



SMART ONLINE = SAFE OFFLINE

Ta sécurité en ligne

Le guide de l'ado : repérer les pièges, protéger tes comptes et savoir à qui demander de l'aide quand quelque chose ne va pas.

Nicholas Carstoïu

Guide gratuit pour les élèves de 13 à 18 ans · Édition française · Mis à jour en octobre 2026

À propos de ce guide

Ce guide a été écrit pour toi, pas pour des spécialistes. Pas besoin de savoir coder ni d'être passionné d'informatique pour le comprendre. Presque tout ce qui suit parle de personnes : de celles qui essaient de te piéger, des astuces qu'elles utilisent et des petites décisions, de quelques secondes, qui font la différence entre un compte volé et un compte protégé. Tu peux le lire du début à la fin ou aller directement au chapitre dont tu as besoin ; chacun se termine par une rubrique **En bref**.

Ce guide est né du cours SMART ONLINE = SAFE OFFLINE, que je présente gratuitement dans les écoles de Bucarest. J'ai gardé l'essentiel, revérifié chaque chiffre et ajouté les sujets devenus importants pour les ados : la sextorsion, les fausses images créées par l'IA, les chatbots, les groupes qui exigent des « preuves » et le vol de comptes au moyen de codes.

À propos du programme SMART ONLINE = SAFE OFFLINE

Ce guide fait partie du programme gratuit **SMART ONLINE = SAFE OFFLINE**, que Nicholas Carstoiu propose aux collèges et lycées de Bucarest, pour les élèves des classes VII à XII du système roumain (13 à 18 ans). Le programme est gratuit pour les écoles, les élèves, les enseignants et les parents. Détails :

www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html

Le contenu de base du cours a été conçu à l'origine par Alexandru Cârstoiu, spécialiste de la sécurité de l'information, puis adapté par Nicholas pour les adolescents.

Le guide et la plateforme TRUST // NO TRUST se complètent. Ici, tu trouves les explications et les étapes à garder sous la main. Sur la plateforme, tu t'entraînes à prendre les bonnes décisions dans des situations fictives, avant d'en avoir besoin pour de vrai. Les deux sont gratuits, pour que l'accès aux informations de sécurité ne dépende pas de la possibilité de payer.

Chaque chiffre est accompagné de sa source, et la liste complète se trouve à la fin. Si un chiffre a changé entre-temps, écris-moi. Édition révisée sur la base des sources disponibles au 23 octobre 2026. Les services d'aide cités sont ceux disponibles en Roumanie.

Tu as besoin d'aide tout de suite ?

112 si toi ou quelqu'un d'autre êtes en danger immédiat. **119** en cas de maltraitance, d'exploitation ou de négligence d'un enfant, gratuit et 24 h sur 24. **116 111** si tu veux parler à un conseiller. Tous les services et les étapes sont au [chapitre 10](#). Ce sont des numéros roumains ; le 112 et le 116 111 fonctionnent aussi dans la plupart des pays de l'UE.

Sommaire

	À propos de ce guide	2
	À propos de l'auteur	4
1	Pourquoi c'est important	5
2	Comment travaillent les attaquants	7
3	Les pièges classiques	11
4	Ceux qui veulent te manipuler	19
5	Tes comptes et ton téléphone	27
6	Jouer en sécurité	31
7	Les réseaux sociaux et ton cerveau	35
8	Deepfakes et intelligence artificielle	38
9	Les arnaques virales	42
10	Si ça t'est arrivé	45
11	Le trident : pourquoi ce cours a sa place à l'école	49
	Sources	50
	Contact, droits d'auteur et sécurité	53

À propos de l'auteur



Salut, je suis **Nicholas Carstoiu** (Nicholas Cârstoiu). J'ai 17 ans, je suis en classe XI au lycée roumano-finlandais de Bucarest et je joue au basket en compétition au CSU ASE Bucarest. Dans mon lycée, je suis entraîneur adjoint des équipes juniors.

Depuis 2023, je suis membre du Conseil des enfants de l'UNICEF Roumanie, depuis 2024 du Conseil consultatif des enfants de la mairie de Bucarest, et en 2026 je suis devenu ambassadeur pour la Roumanie de United Citizens of Europe. Toujours en 2026, j'ai reçu le premier prix « Jeune leader du bénévolat » au Gala du bénévolat social de Roumanie.

La sécurité en ligne n'est pas un sujet nouveau pour moi. J'ai créé le programme SMART ONLINE = SAFE OFFLINE, que je présente depuis trois ans dans les écoles de Bucarest, et The Fake News Factory, un projet d'éducation aux médias qui a remporté deux prix en 2026. Je construis maintenant TRUST // NO TRUST, une plateforme gratuite où les ados s'entraînent aux décisions qui les protègent, avec laquelle je participe au concours Lider European 2026.

« Ma génération n'a pas à être la plus facile à piéger en ligne. Nous pouvons être les plus difficiles à piéger. »

Viens me connaître !

www.looksmart.ro/nicholas

CHAPITRE 1

Pourquoi c'est important

Ta vie se passe de plus en plus sur un écran : les amis, l'école, les jeux, l'argent, même les premiers amours. C'est exactement là que te cherchent ceux qui veulent profiter de toi.

Quand tu entends « cybersécurité », tu imagines sûrement un hacker en capuche qui casse des mots de passe à la vitesse de la lumière. La réalité est beaucoup plus banale, et c'est justement pour ça qu'elle est plus dangereuse. Beaucoup d'attaques ne commencent pas par un ordinateur, mais par une personne : un message qui te presse, un prix trop beau, une voix familière au téléphone, un nouvel « ami » qui te comprend mieux que tous les autres.

≈ 1 sur 5

enfants de 12 à 17 ans utilisant Internet, dans 21 pays, a été victime d'exploitation ou d'abus sexuels facilités par la technologie, en une seule année.

Source : UNICEF Innocenti, rapport Through Children's Eyes, publié le 3 septembre 2026, données issues de la recherche Disrupting Harm

1 sur 6

élèves de 11, 13 et 15 ans, dans 44 pays d'Europe, d'Asie centrale et au Canada, a subi du cyberharcèlement.

Source : OMS Europe, étude HBSC sur le cyberharcèlement, 27 mars 2024, données de 2022

2 sur 5

enfants ayant participé à l'étude de Save the Children Roumanie disent avoir été insultés ou avoir reçu des messages blessants en ligne.

Source : Save the Children Roumanie (Salvați Copiii), communiqué de presse du 28 mars 2025

Plus de 4 sur 10

cas d'abus ou d'exploitation sexuels facilités par la technologie, dans les recherches résumées par l'UNICEF, n'ont été confiés à personne.

Source : UNICEF Innocenti, rapport Through Children's Eyes, publié le 3 septembre 2026, données issues de la recherche Disrupting Harm

Le dernier chiffre est peut-être le plus important. Beaucoup de problèmes grandissent justement parce qu'on n'en parle pas. Si quelque chose t'arrive, tu n'as pas besoin d'avoir toutes les preuves ni toutes les réponses pour demander de l'aide. Et si tu reconnais le piège à temps et que tu sais quoi faire ensuite, beaucoup de ces situations n'auront même pas lieu.

Le modèle **APDR** : quatre questions qui te protègent

Dans ce guide, nous utilisons quatre questions simples, regroupées sous le nom APDR. Tu peux les appliquer à tout : un compte, ton téléphone, tes photos.

1. Anticiper

Qu'est-ce qui pourrait mal tourner ? Qui voudrait accéder à ce que j'ai ?

2. Prévenir

Que fais-je dès maintenant pour que ça n'arrive pas ? Mots de passe, réglages, prudence.

3. Détecter

Comment savoir vite si quelque chose s'est produit ?

4. Réagir

Que fais-je dans les premières minutes ? Qui je préviens ?

Exemple : les photos de ton téléphone

Anticiper : ton téléphone peut être perdu ou volé, ou quelqu'un peut découvrir ton code. Des photos personnelles pourraient arriver chez des gens qui ne devraient pas les voir. **Prévenir** : tu mets un code de déverrouillage d'au moins 6 chiffres, tu actives la sauvegarde dans le cloud protégée par la validation en deux étapes et tu vérifies quelles applis ont accès à ta galerie. **Détecter** : tu reçois une alerte quand quelqu'un se connecte à ton compte depuis un autre appareil. **Réagir** : tu verrouilles et effaces le téléphone à distance, tu changes le mot de passe du cloud et tu préviens un adulte.

Retiens l'ordre. La plupart des gens ne pensent à la sécurité qu'à l'étape quatre, quand le mal est déjà fait. Toi, tu peux commencer par l'étape une.

En bref

- Beaucoup d'attaques reposent sur la manipulation des personnes, pas seulement sur la technologie.
- Les problèmes dont on ne parle pas grandissent. Demande de l'aide dès le premier jour.
- APDR : anticiper, prévenir, détecter, réagir.

CHAPITRE 2

Comment travaillent les attaquants

Oublie le hacker solitaire des films. La criminalité en ligne d'aujourd'hui ressemble plutôt à une entreprise, avec des équipes, des rôles et des délais.



Les grandes attaques sont menées par des équipes, pas par une seule personne.

Un réseau de cybercriminels fonctionne comme une usine. Chaque équipe fait une seule chose et la fait bien. Si tu comprends la chaîne, tu comprends où elle peut être cassée : très souvent, chez toi.

Les **profileurs** rassemblent des informations sur leurs cibles : ce que tu publies, ton école, le nom de tes amis, les jeux auxquels tu joues. L'**équipe d'intrusion** cherche un moyen d'entrer, le plus souvent un message de phishing ou un mot de passe réutilisé. L'**équipe d'attaque** installe des logiciels malveillants ou prend le contrôle du compte. L'**équipe d'extraction** copie les données, les photos et les contacts. Les **négoçiateurs** réclament de l'argent, et l'**équipe de « nettoyage »** efface les traces et revend les données.

Tous les hackers ne sont pas des **criminels**

Le mot « hacker » désigne en réalité quelqu'un qui comprend un système si bien qu'il peut le faire fonctionner autrement que prévu. Certains s'en servent pour voler. D'autres, appelés hackers éthiques, cherchent les failles pour qu'elles soient corrigées avant que les criminels ne les trouvent. Les grandes entreprises les rémunèrent grâce à des programmes de récompenses, appelés bug bounty.

Le savais-tu ?

En 2016, un garçon finlandais de 10 ans, Jani, a découvert une faille qui lui permettait de supprimer les commentaires de n'importe qui sur Instagram. Il l'a signalée, et Facebook lui a versé 10 000 dollars. La cybersécurité est l'un des rares métiers où l'on peut commencer très tôt, à condition de rester du bon côté.

Source : NBC News, sur la récompense versée à un enfant de 10 ans pour une faille d'Instagram, mai 2016.

Le savais-tu ?

La Roumanie a une vraie tradition en sécurité informatique. Bitdefender, l'un des antivirus les plus connus au monde, a été fondé à Bucarest en 2001. Et la technologie antivirus RAV, développée par l'entreprise roumaine GeCAD, a été rachetée par Microsoft en 2003.

Pourquoi s'intéresseraient-ils à toi ?

« Je n'ai rien à voler » est l'erreur la plus fréquente. Ton compte Instagram peut servir à piéger tes amis, ton compte de jeu contient des skins qui se revendent, ton numéro de téléphone ouvre des comptes WhatsApp et tes photos peuvent servir au chantage. Pour un attaquant, peu importe que tu sois « juste un élève ». Ce qui compte, c'est que tu as accès à des gens qui te font confiance.

Internet a trois couches

Le **web de surface** est la partie que tu trouves avec Google : la page publique d'un restaurant, le profil public d'un influenceur, les vidéos publiques de YouTube. Le **web profond** (deep web) a l'air mystérieux, mais c'est tout simplement tout ce qui se trouve derrière un mot de passe : ta boîte mail, tes messages privés, le compte bancaire de tes parents, ta bibliothèque de jeux sur Steam. Rien d'illégal là-dedans : c'est ton espace privé, et c'est exactement ce que les attaquants veulent atteindre.

