

Foire aux questions à l'intention des élèves et des familles de Californie

Dernière mise à jour : 16 octobre 2026

1. Que s'est-il passé et qui est ETS ?

ETS est un organisme d'évaluation à but non lucratif, sous contrat avec l'État de Californie pour administrer les évaluations obligatoires prévues par les réglementations de l'État et les lois fédérales à tous les élèves inscrits dans les établissements scolaires publics de Californie. ETS contribue aux programmes d'évaluation à l'échelle de la Californie, notamment le California Assessment of Student Performance and Progress (CAASPP) et les English Language Proficiency Assessments for California (ELPAC).

Le 25 septembre 2026, ETS a détecté une activité non autorisée impliquant un site utilisant le protocole de transfert sécurisé de fichiers (SFTP) pour échanger avec le CDE des informations relatives aux évaluations à l'échelle de la Californie.

ETS a désactivé le compte concerné, mis hors ligne le site SFTP affecté et ouvert une enquête avec l'aide d'experts externes en cybersécurité. L'enquête a révélé qu'un tiers non autorisé avait utilisé un identifiant de connexion compromis pour accéder au site et copier des fichiers contenant des informations sur des élèves de Californie, à plusieurs reprises entre le 22 mai et le 18 septembre 2026.

Après avoir collaboré avec les forces de l'ordre et des experts en cybersécurité, ETS a pris des mesures pour réduire le risque de divulgation publique des données.

Grâce à une surveillance régulière du Web, ETS n'a découvert à ce jour aucun élément indiquant que les informations ont été rendues publiques.

2. Quelles informations étaient concernées ?

Des informations concernant les élèves californiens, notamment tous les élèves inscrits au cours des trois années scolaires précédentes, ont été consultées et copiées. Les informations consultées et copiées comprenaient des données démographiques, des données relatives à la participation aux programmes et des données d'évaluation des élèves, conservées par ETS dans le cadre des programmes d'évaluation à l'échelle de la Californie.

Les informations des élèves consultées et copiées varient selon les personnes, mais peuvent comprendre :

- le nom de l'élève, sa date de naissance, son adresse de résidence, son établissement scolaire, son district scolaire et son niveau scolaire ;

- l'identifiant de l'élève à l'échelle de l'État (Statewide Student Identifier, SSID) et son identifiant local. L'identifiant de l'élève à l'échelle de l'État (Statewide Student Identifier, SSID) est un numéro unique à 10 chiffres, généré de manière aléatoire et attribué à chaque élève du système scolaire public californien, de la maternelle à la fin du secondaire. Pour en savoir plus, consultez le site www.cde.ca.gov/ds/sp/cl/ssid.asp.
- les informations démographiques, notamment le genre, la race ou l'origine ethnique, la langue principale, le pays d'origine et le statut d'apprenant de l'anglais ;
- le statut de handicap et le statut au titre de la section 504, les aménagements prévus pour les évaluations et le type de handicap principal ;
- le statut d'admissibilité aux programmes suivants : Title I, Part A ; Title I, Part C ; McKinney-Vento ; et Military Connected Student ; et
- les informations relatives à la maîtrise de l'anglais ainsi que les données relatives à l'inscription, à la participation et aux résultats des évaluations à l'échelle de l'État, le cas échéant.

Le dossier de chaque élève ne contenait pas nécessairement tous ces types d'informations.

Les données consultées et copiées ne comprenaient aucun numéro de sécurité sociale, numéro de permis de conduire, numéro de passeport, renseignement sur les comptes financiers, renseignement sur les cartes de crédit ou de débit, ni aucun mot de passe de compte. L'incident n'a concerné aucune information personnelle des parents ou des tuteurs légaux.

Après avoir collaboré avec les forces de l'ordre et des experts en cybersécurité, ETS a pris des mesures pour réduire le risque de divulgation publique des données.

Grâce à une surveillance régulière du Web, ETS n'a découvert à ce jour aucun élément indiquant que les informations ont été rendues publiques.

3. Comment savoir si mes informations ou celles de mon enfant ont été consultées et copiées ?

Sur instruction du CDE, ETS informe les élèves et les familles concernés dont les informations ont été consultées et copiées lors de l'incident.

