

# Falska virusvarningar

Hur slippa falska virusvarningar på dator, iPhone, iPad, Android mobil och surfplatta?

Falska virusvarningar ("du har blivit hackad!", "installera detta nu!") är väldigt vanliga och bygger nästan alltid på att lura dig att klicka, ladda ner eller betala. Här är en tydlig guide för att bli av med dem – och undvika dem i framtiden – oavsett enhet:

---

## Grundregel (gäller ALLA enheter)

- Klicka **aldrig** på popups som säger att du har virus
- Ladda **inte ner appar/program** från okända källor
- Stäng fliken/appen direkt (inte via popup-knappar)
- Ge aldrig ut kortuppgifter eller lösenord

---

## Dator (Windows & Mac)

### Vanlig orsak:

Webbläsaren visar falska varningar via skadliga sidor eller notiser.

### Så fixar du:

1. **Stäng webbläsaren helt**
  - På Windows: Ctrl + Shift + Esc → avsluta webbläsaren
2. **Starta om utan att återställa filer**
3. **Ta bort skadliga tillägg**
  - Chrome: Inställningar → Tillägg → ta bort okända
  - Safari/Edge: samma princip
4. **Rensa notiser (vanlig bov!)**
  - I Chrome: Inställningar → Sekretess → Webbplatsinställningar → Notiser
  - Ta bort konstiga sidor
5. **Kör säkerhetsskanning**
  - Windows: Microsoft Defender
  - Mac: Inbyggt skydd + ev. gratisverktyg som Malwarebytes



## iPhone & iPad

### Viktigt:

iOS kan **inte få virus på det sätt** som dessa varningar påstår.

### Orsak:

Nästan alltid en webbsida i Safari.

### Lösning:

1. Stäng fliken (eller hela Safari)
2. Gå till:
  - Inställningar → Safari → **Rensa historik och webbplatsdata**
3. Blockera popup-fönster:
  - Inställningar → Safari → aktivera “Blockera popupfönster”

👉 Installera aldrig appar via sådana varningar.

---

## Android (mobil & surfplatta)

### Vanlig orsak:

Skadliga appar eller webbsidor.

### Gör så här:

1. **Avinstallera misstänkta appar**
  2. Kontrollera appar med särskilda rättigheter:
    - Inställningar → Appar → Specialåtkomst
  3. Kör skanning med:
    - Google Play Protect
  4. Rensa webbläsaren (Chrome):
    - Inställningar → Sekretess → Rensa data
- 

## Tecken på att det är en bluff

- Räkner ner tid (“du har 30 sekunder!”)
- Skriker i versaler eller med ljud
- Ber dig ringa ett nummer
- Vill att du installerar något direkt
- Påstår att det är från Microsoft eller Apple (de gör inte så)

---

### Extra skydd (rekommenderat)

- Håll system och appar uppdaterade
- Använd annonsblockerare i webbläsaren
- Klicka inte på misstänkta länkar (mail/SMS)
- Aktivera tvåfaktorsinloggning

---

### Om du redan klickat eller laddat ner något

- Ta bort det direkt
- Byt lösenord (speciellt e-post & bank)
- Kontrollera banktransaktioner
- Kör viruskanning