Til rette vedkommende / to whom it may concern

Underretning om brud på persondatasikkerheden / Notification of a personal data breach

28. OKTOBER 2026

Please note that this document contains both a Danish and an English version of the same letter. The English version is included below after the Danish version.

Du modtager denne underretning, fordi Københavns Universitet desværre har konstateret, at universitetet er blevet hacket, og angriberne har hentet personoplysninger, som vedrører dig, ud af de berørte systemer. Københavns Universitet har haft disse oplysninger om dig, fordi du er eller har været tilknyttet universitetet.

Hvad er der sket?

Københavns Universitet blev d. 16. oktober og i dagene herefter ramt af et cyberangreb, som medførte, at angriberen kunne tiltvinge sig adgang til systemer, som normalvis er forbeholdt en begrænset mængde af KU's IT-ansatte. Angrebet har været rettet imod flere forskellige systemer, og Københavns Universitet har desværre konstateret, at angrebet mod ét af systemerne var succesfuldt. Det betyder, at angriberen har haft adgang til en database, som indeholder personoplysninger.

Det er endnu ikke klart for Københavns Universitet, hvad motivet er for angrebet eller hvordan hackerne vil håndtere de stjålne data.

På nuværende tidspunkt har vi konstateret, at angriberen har hentet nedenstående typer af data ud. Bemærk dog at ikke alle typer af oplysninger gælder for alle personer. Jo ældre din tilknytning til Københavns Universitet er, jo færre oplysninger har vi som hovedregel om dig.

- Dit fulde navn, som det fremgår eller fremgik af f.eks. dit pas eller sygesikringsbevis. Det er vigtigt at fastslå, at dit pas og sygesikringsbevis, ikke er omfattet af bruddet.
    - De berørte data stammer fra en årrække. Det betyder, at man i visse tilfælde også kan udlede udviklingen i ens navnehistorik.
    - For folk med navnebeskyttelse vil deres navn fremgå af listen, men bruddet omfatter ikke private fysiske adresser.
- Privat telefonnummer, såfremt du har oplyst dette til os, f.eks. i forbindelse med oprettelse af din brugerkonto, via selvbetjeningssystemet eller som en del af din ansættelse.
- Private e-mailadresser, såfremt du har oplyst dette til os, f.eks. i forbindelse med oprettelse af din brugerkonto, via selvbetjeningssystemet eller som en del af din ansættelse.
- Pinkode til dit KU-adgangskort. Hvis du har skiftet det til en selvvalgt kode på KUnet, skal du være opmærksom på, at såfremt du har genbrugt denne kode på en anden platform, f.eks. din bank, vil vi anbefale, at du straks ændrer koden på de pågældende platforme.
- Statsborgerskab.
- Nationalitet.
- Køn.
- KU-brugernavn (i stil med 'abc123').
- Arbejdsadresse eller hvor du som studerende er tilknyttet (studie).
- Stillingsbetegnelse, såfremt du er/har været ansat eller som studerende har oplyst en stillingsbetegnelse hos os i forbindelse med oprettelse af din brugerkonto til KU's systemer.
- Arbejdstelefonnummer.
- KU-mailadresse. Hvis du er ansat, er denne dog allerede offentlig i bl.a. Københavns Universitets telefonbog.
- Hvorvidt der er en aktiv tilknytning til KU pr. januar 2026.

Hvordan blev sagen opdaget?

Sagen blev opdaget af KU IT's egne medarbejdere d. 20. oktober 2026. Her blev det konstateret, at et IT-system havde foretaget en række handlinger, som det ikke burde have gjort. Dette viste sig at dække over angriberens igangsatte handlinger.

Hvilke konsekvenser kan det have for dig?

De data, som er blevet hentet ud, blev senest delvist opdateret 13. januar 2026. Det betyder, at hvis du f.eks. har skiftet navn eller telefonnummer siden da, så vil angriberne ikke have disse oplysninger.

Hvis angriberne har hentet dit navn, så kan de bruge dette i kombination med kontaktoplysninger om dig. Dermed vil de vide præcist hvad du hedder, hvilket kan gøre f.eks. svindelforsøg mere overbevisende.

Dit arbejdstelefonnummer eller private telefonnummer kan misbruges til at forsøge at kontakte dig med svigagtige formål.

Din private mailadresse kan bruges til at kontakte dig skriftligt med svigagtige formål. Det kan eksempelvis være såkaldte phishing-forsøg, hvor en afsender kan forsøge at lokke dig til at afgive flere personoplysninger, f.eks. betalingsoplysninger. Disse forsøg er desværre almindelige, og jo flere oplysninger en angriber allerede har om dig, desto mere troværdige bliver sådanne forsøg.

Oplysninger om din pinkode kan bruges til forsøg på misbrug andre steder, hvor du måtte have en firecifret kode.

Selvom de kompromitterede oplysninger normalt ikke i sig selv er tilstrækkelige til at oprette bankkonti, optage lån eller få adgang til digitale selvbetjeningsløsninger hos f.eks. offentlige myndigheder, kan de indgå som led i forsøg på identitetstyveri og anden økonomisk kriminalitet.