Le **dark web** est une petite partie d'Internet, accessible seulement avec des logiciels spéciaux, où l'identité des utilisateurs est cachée. Il a aussi des usages légitimes, par exemple pour les journalistes de pays sans liberté d'expression. Mais c'est aussi là que se vendent des données volées, des comptes piratés et des choses bien pires.



Pourquoi tu n'as rien à faire sur le dark web

Ce n'est pas un endroit « cool » à explorer par curiosité. Tu peux tomber sur des contenus illégaux et traumatisants, télécharger des logiciels malveillants, et certains sites sont des pièges tendus par des criminels ou surveillés par la police. Si quelqu'un te propose d'y aller « juste pour voir », la réponse est non. Si tu vois un lien vers un contenu illégal impliquant un enfant, ne l'ouvre pas et signale-le anonymement à la ligne esc_ABUZ (chapitre 10).

En bref

- La criminalité en ligne est organisée comme une entreprise, avec des équipes et des rôles.
- Certaines attaques sont personnalisées avec des informations sur toi, d'autres sont envoyées automatiquement à des milliers de personnes. Dans les deux cas, ce que tu publies compte.
- Le web profond, ce sont tes comptes privés, pas quelque chose d'illégal. Le dark web, c'est autre chose, et ce n'est pas un endroit à explorer.
- Tu n'es pas trop jeune pour être une cible : tu as des comptes, des contacts et la confiance des autres.

Exercice : avec quelle facilité un profileur te trouve-t-il ?

Prends cinq minutes et cherche-toi sur Google, avec ton nom complet entre guillemets. Ouvre ensuite ton profil Instagram ou TikTok comme si tu étais un inconnu. Note tout ce que peut apprendre quelqu'un qui ne te connaît pas : ton école, ton quartier, la salle où tu t'entraînes, le nom de tes parents ou de ton frère, ta date de naissance, ton emploi du temps.

Puis demande-toi : si un inconnu avait toutes ces informations, quel message crédible pourrait-il m'écrire ? « Salut, je suis le nouveau coach de la salle » ou « Ton professeur principal te cherche, voici le lien vers le nouvel emploi du temps » paraît bien plus convaincant venant de quelqu'un qui connaît déjà des détails sur toi. C'est comme ça que travaillent les profileurs, et c'est comme ça que tu peux te protéger : moins tu laisses d'indices, plus il est difficile de te piéger.

Comment repérer un faux profil

- Un compte récent, avec peu de publications mais beaucoup d'abonnés ou beaucoup d'amis communs ajoutés récemment.
- Des photos trop parfaites, style mannequin, ou des photos qui apparaissent aussi sur d'autres comptes (tu peux les rechercher avec Google Lens).
- Il t'écrit en premier, te complimente beaucoup et pousse pour passer sur une autre appli.
- Il n'accepte jamais d'appel vidéo ou invente toujours une excuse.

Ce que tu fais maintenant

- Passe ton compte en privé partout où il n'a pas besoin d'être public.
- Retire de ta bio ton école, ta classe et ta ville si ce n'est pas nécessaire.
- Ne publie pas en temps réel où tu te trouves. Publie après être parti.
- Vérifie qui te suit et supprime les comptes que tu ne connais pas.

CHAPITRE 3

Les pièges classiques

Phishing, faux messages, appels qui te pressent et logiciels qui s'installent en cachette. Ils sont anciens, mais ils fonctionnent toujours, parce qu'ils s'adaptent sans cesse.



Le **phishing** (hameçonnage) vient de « fishing », la pêche. L'attaquant lance un appât, un e-mail, un SMS ou un message sur les réseaux sociaux, et attend que tu mordes. Le message semble venir de quelqu'un de confiance : une banque, un transporteur, Instagram, l'école ou un ami. Il n'a qu'un seul but : que tu cliques, que tu saisisse ton mot de passe ou un code, ou que tu télécharges un fichier.

Comment reconnaître un message de phishing

Presque tous les faux messages utilisent les mêmes quelques leviers psychologiques. Quand tu apprends à les sentir, peu importe la qualité du message.

Urgence

« Ton compte sera supprimé dans 24 heures. »
Quand on te presse, tu ne vérifies plus.

Peur

« Quelqu'un s'est connecté à ton compte. » La peur te fait agir sans réfléchir.

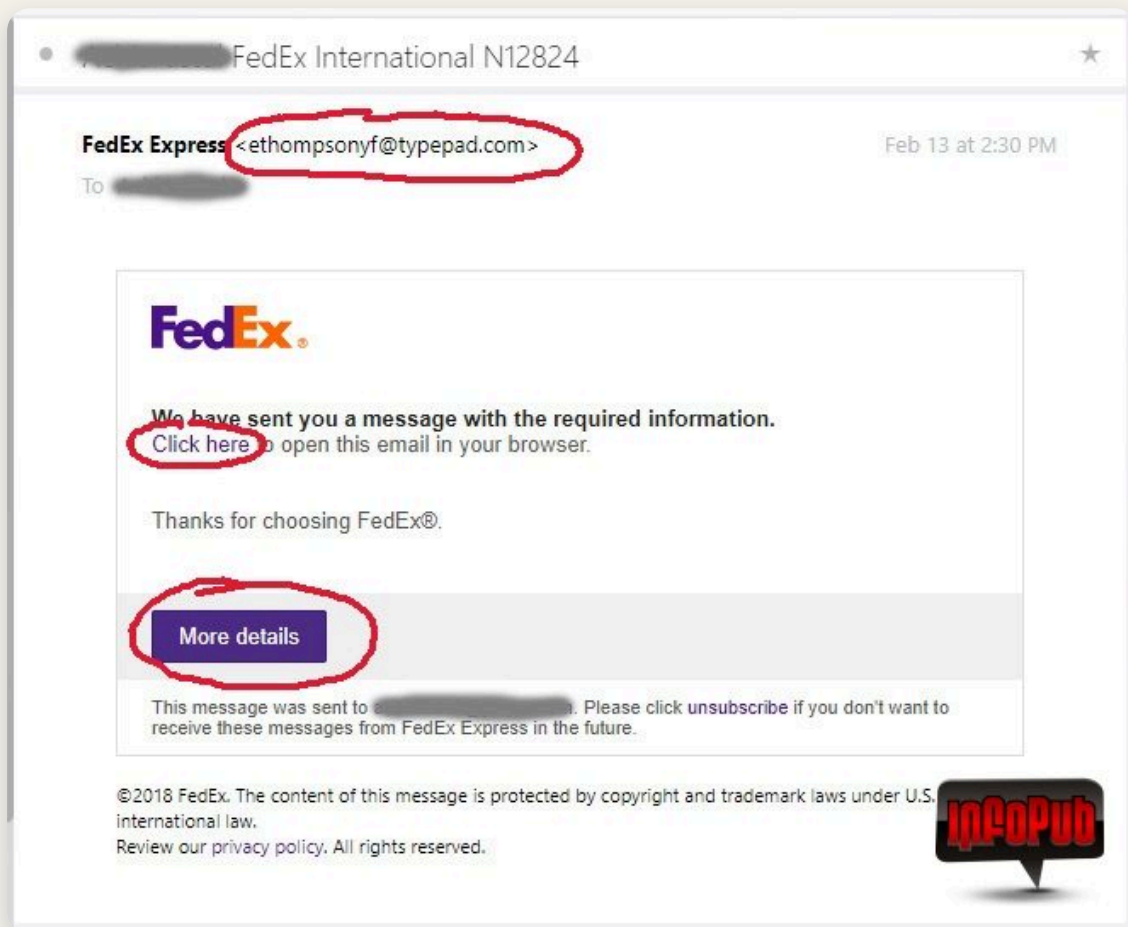
Curiosité

« Regarde cette photo de toi qui circule. » Tu veux voir, alors tu cliques.

Gain

« Tu as gagné un iPhone. » Si c'est trop beau pour être vrai, ce n'est pas vrai.

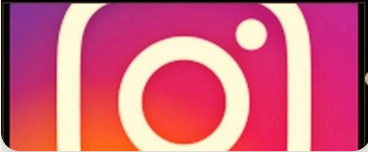
Au-delà de l'émotion, vérifie trois choses concrètes. D'abord, l'adresse réelle de l'expéditeur ou du lien, pas le nom affiché : un message « de FedEx » envoyé depuis une adresse du type ethompsonyf@typepad.com ne vient pas de FedEx. Ensuite, le domaine : [instagram.com](https://www.instagram.com) est réel, mais [instagram-help.buzz](https://www.instagram-help.buzz) ou [lgotyou125.xyz](https://www.lgotyou125.xyz) ne le sont pas. Enfin, la demande elle-même : aucune plateforme sérieuse ne te demande ton mot de passe ou un code reçu par SMS dans un message.



Un vrai exemple de phishing : le nom dit FedEx, l'adresse dit autre chose.

Est-ce une attaque ou pas ?

This took me about 3 hours to make. I really hope you love it, Look: http://iGotYouThis125.xyz/g/?&ure=dnf_tweets



Le message : « Took me about 3 hours to make. I really hope you love it. Look: <http://iGotYouThis125.xyz/g/?&ure=...> », reçu en privé de la part d'un ami.

Oui, c'est une attaque. Le texte est conçu pour piquer ta curiosité, et le lien contient parfois même ton nom d'utilisateur pour paraître personnel. La page sur laquelle tu arrives ressemble à l'écran de connexion d'Instagram, mais le domaine est complètement différent. Dès que tu saisis ton mot de passe, le compte est piraté et le même message part automatiquement vers tous tes abonnés. C'est pour ça qu'il semble venir d'un ami : il vient vraiment de son compte, sauf que ce n'est pas lui qui l'a écrit.

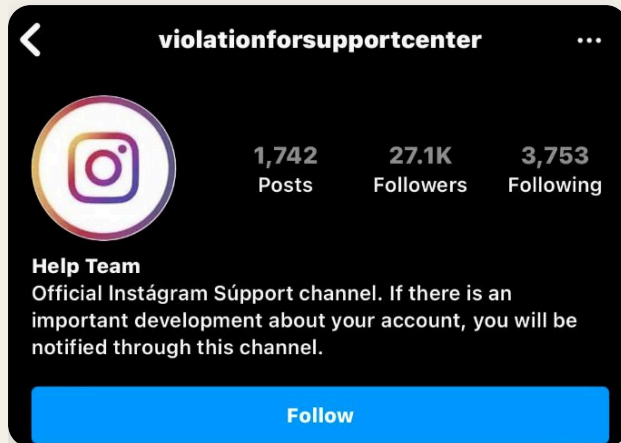
Comment vérifier un lien sans l'ouvrir

- Sur ordinateur, passe la souris sur le lien et lis l'adresse qui s'affiche dans le coin de l'écran.
- Sur téléphone, appuie longuement sur le lien et lis l'adresse sans l'ouvrir.
- Lis l'adresse entre « https:// » et le « / » suivant. Un nom connu placé au début ne signifie pas que le site lui appartient : dans « [instagram.com.verification-compte.example](https://instagram.com/verification-compte.example) », le domaine est « verification-compte.example », pas « instagram.com ».
- Si tu as un doute, ouvre directement l'appli officielle ou tape toi-même l'adresse au lieu d'utiliser le lien.

Que faire si tu as déjà cliqué et saisi ton mot de passe

- Change immédiatement le mot de passe de ce compte et de tout autre compte où tu l'as utilisé.
- Active la validation en deux étapes.
- Va dans Paramètres, Activité de connexion, et déconnecte les sessions que tu ne reconnais pas.
- Préviens tes abonnés de ne pas cliquer sur les messages envoyés depuis ton compte.
- Si tu ne peux plus te connecter, utilise la page officielle de récupération de la plateforme, pas « l'aide » qui t'écrit en privé.

