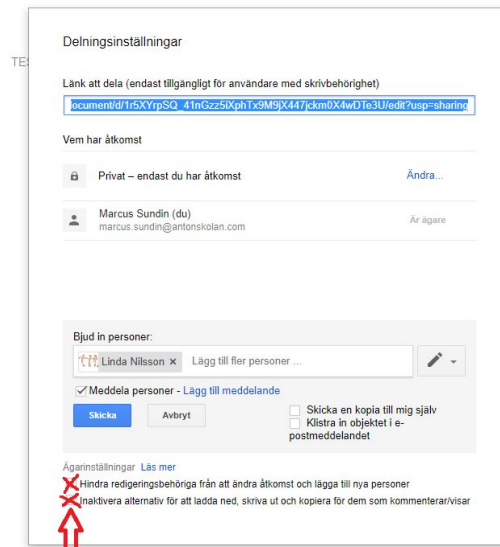


Rutiner för hantering av personuppgifter i Google Drive

- Följ instruktioner för "Google Drive tvåfaktorsautentisering" för att få igång det
- Efter en arbetsdag skall du logga ut från Google Drive på alla enheter du innan loggat in på
- Gallra och rensa din Google Drive ifrån personuppgifter vi inte har laglig grund att spara
 - obs, vissa personuppgifter behöver vi spara långt efter ex eleven slutat men ska då lagras på annat sätt - se "Arkiveringsrutiner"
- Vid delning av ett google-dokument observera den andres behörighet till dokumentet, se bild



Google Drive tvåfaktorsautentisering

Google-kontot är ofta det konto vi använder till flest olika tjänster, till exempel e-posttjänsten Gmail. Att sätta på tvåfaktorsautentisering för ditt Google-konto är enkelt.

Google har [en speciell sida](#) för tvåfaktorsautentisering. Där skrollar du ned och trycker på "Kom igång". Då möts du av ett till steg där du återigen får trycka på "Kom igång". Du får sedan skriva in ditt lösenord.

Skydda ditt konto med tvåstegsverifiering

Du behöver lösenordet och en verifieringskod varje gång du loggar in på Google-kontot. [Läs mer](#)



Lägg till en extra säkerhetsnivå

Ange ditt lösenord och en unik verifieringskod som har skickats till mobilen.



Håll skurkarna borta

Även om någon får reda på ditt lösenord så räcker det inte för att logga in på ditt konto.

KOM IGÅNG

Du får sedan uppge om du vill autentisera med hjälp av sms eller via telefonsamtal, och till vilket telefonnummer. Google skickar sedan en kod till dig via mobilen som du får bekräfta, och du kan sedan välja "Aktivera". Sedan är tvåfaktorsautentisering aktiverat.

KONFIGURERA



Meddelande från Google

Du får ett meddelande från Google till mobilen. Tryck bara på **Ja** för att logga in.

LÄGG TILL TELEFONNUMMER



Appen Authenticator

Använd appen Authenticator för att få verifieringskoder gratis, även när mobilen är offline. Tillgängligt för Android och iPhone.

KONFIGURERA

LOGGA IN

Du kan komma att behöva logga in igen med ditt Google-konto på till exempel din mobil eller din dator. På sidan du då kommer till kan du se att tvåfaktorsautentisering är påslaget, och du kan också välja att aktivera fler alternativ om du till exempel skulle tappa bort din mobil eller om du skulle vara utomlands utan mobiltäckning. Ett alternativ är till exempel reservkoder som du kan skriva ut och använda i nödfall när du inte har tillgång till din mobil.

AVAKTIVERA

Du kan avaktivera tvåfaktorsautentisering genom att klicka på "Inaktivera". I samband med att du loggar in på en enhet kan du också välja att lägga till den som en "Betrodd enhet", då behöver du inte din mobil för att logga in på den. Det minskar dock säkerheten.