KØBENHAVNS UNIVERSITET

06. MAJ 2026

Københavns Universitet beklager at måtte oplyse at et sikkerhedsbrud hos en leverandør til KU har fundet sted. Det betyder, at dine personlige oplysninger kan være stjålet eller kommet til kendskab for en uvedkommende aktør.

Ramte system:

Absalon, undertiden kendt som Canvas (systemnavn).

Omfattede data

Københavns Universitet har endnu ikke fået fuld information fra leverandøren om alle aspekter af sagen, men vi forventer at navne, KU-E-mailadresser og beskeder sendt i Absalon/Canvas er omfattet. Eksempelvis beskeder mellem studerende og studerende, samt studerende og undervisere. I Absalon/Canvas har du fortsat adgang til at se hvilke oplysninger du har udvekslet via beskeder, så du kan skabe dit personlige overblik over omfanget af bruddet.
Det er vigtigt at understrege, at der ikke har været adgang til CPR-oplysninger, da disse ikke opbevares i Absalon/Canvas, medmindre du har delt det via beskeder i Absalon/Canvas.

Hvad er der sket

Københavns Universitet har på nuværende tidspunkt ikke fuldt overblik over hvad der er sket eller hvordan det er sket, og hvad der er gjort for at stoppe det. Den nuværende opfattelse er, at en afpresningsgruppe har udført et angreb på vores leverandør, og at denne gruppe nu forsøger at afpresse leverandøren i bytte for ikke at offentliggøre filerne.

Leverandøren har endnu ikke oplyst, om det er alle Københavns Universitets brugere i Absalon/Canvas, der er omfattet af bruddet, men der er en formodning for at dette er tilfældet.
Den uvedkommende aktør er på nuværende tidspunkt ukendt for Københavns Universitet. Københavns Universitet er dog bekendt med, at en navngiven afpresningsgruppe tilsyneladende har taget ansvaret for bruddet, og hævder at have adgang til oplysninger om 275 millioner brugere på tværs af ca. 8800 organisationer. Vores vurdering er på nuværende tidspunkt, at hændelsen påvirker globalt. Leverandøren bekræftede dette sent 5. maj, 2026.

Hvad gør Københavns Universitet

Københavns Universitet har forsøgt at samle al tilgængelig information ift. hændelsen, på et tidspunkt hvor oplysningerne er få fra leverandøren. Københavns Universitet har derfor udført sin egen undersøgelse med henblik på at skaffe så mange oplysninger som muligt.
Københavns Universitet har herudover rejst flere spørgsmål og bekymringer overfor leverandøren, og forventer at få svar herpå snarest muligt omkring hændelsens karakter.
Herudover har vi bedt om at få yderligere oplysninger omkring sikkerheden umiddelbart før og efter hændelsen. Vi vil bruge disse oplysninger til at sikre os, at leverandøren lever op til sine forpligtelser til at beskytte informationer, som Københavns Universitet har betroet leverandøren med.
Slutteligt har Københavns Universitet underrettet det danske Datatilsyn d. 5. maj, 2026.

Fremtidig brug af Absalon/Canvas

Systemet er stadig i drift. Absalon er en nødvendig del af Københavns Universitets drift, og du kan fortsætte med at bruge det. Leverandøren informerer os om, at de har fortaget sikkerhedsopdateringer af systemet. Vi anbefaler dog, at du overvejer nøje hvilke oplysninger du vælger at udveksle i private beskeder i Absalon/Canvas. Absalon/Canvas er ikke godkendt til følsomme eller fortrolige personoplysninger og vi fraråder at der udveksles beskeder med sådant indhold på platformen.

Hvad kan du gøre nu

Relevansen af de følgende råd afhænger af, at vores nuværende forståelse af situationen er korrekt:

- Hvis din e-mail eller telefonnummer bliver lækket, stjålet eller på anden vis kommer til uvedkommendes kendskab, så kan disse oplysninger bruges til at kontakte dig. Hvis en angriber på samme tid

har øvrige oplysninger om dig, for eksempel at du arbejder eller læser på Københavns Universitet, så kan disse oplysninger bruges til at udsætte dig for mere troværdige phishing (e-mail) / smishing (SMS)-angreb. Disse angreb forsøger at få oplysninger ud af dig. Ofte fx password eller kreditkort-information. Det sker oftest ved, at en angriber sender links vedrørende meget hastende forhold. På den baggrund råder Københavns Universitet til, at alle studerende og ansatte udviser ekstra agtpågivenhed når de modtager uventet kommunikation der vedrører hastende forhold, som kræver øjeblikkelig opmærksomhed.
Husk at du altid kan få bekræftet en henvendelse hos Københavns Universitet, ved at kontakte universitetet direkte gennem via de kommunikationsoplysninger, som er listet på KU's hjemmeside.

- Private beskeder: Afhængig af hvad de indeholder kunne en sofistikeret angriber forsøge at bruge sådanne oplysninger til, at overbevise dig om, at de er nogen du kender personligt. Overvej altid muligheden for, at selv personer du kender, kunne være nogen der har fået sin konto stjålet eller efterlignet af en angriber. Del aldrig betalingsoplysninger eller passwords med nogen.

- Faglig tilknytning: Konsekvensen af disse data afhænger meget af personlige omstændigheder. For mange mennesker er sådanne oplysninger fuldt ud offentlige, mens andre ønsker at holde det mere privat. Af disse grunde er det vanskeligt at give specifik rådgivning.

- Herudover råder Københavns Universitet altid sine studerende og sine ansatte til at slå multifaktorvalidering til på alle digitale services, hvor det er muligt.

Københavns Universitet vil dog gerne understrege, at Absalon/Canvas respekterer navne- og adressebeskyttelse registreret via borger.dk. Det betyder, at hvis du har navne- og adressebeskyttelse, så vil dit navn tilknyttet dine fag og beskeder fremstå som dit brugernavn for både for- og efternavn.

Skulle du have navne- og adressebeskyttelse, men samtidig have valgt at bruge KU's aliassystem og indtastet et navn der, da skal du være opmærksom på, at det sandsynligvis er det valgte alias, der vil fremgå af sikkerhedsbruddet.

Hvis du har nogen spørgsmål, er du velkommen til at kontakte Københavns Universitet på: digitalisering@adm.ku.dk

Som altid: Hvis du mistænker at nogen har misbrugt din konto eller dine data, kontakt da IT-support: KU IT – Københavns Universitet

Hvis du har spørgsmål til dine rettigheder eller har bekymringer i forhold hvad delingen af dine oplysninger har af betydning for dig som person, kan du kontakte Københavns Universitets Databeskyttelsesrådgiver findes kontaktoplysningerne herunder:
Databeskyttelsesrådgiver: Mads Tolderlund
E-mail: dpo@adm.ku.dk

Dine spørgsmål vil blive besvaret så hurtigt som muligt, men vi forventer mange spørgsmål, og vil sandsynligvis ikke kunne svare alle med det samme.