Le « support » qui t'écrit en premier



Un faux compte « Help Team », avec le logo d'Instagram et des milliers d'abonnés.



« Last Warning: your account will be disabled. » Le grand classique du message qui fait peur.

Un compte qui se présente comme l'équipe d'assistance, avec un logo officiel et beaucoup d'abonnés, t'annonce que tu as enfreint les règles et que tu dois « confirmer » ton compte via un lien. Ne vérifie pas l'avertissement avec le lien reçu. Ouvre directement l'appli et cherche la notification dans la rubrique officielle de sécurité ou d'assistance.

Les concours qui récoltent tes données



« Giveaway alert : like, identifie 3 amis et partage. » Ça a l'air inoffensif, mais chaque étape sert celui qui a créé le concours. Le **like** confirme que ton compte est actif, donc attends-toi à encore plus de messages. **Identifier** tes amis les expose : ils deviennent les prochaines cibles. **Partager** prépare le terrain pour que d'autres amis soient exposés. Avant de participer, vérifie que l'organisateur est bien le compte officiel et certifié de la marque.

SMS, appels et codes



Le **smishing**, c'est le phishing par SMS : « Ton colis est bloqué, paie les 2 lei de frais ici. » Le **vishing**, c'est le phishing par appel vocal : quelqu'un se présente comme un employé de la banque, de la police ou de ton opérateur et te demande des informations « pour vérification ». Avec l'intelligence artificielle, la voix peut même être celle d'une personne que tu connais (voir le chapitre 8).

La règle d'or des codes

Un code reçu par SMS ou dans une appli est la clé de ton compte. **Tu ne le donnes jamais à personne**, ni à un « ami » qui dit te l'avoir envoyé par erreur, ni à un « employé » de la banque ou de WhatsApp. Un vrai employé ne te demandera jamais ton code. Si quelqu'un insiste, c'est une attaque.

Si tu reçois un appel suspect, raccroche et rappelle toi-même le numéro officiel, que tu trouves sur le site de l'organisme ou au dos de la carte bancaire. N'appelle pas le numéro du SMS et n'appuie pas sur le lien reçu.

Deux pièges qui ne ressemblent pas au phishing

Le code QR

Un code QR peut contenir un lien ou les données d'une action précise, et tu ne vois pas ce qu'il contient avant de le scanner. Ce n'est pas une preuve de sécurité. Avant de continuer, lis l'adresse que ton téléphone t'affiche. Fais très attention aux codes QR reçus pour « voter », gagner un prix ou « confirmer » ton compte : certains servent en réalité à connecter l'appareil d'un inconnu à ton compte WhatsApp, Telegram ou Discord. Ne confirme jamais l'association d'un appareil que tu n'as pas lancée toi-même.

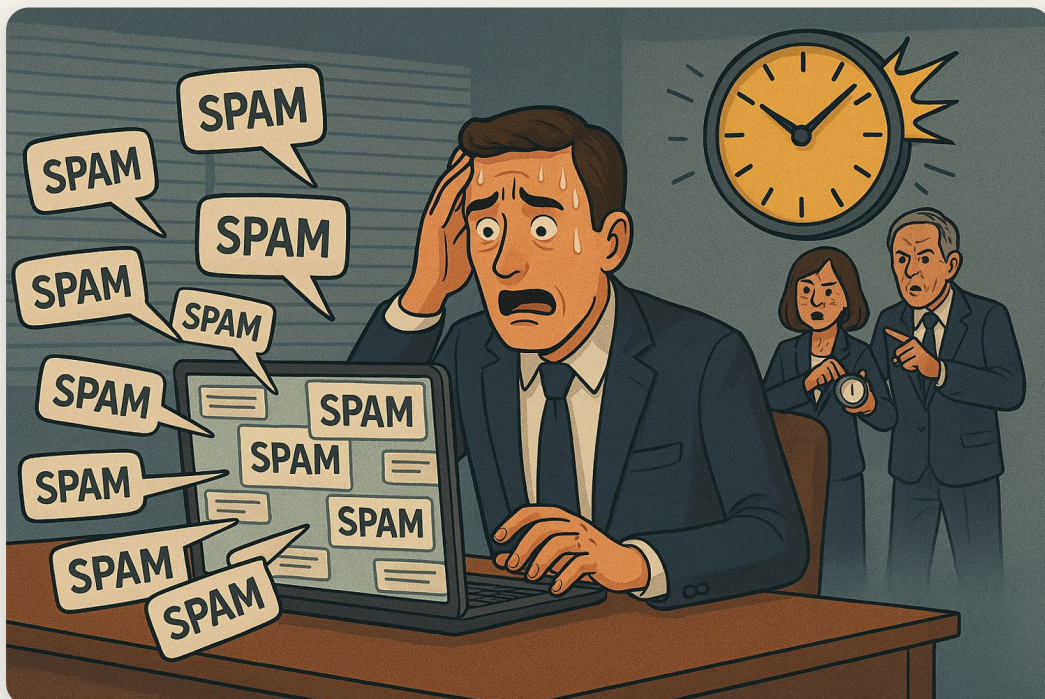
La fausse vérification « Je ne suis pas un robot »

Une vraie vérification CAPTCHA te demande de cocher une case ou de choisir des images. Si une page te demande d'ouvrir une fenêtre de commandes, d'y coller un texte et d'appuyer sur Entrée « pour prouver que tu es humain », arrête-toi immédiatement. C'est une méthode pour te faire installer toi-même un logiciel malveillant. En août 2026, Microsoft a décrit une campagne qui utilisait exactement ce type de fausse vérification.

Source : Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 août 2026.

Si tu as déjà exécuté la commande

- Déconnecte l'appareil d'Internet.
- Demande à un adulte ou à un spécialiste de t'aider à vérifier l'appareil.
- Change tes mots de passe importants depuis un autre appareil, sûr, pas depuis celui qui est touché.



Les logiciels qui s'installent en **cachette**

Un **malware** (logiciel malveillant) est n'importe quel programme conçu pour te nuire. Il arrive souvent sur ton appareil par une installation trompeuse, quand tu crois installer autre chose : une « triche » pour un jeu, une appli piratée, un fichier reçu sur Discord. Mais il peut aussi entrer par des failles du système qui n'ont pas encore été corrigées par les mises à jour.

Type	Ce qu'il fait
Virus	S'attache à d'autres fichiers et se propage quand tu les ouvres ou les envoies.
Cheval de Troie	Se cache dans un programme qui semble utile, comme les soldats dans le cheval de Troie, et donne à l'attaquant l'accès à l'appareil.
Logiciel espion	T'espionne : ce que tu tapes, tes mots de passe, tes messages, parfois même la caméra et le micro.
Rançongiciel	Bloque ou chiffre tes fichiers et réclame de l'argent pour te les « rendre ».
Logiciel publicitaire	T'inonde de publicités et de fenêtres pop-up, souvent avec des liens dangereux.



Le savais-tu ?

Le premier rançongiciel connu est apparu en 1989 et a été distribué sur disquettes lors d'une conférence sur le sida. Plus de 35 ans plus tard, en février 2024, une attaque par rançongiciel contre la plateforme Hipocrate a touché directement 26 hôpitaux en Roumanie, et des dizaines d'autres ont été déconnectés par précaution. Les attaquants réclamaient 3,5 bitcoins, environ 157 000 euros. La direction roumaine de la cybersécurité (DNSC) a vivement recommandé de ne pas payer la rançon.

Source : TVR Info, sur l'attaque contre la plateforme Hipocrate, 13 février 2024.

Comment te protéger des logiciels malveillants

Tu n'as pas besoin de dix logiciels de sécurité. Tu as besoin de quelques bonnes habitudes, répétées jusqu'à devenir automatiques.

- Tu installes des applis uniquement depuis les boutiques officielles (Google Play, App Store) et des jeux uniquement depuis les plateformes officielles (Steam, Epic, le site de l'éditeur).
- Tu ne télécharges pas de « triches », de « générateurs » ni de versions « crackées ». C'est le moyen le plus sûr d'installer toi-même un cheval de Troie.
- Tu fais les mises à jour du système dès qu'elles apparaissent. Beaucoup corrigent exactement les failles utilisées par les attaquants.
- Tu vérifies les autorisations demandées par une appli. Un jeu simple n'a pas besoin de tes contacts, de ton micro ni de ta position.
- Tu gardes une sauvegarde de tes fichiers importants, pour qu'un rançongiciel ne puisse pas te faire chanter.
- Si un message à l'écran dit que tu « as un virus » et que tu dois appeler ou payer quelque chose, c'est presque à coup sûr une arnaque. Ferme la page et demande de l'aide à un adulte.



En bref

- Le phishing t'attrape par l'urgence, la peur, la curiosité ou le gain.
- Tu vérifies l'adresse réelle, le domaine et la demande, pas seulement le nom affiché.
- Tu ne donnes jamais les codes reçus par SMS.
- Un logiciel malveillant peut arriver par une installation trompeuse, mais aussi par une faille. Mises à jour et prudence vont ensemble.

CHAPITRE 4

Ceux qui veulent te manipuler

Les attaques les plus douloureuses ne volent pas ton mot de passe, mais ta confiance. Le cyberharcèlement, le grooming, la méthode du « loverboy » et la sextorsion reposent sur les émotions, pas sur la technologie.



Le **cyberharcèlement**, c'est humilier, menacer, exclure ou harceler quelqu'un par des moyens numériques : messages, commentaires, photos ou vidéos partagées sans accord, groupes créés pour se moquer de quelqu'un, faux comptes. Contrairement au harcèlement dans la cour de récré, celui en ligne te suit jusqu'à la maison, à toute heure, et le public peut être immense.

Cyberharcèlement : à quelle fréquence ?

49 %

des 4 449 élèves ayant répondu à une enquête de Save the Children Roumanie disent avoir été victimes de harcèlement. 27 % reconnaissent avoir été agresseurs.

Source : Save the Children Roumanie (Salvați Copiii), étude sur le harcèlement à l'école, communiqué du 18 octobre 2022

79 %

de ces mêmes élèves disent avoir été témoins de harcèlement sur les réseaux sociaux, et 45 % voient du cyberharcèlement souvent ou très souvent.

Source : Save the Children Roumanie (Salvați Copiii), étude sur le harcèlement à l'école, communiqué du 18 octobre 2022

48,3 %

des enfants ayant participé à l'étude citée passent plus de six heures par jour dans l'environnement numérique.

Source : Save the Children Roumanie (Salvați Copiii), communiqué de presse du 28 mars 2025

45 245

signalements (et non victimes ou cas confirmés) de contenus en ligne illégaux ou préjudiciables pour les enfants sont arrivés à la ligne esc_ABUZ entre le 1er janvier et le 3 décembre 2025.

Source : Save the Children Roumanie (Salvați Copiii), ligne de signalement esc_ABUZ, communiqué du 10 décembre 2025

L'enquête de Save the Children de 2022 a utilisé un échantillon non probabiliste : elle montre une tendance, pas une mesure exacte pour tous les élèves de Roumanie.

Que faire si tu es la cible

- Ne réponds pas sur le coup et ne te venge pas. L'agresseur attend justement ta réaction.
- Garde les preuves : captures d'écran des messages, nom du compte, date et heure.
- Bloque le compte et signale-le à la plateforme.
- Parle à un adulte de confiance : un parent, ton professeur principal, le conseiller scolaire. Ce n'est pas ta faute et tu n'as pas à porter ça seul.
- Si tu reçois des menaces de violence, c'est une affaire pour la police, pas seulement pour l'école.