Si vous recevez un courrier de notification et/ou un e-mail concernant cet incident, cela signifie que vos informations et/ou celles de votre enfant figuraient dans les fichiers consultés et copiés.

L'absence de notification ne signifie pas nécessairement que vos informations et/ou celles de votre enfant n'ont pas été concernées.

Les personnes concernées comprennent des élèves et d'anciens élèves ayant été inscrits dans des établissements scolaires publics de Californie entre 2023 et l'année scolaire en cours, ainsi que des élèves ayant quitté un établissement scolaire de Californie depuis 2006 sans avoir confirmé auprès du CDE leur transfert dans un autre établissement.

La notification explique ce qui s'est passé, les types d'informations concernés, les mesures prises par l'État, les mesures prises par ETS, les services de protection contre l'usurpation d'identité disponibles et les mesures que vous pouvez prendre pour protéger les informations personnelles.

4. Cet incident concerne-t-il d'anciens élèves, y compris ceux qui sont aujourd'hui adultes ?

Oui. L'incident peut concerner d'anciens élèves, notamment, mais pas uniquement, des personnes qui étaient inscrites dans un établissement scolaire de Californie au cours des trois années scolaires précédentes.

Les anciens élèves concernés, y compris ceux qui sont aujourd'hui adultes, peuvent bénéficier gratuitement de services de protection contre l'usurpation d'identité si leurs informations ont été consultées et copiées lors de l'incident.

5. Qui peut bénéficier des services gratuits de protection contre l'usurpation d'identité et comment s'y inscrire ?

ETS offre aux élèves et anciens élèves concernés dont les informations ont été consultées et copiées un accès gratuit, pendant 24 mois, aux services de protection contre l'usurpation d'identité Experian IdentityWorks.

Deux offres de services sont disponibles :

- **Mineurs de moins de 18 ans** : Les parents ou tuteurs légaux peuvent inscrire les élèves concernés à Experian IdentityWorks Minor Plus. L'inscription à cette offre doit être effectuée au plus tard le 19 mars 2027. **Rendez-vous sur le site Web d'Experian IdentityWorks pour vous inscrire : www.experianidworks.com/minorplus.**

Les mineurs concernés qui atteignent l'âge de 18 ans avant le 19 mars 2029 peuvent s'inscrire à l'offre pour adultes dès leur 18e anniversaire, en utilisant le code d'activation de cette offre fourni avec la notification.

- **Adultes de 18 ans et plus** : Les adultes concernés, y compris les anciens élèves, peuvent s'inscrire directement à Experian IdentityWorks. L'inscription à cette offre doit être effectuée au plus tard le 19 mars 2027. **Rendez-vous**

sur le site Web d'Experian IdentityWorks pour vous inscrire :
www.experianidworks.com/identity

Les instructions d'inscription, notamment l'adresse du site Web et le code d'activation, figurent sur la page de notification www.cde.ca.gov/ets.

L'inscription est gratuite pour la personne concernée et aucune carte de crédit n'est requise.

Experian propose également une assistance au rétablissement de l'identité aux personnes concernées qui remplissent les conditions requises et qui sont victimes d'usurpation d'identité. Cette assistance est disponible pendant 24 mois à compter de la date de notification et ne nécessite pas d'inscription aux services de surveillance.

6. Que faire si je ne reçois pas de courrier de notification ?

L'absence de courrier de notification ne signifie pas nécessairement que vos informations n'ont pas été concernées. Certains élèves et anciens élèves peuvent ne pas recevoir de notification, notamment si leurs coordonnées ont changé.

Les personnes concernées comprennent des élèves et d'anciens élèves ayant été inscrits dans des établissements scolaires publics de Californie entre 2023 et l'année scolaire en cours, ainsi que des élèves ayant quitté un établissement scolaire de Californie depuis 2006 sans avoir confirmé auprès du CDE leur transfert dans un autre établissement.

Consultez la page www.cde.ca.gov/ets pour obtenir des informations sur les services de protection contre l'usurpation d'identité et connaître les démarches à suivre pour obtenir de l'aide.

7. Que peuvent faire les personnes concernées pour protéger leurs informations ?

Nous invitons les personnes concernées à envisager d'inscrire les élèves concernés aux services de protection de l'identité et à rester vigilantes face à toute utilisation abusive éventuelle de leurs informations personnelles.

