École virtuelle:

11 façons d'assurer la sécurité de votre enfant en ligne

Septembre 2020 (mise à jour avril 2022)

Consultez notre liste de contrôle de sécurité en ligne. Elle vise à aider les parents ou les tuteurs à s'assurer que les enfants restent en sécurité tout en apprenant en ligne.

La rentrée scolaire signifie souvent de nouveaux crayons bien taillés, de nouvelles classes et de nouvelles routines. La pandémie de COVID-19 continue d'apporter de nouvelles structures et processus d'apprentissage à l'éducation. Quelques élèves poursuivent leurs études entièrement en ligne, certains suivront un mélange d'apprentissage virtuel et présentiel, et d'autres suivront en personne tous leurs cours. Quelle que soit la forme que prend la scolarité de vos enfants, il y a de fortes chances qu'ils doivent participer à des activités en ligne d'une manière ou d'une autre. Suivez ces étapes pour les protéger.

1. Supprimer la configuration des assistants intelligents pendant les heures de cours

Votre assistant intelligent est en permanence à l'affût d'un mot de « réveil », ce qui signifie qu'il peut écouter les cours de votre enfant et les conversations avec ses ami(e)s. Demandez à votre enfant de désactiver l'assistant vocal sur son ordinateur portable, sa tablette ou son téléphone. Si vous souhaitez supprimer des enregistrements, vous pouvez le faire sur les appareils Amazon Echo, Siri d'Apple et Google Home.

2. Utiliser un gestionnaire de mots de passe et des mots de passe uniques

Votre enfant peut utiliser plusieurs services sur son ordinateur portable, sa tablette ou son téléphone. Encouragez-le/la à utiliser des mots de passe uniques et un gestionnaire de mots de passe. Cela signifie qu'il/elle ne doit retenir qu'un seul mot de passe pour accéder à tous les autres mots de passe uniques qui lui permettent d'accéder à ses comptes sur tous les appareils. Vous et votre enfant pouvez en savoir

plus sur les différents gestionnaires de mots de passe en effectuant une recherche en ligne et en lisant les articles ici, ici et ici.

Les mots de passe ne doivent pas être faciles à deviner ni contenir des informations personnelles telles que les noms des animaux domestiques. Ils ne doivent pas être trop courts, car ils peuvent être faciles à craquer par les malfaiteurs. L'utilisation du même mot de passe pour tous les services peut exposer les informations de votre enfant à un risque accru de piratage. Il est beaucoup plus facile pour les malfaiteurs d'accéder aux comptes s'ils ont tous le même mot de passe. Rappelez-lui/la de ne jamais partager son mot de passe avec qui que ce soit.

3. Conserver un compte de messagerie principal

Expliquez à votre enfant qu'il est important de conserver son compte de messagerie principal, car de nombreux services utilisent cette adresse comme nom d'utilisateur de compte, pour communiquer les réinitialisations de mot de passe lorsqu'un mot de passe est oublié ou perdu, et pour l'identifier. Si son compte est piraté, un malfaiteur pourrait utiliser cet accès pour prendre le contrôle de ses autres comptes, y compris des personnages de jeu, et même se faire passer pour lui sur les réseaux sociaux. Utilisez un mot de passe fort et évitez d'utiliser des services qui suppriment automatiquement les comptes de messagerie après une période d'inactivité. N'oubliez pas de modifier l'adresse de courriel de tous les comptes de votre enfant avant de passer à une nouvelle adresse de courriel.

4. Utiliser l'authentification à deux facteurs

Certaines écoles utilisent peut-être déjà l'authentification à deux facteurs pour certains services, mais vous pouvez également vérifier quels services vous permettent d'ajouter cette couche de sécurité supplémentaire. Les meilleures options sont les applications d'authentification et les jetons d'authentification physiques que votre enfant peut brancher sur son ordinateur en tant que clé USB.