Que faire si tu es témoin

Les témoins ont plus de pouvoir qu'ils ne le pensent. Ne like pas, ne partage pas et ne commente pas. Écris en privé à la personne visée qu'elle n'est pas seule. Signale la publication et préviens un adulte. Une seule personne qui dit « ce n'est pas OK » peut changer l'ambiance de tout un groupe.

Le grooming : l'ami trop parfait pour être vrai

Le grooming (ou pédopiégeage) est la manipulation par laquelle quelqu'un gagne peu à peu la confiance ou la soumission d'un enfant ou d'un adolescent, souvent en ligne, pour l'abuser ou l'exploiter. Ça ne ressemble pas à un danger. Ça ressemble à une amitié : quelqu'un d'attentif, qui t'écoute, te complimente, te fait des cadeaux dans un jeu ou t'offre ce que tu as l'impression de ne pas avoir.



Le schéma se répète presque toujours. D'abord viennent l'attention et les compliments. Puis la conversation passe sur une appli plus privée, avec l'idée que « ce qu'on se dit reste entre nous ». Ensuite, la personne essaie de t'éloigner de ta famille et de tes amis (« eux, ils ne te comprennent pas comme moi »), et les demandes deviennent de plus en plus personnelles. À la fin peuvent arriver la demande de photos, la proposition de rencontre ou les menaces.

Signaux d'alerte

- Un adulte qui te demande de garder la conversation secrète.
- Quelqu'un qui veut déplacer la discussion vers une appli plus discrète.
- Des cadeaux, de l'argent ou des pièces virtuelles sans raison.
- Des questions sur ton corps ou des demandes de photos.
- De la pression pour vous rencontrer, surtout sans que personne ne le sache.

Ne te fie pas à l'âge annoncé : la pression et l'exploitation peuvent aussi venir de personnes que tu connais ou de ton âge. Si tu reconnais un de ces signaux, arrête la conversation, ne supprime pas les messages écrits (ce sont des preuves) et préviens tout de suite un adulte. Tu n'as rien fait de mal. Ceux qui font ça sont doués pour manipuler et comptent justement sur ta honte et ton silence.

« Si tu me fais confiance, **donne-moi ton mot de passe** »

Le risque ne vient pas seulement d'inconnus. Parfois, il vient de quelqu'un que tu connais bien : un copain, une copine, un ami proche. Tu n'as pas à prouver ton amour ou ton amitié en donnant accès à tes comptes, ta localisation permanente ou des images intimes. La pression, le contrôle du téléphone, l'exigence des mots de passe et la menace de publier quelque chose sur toi sont des signes de contrôle, pas d'amour.

Publier ton adresse, ton numéro de téléphone ou ton emploi du temps pour t'exposer s'appelle le **doxing**. Si ça t'arrive, garde les liens et les menaces, signale les publications et demande de l'aide à un adulte. Si ton école ou la salle où tu t'entraînes sont concernées, préviens aussi un adulte responsable sur place.

Si tu crains que la personne devienne violente

Demande de l'aide depuis un appareil auquel la personne n'a pas accès. Prépare avec un adulte de confiance ou un spécialiste les changements de mots de passe et de localisation : certains peuvent envoyer des notifications ou être remarqués. Ta sécurité physique passe avant tout. En cas de danger immédiat, appelle le 112.

Source : eSafety Commissioner (Australie), suivi, surveillance et harcèlement non consentis chez les enfants, mis à jour le 1er juillet 2025, enquête de décembre 2024 à février 2025.

Accepter une photo, ce n'est pas accepter qu'elle soit partagée

Le fait que quelqu'un t'ait envoyé une photo ou ait accepté d'être photographié ne te donne pas le droit de la faire circuler. La règle vaut aussi entre camarades ou entre partenaires, y compris quand l'image a été modifiée par l'IA. Celui qui partage sans accord fait du mal, même si « tout le monde l'a déjà vue ».

Si le premier adulte ne t'aide pas

Demande de l'aide à un autre adulte : le conseiller scolaire, un professeur, ton entraîneur ou un service de protection de l'enfance. N'abandonne pas parce que la première personne t'a ignoré ou t'a fait des reproches.

La méthode du **loverboy**



La méthode du « loverboy » est l'une des plus utilisées par les trafiquants d'êtres humains pour recruter des filles, souvent mineures. Le trafiquant fait croire à la victime qu'il est tombé amoureux d'elle. Il lui promet une vie de rêve, la sécurité affective qu'elle n'a peut-être pas à la maison, parfois un départ à l'étranger « pour un petit moment », le temps de mettre de l'argent de côté pour leur avenir. Peu à peu, la victime devient dépendante affectivement, puis contrôlée, et l'exploitation commence souvent par « fais-le pour nous, juste une fois ».

6,3 millions

de personnes se trouvaient, à un moment donné en 2021, en situation d'exploitation sexuelle commerciale forcée. 1,7 million d'entre elles étaient des enfants, et près de 4 victimes sur 5 sont des femmes et des filles.

Source : Organisation internationale du Travail (OIT), Walk Free et Organisation internationale pour les migrations (OIM), Global Estimates of Modern Slavery, septembre 2022

Si ton copain, ou celui d'une amie, lui demande de couper les ponts avec sa famille, contrôle son téléphone, lui réclame de l'argent ou lui propose un « travail » à l'étranger, parlez-en à quelqu'un. En Roumanie, l'ANITP a une ligne gratuite : **0800 800 678**.

La sextorsion et les fausses images créées par l'IA

La sextorsion, c'est le chantage avec des images intimes. Un compte qui semble appartenir à une fille ou à un garçon de ton âge lance une conversation, flirte, envoie une photo et t'en demande une en retour. Dès qu'il l'a reçue, le ton change : « Paie, ou je l'envoie à tous tes amis. » Les attaquants ont déjà la liste de tes abonnés. Ils sont rapides, agressifs et, la plupart du temps, ce sont des réseaux organisés depuis d'autres pays, qui veulent de l'argent.

Ces dernières années est apparue une version encore plus cynique : ils n'ont même plus besoin d'une vraie photo. Ils prennent une photo ordinaire de ton profil et créent, grâce à l'intelligence artificielle, une fausse image qui semble intime.

137 par jour

En 2025, le centre américain NCMEC a reçu plus de 50 000 signalements de sextorsion financière, en moyenne 137 par jour.

Source : NCMEC, communiqué sur la sextorsion, publié le 25 juin 2026, données de 2025

Plus de 400 000

signalements d'exploitation d'enfants liés à l'intelligence artificielle générative ont été reçus par le NCMEC en 2025.

Source : NCMEC, données CyberTipline, publiées en 2026, données de 2025

Il s'agit de signalements reçus par un centre de signalement, pas du nombre de victimes, ni d'une mesure pour la Roumanie.

Si ça t'arrive

- **Ne paie pas.** Payer ne garantit pas que le chantage s'arrête et peut entraîner d'autres demandes.
- Arrête la conversation. Garde les messages de menace et les informations du compte. Pour les images intimes, suis les règles du chapitre 10.
- Bloque et signale le compte.
- Parles-en à un adulte. Le maître chanteur veut que tu sois seul et honteux.
- Pour les images, utilise **Take It Down** (page suivante) et la ligne **esc_ABUZ** de Save the Children Roumanie. En Roumanie, tu peux aussi appeler le **119**.

Ce n'est pas toi qui as mal agi. Le délit est commis par celui qui te fait chanter.

Ce que peut faire **Take It Down**

Si tu avais moins de 18 ans quand l'image intime a été prise, tu peux utiliser gratuitement Take It Down (takeitdown.ncmec.org), même si tu es devenu majeur depuis. Le fichier doit déjà se trouver sur ton appareil : l'image y reste, tu ne l'envoies à personne, et le service crée seulement une empreinte numérique que reçoivent les plateformes participantes pour pouvoir la bloquer.

Ne télécharge pas l'image et ne demande à personne de te l'envoyer dans ce but. Si tu ne l'as pas, demande de l'aide en faisant un signalement : à la plateforme, à la ligne esc_ABUZ, au 119 ou à la police. Le service peut limiter la diffusion, mais il ne garantit pas la suppression sur tout Internet et ne fonctionne pas dans toutes les conversations chiffrées. Les fausses images créées par l'IA se signalent à la plateforme, à la ligne esc_ABUZ et à la police.

Source : NCMEC, Take It Down, questions fréquentes.

Pour les parents : si votre enfant vous en parle

Restez calme et remerciez-le de vous l'avoir dit. Le fait qu'il soit venu vers vous est le plus important. Ne cherchez pas de coupable, ne lui confisquez pas son téléphone pour le punir et ne payez pas. Notez les informations du compte et conservez les messages de menace, sans copier ni transférer les images. Signalez le compte et demandez de l'aide au 119 ou à la police.

Quand un groupe te demande de **prouver** quelque chose

Certains groupes en ligne commencent par des blagues, des jeux ou la promesse que tu as enfin ta place quelque part. Europol avertit que ce type de communautés cherche ses victimes sur les plateformes de jeu, de streaming et sur les réseaux sociaux, puis déplace la conversation vers des canaux privés. Viennent ensuite les demandes de « preuves » : humilier quelqu'un, envoyer des images intimes, faire du mal à un animal, te faire du mal ou faire du mal à quelqu'un d'autre. Ils utilisent des menaces ou les informations qu'ils ont rassemblées sur toi pour t'obliger à continuer.

Tu n'as pas à accomplir une dernière demande

Ne te fie pas à la promesse qu'ils te laisseront tranquille après une demande de plus. Arrête l'échange et demande de l'aide à un adulte. Garde le nom du groupe et les messages de menace, sans copier ni diffuser les contenus d'abus. N'enquête pas sur le groupe et n'essaie pas de le confronter seul. S'il y a un danger immédiat pour toi ou pour quelqu'un d'autre, appelle le 112.

Source : Europol, The rise of online cult communities dedicated to extremely violent child abuse, janvier 2025.

Ce que **ressentent** les victimes et ce qui les aide

Ceux qui vivent du cyberharcèlement, du grooming ou de la sextorsion ressentent en général le même mélange : honte, peur, culpabilité et l'impression que personne ne peut les aider. C'est justement pour ça que les agresseurs insistent sur le secret. La chose la plus importante que tu puisses faire pour toi ou pour un ami, c'est briser le silence.

Pour toi

Parles-en à quelqu'un le jour même. Tu n'as pas besoin d'avoir toutes les réponses ; il suffit de dire « j'ai un problème et j'ai besoin d'aide ».

Pour un ami

Écoute sans juger, ne partage rien de ce qu'il t'a montré et aide-le à aller voir un adulte. Ne promets pas de garder le secret s'il est en danger.

Pour les parents

Changements d'humeur soudains, repli sur soi, peur du téléphone ou, au contraire, impossibilité de le lâcher, notes en baisse. Posez des questions calmement et ne confisquez pas le téléphone pour punir.

Pour les enseignants

Traitez chaque cas signalé comme réel, protégez l'identité de l'élève et impliquez le conseiller scolaire.



Le 119, numéro national unique en Roumanie : maltraitance, négligence ou exploitation d'un enfant. Gratuit et 24 h sur 24.

En bref

- La manipulation ressemble presque toujours à une amitié, à un amour ou à un compliment.
- Le secret exigé par un adulte est le signe de danger le plus clair.
- Tu ne paies jamais un maître chanteur.
- La honte appartient à l'agresseur, pas à toi.

CHAPITRE 5

Tes comptes et ton téléphone

Les mots de passe, la validation en deux étapes et quelques réglages bien choisis te protègent mieux que n'importe quel logiciel. Voici ce qui a changé dans les règles sur les mots de passe.

Mots de passe : la longueur bat la complexité

Majuscules, chiffres, symboles et changement tous les trois mois : ces règles ont changé. Les recommandations du NIST d'août 2025, une norme américaine pour les services d'identité numérique utilisée comme référence dans de nombreux pays, sont plus simples : c'est la longueur qui compte le plus, et les changements imposés à intervalles fixes n'aident pas.