Par mesure de précaution, méfiez-vous également des e-mails, SMS ou appels téléphoniques inattendus faisant référence à l'établissement scolaire d'un élève, aux évaluations à l'échelle de l'État ou à cet incident. Ne communiquez aucune information personnelle, aucun mot de passe ni aucune information financière en réponse à des demandes non sollicitées. Vérifiez les adresses des sites Web avant de saisir des informations personnelles pour vous inscrire aux services de protection contre l'usurpation d'identité.

Les adultes peuvent obtenir gratuitement leurs rapports de crédit sur www.annualcreditreport.com ou en appelant le 1-877-322-8228. Les adultes peuvent demander gratuitement le gel de leur propre dossier de crédit.

Les parents et tuteurs peuvent également envisager de demander gratuitement le gel du dossier de crédit de leurs enfants de moins de 16 ans, afin de contribuer à empêcher l'ouverture de comptes à leur nom sans autorisation.

Pour obtenir des informations complémentaires sur les rapports de crédit, les alertes à la fraude et le gel des dossiers de crédit, contactez :

- Equifax : 800-685-1111 | www.equifax.com
- Experian : 888-397-3742 | www.experian.com
- TransUnion : 833-799-5355 | www.transunion.com

Bien que les numéros de sécurité sociale et les informations relatives aux comptes financiers n'aient pas été concernés par l'incident, il est recommandé de prendre des précautions pour protéger les informations personnelles.

8. Comment savoir si une communication concernant cet incident est authentique ?

Faites preuve de prudence face aux e-mails, appels téléphoniques ou SMS inattendus qui prétendent émaner d'ETS, du CDE ou d'Experian au sujet de cet incident.

Ne communiquez aucun numéro de sécurité sociale, mot de passe, renseignement financier ou autre information personnelle sensible en réponse à des demandes non sollicitées.

Les personnes concernées recevront les instructions d'inscription aux services gratuits de protection contre l'usurpation d'identité dans leur courrier de notification www.cde.ca.gov/ets.

L'inscription est gratuite et ne nécessite pas de carte de crédit.

En cas de doute sur l'authenticité d'une communication, consultez la page Web officielle du CDE consacrée à l'incident à l'adresse www.cde.ca.gov/ets pour obtenir des informations.

9. Quelles mesures ETS et l'État prennent-ils pour faire face à l'incident et prévenir de nouveaux incidents ?

Depuis la découverte de l'incident, ETS a pris de nombreuses mesures pour renforcer la sécurité du site SFTP, notamment en mettant le site concerné hors

ligne et en créant un tout nouveau site SFTP doté de contrôles de sécurité renforcés. ETS continue d'évaluer les mesures de sécurité supplémentaires qui pourraient être appropriées.

Après avoir collaboré avec les forces de l'ordre et des experts en cybersécurité, ETS a pris des mesures pour réduire le risque de divulgation publique des données. En outre, grâce à une surveillance régulière du Web, ETS n'a découvert à ce jour aucun élément indiquant que les informations ont été rendues publiques.

Le CDE et le Conseil de l'éducation de l'État (SBE) collaborent avec des experts de l'État en cybersécurité afin d'évaluer les conséquences de l'incident pour les élèves et les familles de Californie et de veiller à ce que les personnes concernées reçoivent des informations et un soutien adaptés.

Le Centre californien d'intégration de la cybersécurité (Cal-CSIC) apporte son concours aux investigations numériques et à la réponse à l'incident. Le California Department of Technology (CDT) et le California Governor's Office of Emergency Services (Cal OES) contribuent également à la réponse de l'État sur les plans technique, juridique et opérationnel.

Le CDE et le SBE examinent l'incident ainsi que le respect, par ETS, des exigences applicables en matière de sécurité des données et de ses obligations contractuelles.

10. Pourquoi ETS avait-il accès à ces informations ?

ETS est un organisme d'évaluation à but non lucratif, sous contrat avec l'État de Californie pour administrer les évaluations obligatoires prévues par les réglementations de l'État et les lois fédérales à tous les élèves inscrits dans les établissements scolaires publics de Californie.

ETS conserve des données démographiques sur les élèves, des données sur leur participation à des programmes et des données d'évaluation dans le cadre des programmes d'évaluation organisés à l'échelle de l'État de Californie.