ARGENT & SÉCURITÉ

GUIDE N°9

ON

MODE PARENT : ON

LA COLLECTION DES PARENTS QUI GÈRENT

09

La sécurité numérique en famille

Mots de passe, arnaques, vie privée, IA, paiements : comprendre les risques et prendre les bons réflexes, parents et enfants ensemble. De 8 à 18 ans.

PAR THÈME

Mots de passe · Arnaques · Vie privée · IA · Paiements

INCLUS

Pages « Côté jeunes » · Plan d'urgence · 12 fiches



EXTRAIT GRATUIT

Collection Mode Parent : ON · Édition 2026 · France · Suisse · Belgique · Fondé sur les recommandations de l'OFCS, de Cybermalveillance.gouv.fr, de la CNIL, de la Banque de France, du Centre pour la cybersécurité Belgique et de Child Focus, avec activités en famille et fiches à imprimer

SOMMAIRE

Au programme

1	Pourquoi c'est l'affaire de toute la famille	4
2	Des mots de passe solides et un coffre-fort	6
3	La double authentification	8
4	Vie privée : ce qu'on partage en ligne	10
5	Les arnaques qui visent les jeunes	12
6	Les arnaques qui visent les parents	14
7	L'IA : voix clonées et fausses images	16
8	Payer en ligne quand on est jeune	18
9	Appareils, Wi-Fi et fuites de données	19
10	Le plan d'urgence : que faire, qui appeler	20
11	Quatre cas pratiques et la FAQ	22
12	Les 12 fiches à imprimer	23
13	Sources	35

Le principe du guide en une phrase

Dans notre famille, **un code ne se donne jamais**, **on vérifie avant de cliquer ou de payer**, et celui qui se fait avoir **le dit tout de suite, sans être puni**.

01

CHAPITRE 1

Pourquoi c'est l'affaire de toute la famille

Un compte de jeu rempli de skins, un compte WhatsApp qui permet d'écrire à toute la famille, des photos de vacances publiques, une carte prépayée chargée : pour un escroc, chaque membre de la famille a de la valeur. Le comprendre aide à protéger sans dramatiser.



Ce que disent les chiffres

79 %

des 8–17 ans voient des arnaques en ligne au moins une fois par mois (20 % tous les jours).

UK Safer Internet Centre, 2025

46 %

disent s'être déjà fait arnaquer en ligne ; 9 % y ont perdu de l'argent.

UK Safer Internet Centre, 2025

47 %

citent la honte comme premier frein pour en parler ; 40 % la peur d'avoir des ennuis.

UK Safer Internet Centre, 2025

Source : UK Safer Internet Centre, enquête Censuswide de septembre-octobre 2024 auprès de 2 013 enfants de 8 à 17 ans et 2 013 parents, publiée le 11 février 2025. Aucune enquête équivalente n'a été trouvée pour la Suisse, la France ou la Belgique.

Les jeunes rencontrent surtout les arnaques sur les **réseaux sociaux** (35 %), par **e-mail** (17 %) et dans les **jeux en ligne** (15 %, et 22 % chez les 8–11 ans). Les adultes ne sont pas épargnés : en France, la fraude par manipulation (faux conseiller bancaire, par exemple) a atteint 516 millions d'euros en 2025, en hausse de 34 % (Banque de France).

Ce qui intéresse les escrocs

Ce que la famille possède	Pourquoi ça vaut de l'argent
Un compte de jeu	Les objets virtuels (skins, monnaies) se revendent. L'OFCS décrit de fausses pages de connexion Steam visant les comptes qui contiennent des skins de valeur.
Un compte de messagerie	Une fois volé, il sert à écrire aux contacts, parents compris, pour réclamer de l'argent au nom de son propriétaire.
Une adresse e-mail	Elle sert à réinitialiser tous les autres comptes : celui qui la contrôle contrôle le reste.
Des photos et des infos publiques	Elles révèlent l'école, le quartier, les habitudes, et peuvent être détournées, y compris par l'IA (chapitres 4 et 7).
Une carte, un compte TWINT	L'argent qui s'y trouve, mais aussi le compte lui-même, qui peut servir à faire transiter de l'argent volé.

Le vrai risque : qu'il n'ose pas vous le dire

D'après la même enquête, **72 %** des jeunes iraient vers un parent en cas de problème, mais la honte et la peur d'avoir des ennuis, par exemple qu'on leur confisque leur appareil, en freinent beaucoup. Or, face à une

02

CHAPITRE 2

Des mots de passe solides et un coffre-fort

La Suisse, la France et la Belgique s'accordent sur l'essentiel : un mot de passe long, différent pour chaque compte, jamais partagé. Et pour ne pas devoir tous les retenir, un coffre-fort à mots de passe.