Utilise une phrase de passe

Quatre ou cinq mots sans rapport entre eux, par exemple « cactus violet court à Constanța ». Elle est longue, facile à retenir et difficile à deviner.

Au moins 15 caractères

Pour les comptes protégés uniquement par un mot de passe, le NIST recommande au moins 15 caractères.

Un mot de passe par compte

Si un site est piraté, les attaquants essaient le même mot de passe partout. Un mot de passe réutilisé met plusieurs comptes en danger à la fois.

Change-le quand c'est nécessaire

Pas selon le calendrier, mais quand tu as des raisons de penser qu'il a été compromis.

Mot de passe	Pourquoi
Andrei2009	Faible : un prénom et une année, les premières choses qu'un attaquant essaie.
M@r1aB3st!	Il a l'air compliqué, mais il est court, et les astuces avec des symboles sont bien connues des logiciels de cassage.
cactus violet court à Constanța	Bon comme idée : long, sans lien avec toi, facile à retenir. N'utilise pas exactement celui-ci : il est paru dans un guide public.

Ce qui ne marche plus

Remplacer des lettres par des symboles (« m0t2p@sse ») ne trompe pas les logiciels de cassage. Évite aussi ton nom, ta date de naissance ou « 123456 ».

Source : NIST, SP 800-63B-4, Digital Identity Guidelines, août 2025.

Gestionnaires de mots de passe et clés d'accès

Personne ne peut retenir 40 phrases de passe différentes. C'est pour ça qu'existent les gestionnaires de mots de passe : des applis qui créent, stockent et remplissent les mots de passe à ta place. Tu en retiens un seul, très bon, et l'appli s'occupe du reste. Les téléphones et les navigateurs ont déjà des gestionnaires intégrés (Gestionnaire de mots de passe de Google, Mots de passe d'Apple), et des applis comme Bitwarden ou 1Password font la même chose sur tous tes appareils.

Les **clés d'accès** (passkeys) sont l'étape suivante : une clé numérique liée à ton téléphone, déverrouillée avec ton empreinte, ton visage ou le code de l'écran. Il n'y a rien à mal taper sur un faux site, et une clé d'accès ne peut pas être volée par phishing comme un mot de passe. Si un compte te propose cette option, active-la.

La validation en deux étapes

La validation en deux étapes (A2F) demande, en plus du mot de passe, quelque chose que toi seul possèdes : un code dans une appli, une confirmation sur ton téléphone ou une clé d'accès. Elle réduit beaucoup le risque qu'un mot de passe volé suffise pour prendre le contrôle du compte. Elle ne te protège pas pour autant de toutes les attaques : un faux site peut aussi te demander le code, et un logiciel malveillant peut voler une session où tu étais déjà connecté. Choisis les clés d'accès ou les clés de sécurité quand elles sont disponibles. Si tu utilises des codes, une appli d'authentification est en général préférable au SMS, mais si le SMS est la seule option, active-le : c'est mieux qu'un mot de passe seul. N'approuve jamais une connexion que tu n'as pas lancée toi-même. Active la validation en deux étapes en priorité sur ta boîte mail, ton compte Google ou Apple principal, tes réseaux sociaux, WhatsApp (validation en deux étapes avec un code PIN) et tes comptes de jeu.

Source : CISA, Implementing Phishing-Resistant MFA (fiche d'information) ; Microsoft, Token theft playbook.

Le bon ordre

1. Ta boîte mail principale : celui qui la contrôle peut réinitialiser le mot de passe de tous tes autres comptes.
2. Le compte Google ou Apple de ton téléphone.
3. WhatsApp, Instagram, TikTok, Snapchat.
4. Les comptes de jeu et les plateformes avec de l'argent ou une carte enregistrée.

Les réseaux Wi-Fi publics



Cafés, aéroports, hôtels, centres commerciaux : le Wi-Fi gratuit est partout. Aujourd'hui, la plupart des sites et des applis chiffrent les données (l'adresse commence par **https**), donc se connecter à un réseau public est en général plus sûr qu'il y a dix ans. Le danger vient surtout des faux réseaux : n'importe qui peut créer un réseau appelé « Free_Airport_WiFi ». Un tel réseau peut t'envoyer vers des pages frauduleuses ou te demander d'installer quelque chose. En revanche, le simple fait de t'y connecter ne permet pas automatiquement à celui qui le contrôle de lire les mots de passe et les messages envoyés par des connexions correctement chiffrées.

N'ignore pas les avertissements de sécurité du navigateur et n'installe pas de certificats, d'applis ou de « mises à jour » demandés pour te connecter. Le HTTPS protège la liaison avec le site, mais il ne prouve pas que le site est légitime. Un VPN ne transforme pas un faux site en site sûr.

Source : FTC (États-Unis), Are Public Wi-Fi Networks Safe? What You Need To Know.

Le savais-tu ?

Quand tu actives la validation en deux étapes, la plupart des plateformes te donnent aussi des **codes de secours**. Range-les dans un endroit sûr, par exemple dans ton gestionnaire de mots de passe ou imprimés à la maison. Ils peuvent t'aider à récupérer l'accès si tu perds ton téléphone. Vérifie aussi à l'avance les autres méthodes de récupération proposées par la plateforme.

Règles simples pour le Wi-Fi public

- Demande au personnel le nom exact du réseau.
- Pour la banque, les paiements ou les mots de passe importants, utilise les données mobiles.
- N'installe rien et n'accepte pas de « mises à jour » demandées par la page de connexion.
- Désactive la connexion automatique aux réseaux ouverts.
- Si tu utilises souvent des réseaux publics, un VPN d'une entreprise connue ajoute une protection, mais ne remplace pas l'attention.

Ton téléphone, ton coffre-fort

Ton téléphone contient tes photos, tes conversations, tes comptes, ta position et parfois ta carte. Il mérite d'être protégé comme un coffre-fort.

Verrouillage de l'écran

Un code d'au moins 6 chiffres, plus l'empreinte ou la reconnaissance faciale. Pas 123456, pas ton année de naissance.

Mises à jour

Tu installes tout de suite les mises à jour du système et des applis. La plupart corrigent des failles de sécurité.

Autorisations

Chaque mois, tu vérifies quelles applis ont accès à la caméra, au micro, à la position et aux contacts. Tu supprimes celles que tu n'utilises plus.

Sauvegarde

Une sauvegarde automatique dans le cloud, protégée par la validation en deux étapes.

Position et partage

Limite l'accès des applications à ta position et vérifie qui peut voir où tu te trouves. Garde les réglages nécessaires au service de localisation du téléphone. Le partage permanent de ta position ne doit pas être une condition d'une amitié ou d'une relation.

Localiser mon appareil

Tu actives Localiser (iPhone) ou Localiser mon appareil (Android) avant d'en avoir besoin.

Source : Aide Compte Google, Be ready to find a lost Android device.

De temps en temps, vérifie sur haveibeenpwned.com si ton e-mail figure dans une fuite de données. Si oui, change le mot de passe de ce compte et de tous ceux où tu l'as réutilisé.

Si ton téléphone est perdu ou volé

1. Tu le localises ou le verrouilles à distance depuis ton compte Google ou Apple.
2. Tu changes le mot de passe de ta boîte mail et de tes comptes importants.
3. Tu demandes à ton opérateur de bloquer la carte SIM, pour que personne ne reçoive tes codes par SMS.
4. Si nécessaire, tu effaces les données à distance.

En bref

- Des phrases de passe longues, une par compte, rangées dans un gestionnaire de mots de passe.
- La validation en deux étapes partout, en commençant par ta boîte mail.
- Sur un Wi-Fi public, tu vérifies le réseau, tu respectes les avertissements de sécurité et tu n'installes rien pour te connecter.
- Un téléphone verrouillé, à jour et sauvegardé.

CHAPITRE 6

Jouer en sécurité

Les jeux font partie des endroits préférés des arnaqueurs, parce qu'on y trouve beaucoup de jeunes, de l'argent virtuel et beaucoup de confiance entre joueurs.



Ton compte Fortnite, Roblox, Minecraft, Counter-Strike, League of Legends, EA Sports FC ou NBA 2K a une vraie valeur : skins, pièces, progression, parfois une carte enregistrée. Les arnaqueurs le savent et ont inventé quelques pièges qui se répètent d'un jeu à l'autre.

Les pièges qui reviennent dans **tous les jeux**

« Générateurs » de pièces

Des sites qui promettent des V-Bucks, des Robux ou des pièces gratuites en échange de tes identifiants. Les vraies récompenses gratuites se trouvent uniquement dans le jeu ou sur le site officiel.

Faux skins et faux échanges

Des sites d'échange ou de paris qui ont l'air officiels, mais vident ton inventaire dès que tu te connectes.

Faux tournois et événements

Des serveurs Discord qui promettent des prix et demandent des « frais d'inscription » ou une connexion par un lien.

Triches et mods

Des programmes qui promettent un avantage dans le jeu, mais installent en réalité un cheval de Troie ou un logiciel qui vole tes mots de passe.

Faux streams

Des diffusions qui promettent des skins gratuits à ceux qui suivent un lien et se connectent.

Achat de comptes

Tu achètes un compte « avec tous les skins », et le vendeur le récupère grâce à la réinitialisation du mot de passe. Tu peux perdre l'argent et le compte.

Le savais-tu ?

En janvier 2019, des chercheurs de Check Point ont montré que des attaquants auraient pu prendre le contrôle de comptes Fortnite simplement en faisant cliquer le joueur sur un lien, sans connaître son mot de passe. Epic Games a corrigé le problème, mais l'affaire a montré que même le jeu le plus populaire du monde peut avoir des failles.

Source : Check Point Research, Hacking Fortnite, 16 janvier 2019.

Attention aux « amis » dans le jeu

Le chat des jeux et les serveurs Discord sont aussi des endroits où des adultes mal intentionnés cherchent des ados. Le schéma est celui du chapitre 4 : de l'attention, des cadeaux dans le jeu, le passage en privé, des demandes de photos ou de « preuves ». Si quelqu'un que tu ne connais pas dans la vraie vie t'offre des skins ou des pièces sans raison, demande-toi ce qu'il veut en échange.

Quand le jeu te pousse à **acheter** encore une fois

Toutes les pertes dans les jeux ne viennent pas d'arnaqueurs. Certains packs, coffres ou loot boxes te donnent des récompenses aléatoires : tu paies sans savoir exactement ce que tu vas obtenir. Les pièces virtuelles rendent plus difficile de voir combien d'argent réel tu as vraiment dépensé, et les skins peuvent finir sur des sites de paris en dehors du jeu.

Ce que tu fais

- Tu fixes un budget avant de commencer et tu actives la confirmation de chaque achat.
- Tu n'empruntes pas d'argent pour te refaire.
- Tu n'utilises pas le compte d'un adulte pour contourner les restrictions.
- Si tu caches tes dépenses ou si tu continues parce que « la prochaine fois, ça va marcher », tu arrêtes de payer et tu en parles à un adulte.

Source : eSafety Commissioner, How to manage money in games.

Si ton compte de jeu a été volé

1. Essaie de le récupérer via la page d'assistance officielle du jeu, pas par quelqu'un qui t'écrit qu'il peut t'aider.
2. Change le mot de passe de l'e-mail associé au compte.
3. Préviens tes amis du jeu que ce n'est pas toi qui leur écris.
4. Si des cartes étaient enregistrées, demande à tes parents de les faire bloquer.



