Lorsqu'un problème lié à l'IA est réel

Utilisez cette fiche plutôt que de poursuivre une leçon. La réaction dépend de la sécurité immédiate, du contenu concerné et des services d'aide locaux.

PREMIÈRE RÉACTION

« Merci de me l'avoir dit. Tu ne seras pas puni pour avoir demandé de l'aide. Nous allons résoudre cela ensemble. »

Dans toutes les situations : les six étapes

1. Mettez l'interaction en pause et vérifiez la sécurité physique et émotionnelle immédiate.
2. Écoutez sans blâmer ni interroger de manière insistante ; déterminez ce dont l'enfant a besoin maintenant.
3. En cas de danger immédiat ou de crainte que l'enfant se fasse du mal, sollicitez une aide humaine locale qualifiée en urgence. Ne demandez pas à l'IA de décider.
4. Conservez en lieu sûr les informations essentielles sur le problème, avec les conseils appropriés d'un adulte ou d'un professionnel ; ne transférez ni ne téléchargez d'images explicites.
5. Sécurisez les comptes et les autorisations selon les besoins ; utilisez les voies officielles de signalement du produit et de l'établissement scolaire.
6. Assurez un suivi, faites appel à une aide qualifiée lorsque c'est approprié et expliquez tout changement visant à protéger, sans punir.

Choisissez la réaction adaptée

ERREUR OU EXPOSITION : téléversement accidentel de données non sensibles ou autorisation accordée par erreur — cessez le partage, examinez les options de confidentialité et de suppression ainsi que les paramètres, et évaluez tout risque supplémentaire.

COMPTE COMPROMIS : utilisez la procédure officielle de récupération, changez les identifiants de connexion compromis, activez l'authentification multifacteur (MFA) et vérifiez les appareils ou les sessions associés.

MENACES, EXTORSION OU IMAGES ABUSIVES : ne payez pas, ne négociez pas, n'envoyez pas de contenu supplémentaire et ne redistribuez pas les images ; sollicitez une aide qualifiée en matière de protection et de signalement.

CONSEILS DANGEREUX OU DÉTRESSE : arrêtez l'interaction avec l'IA et mettez l'enfant en contact avec un véritable adulte de confiance et une aide professionnelle adaptée.

À RETENIR

Ne promettez pas de garder le secret si une intervention professionnelle de protection peut être nécessaire. Si des preuves peuvent être importantes, n'effacez pas automatiquement tous les messages ou comptes. Ne manipulez ni ne partagez d'images intimes pour « prouver » ce qui s'est passé.

Entraînez-vous avant une crise

Lisez ces scénarios fictifs à voix haute avec un autre adulte. L'objectif est de réagir calmement dans un premier temps et de choisir le bon interlocuteur à contacter ensuite, pas d'aller vite ni de donner une réponse parfaite.

A / Une autorisation accordée par erreur

Un enfant a autorisé une application de dessin à accéder à ses contacts et à sa localisation, mais dit qu'il ne voulait pas le faire.

Quelle première mesure de protection prendre ? Quels paramètres et quels éventuels partages examineriez-vous ?

B / Une fausse image d'un camarade de classe

Un élève reçoit une image retouchée humiliante d'un camarade de classe et on lui demande de la partager.

Comment soutenir l'enfant et éviter de propager le préjudice ?

C / Un agent conversationnel devient insistant

Un agent conversationnel dit à un adolescent de ne pas partir et lui suggère que personne dans sa famille ne le comprend.

Quels mots utiliseriez-vous pour le soutenir ? Quelle personne réelle pourrait l'aider ?

D / Un compte menaçant

Un compte inconnu menace de publier une image modifiée si on ne lui envoie pas d'argent ou d'autres contenus.

Que faut-il éviter ? Quelles personnes convient-il de faire intervenir ?

Approche suggérée : faire une pause ; reconnaître ce que la personne ressent ; vérifier sa sécurité immédiate ; éviter de partager, de payer ou de négocier ; conserver les éléments d'identification sans risque, avec l'aide d'un adulte ; solliciter une aide locale qualifiée selon les besoins.