Les 5 règles communes

1. **Un mot de passe différent pour chaque compte.** C'est la règle n° 1 de l'OFCS, de Cybermalveillance.gouv.fr et du Centre pour la cybersécurité Belgique (CCB). Si un site se fait pirater, seul ce compte est touché.
2. **Au moins 12 caractères**, en mélangeant majuscules, minuscules, chiffres et caractères spéciaux (OFCS, Cybermalveillance.gouv.fr, Prévention Suisse de la Criminalité). La Police fédérale belge fixe le minimum à 8 : visez 12.
3. **Rien de prévisible :** ni prénom, ni date de naissance, ni nom du chien, ni « 123456 » ou « azerty ».
4. **Ne jamais le communiquer :** ni à un copain, ni à un « support ». Les banques et les opérateurs ne demandent jamais un mot de passe par e-mail ou par téléphone (OFCS).
5. **Le changer au moindre doute**, et partout où il était réutilisé. Pour un compte ordinaire, la CNIL ne recommande plus de le changer à intervalles réguliers ; la Police fédérale belge conseille encore de le faire.

Deux méthodes pour en créer un qu'on retient

La méthode des initiales

On garde la première lettre de chaque mot d'une phrase, avec les chiffres et la ponctuation. Exemple de la Prévention Suisse de la Criminalité : **« Ma fille Tamara Martin a sa fête le 19 janvier! »** → `MfTMasfl19j!`

La phrase de passe

Plusieurs mots au hasard, sans lien logique. Pour la CNIL, une phrase de passe d'**au moins 7 mots** vaut 12 caractères mélangés. Exemple (à ne pas réutiliser) : `girafe-tunnel-violon-sable-orage-lundi-pomme`

Le compte à protéger en premier : l'e-mail

La boîte e-mail sert à **réinitialiser tous les autres comptes** (Cybermalveillance.gouv.fr). Il lui faut le mot de passe le plus long, jamais réutilisé, et c'est le premier compte à protéger par la double authentification.

Le coffre-fort à mots de passe

Personne ne peut retenir 80 mots de passe différents. Un **gestionnaire de mots de passe** les retient pour vous, en invente de nouveaux et les remplit tout seul. Vous ne retenez plus qu'un **mot de passe maître**, qui doit être très fort, car son vol exposerait tous les autres (OFCS). Cybermalveillance.gouv.fr le préfère au carnet papier ou au fichier sur l'ordinateur.

FICHE 1 · À SIGNER ENSEMBLE

Notre charte de sécurité numérique

À lire à voix haute, à signer par tous et à afficher près de l'ordinateur familial.

Dans notre famille…

- ☐ Chacun a un mot de passe **différent** pour chaque compte, d'au moins 12 caractères.
- ☐ On ne donne **jamais** un mot de passe, un code SMS ou un PIN, même à un ami, même à quelqu'un qui dit être de la banque.
- ☐ On active la double authentification dès que c'est possible.
- ☐ On ne clique pas sur un lien reçu d'un inconnu ; on tape l'adresse soi-même.
- ☐ On réfléchit avant de publier : pas d'adresse, d'école ni de position en direct.
- ☐ On ne publie pas la photo de quelqu'un sans son accord, parents compris.
- ☐ Avant de payer en ligne, on vérifie le site et on en parle si on a un doute.
- ☐ Si quelque chose de bizarre arrive, on le dit tout de suite à un adulte.
- ☐ Celui qui se fait avoir et le dit n'est **jamais puni**.
- ☐ Les parents aussi demandent conseil quand ils ont un doute.

Nos règles en plus

Fait le ..... · Prochaine relecture le .....

Parent	Parent	Enfant	Enfant

EXTRAIT GRATUIT · GUIDE N°9

Vous avez lu 5 pages. Le guide en compte 35.

La version complète de « La sécurité numérique en famille » vous accompagne pas à pas, avec des repères vérifiés pour la Suisse, la France et la Belgique.

Au programme du guide complet

- Pourquoi c'est l'affaire de toute la famille
- Des mots de passe solides et un coffre-fort
- La double authentification
- Vie privée : ce qu'on partage en ligne
- Les arnaques qui visent les jeunes
- Les arnaques qui visent les parents
- L'IA : voix clonées et fausses images
- Payer en ligne quand on est jeune
- Appareils, Wi-Fi et fuites de données
- **et 3 autres chapitres**, jusqu'aux fiches à imprimer

Découvrir le guide complet

www.modeparenton.com · téléchargement immédiat