Jouer en sécurité : cinq règles

- 1** La validation en deux étapes sur chaque compte de jeu. Epic, Roblox, Steam, Riot, EA et les autres la proposent gratuitement.
- 2** Les récompenses « gratuites », tu les vérifies dans le jeu ou sur le site officiel. Tu ne donnes pas ton mot de passe ni tes codes à un intermédiaire.
- 3** Ne télécharge jamais de hacks, de triches ou de générateurs. C'est le moyen le plus sûr de perdre ton compte et ton ordinateur.
- 4** Ne partage ton mot de passe avec personne. Ni avec ton meilleur ami, ni avec quelqu'un qui promet de faire monter ton rang.
- 5** Vérifie chaque lien avant de cliquer, surtout ceux reçus sur Discord ou dans le chat du jeu.

Pour les parents

Activez le contrôle parental sur la console ou le compte pour limiter les dépenses et le temps, pas pour une surveillance permanente. N'enregistrez pas de carte sur le compte sans confirmation à chaque paiement. Et surtout, jouez ensemble de temps en temps : c'est le moyen le plus simple de savoir avec qui votre enfant parle en ligne.

En bref

- Un compte de jeu a une vraie valeur et c'est une vraie cible.
- Les offres « gratuites » en dehors du jeu officiel sont, en général, des appâts.
- Les loot boxes, ce sont des dépenses aléatoires : fixe-toi un budget.
- Les triches et les générateurs apportent des logiciels malveillants.
- Un inconnu généreux dans le jeu veut quelque chose en échange.

CHAPITRE 7

Les réseaux sociaux et ton cerveau

Les applis que tu utilises tous les jours sont conçues par des gens très doués, dont le but est de te garder le plus longtemps possible devant l'écran.



Les réseaux sociaux t'aident à rester en contact avec tes amis et avec ta famille dans d'autres villes, te montrent des choses qui t'intéressent et t'évitent de t'ennuyer. Mais ce sont aussi des produits commerciaux. Plus tu restes, plus tu vois de publicités, et plus la plateforme gagne d'argent. C'est pour ça que de véritables « ingénieurs de l'attention » travaillent derrière, en utilisant la psychologie comportementale pour rendre l'appli la plus difficile possible à fermer.

Un peu de **chimie** : pourquoi c'est dur de s'arrêter

Le cerveau a un système de récompense qui nous pousse à répéter ce qui nous fait du bien. La dopamine joue un rôle important dans ce système, surtout dans l'attente de la récompense. Chaque like, chaque notification et chaque nouvelle vidéo peut être une petite récompense, mais tu ne sais jamais quand viendra la suivante. Cette incertitude, appelée récompense variable, est le même mécanisme qui rend les jeux d'argent si difficiles à arrêter.

Chez les ados, les zones du cerveau liées à la récompense sont très actives, tandis que les zones impliquées dans la planification, la prise de décision et le contrôle des impulsions continuent de mûrir jusqu'au début de l'âge adulte. Ça ne veut pas dire que tu es « accro » juste parce que tu aimes TikTok. Ça veut dire qu'il est normal d'avoir du mal à t'arrêter, et que ça vaut la peine de te construire quelques freins.

Source : National Institute of Mental Health (États-Unis), The Teen Brain: 7 Things to Know.

L'expérience d'une semaine

Note ton temps d'écran dans les réglages du téléphone. Puis, pendant une semaine, coupe les notifications des réseaux sociaux et laisse ton téléphone dans une autre pièce la nuit. À la fin, compare ton temps d'écran, ton sommeil et ton humeur. Beaucoup d'ados qui essaient sont surpris du résultat.

11 %

des adolescents de 11, 13 et 15 ans, dans 44 pays, présentaient en 2022 des signes d'usage problématique des réseaux sociaux (7 % en 2018). Ceux qui les utilisent beaucoup, mais sans perdre le contrôle, déclarent même plus de soutien de la part de leurs amis.

Source : OMS Europe, étude HBSC sur les adolescents, les écrans et la santé mentale, 25 septembre 2024, données de 2022

Les signes que les réseaux te **prennent** plus qu'ils ne te donnent

- Tu y vas « juste deux minutes » et tu en ressors une heure plus tard, sans savoir où est passé le temps.
- Ton téléphone est la dernière chose que tu vois le soir et la première le matin, et ton sommeil en souffre.
- Tu te sens irrité ou agité quand tu n'as pas accès à Internet.
- Tu vois de moins en moins tes amis dans la vraie vie.
- Ça t'affecte quand tu n'as pas les likes ou les commentaires que tu attendais.
- Tu repousses tes devoirs, ton entraînement ou ton sommeil pour une vidéo de plus.

Comment reprendre le **contrôle**

Notifications

Coupe-les toutes, sauf les messages de vraies personnes. C'est toi qui décides quand tu y vas, pas l'appli.

Limites de temps

Utilise Temps d'écran (iPhone) ou Bien-être numérique (Android) pour fixer des limites quotidiennes.

Le téléphone dans une autre pièce

La nuit, le téléphone se recharge hors de ta chambre. Le sommeil est la meilleure mise à niveau que tu puisses t'offrir.

Un fil que tu choisis

Désabonne-toi des comptes qui te font te sentir moins bien. L'algorithme apprend de ce que tu regardes.

Ce n'est pas seulement le temps passé qui compte, mais ce que le **contenu** te fait

Si un compte te pousse à ne plus manger, à te faire du mal, à détester un groupe ou à faire quelque chose de dangereux pour être accepté, tu n'as pas à continuer à le suivre. Ni le nombre d'abonnés, ni le fait qu'il apparaisse dans ton fil n'en font une source sûre.

Utilise « Pas intéressé », bloque ou signale le compte et cherche l'information dans des sources indépendantes. N'envoie pas à un ami une vidéo traumatisante pour lui montrer ce que tu as vu : tu peux demander de l'aide en décrivant la situation. Si ça continue à t'affecter, parles-en à un adulte ou à un conseiller.

En bref

- Les applis sont conçues pour te garder le plus longtemps possible devant l'écran.
- Les récompenses imprévisibles rendent le défilement difficile à arrêter.
- Couper les notifications et sortir le téléphone de la chambre fait une énorme différence.
- Un contenu qui te fait du mal se bloque et se signale, il ne se partage pas.

CHAPITRE 8

Deepfakes et intelligence artificielle

Ce que tu vois et entends n'est plus une preuve en soi. Un visage, une voix ou une vidéo peuvent être créés en quelques minutes.



Deepfake réunit deux mots anglais : deep learning, la méthode par laquelle les ordinateurs apprennent à partir d'un très grand nombre d'exemples, et fake, faux. Un deepfake (ou hypertrucage) est une image, une vidéo ou un enregistrement audio modifié ou créé par l'intelligence artificielle, qui ressemble à une personne réelle ou qui en a la voix. Pour cela, le logiciel a besoin de photos, de vidéos et d'enregistrements de cette personne, et plus il en a, plus le résultat est convaincant.

Comment on l'utilise **contre** les gens

Les deepfakes peuvent servir à faire des blagues ou des films, mais aussi à tromper, à faire chanter ou à détruire la réputation de quelqu'un. Trois risques importants pour les ados sont : les fausses images intimes créées à partir de photos ordinaires (chapitre 4), les fausses vidéos de personnes connues qui recommandent des placements ou des concours, et les appels dans lesquels la voix clonée d'un membre de la famille réclame de l'argent en urgence.

Un cas réel

En 2024, un employé de l'entreprise d'ingénierie Arup à Hong Kong a participé à une visioconférence avec le directeur financier et d'autres collègues. Tous étaient faux, créés par l'intelligence artificielle. Convaincu de parler à de vraies personnes, l'employé a transféré 200 millions de dollars de Hong Kong, environ 25 millions de dollars américains, sur les comptes des escrocs.

Source : CNN, sur la fraude par deepfake chez Arup, 16 mai 2024.

Comment vérifier, sans te fier seulement aux apparences

Des doigts déformés, des ombres impossibles, des boutons qui apparaissent et disparaissent ou des lèvres désynchronisées peuvent éveiller les soupçons. Leur absence ne prouve pas pour autant que l'image ou l'enregistrement est authentique. Aucun détecteur d'IA ne doit être considéré comme un verdict définitif : une étude publiée par le gouvernement britannique en 2026 montre que ces outils fonctionnent moins bien en conditions réelles qu'en laboratoire.

Cherche la source d'origine, la date et le contexte. Vérifie si l'information est confirmée de façon indépendante. Une vraie photo peut être utilisée avec une fausse histoire, et une image générée peut paraître parfaite. Si le message demande de l'argent, des données, des images intimes ou une action urgente, vérifie auprès de la personne par un moyen que tu connaissais déjà. Ne décide pas seulement parce que tu as reconnu un visage ou une voix.

Source : Department for Science, Innovation and Technology (Royaume-Uni), Deepfake detection technology, 26 mars 2026.

Vérifier une urgence familiale

Convenez d'un mot de sécurité que vous ne publiez jamais et n'utilisez pas dans les conversations ordinaires. C'est un indice de plus, pas une garantie. Si quelqu'un réclame de l'argent en urgence, raccroche et appelle la personne au numéro que tu avais déjà enregistré. Si elle ne répond pas, vérifie auprès d'un autre membre de la famille. Ne transfère pas d'argent sur la seule base d'une voix, d'un appel vidéo ou de la bonne réponse à une seule question.

Exercice : réelle ou générée par l'IA ?

Les deux images ci-dessous font partie du module REAL / FAKE / AI de la plateforme TRUST // NO TRUST. Nous savons exactement d'où elles viennent, parce que nous les avons créées pour l'exercice. Regarde-les comme si tu les voyais dans ton fil, avant de lire la réponse.



« **URGENT** : le boulevard est une rivière en ce moment ! » Réponse : **image générée par l'IA pour cet exercice**. Nous le savons grâce à sa provenance. Si tu tombais sur cette publication en ligne, tu vérifierais le lieu, la date et les confirmations indépendantes. L'absence de confirmations voudrait dire que l'information reste non vérifiée, pas que tu as prouvé l'usage de l'IA.



« Je donne 10 téléphones, envoie-moi ton adresse ! » Réponse : **générée par l'IA** ; cette personne n'existe pas. Une peau sans aucune texture peut être un indice, mais le message compte davantage : un inconnu qui demande ton adresse en échange d'un cadeau tend un piège, que le visage soit réel ou non.

La leçon : nous savons que ces images sont générées parce que nous connaissons leur provenance. Face à une publication inconnue, sépare deux questions : « L'image est-elle authentique ? » et « Le message est-il crédible ? ». Tu n'as pas besoin de prouver l'usage de l'IA pour refuser une demande suspecte.

En bref

- Une image ou une voix n'est plus une preuve en soi.
- L'absence de défauts ne prouve pas que quelque chose est réel.
- Tu vérifies la source et par un autre moyen, surtout quand on te demande de l'argent ou des données.

L'IA qui semble te comprendre

Un chatbot peut t'expliquer une leçon ou t'aider à formuler une idée. Mais il peut aussi se tromper, inventer des sources ou donner un conseil inadapté, même quand il répond de façon très convaincante.

Certaines applis sont conçues pour ressembler à des amis ou à des partenaires. Le fait qu'elles te répondent avec empathie ne veut pas dire qu'elles te connaissent, qu'elles ont des sentiments ou qu'elles peuvent prendre soin de toi.

32 %

des enfants australiens de 10 à 17 ans ayant utilisé un assistant ou un compagnon IA disaient lui avoir confié des informations personnelles ou sensibles, y compris des photos ou des secrets. L'enquête portait sur près de 2 000 enfants.

Source : eSafety Commissioner (Australie), Talking to machines, rapport publié en août 2026, enquête réalisée en 2026

Ce que tu ne dis pas à un chatbot

- Mots de passe, codes, informations de tes papiers d'identité, ton adresse.
- Des images intimes, de toi ou de quelqu'un d'autre.
- Les conversations privées d'autres personnes.

Ne pars pas du principe que la discussion est aussi confidentielle qu'un rendez-vous chez un psychologue. Vérifie les réglages et les règles du service sur la conservation et l'utilisation des données.

