

**Skydd mot dataintrång**



**Protection against data breaches**

# Skydda dig mot dataintrång

## Protect yourself against a data breach

- Håll programvara och system uppdaterade
  - Uppdateringar korrigerar sårbarheter
- Använd multifaktorsautentisering
  - Multifaktorsautentisering kompletterar användningen av användarnamn och lösenord
- Använd inte samma lösenord i flera olika tjänster
  - Genom att använda olika lösenord i varje tjänst kan du förhindra ett mer omfattande utnyttjande av de användaruppgifter som läckt ut
- Kom ihåg att säkerhetskopiera
  - Gör säkerhetskopior av de viktigaste uppgifterna och tjänsterna
- Keep your software and systems updated
  - Updates contain vulnerability fixes
- Use multi-factor authentication
  - Multi-factor authentication complements the use of a user ID and password
- Do not use the same passwords in several different services
  - By using different passwords for each service, you can prevent extensive exploitation of leaked IDs
- Remember to take backups
  - Make backup copies of key data and services

**Varför görs dataintrång och varför  
lönar det sig att skydda sig mot  
dem?**

**Why are data breaches made and  
why is it worth protecting against  
them?**

# Gör så här om du blivit föremål för dataintrång

## Do the following if you have been the target of a data breach

- Anmäl
    - Om du upptäcker eller misstänker att du blivit föremål för ett dataintrång, ska du alltid göra en anmälan till Cybersäkerhetscentret samt göra en polisanmälan
    - Om angriparen till följd av ett dataintrång har fått tillgång till skyddad eller sekretessbelagd information, är det fråga om en dataläcka
    - Om du misstänker att de uppgifter som läckt ut omfattar andra personers personuppgifter är det fråga om en dataskyddsförseelse som ska anmälas till dataombudsmannen
  - Isolera hackade objekt
  - Byt lösenord / lås användaruppgifter
  - Säkra loggarna
  - Återställ säkerhetskopior
  - Kom ihåg kommunikationen
- Report it
    - If you discover or suspect that you have been the subject of a data breach, you must always report it to the National Cyber Security Centre in Finland and also to the Police
    - If, as a result of a data breach, the attacker has gained access to protected or classified information, it is a data breach
    - If you suspect that the leaked information includes other people's personal data, it is a data protection offense that must be reported to the Data Protection Ombudsman
  - Isolate hacked objects
  - Change passwords / Lock user IDs
  - Secure the logs
  - Restore backups
  - Remember the communication



**Tom Tuunainen**  
**Centria SecuLab**  
**seculab@centria.fi**  
**<https://seculab.fi>**

