



Q-global

Guide til anvendelse af tofaktoraутентisering (2FA)

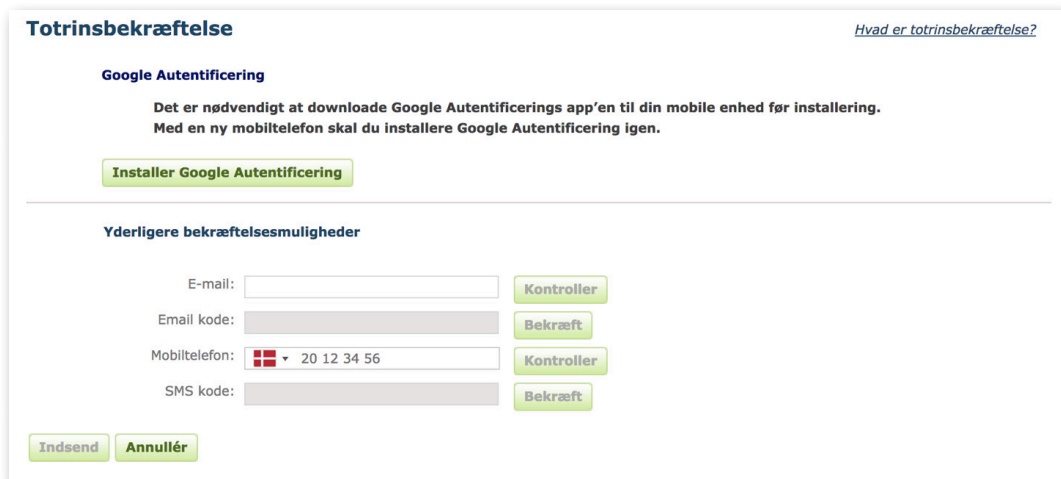
Q-global Brugervejledning

Marts 2018

Tofaktorautentisering (2FA) er et supplement til brugernavn og adgangskode, for yderligere at øge sikkerheden til kontoer på Q-interactive og Q-global. Når man logger ind med tofaktorautentisering angives brugernavn og adgangskode som vanligt, men også en engangskode, som kun du har adgang til. Således er der mindre risiko for, at andre kan få adgang til din data. Du har sandsynligvis brugt 2FA tidligere, for eksempel via netbank, sociale medier eller nem-id.

Pearson har implementeret tofaktorautentisering på Q-interaktive og Q-global for at imødekomme kravene fra den nye lov om personoplysninger og datasikkerhed, GDPR (General Data Protection Regulation).

Første gang du logger ind inden 2FA er aktiveret vil du blive mødt af et vindue, hvor du kan aktivere 2FA. Hvis du ønsker yderligere information om, hvad 2FA er kan du klikke på **Hvad er tofaktorautentisering?**.



Man kan ikke fortsætte på platformen før mindst én autentiseringsmetode er konfigureret. Nedenfor præsenteres fremgangsmåden for Q-global.

Du kan angive tre forskellige metoder til 2FA: Google Authenticator, SMS eller e-mail. Førstnævnte er en gratis applikation, som kan downloades på de fleste smartphones. Applikationen genererer engangskoder, som kan bruges til at verificere indlogging på en række forskellige hjemmesider og programmer. Google Authenticator er enkel at anvende og fungerer uden brug af internet eller netværkstilslutning. Applikationen genererer nye engangskoder hvert 30. Sekund, og er derfor en sikker metode til tofaktorautentisering.

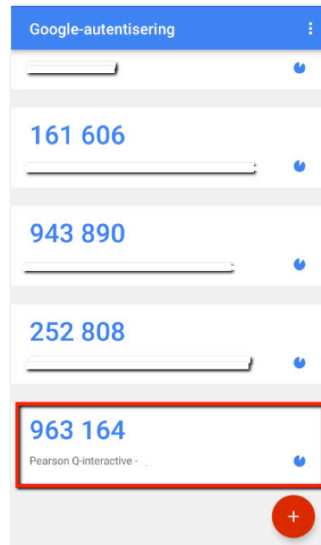
For at aktivere *Google Authenticator* skal du først downloade applikationen. Søg på Google Authenticator i App Store eller Google Play afhængigt af, om du har en iPhone - eller androidtelefon. Når Google Authenticator er installeret på telefonen, åbner du programmet og trykker på +tegnet. Vælg "Scan en strejkode" og godkend, at applikationen må få adgang til kameraet.

Klik på **Konfigurer Google Authenticator**.

Her præsenteres en strejkode (QR-kode), som skal scannes med mobiltelefonen.



Tag telefonen og peg kameraet mod stregkoden på Q-global, således at stregkoden vises på skærmen på telefonen. Et 6-cifret tal præsenteres på telefonen:




Angiv tallet (6 cifre, mellemrum er ikke nødvendigt) i feltet "Skriv koden fra appen:" og klik på **Bekræft**. Et grønt flueben vises, som bekræfter, at koden er verificeret. Klik derefter på **Indsend**.

Bekræft, at 2FA er aktiveret. Du kan nu klikke på **Hjem** øverst til venstre for at gå til Q-global.

Google Authenticator er nu aktiveret på kontoen og du skal angive et 6-cifret tal fra applikationen, når du logger ind på Q-global. 2FA er gyldig i 12 timer på samme enhed.

2FA per SMS eller e-mail kan konfigureres på lignende måde.



Yderligere bekræftelsesmuligheder

E-mail:

Email kode:

Mobiltelefon:

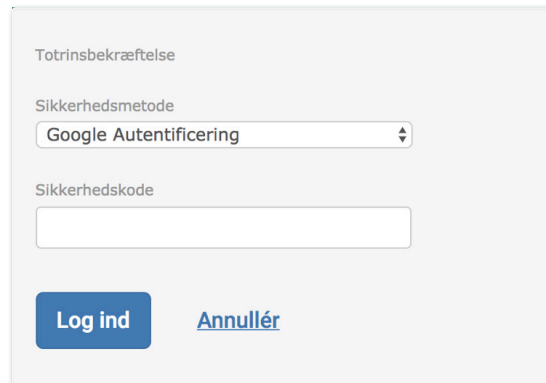
SMS kode:

Angiv e-mail eller mobiltelefonnummer og klik på **Valider**. En engangskode sendes til din e-mail eller telefon afhængigt af metoden, som du har valgt. Angiv koden i feltet nedenfor og klik på **Bekræft**. Et grønt flueben verificere at configurationen er fuldført. Klik på **Indsend** nederst til venstre for at gemme.

Næste gang du logger ind får du besked på at angive 2FA metoden. Hvis du har valgt flere forskellige metoder, kan du vælge mellem disse. Vælg for eksempel at modtage en kode per e-mail eller anvend Google Authenticator.

Angiv koden fra Google Authenticator og klik på **Log ind**.

Hvis du har valgt SMS eller e-mail, klik på **Indsend** og skriv koden ind, som du modtager. Klik derefter på **Log ind**.



Totrinsbekræftelse

Sikkerhedsmetode

Sikkerhedskode