Københavns Universitet anbefaler derfor, at du er særligt opmærksom på uventede henvendelser via e-mail, SMS eller telefon, og at du ikke deler adgangskoder, MitID-oplysninger eller andre fortrolige oplysninger som følge af sådanne henvendelser.

Særligt hvis du har navne- og adressebeskyttelse

Selvom du har navnebeskyttelse, så vil dit navn med stor sandsynlighed fremgå i de hentede oplysninger. Årsagen er, at selvom Københavns Universitet har foranstaltninger til at sikre imod tilgang til beskyttede navne, så kan man ud fra de stjålne data i mange tilfælde udlede, hvad det oprindelige navn var.

Din private fysiske adresse har ikke været omfattet af bruddet.

Du kan se mere her i forhold til gode råd, hvis du er særlig udsat: https://samsik.dk/artikler/2026/10/ny-vejledning-raad-til-borgere-med-behov-for-ekstra-sikkerhed-ved-laek-af-personoplysninger/

For nuværende ansatte og studerende

Det betyder, at man ud fra kombinationen af oplysninger kan udlede i hvilke bygninger, du har en tilknytning til Københavns Universitet. Disse oplysninger er i mange tilfælde historiske, men kan også i en række tilfælde være aktuelle pr. 13. januar 2026. Hvis du måtte have ønske om at få oplysninger om, hvilke lokaliteter, der er knyttet til dig i materialet, så er du velkommen til at kontakte os.

Hvad har vi gjort?

Københavns Universitet har naturligvis straks lukket for adgangen til de berørte systemer og indledt en grundig undersøgelse af hændelsen. Sådanne undersøgelser er desværre komplekse og kræver både mange fagligheder og stor grundighed.

Undersøgelsen kompliceres også af, at angribere stort set altid vil forsøge at slette deres spor.

Herudover har Københavns Universitet anmeldt bruddet til de relevante myndigheder, herunder Politiet og Datatilsynet. Dette er sket d. 23. oktober 2026.

Hvad kan du selv gøre?

Københavns Universitet anbefaler, at du udviser høj agtpågivenhed ved uventede henvendelser, uanset om de er telefoniske eller skriftlige. Københavns Universitet anbefaler ligeledes, at du reagerer prompte, hvis du måtte modtage varer eller blive opkrævet betalinger, som du ikke kender til. I så fald anbefaler vi, at du kontakter din bank og eventuelt indgiver en politianmeldelse.

I den forbindelse skal Københavns Universitet naturligvis gøre opmærksom på, at du skal være særligt opmærksom på henvendelser, som giver sig ud for at komme fra din bank, dit forsikringsselskab eller pensionsselskab. Hvis du har brug for at kontakte dem for at bekræfte, om en henvendelse er ægte, så find altid selskabets telefonnummer på dets officielle hjemmeside. Klik aldrig på links i de henvendelser, som du mistænker for at være svindel.

Vær også særligt opmærksom, hvis du har genbrugt din pinkode til dit KU-adgangskort andre steder, f.eks. til dine bankkort eller pinkoder til elektronisk udstyr. I så fald anbefales du at skifte disse.

Følg sagens udvikling

Københavns Universitet foretager fortsat undersøgelser af sagen. Du kan på www.ku.dk og www.KUnet.dk følge med i de konklusioner, som Københavns Universitet når frem til, efterhånden som vi bliver sikre på svarene.

Bemærk, at det kan være nødvendigt selv at indtaste www. før ku.dk for at få adgang hertil.

Du kan også, på denne side, finde kontaktoplysninger til Københavns Universitets databeskyttelsesrådgiver.

Klage til Datatilsynet

Hvis du ønsker at klage over Københavns Universitets behandling af dine personoplysninger, kan du kontakte:

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
Telefon: 33 19 32 00
E-mail: dt@datatilsynet.dk
Hjemmeside: https://www.datatilsynet.dk/

Venlig hilsen

Københavns Universitet

You are receiving this notification because the University of Copenhagen unfortunately has confirmed that the university has been hacked and that the attackers have extracted personal data relating to you from the affected systems. The University of Copenhagen held this information about you because you are, or have been, affiliated with the university.

What has happened?

On 16 October and in the days that followed, the University of Copenhagen was hit by a cyberattack, which enabled the attacker to gain unauthorised access to systems normally restricted to a limited number of the University's IT staff. The attack targeted several different systems, and the University of Copenhagen has unfortunately confirmed that the attacks on one of the systems were successful. As a result, the attacker gained access to a database containing personal data

It is not yet clear to the University of Copenhagen what the motive for the attack is or how the hackers intend to handle the stolen data.

At this time, we have determined that the attacker extracted the types of data listed below. Please note, however, that not all categories of information apply to every individual. As a general rule, the longer ago your affiliation with the University of Copenhagen was, the less information we hold about you.

- Your full name, as it appears or appeared on, for example, your passport or national insurance card. It is important to note that your passport and national insurance card are not affected by the breach.
    - The affected data spans a number of years. This means that, in certain cases, it is also possible to trace the development of one's name history.
    - For people with name protection, their name will appear in the compromised data, but the breach does not include private physical addresses.
- Private telephone number, if you have provided this to us, for example when creating your user account, via the self-service system or as part of your employment.

