt lösenord på alla viktiga konton

Prioritera:

- **E-post** (det viktigaste kontot av alla)
- Bank/Finans
- Sociala medier
- Viktiga abonnemang

Om du återanvänt samma lösenord på flera ställen måste du byta **överallt**.

---

2. Aktivera tvåfaktorsautentisering (2FA)

Detta ger starkt skydd även om ett lösenord kommit på villovägar.
Använd helst en autentiseringsapp (t.ex. Google Authenticator, Microsoft Authenticator) istället för SMS.

---

3. Kontrollera om din e-post förekommer i kända läckor

Använd en säker och etablerad tjänst, som https://internetkunskap.se/ eller **haveibeenpwned.com**.
(Ange endast din e-postadress – aldrig lösenord.)

---

4. Var extra vaksam på bluffmejl och bluff-SMS

Efter läckor ökar ofta försök till:

- lösenordsåterställningsbluffar
- falska paketleveranser
- bank- och Skatteverket-bluffar

Klicka **aldrig** på länkar i oväntade meddelanden. Besök tjänsten via webbläsaren själv.

---

5. Använd säkra lösenord och helst en lösenordshanterare

En lösenordshanterare hjälper dig att skapa:

- **långa**
- **unika**
- **svåra att gissa**

lösenord för varje tjänst.

---

6. Byt eller uppdatera säkerhetsfrågor

Om säkerhetsfrågor (”Vad heter din första hund?”) kan vara kända eller gissningsbara – uppdatera dem.

---

7. Granska ovanlig aktivitet

Logga in på viktiga tjänster och kontrollera:

- okända inloggningar
- okända enheter
- ändrade inställningar

Stäng av eller ta bort allt du inte känner igen.

8. Följ information från myndigheter och företag

Drabbade tjänster brukar gå ut med:

- vilka som påverkas
- vad du måste göra
- om du behöver byta lösenord

Så kontrollerar du om din e-post har läckt

1. **Gå till https://internetkunskap.se/**
    - Skriv in din e-postadress i sökfältet
2. **Tolka resultaten**
    - Om din e-post har dykt upp i en läcka får du en lista över vilka dataintrång (“breaches”) som berör dig → vilka tjänster, vilken typ av data (t.ex. lösenord, e-post, utloggningsinfo) och datum.

Vad du bör göra **om** din e-post finns i en läcka

- Byt lösenord på de konton där e-postadressen används.
- Aktivera tvåfaktorsautentisering (2FA) där det är möjligt.
- Se till att du använder unika lösenord för varje tjänst (gärna via en lösenordshanterare).
- Håll koll på dina inloggningar – se om det finns okända inloggningar, särskilt på e-postkontot.
- Var extra försiktig med phishing-försök (mejl som försöker få dig att logga in via falska länkar).

- https://internetkunskap.se/
- https://internetkunskap.se/sakerhet-pa-natet/

Lösenordshanterare

- https://internetkunskap.se/artiklar/sakerhet-pa-natet/losenordshanterare-loser-dina-losenordsproblem/