5. Rechercher des services avec un cryptage fort

Les commissions scolaires choisiront souvent les services utilisés pour le travail scolaire, mais vous pouvez également avoir votre mot à dire en vous assurant que votre enfant utilise d'autres services qui offrent un cryptage fort. Il/elle peut utiliser des services de messagerie cryptés de bout en bout pour communiquer avec ses camarades de classe. Encouragez-le/la à ne communiquer avec des ami(e)s qu'en groupes fermés et à signaler tout message indésirable. Rappelez-lui/la que ce qu'il/elle publie peut être copié et transmis sans sa permission, voire utilisé contre lui/elle. Effectuez des recherches en ligne pour déterminer quels services offrent un cryptage de bout en bout.

6. Choisir un navigateur et un moteur de recherche qui respectent la confidentialité

Les enfants peuvent passer beaucoup de temps à naviguer sur Internet pour leurs projets scolaires et à explorer ce qui est disponible en ligne à un niveau plus personnel. Une partie de ces recherches consiste à découvrir qui ils sont, leurs intérêts et leurs valeurs. L'historique de recherche de votre enfant peut révéler beaucoup de choses sur ses sentiments, ses espoirs et ses peurs les plus intimes. Choisissez un navigateur qui le/la protège des trackers et un moteur de recherche qui ne suit pas votre historique de recherche.

7. Utiliser un VPN

Un réseau privé virtuel (en anglais, Virtual Private Network ou VPN) peut empêcher l'utilisation d'Internet par votre enfant d'être observée par votre fournisseur d'accès Internet (FAI) et des tiers malveillants qui pourraient essayer d'espionner ou d'intercepter le trafic Internet. Si votre commission scolaire distribue des appareils, ceux-ci peuvent déjà inclure des VPN. Vous pouvez rechercher quel type de VPN vous conviendrait le mieux, à vous et à votre enfant.

8. Mises à jour logicielles régulières

Les mises à jour logicielles sont un moyen simple de s'assurer que les informations sont aussi sécurisées que possible. Les mises à jour logicielles corrigent les bogues et les vulnérabilités de sécurité et peuvent rendre les informations de votre enfant plus sûres. Exécutez les mises à jour logicielles pendant les pauses déjeuner ou après la fin de la journée de cours.

9. Sauvegarder les fichiers

Personne n'a envie de refaire ses devoirs. Encouragez votre enfant à enregistrer régulièrement ses devoirs et à faire une sauvegarde en cas de problème. Si votre enfant ou son école est victime d'une attaque, un malfaiteur peut compromettre des fichiers, notamment des documents scolaires importants, des notes de cours et des résultats, ou les verrouiller. Les commissions scolaires peuvent proposer des options de sauvegarde, mais vous pouvez également rechercher des fournisseurs de cloud et/ou des périphériques de stockage externes pour vous assurer que les fichiers de votre enfant sont en sécurité. N'oubliez pas de rechercher une option de sauvegarde cryptée et protégée par mot de passe.

10. Mettre en place un coffre-fort numérique

Il n'est jamais trop tôt pour encourager votre enfant à mettre en place un coffre-fort numérique sécurisé contenant des documents et des informations importants dont il pourrait avoir besoin en cas de catastrophe naturelle, d'urgence familiale ou d'une autre situation. C'est aussi un bon endroit pour stocker des copies de références professionnelles et de certificats de travail après ses études. Demandez à votre enfant s'il/elle a des souvenirs ou des fichiers qu'il/elle ne veut pas perdre (comme des romans graphiques, des histoires, des photos, des vidéos ou des œuvres d'art qu'il/elle a créées) et mettez une copie numérique dans son coffre-fort. Aidez-le/la à développer une stratégie pour s'assurer qu'il/elle ne « perd pas la clé » du coffre-fort!

11. Demander une formation à la sécurité en ligne

Suggérez à votre école ou à votre médiathèque d'introduire une formation sur la confidentialité et la sécurité en ligne dispensée par des étudiants plus âgés inscrits en informatique, en binôme avec des élèves plus jeunes. Toutes les commissions scolaires ou médiathèques n'auront pas les ressources pour offrir ces services, mais quelqu'un au sein de la communauté peut connaître quelqu'un qui pourrait aider à trouver les ressources humaines et financières pour le faire.