En översikt till

Lösenord

Lösenord - Principer

1. **Var komplex**: Bokstäver(AAbbÖö), siffror och specialtecken (!?*).
2. **Längd:**
   - Minst 12 tecken långt.
3. **Var unik**: Använd aldrig samma lösenord för flera konton
4. **Undvik enkla mönster:**
   - 123456, Lösenord987, qwerty
5. **Undvik personlig information**:
   - födelsedagar,
   - namn på familjemedlemmar
   - kända ord (namn på husdjur)
6. **Byt lösenord regelbundet** och om det har blivit stulet

Lösenord – Principer forts.

1. **Tvåfaktorsautentisering (2FA)**
2. **Använd lösenordshanterare**
3. **Fysisk säkerhet**: Om du skriver ner dina lösenord fysiskt, se till att de förvaras säkert och är svåra att hitta för obehöriga.
4. **Dela inte lösenord** med anhöriga
5. **Medvetenhet och utbildning**: Utbilda dig själv och andra om säker lösenordshantering. Många brott kan undvikas genom att öka medvetenheten om säkerhetsrisker.
6. **Säker anslutning**
7. **Undvik skadliga program**
8. **Uppdatera**

Att följa dessa grundprinciper för lösenordshantering hjälper dig att skydda dina digitala konton och personlig information från potentiella angrepp och intrång.

Hur läcker ditt lösenord?

- **Lösenordsspricka**: Datorprogram kan systematiskt gissa lösenord genom att prova olika kombinationer av tecken. Ex: Hund123, Solros321 (Ordlistor)
- **Phishing-attacker:**
  - Falska webbplatser, e-post, sms
- **Säkerhets intrång på webbplatser**
  - användaruppgifter stulna
  -lösenord exponerat om det inte är ordentligt skyddat.
- **Keyloggers**: Skadlig programvara som kan spåra och registrera tangenttryckningar
- **Dålig säkerhetspraxis**: Dela lösenord med andra, enkla lösenord, Lösenord på en synlig plats eller dela dem i e-postmeddelanden
- **Samma lösenord** för flera olika konton - riskfyllt
- **Socialt angrepp**: Angripare kan utge sig för att vara från banken eller använda psykologiska knep. Få info från sociala medier
- **Tjänsteleverantörens fel**: Ibland kan lösenord läcka på grund av misstag eller brister hos tjänsteleverantören. Ex. dåligt skyddade databaser eller tekniska problem som gör att lösenord blir tillgängliga.

Titta själv:
https://svenska.yle.fi/a/7-1164054
https://haveibeenpwned.com/
https://www.f-secure.com/en/identity-theft-checker

haveibeenpwned.com

';--have i been pwned?

Check if your email address is in a data breach

andreas.hoglund4@gmail.com pwned?

Oh no — pwned!

Pwned in 2 data breaches and found no pastes (subscribe to search sensitive breaches)

Donate

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

BlankMediaGames: In December 2018, the Town of Salem website produced by BlankMediaGames suffered a data breach. Reported to HIBP by DeHashed, the data contained 7.6M unique user email addresses alongside usernames, IP addresses, purchase histories and passwords stored as phpass hashes. DeHashed made multiple attempts to contact BlankMediaGames over various channels and many days but had yet to receive a response at the time of publishing.

Compromised data: Browser user agent details, Email addresses, IP addresses, Passwords, Purchases, Usernames, Website activity

Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

Bygg ett bra lösenord

1. **Längden** – 12 tecken
2. **Blandning av olika tecken**, stora och små bokstäver, siffror och specialtecken (till exempel !, @, #, $, %).
3. **Unika ord:** Pannstejji (Dialekt ord) Hackare använder ofta ordlistor för att gissa lösenord.
4. **Använd inte personlig information**
5. **Undvik mönster**
6. **Unika lösenord** för varje konto: **Använd aldrig samma lösenord** för flera konton. Om ett konto blir kompromettерat påverkar det inte andra konton.
7. **Använd lösenordsfraser:** "GrönElefantHoppadeOverFloden!".
8. **Randomisera lösenord**

   Använd en lösenordsgenerator för att slumpmässigt generera starka lösenord
9. **Överväg lösenordsfraser**

   EX. citat eller en mening som är meningsfull för dig. Till exempel, om du älskar att resa: "Paris_ÄrMin_FavoritDestination!".
10. **Kombinera ord och symboler:** Ersätta vissa bokstäver med siffror eller specialtecken. Till exempel, "P@ris_ÄrMin_#1_Resa!".