De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Ministerie van Onderwijs, Cultuur en Wetenschap

Hoger Onderwijs en Studiefinanciering
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Contactpersoon

Onze referentie
64012317

Uw brief
13 mei 2026

Uw referentie
2026Z09749

>Retouradres Postbus 16375 2500 BJ Den Haag

Datum 24 juni 2026

Betreft Antwoord op schriftelijke vragen van de leden El Boujdaini en Rooderkerk (beiden D66) over het bericht 'Studenten gewaarschuwd voor phishing na hack softwarebedrijf'

Hierbij stuur ik u de antwoorden op de vragen van de leden El Boujdaini en Rooderkerk (beiden D66) over het bericht 'Studenten gewaarschuwd voor phishing na hack softwarebedrijf'.

De vragen werden ingezonden op 13 mei 2026 met kenmerk 2026Z09749.

De minister van Onderwijs, Cultuur en Wetenschap,

Rianne Letschert

De antwoorden op de schriftelijke vragen van het lid El Boujdaini en Rooderkerk (beiden D66) over het bericht 'Studenten gewaarschuwd voor phishing na hack softwarebedrijf' met kenmerk 2026Z09749, ingezonden op 13 mei 2026.

Vraag 1
Bent u bekend met het bericht van de NOS dat hackersgroep ShinyHunters, die eerder verantwoordelijk was voor de hack bij Odido, nu ook gegevens van miljoenen studenten, docenten en onderwijsmedewerkers via onderwijsplatform Canvas heeft buitgemaakt? [1]

Antwoord 1
Ja, daar ben ik mee bekend.

Vraag 2
Hoe beoordeelt u de ernst van dit datalek, mede gelet op de gevoeligheid van de buitgemaakte persoonsgegevens en mogelijk ook privécommunicatie van studenten, docenten en onderwijsmedewerkers?

Antwoord 2
De hack en de tijdelijke ontkoppeling van het systeem Canvas zorgde voor een enorm vervelende situatie voor diegenen van wie mogelijk data is buitgemaakt en voor studenten en medewerkers die hiervan hinder hebben ondervonden in het onderwijs en hun werk. De MBO-raad, UNL en VH hebben mij laten weten dat het op dit moment niet volledig is vastgesteld welke gegevens de hackersgroep precies heeft buitgemaakt. Hierover is contact tussen de instellingen en het bedrijf Instructure als leverancier van Canvas. Dit betekent dat er op dit moment nog geen goede schatting kan worden gemaakt door de instellingen van hoeveel studenten, docenten en onderwijsmedewerkers naar schatting zijn getroffen. De AVG is van toepassing op inbreuken in verband met persoonsgegevens (kortweg: datalekken). Er is door instellingen een voorlopige melding gedaan bij de Autoriteit Persoonsgegevens.

Vraag 3
Hoeveel studenten, docenten en onderwijsmedewerkers van Nederlandse onderwijsinstellingen zijn naar schatting getroffen en welke typen persoonsgegevens zijn daarbij buitgemaakt?

Antwoord 3
De MBO-raad, UNL en VH hebben mij laten weten dat op dit moment alleen bekend is welke instellingen getroffen zijn. Zij geven aan dat Instructure, de leverancier van Canvas, nog niet heeft aangegeven welke gegevens precies zijn buitgemaakt. Vermoedelijk gaat het om gegevens zoals namen en e-mailadressen van studenten en medewerkers en berichtenverkeer. De instellingen staan in contact met Instructure om hier meer duidelijkheid over te krijgen. Dat doen zij afzonderlijk van elkaar in verband met de individuele contracten van instellingen met deze leverancier. Instructure heeft de instellingen toegezegd dit overzicht op korte termijn te zullen verschaffen. Op dit moment kan er daarom nog geen goede schatting worden gemaakt van het aantal personen dat is getroffen door de hack.

Vraag 4
Welke gevolgen kan dit datalek hebben voor studenten, docenten en onderwijsmedewerkers, bijvoorbeeld in de vorm van phishing, identiteitsfraude of andere vormen van digitale criminaliteit en hoe kan worden voorkomen dat zij hiervan slachtoffer worden?

Antwoord 4
Als er sprake is van een datalek is het belangrijk om nu en in de komende tijd extra waakzaam te zijn voor mogelijke phishingmails en andere verzoeken waarbij persoonsgegevens of inloggegevens worden gevraagd. De instellingen wijzen hun studenten en medewerkers hier ook op. Op dit moment is nog niet volledig vastgesteld welke gegevens precies zijn buitgemaakt. Zodra hierover meer duidelijk is, zullen betrokkenen volgens de geldende procedures door de instellingen hierover worden geïnformeerd. De instellingen hebben hun studenten en medewerkers ook opgeroepen om zich te melden als zij getroffen worden naar aanleiding van de hack en zullen waar nodig passende ondersteuning bieden.

