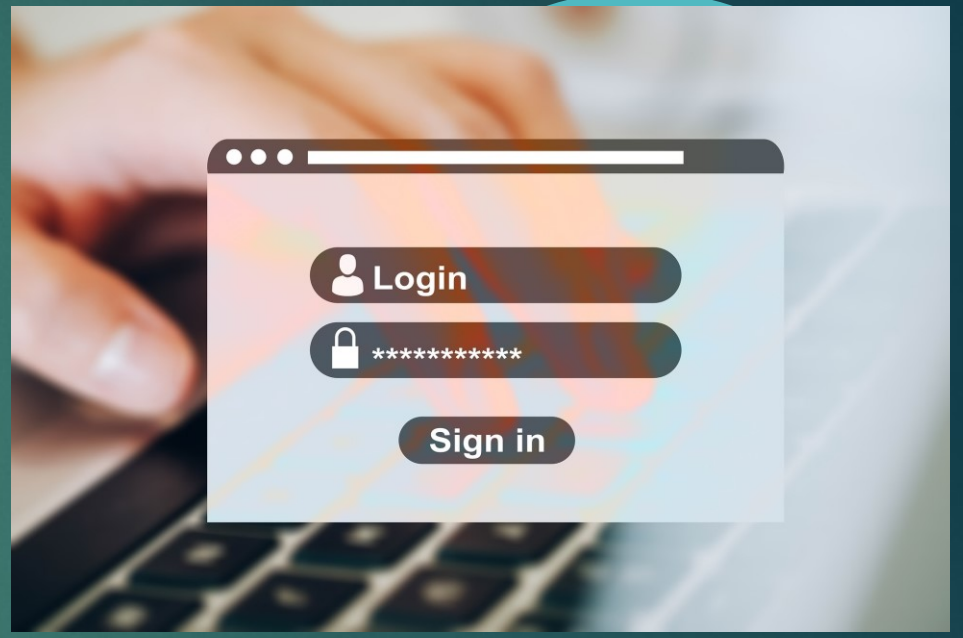
Allmänt säkerhetsnycklar

- Typ av autentiseringsteknik
- Starkaste skyddet mot nätfiske
- Säkerhetsnycklar kan bara finnas på dina enheter som t.ex. smarttelefonen eller som en fysisk nyckel.
- Finns flera typer av säkerhetsnycklar (programvarunycklar, hårdvarunycklar)



Progamvarunycklar

- Programvarunycklar eller virtuella nycklar som genereras av applikationer som t.ex. Microsoft Authenticator, Google Authenticator

Kort beskrivning:

1. Ladda ner en authenticator app

2. Sammankopplar
   Gmail > Säkerhet > Tvåstegsverifiering
   (bild nästa sida)

3. Välj det alternativ du söker och följ de anvisningar som kommer fram

← Tvåstegsverifiering

Lägg till ett andra steg i kontot

Om du vill aktivera tvåstegsverifiering måste du först lägga till ett andra steg i Google-kontot, till exempel ett telefonnummer

Lägg till telefonnummer

Aktivera tvåstegsverifiering

Förhindra att hackare får åtkomst till ditt konto med hjälp av ett extra skydd.

Om du inte loggar in med en nyckel blir du ombedd att slutföra det säkraste andra steget som lagts till i kontot. Du kan uppdatera dina andra steg och inloggningsalternativ när som helst i inställningarna. Öppna säkerhetsinställningarna

Aktivera tvåstegsverifiering

Andra steg

Se till att de här uppgifterna är aktuella och lägg till fler inloggningsalternativ så att du alltid kan komma åt Google-kontot

Nycklar och säkerhetsnycklar	Lägg till en säkerhetsnyckel	>
Meddelande från Google	1 enhet	>
Autentisering	Lägg till autentiseringsapp	>
Telefonnummer	Lägg till ett telefonnummer	+

Hårdvarunycklar

- Hårdvarunycklar eller ”hardware keys” t.ex. Titan security Key, Yubikey
- Skyddar tjänster eller programvara då en **fysisk** enhet krävs för att få åtkomst till saker
- Autentisering via USB, NFC, Bluetooth (kan variera mellan modeller)
- Hårdvarunycklar stöder bl.a. Googles och Microsofts tjänster samt metaplattformernas (Facebook, Instagram...)
- Vid inloggning skrivs användarnamn, lösenord och sedan uppmanas du bekräfta med säkerhetsnyckeln genom att antingen ansluta den eller svepa över den eller trycka på den

← Tvåstegsverifiering

Lägg till ett andra steg i kontot

Om du vill aktivera tvåstegsverifiering måste du först lägga till ett andra steg i Google-kontot, till exempel ett telefonnummer

Lägg till telefonnummer

Aktivera tvåstegsverifiering

Förhindra att hackare får åtkomst till ditt konto med hjälp av ett extra skydd.

Om du inte loggar in med en nyckel blir du ombedd att slutföra det säkraste andra steget som lagts till i kontot. Du kan uppdatera dina andra steg och inloggningsalternativ när som helst i inställningarna. Öppna säkerhetsinställningarna

Aktivera tvåstegsverifiering

Andra steg

Se till att de här uppgifterna är aktuella och lägg till fler inloggningsalternativ så att du alltid kan komma åt Google-kontot

Nycklar och säkerhetsnycklar	Lägg till en säkerhetsnyckel	>
Meddelande från Google	1 enhet	>
Autentisering	Lägg till autentiseringsapp	>
Telefonnummer	Lägg till ett telefonnummer	+