Si les discussions avec un chatbot commencent à remplacer ton sommeil, tes amis ou l'aide des gens, parles-en à quelqu'un de confiance. En cas d'abus, de chantage, de problème de santé ou de danger, demande de l'aide à un adulte ou à un professionnel. Ne laisse pas un chatbot être ton seul soutien.

Tu peux t'entraîner davantage dans le module REAL / FAKE / AI de la plateforme TRUST // NO TRUST, où tu choisis entre vraies photos, images retouchées et images entièrement générées par l'IA.

CHAPITRE 9

Les arnaques virales

Certaines arnaques ne ressemblent pas à des attaques, mais à des services rendus : un vote pour la fille d'une amie, un petit boulot facile depuis chez soi, un cadeau d'un magasin connu.

« Vote pour Adeline, s'il te plaît »

Bună, ați putea vota pentru Adeline aici, vă rog? Aceasta este fiica prietenilor mei. Școala organizează un concurs pentru ei, al cărui premiu este grantul educațional al anului. Vă mulțumesc foarte mult pentru ajutor!

<https://dancingvot.top/home/vote1>

18:03

Le message arrive sur WhatsApp, en général de la part de quelqu'un que tu connais : « Bonjour ! Votez pour Adeline dans ce sondage, s'il vous plaît, c'est la fille d'une amie, le premier prix est une bourse d'études. Merci beaucoup ! » Le lien mène à un site avec deux filles et un bouton de vote. (La capture est un vrai exemple venu de Roumanie.)

Quand tu appuies sur « Voter », une fenêtre te demande ton numéro de téléphone, puis le code que tu viens de recevoir sur WhatsApp. Tu crois avoir voté. En réalité, tu as saisi le code qui associe un nouvel appareil, et les attaquants ont maintenant accès à ton compte WhatsApp. Aussitôt, le même message part vers tous tes contacts, et parfois ton compte est suspendu pour spam.

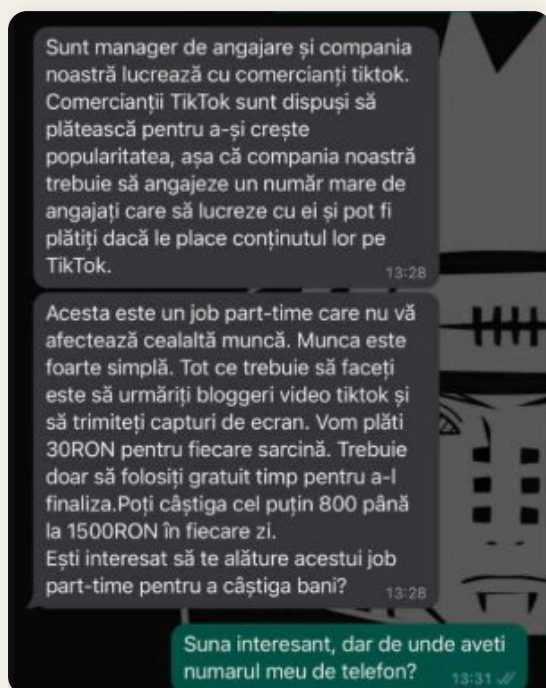
Comment te protéger

- Tu ne saisis pas un code reçu sur WhatsApp dans une page ouverte depuis un message.
- Tu actives la validation en deux étapes de WhatsApp : Paramètres, Compte, Validation en deux étapes.
- Tu vérifies régulièrement Paramètres, Appareils connectés et tu déconnectes ce que tu ne reconnais pas.
- Si un ami te demande quelque chose d'inhabituel, tu l'appelles.

Même astuce, autres habits

- **L'acheteur pressé** sur un site de petites annonces, qui t'envoie un lien « pour recevoir l'argent » et te demande les données de ta carte.
- **Les billets de concert** vendus par « quelqu'un qui ne peut plus y aller », payés d'avance et jamais reçus.
- **Le SMS du transporteur** qui réclame de petits frais pour un colis que tu n'as jamais commandé.

Le petit boulot depuis chez soi qui te coûte cher



« Un job à temps partiel, ça t'intéresse ? Tu likes des vidéos TikTok et tu reçois 30 lei (quelques euros) par capture d'écran. Tu peux gagner de 800 à 1 500 lei par jour. » Au début, tu reçois vraiment quelques lei, pour que tu leur fasses confiance. Puis on te demande d'« investir » une somme pour débloquent des tâches mieux payées. Cet argent ne revient jamais.

Le moyen par lequel on te contacte ne prouve pas que l'offre est réelle. Vérifie l'employeur de façon indépendante et ne paie jamais pour recevoir ton salaire ou débloquent des tâches.

Que donnes-tu en échange ?



Les concours avec de gros lots, les cadeaux de magasins connus, les applis qui te montrent « à quoi tu ressembleras dans 30 ans » et les quiz qui te disent « quel personnage tu es » ont souvent un prix caché : tes données, tes contacts ou l'accès à ton compte. Tout ce qui est gratuit n'est pas un piège, et ce guide en est un exemple. Avant d'accepter quelque chose, demande-toi ce que tu donnes en échange et à qui.

Ton compte n'est pas un service de **virement** pour les autres

« Tu reçois de l'argent sur ton compte, tu le renvoies et tu gardes une commission. » Ça peut ressembler à un petit boulot simple ou à un service rendu à un ami. En réalité, tu peux être utilisé pour faire circuler de l'argent issu de fraudes. Europol décrit ce système comme du **money muling**, une forme de blanchiment d'argent, et la personne qui reçoit et transfère l'argent pour quelqu'un d'autre est appelée une « mule financière ».

Ce que tu fais

- Tu ne prêtes pas l'accès à ton compte bancaire et tu n'ouvres pas de compte pour quelqu'un d'autre.
- Tu ne donnes pas ta carte, tes codes ni des photos de tes papiers pour une offre non vérifiée.
- Si l'argent est déjà arrivé, tu ne le retires pas et tu ne le renvoies pas selon les instructions de celui qui t'a contacté.
- Tu préviens immédiatement ta banque, tu en parles à un adulte et tu demandes conseil à la police. Tu gardes la conversation et les détails du virement.

Source : Europol, guide de prévention sur les mules financières (money muling).



En bref

- Les codes ne s'utilisent que dans la procédure officielle que tu as lancée toi-même ; tu ne les communique pas et tu ne les saisis pas dans des pages reçues pour des votes ou des cadeaux.
- Un petit paiement reçu au début ne prouve pas que le job est réel. Tu n'envoies pas d'argent pour continuer ou pour retirer de prétendus gains.
- Un job qui te demande de l'argent pour commencer est une arnaque.
- Ton compte bancaire ne se prête pas.

CHAPITRE 10

Si ça t'est arrivé

Tout le monde peut se faire piéger, y compris les adultes et les spécialistes. Ce qui compte, c'est ce que tu fais dans les premières minutes, et de ne pas rester seul avec le problème.

- 1 Arrête-toi.** Ne réponds plus, ne clique plus, ne paie rien. Respire. L'attaquant compte sur ta panique.
- 2 Garde les preuves sans diffuser l'abus.** Note le nom du compte, le lien du profil ou de la publication, la date et l'heure. Garde les messages de menace et les demandes d'argent. S'il y a des images sexuelles d'un mineur, ne les télécharge pas, ne les copie pas et ne les transfère pas « comme preuve » : demande des instructions à la police ou au service de signalement. Ne supprime pas tes messages ou ton compte dans la panique.
- 3 Parles-en à un adulte de confiance.** Un parent, ton professeur principal, le conseiller scolaire, ton entraîneur. Aujourd'hui, pas demain.
- 4 Sécurise tes comptes depuis un appareil sûr.** Change tes mots de passe, en commençant par ta boîte mail, vérifie les méthodes de récupération et ferme les sessions inconnues. Si tu as installé quelque chose de suspect, ne saisis pas de nouveaux mots de passe sur l'appareil touché. Suis les étapes adaptées à ta situation à la page suivante.
- 5 Signale.** À la plateforme (le bouton Signaler), puis aux organismes compétents, aux pages suivantes.
- 6 Prends soin de toi.** Ce que tu ressens est normal. Si ça te pèse, parle à un conseiller, par exemple au 116 111.

Ce que tu ne fais pas

- Tu ne paies pas et tu n'envoies pas d'autres photos ou données, même sous la pression.
- Tu ne te venges pas et tu ne menaces pas en retour.
- Tu ne supprimes pas les conversations ni ton compte dans la panique.
- Tu ne paies pas quelqu'un qui te promet de récupérer ton compte contre de l'argent, et tu ne lui donnes pas accès à ton téléphone ou à tes codes.
- Tu n'essaies pas de tout régler seul. Les problèmes en ligne se règlent plus vite avec un adulte à tes côtés.

La première étape dépend de **ce qui s'est passé**

Tu as saisi ton mot de passe sur un faux site

Depuis un appareil sûr, va directement dans l'appli ou sur le site officiel, change le mot de passe et ferme les sessions inconnues. Vérifie les méthodes de récupération (e-mail, téléphone) et les applis connectées. Si le mot de passe était utilisé ailleurs, change-le aussi là-bas.

Tu as donné les données de ta carte ou envoyé de l'argent

Contacte immédiatement la banque, par l'appli officielle ou au numéro au dos de la carte, et demande le soutien d'un parent ou d'un adulte de confiance. Demande le blocage de la carte et la vérification des transactions. N'attends pas la réponse d'un site de signalement.

Tu as installé quelque chose de suspect ou exécuté une commande

Déconnecte l'appareil d'Internet et demande une aide technique. N'y saisis pas de nouveaux mots de passe tant qu'il n'a pas été vérifié. Change tes mots de passe importants depuis un autre appareil.

On te fait chanter avec des images

Ne paie pas, n'envoie pas d'autres contenus et demande de l'aide à un adulte. Garde les messages de menace sans diffuser les images. Utilise Take It Down, esc_ABUZ ou le 119.

Quelqu'un te promet une récupération payante

Ne lui donne accès ni à ton téléphone, ni à ton argent, ni à tes codes. Utilise uniquement la récupération officielle de la plateforme et les organismes de la page suivante.

Source : Microsoft, Token theft playbook.

Où trouver de l'aide en Roumanie

112	Urgences. Appelle si quelqu'un est en danger immédiat ou si on te menace de violence.
119	Protection de l'enfance : maltraitance, négligence ou exploitation d'un enfant. Gratuit, 24 h sur 24, et tu peux demander à rester anonyme.
116 111	Telefonul Copilului (ligne d'écoute pour enfants) : tu parles à un conseiller. Gratuit depuis Orange, Telekom et Vodafone, du lundi au vendredi, de 10 h à 20 h, ou par e-mail à vorbestecunoi@telefonulcopilului.ro Horaires à jour : telefonulcopilului.ro
0744 360 446	Ligne d'aide Ora de Net (Save the Children Roumanie) : questions sur la sécurité en ligne, de 10 h à 17 h. Coordonnées à jour : oradenet.ro/helpline
esc_ABUZ	Ligne de signalement de Save the Children Roumanie pour les contenus illégaux impliquant des enfants. Tu peux signaler seulement le lien, anonymement : oradenet.ro/linia-de-raportare
Take It Down	NCMEC : aide à retirer les images intimes de mineurs des plateformes participantes, sans envoyer l'image. Disponible partout dans le monde : takeitdown.ncmec.org
1911	DNSC : phishing, comptes piratés et fraudes en ligne. Tu peux aussi écrire à alerts@dnsc.ro
0800 800 678	ANITP, traite des êtres humains : appel gratuit en Roumanie. Depuis l'étranger : +40 21 313 31 00.
Police	Demande de l'aide à la police. Si tu peux, vas-y avec un adulte de confiance, mais ne repousse pas ta demande d'aide si tu n'as personne avec toi tout de suite. En cas d'urgence, appelle le 112.