Vraag 5
Heeft u contact met de onderwijskoepels over wat nodig is om de gevolgen van dit datalek te beperken? Zo nee, bent u bereid hierover alsnog contact met hen op te nemen?

Antwoord 5
Het ministerie van OCW heeft nauw contact met de onderwijskoepels en SURF over de situatie en gevolgen van de hack. De instellingen houden zelf, als contracthouders met Instructure voor deze onderwijssoftware, contact met de leverancier. Daarin is het ministerie geen partij. Voorts nemen de instellingen hun verantwoordelijkheid in het informeren van hun studenten en medewerkers over de situatie en de gevolgen van de hack.

Vraag 6
Welke ondersteuning en informatie worden momenteel geboden aan getroffen studenten, docenten en onderwijsmedewerkers om misbruik van hun persoonsgegevens te voorkomen? Acht u deze ondersteuning voldoende en welke rol ziet u hierin voor uzelf?

Antwoord 6
Zie hiervoor het antwoord op vraag 4 en vraag 5.

Vraag 7
Is voor studenten, docenten en onderwijsmedewerkers voldoende duidelijk welke persoonsgegevens via onderwijsplatformen zoals Canvas worden verwerkt, met welke externe partijen deze gegevens worden gedeeld en hoe deze gegevens worden beschermd?

Antwoord 7
Het is de bevoegdheid van instellingen zelf om te bepalen of, en zo ja hoe, zij onderwijsplatformen zoals Canvas inzetten. Het is daarbij hun verantwoordelijkheid zich bewust te zijn van de gegevens die daarmee worden verwerkt. Daarbij zijn ze gehouden aan de hiervoor geldende wet- en regelgeving (AVG). Het verschilt per instelling welke

keuzes zij daarbij hebben gemaakt en welke gegevens worden verwerkt, met welke externe partijen deze worden gedeeld en hoe deze gegevens worden beschermd. Conform de geldende wet- en regelgeving is de instelling vervolgens ook zelf verantwoordelijk om in een (privacy) statement aan de betrokkenen gebruikers aan te geven welke gegevens er worden verwerkt en hoe deze worden beschermd.

Vraag 8
Vindt u het wenselijk dat Nederlandse onderwijsinstellingen onderhandelen met hackersgroep ShinyHunters naar aanleiding van het ultimatum rondom de hack op Canvas, waarbij wordt gedreigd buitgemaakte gegevens van studenten, docenten en medewerkers openbaar te maken, of bent u van mening dat overheids- en onderwijsinstellingen nooit zouden moeten ingaan op dergelijke eisen van cybercriminelen?

Antwoord 8
Instellingen geven aan niet benaderd te zijn door de hackgroep om losgeld te betalen. Instructure heeft gemeld een akkoord te hebben gesloten met de hackers en dat de buitgemaakte gegevens zouden zijn vernietigd. Instructure zegt hiervan bewijs te hebben ontvangen. Of er losgeld is betaald door Instructure is mij en de instellingen niet bekend. Het is aan ieder bedrijf om een eigen afweging te maken. Het dringende advies vanuit de overheid is om geen losgeld te betalen. Het betalen van losgeld biedt geen garantie dat criminelen systemen weer toegankelijk maken of gestolen data niet doorverkopen aan andere criminelen. Het uitbetalen van losgeld houdt bovendien het verdienmodel van criminelen in stand en lokt daarmee mogelijk nieuwe aanvallen op organisaties uit.

Vraag 9
Welke lessen trekt u uit dit incident en op welke wijze wordt deze kwestie betrokken bij de ontwikkeling van een duidelijk handelingskader voor slachtoffers van datalekken? [2]

Antwoord 9
De instellingen hebben aangegeven dit incident zowel afzonderlijk als in de sector te evalueren en de lessen die hieruit getrokken worden mee te nemen in de verdere ontwikkeling van hun beleid. Ik blijf hierover met hen in contact.
Het kabinet geeft in overleg met betrokken toezichthouders en andere experts uitvoering aan de motie-Rajkowksi c.a. (36800-VII, nr.78), opdat een duidelijk handelingskader voor slachtoffers van grote datalekken beschikbaar is. Ook de relevante lessen uit dit incident worden daarbij betrokken. Het streven is om uw Kamer spoedig nader te informeren over de uitvoering van deze motie.

[1] NOS, d.d. 6 mei 2026 'Studenten gewaarschuwd voor phishing na hack softwarebedrijf', nos.nl/artikel/2613377-studenten-gewaarschuwd-voor-phishing-na-hack-softwarebedrijf

[2] Kamerstuk 36800-VII, nr. 78.