- Private email addresses, if you have provided these to us, e.g. when creating your user account, via the self-service system or as part of your employment.

- PIN for your UCPH access card. If you have changed this to a PIN of your own choosing on KUnet, please be aware that if you have reused this PIN on another platform, e.g. your bank, we recommend that you change the PIN on those platforms immediately.

- Citizenship.

- Nationality.
- Gender.
- UCPH username (e.g. ‘abc123’).
- Work address or where you are affiliated as a student (your UCPH department).
- Job title, if you are or have been employed, or if, as a student, you provided a job title to us when creating your user account for the University of Copenhagen’s systems.
- Work telephone number.
- University of Copenhagen email address. However, if you are an employee, this is already publicly available in, for example, the University of Copenhagen’s telephone directory.
- Whether you have an active affiliation with the University of Copenhagen as of January 2026.

How was the incident discovered?

The incident was discovered by KU IT’s own staff on 20 October 2026. It was found that an IT system had carried out a series of actions that it should not have performed. This turned out to be a cover-up for the actions initiated by the attacker.

What consequences might this have for you?

The data that was extracted was last partially updated on 13 January 2026. This means that if you have changed your name or telephone number since then, the attackers will not have this information.

If the attackers have obtained your name, they can use this in combination with your contact details. This means they will know exactly what your name is, which could make attempts at fraud, for example, more convincing.

Your work or home telephone number could be misused to try to contact you for fraudulent purposes.

Your personal email address could be used to contact you in writing for fraudulent purposes. This could, for example, involve so-called phishing attempts, where a sender may try to trick you into disclosing further personal details, such as payment details. Unfortunately, these attempts are

common, and the more information an attacker already has about you, the more credible such attempts become.

Information about your PIN can be used in attempts to commit fraud elsewhere where you may have a four-digit code.

Although the compromised information is not usually sufficient in itself to open bank accounts, take out loans or gain access to digital self-service solutions with, for example, public authorities, it may form part of attempts at identity theft and other financial crime.

The University of Copenhagen therefore recommends that you pay particular attention to unexpected communications via email, text message or telephone, and that you do not share passwords, MitID details or other confidential information in response to such communications.

Especially if you have name and address protection

Even if you have name protection, your name is highly likely to appear in the retrieved information. The reason is that, although the University of Copenhagen has measures in place to prevent access to protected names, in many cases it is possible to deduce what the original name was from the stolen data.

You can find more information and practical advice here if you are particularly vulnerable or exposed (in Danish): https://samsik.dk/artikler/2026/10/ny-vejledning-raad-til-borgere-med-behov-for-ekstra-sikkerhed-ved-laek-af-personoplysninger/

Your private home address has not been affected by the breach.

For current staff and students

This means that, based on the combination of information, it is possible to deduce in which buildings you have an affiliation with the University of Copenhagen. In many cases, this information is historical, but in a number of cases it may also be current as at 13 January 2026. If you would like information about which locations are linked to you in the data, please feel free to contact us.

What has UCPH done?

The University of Copenhagen has, of course, immediately blocked access to the affected systems and launched a thorough investigation into the

incident. Unfortunately, such investigations are complex and require both a wide range of specialist expertise and a high degree of thoroughness.

The investigation is also complicated by the fact that attackers will almost always attempt to cover their tracks.

In addition, the University of Copenhagen has reported the breach to the relevant authorities, including the police and the Danish Data Protection Agency. This took place on 23 October 2026.

What can you do yourself?

The University of Copenhagen recommends that you exercise a high degree of caution when receiving unexpected communications, whether by telephone or in writing. The University of Copenhagen also recommends that you react promptly if you receive goods or are charged for payments that you are not aware of. In such cases, we recommend that you contact your bank and, if necessary, report the matter to the police.

In this context, the University of Copenhagen must emphasise that you should be particularly vigilant regarding communications that purport to come from your bank, your insurance company or your pension provider. If you need to contact them to confirm whether a communication is genuine, always find the company’s telephone number on its official website. Never click on links in communications that you suspect may be fraudulent.

You should also be particularly vigilant if you have reused the PIN for your UCPH access card elsewhere, for example for your bank cards or PINs for electronic devices. In such cases, you are advised to change them.

Follow developments in the case

The University of Copenhagen is continuing its investigations into the incident. You can follow the conclusions reached by the University of Copenhagen on www.ku.dk and www.KUnet.dk as we gradually become certain of the facts and findings.

Please note that it may be necessary to manually enter www. before ku.dk in order to access the website.

You can also find the contact details of the University of Copenhagen's Data Protection Officer on this page.

Complaints to the Danish Data Protection Agency

If you wish to lodge a complaint regarding the University of Copenhagen's processing of your personal data, please contact:

The Danish Data Protection Agency

Carl Jacobsens Vej 35

2500 Valby

Telephone: 33 19 32 00

Email: dt@datatilsynet.dk

Website: https://www.datatilsynet.dk/

Yours faithfully,

The University of Copenhagen