Sources et pages de contact : 112.ro, serviciipublice.gov.ro, edupedu.ro (lancement du 119), telefonulcopilului.ro, oradenet.ro, takeitdown.ncmec.org, dnsc.ro, anitp.mai.gov.ro. Vérifié en octobre 2026 ; chaque service peut modifier ses horaires et ses conditions.

Quand tu appelles ou écris, prépare

Ce qui s'est passé et quand, le nom des comptes concernés, les liens et les messages de menace. Pour les images intimes, ne fais aucune copie : suis la règle de l'étape 2. Pas besoin de tout avoir : dis ce que tu sais, on t'aidera pour le reste.

Besoin d'aide pour d'autres situations ? Le module HELP de la plateforme TRUST // NO TRUST te demande ce qui s'est passé et te montre exactement à qui t'adresser.

Ce que tu retiens de ce guide

Ta tête

- Les problèmes dont on ne parle pas grandissent : tu demandes de l'aide dès le premier jour.
- L'urgence, la peur, la curiosité et le gain sont des signaux d'alerte.
- Si c'est trop beau pour être vrai, ce n'est pas vrai.
- Une image ou une voix n'est plus une preuve en soi.

Tes comptes

- Des phrases de passe longues et différentes, dans un gestionnaire de mots de passe.
- La validation en deux étapes, en commençant par ta boîte mail ; tu n'approuves pas de connexion que tu n'as pas lancée.
- Les codes reçus par SMS ou sur WhatsApp ne se donnent à personne.
- Les clés d'accès partout où elles sont disponibles.

Tes appareils

- Les mises à jour dès qu'elles arrivent.
- Des applis uniquement depuis les boutiques officielles.
- Pas de triches, de générateurs ni de logiciels piratés.
- Sauvegarde et localisation activées.

Les gens

- Quelqu'un qui te demande de cacher des pressions, des demandes intimes ou des menaces, c'est un signal de danger.
- Tu ne paies jamais un maître chanteur.
- Tu ne partages pas et ne likes pas l'humiliation de quelqu'un d'autre.
- Tu demandes de l'aide dès le premier jour. La honte appartient à l'agresseur.

Le test des 10 secondes avant chaque clic

1. Qui m'écrit vraiment ? L'adresse réelle, pas le nom affiché.
2. Est-ce que ça me presse, me fait peur ou me promet quelque chose ?
3. Est-ce qu'on me demande un mot de passe, un code, de l'argent ou une photo ?
4. Est-ce que je peux vérifier par un autre moyen, en appelant ou en allant directement dans l'appli ?
5. Ai-je l'accord de la personne concernée, et est-ce que je comprends ce qui peut arriver à ce contenu ?

Tu peux tomber sur des tentatives de fraude même en étant prudent. Être préparé t'aide à les reconnaître et à en limiter les conséquences.

CHAPITRE 11

Le trident : pourquoi ce cours a sa place à l'école

La sécurité en ligne ne se construit pas seulement dans le téléphone d'un ado. Elle a besoin de trois pointes qui travaillent ensemble : les élèves, les parents et les enseignants.

Les élèves

Ils apprennent à reconnaître la manipulation avec de vrais exemples tirés de leur vie : Instagram, WhatsApp, les jeux, TikTok. Ils partagent un langage commun avec leurs camarades, pour que « c'est du phishing » ou « ne donne pas le code » devienne un réflexe de groupe. Ils savent où trouver de l'aide avant d'en avoir besoin et découvrent qu'ils ne sont pas seuls, ce qui réduit la honte et le silence, justement les armes des agresseurs.

Les parents

Ils comprennent les vrais risques, pas ceux des gros titres, et reçoivent les signaux à surveiller. Ils apprennent à parler à leur enfant sans lui faire peur et sans lui confisquer son téléphone pour le punir, ce qui le pousserait à cacher le prochain problème. Ils peuvent sécuriser les comptes de la famille et convenir ensemble de règles et d'un mot de sécurité.

Les enseignants

Ils reçoivent un contenu prêt à l'emploi pour les heures de vie de classe, d'informatique ou d'éducation civique, et un moyen de reconnaître et de traiter les cas de cyberharcèlement ou de grooming. L'école devient un lieu où les élèves signalent au lieu de cacher.

La plateforme TRUST // NO TRUST comprend des exercices et un outil d'évaluation pédagogique, le CDRS, en cours de développement et d'expérimentation. Les résultats peuvent montrer les réponses que les élèves maîtrisent et les sujets à reprendre. Le score n'est pas un diagnostic et ne garantit pas qu'un élève ou une école soit à l'abri des incidents.

Quand les trois pointes travaillent ensemble, l'ado n'est plus seul face à un écran. Il a des camarades qui reconnaissent les mêmes pièges, des parents qui savent quoi demander et des enseignants qui savent quoi faire. C'est ce qui transforme une leçon de quelques heures en une culture de la sécurité.

Faites venir le cours dans votre école

SMART ONLINE = SAFE OFFLINE est gratuit pour les écoles, les élèves, les enseignants et les parents. Une séance dure une journée, dans une salle équipée d'un vidéoprojecteur, sans aucun matériel particulier. Elle est actuellement donnée en roumain, dans des écoles de Bucarest. Pour réserver une séance, écrivez à nicholas.carstoiu@gmail.com ou appelez le +40 743 332 318.

Sources

Chaque chiffre de ce guide a été vérifié à sa source en octobre 2026. Les sources comprennent des rapports, des communiqués et des pages officielles. Quand c'est utile, la date de publication est distinguée de la période à laquelle se rapportent les données.

1. UNICEF Innocenti, rapport Through Children's Eyes, publié le 3 septembre 2026, données issues de la recherche Disrupting Harm.
<https://www.unicef.org/innocenti/reports/through-childrens-eyes>
2. OMS Europe, étude HBSC sur le cyberharcèlement, 27 mars 2024, données de 2022.
<https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study>
3. OMS Europe, étude HBSC sur les adolescents, les écrans et la santé mentale, 25 septembre 2024, données de 2022.
<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>
4. National Institute of Mental Health (États-Unis), The Teen Brain: 7 Things to Know.
<https://www.nimh.nih.gov/health/publications/the-teen-brain-7-things-to-know>
5. Save the Children Roumanie (Salvați Copiii), étude sur le harcèlement à l'école, communiqué du 18 octobre 2022.
<https://www.salvaticopiii.ro/sites/ro/files/2023-11/studiu-peste-un-sfert-dintre-copii-au-fost-agresori-jumatate-spun-ca-au-fost-victime-ale-bullying-ului.pdf>
6. Save the Children Roumanie (Salvați Copiii), communiqué de presse du 28 mars 2025.
<https://salvaticopiii.ro/sites/ro/files/2025-03/5-ani-a-scazut-pragul-de-varsta-pentru-copii-pe-retele-sociale-avertisment.pdf>
7. Save the Children Roumanie (Salvați Copiii), ligne de signalement esc_ABUZ, communiqué du 10 décembre 2025.
<https://www.salvaticopiii.ro/sites/ro/files/2025-12/expunere-si-continut-daunator-copii-online-crestere-alarmana-a-sesizarii.pdf>
8. NCMEC, communiqué sur la sextorsion, publié le 25 juin 2026, données de 2025.
<https://www.missingkids.org/blog/2026/ncmec-releases-new-sex-tortion-data-2025>
9. NCMEC, données CyberTipline, publiées en 2026, données de 2025.
<https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata>
10. NCMEC, Take It Down, questions fréquentes.
<https://takeitdown.ncmec.org/faq/>
11. Europol, The rise of online cult communities dedicated to extremely violent child abuse, janvier 2025.
https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The_rise_of_online_cult_communities_dedicated_to_extremely_violent_child_abuse.pdf
12. eSafety Commissioner (Australie), suivi, surveillance et harcèlement non consentis chez les enfants, mis à jour le 1er juillet 2025, enquête de décembre 2024 à février 2025.
<https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/snapshot-non-consensual-tracking-monitoring-harassment>

Sources (suite)

13. eSafety Commissioner (Australie), Talking to machines, rapport publié en août 2026, enquête réalisée en 2026.
<https://www.esafety.gov.au/research/talking-to-machines-childrens-experiences-with-ai-assistants-and-companions>
14. Europol, guide de prévention sur les mules financières (money muling).
<https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling>
15. NIST, SP 800-63B-4, Digital Identity Guidelines, août 2025.
<https://pages.nist.gov/800-63-4/sp800-63b.html>
16. CISA, Implementing Phishing-Resistant MFA (fiche d'information).
<https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf>
17. Microsoft, Token theft playbook.
<https://learn.microsoft.com/en-us/security/operations/token-theft-playbook>
18. FTC (États-Unis), Are Public Wi-Fi Networks Safe? What You Need To Know.
<https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know>
19. Microsoft Security Blog, TerminalFix campaign deploys a reverse tunnel through multistage intrusion, 28 août 2026.
<https://www.microsoft.com/en-us/security/blog/2026/08/28/terminalfix-campaign-deploys-reverse-tunnel-through-multistage-intrusion/>
20. Department for Science, Innovation and Technology (Royaume-Uni), Deepfake detection technology, 26 mars 2026.
<https://www.gov.uk/government/publications/deepfake-detection-technology/deepfake-detection-technology>
21. Organisation internationale du Travail (OIT), Walk Free et Organisation internationale pour les migrations (OIM), Global Estimates of Modern Slavery, septembre 2022.
<https://www.ilo.org/publications/major-publications/global-estimates-modern-slavery-forced-labour-and-forced-marriage>
22. TVR Info, sur l'attaque contre la plateforme Hipocrate, 13 février 2024.
<https://tvrinfo.ro/blocajul-generat-de-atacul-cibernetice-asupra-spitalelor-continua-hackerii-au-cerut-o-rascumparare-de-peste-150-de-mii-de-euro-in-bitcoin/>
23. CNN, sur la fraude par deepfake chez Arup, 16 mai 2024.
<https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>
24. Check Point Research, Hacking Fortnite, 16 janvier 2019.
<https://research.checkpoint.com/2019/hacking-fortnite/>
25. NBC News, sur la récompense versée à un enfant de 10 ans pour une faille d'Instagram, mai 2016.
<https://www.nbcnews.com/tech/social-media/facebook-pays-10-000-10-year-old-instagram-hacker-n568026>

Sources (suite)

26. Aide Compte Google, Be ready to find a lost Android device.
<https://support.google.com/accounts/answer/3265955?hl=en>
27. eSafety Commissioner, How to manage money in games.
<https://www.esafety.gov.au/parents/issues-and-advice/gaming/how-to-manage-money-in-games>
28. TRUST // NO TRUST, module REAL / FAKE / AI (images générées par IA pour l'exercice).
<https://www.looksmart.ro/trustnotrust/fr/real-fake-ai/>
29. DNSC, Direction nationale de la cybersécurité de Roumanie, numéro 1911 pour signaler les incidents.
<https://www.dnsc.ro/>
30. Have I Been Pwned, vérification des adresses e-mail compromises.
<https://haveibeenpwned.com/>
31. Ora de Net, Save the Children Roumanie : ligne d'aide et ligne de signalement esc_ABUZ.
<https://www.oradenet.ro/linia-de-raportare/>
32. Association Telefonul Copilului, fonctionnement du 116 111.
<https://telefonulcopilului.ro/116111/afla-cum-functioneaza-telefonul-copilului-116111/>
33. Portail roumain des services publics gov.ro, assistance sociale et protection de l'enfance (119).
<https://serviciipublice.gov.ro/servicii?domainSlug=asistenta-sociala-si-adoptii>
34. Edupedu, sur le lancement du numéro 119, 5 janvier 2022.
<https://www.edupedu.ro/cazurile-de-copii-abuzati-pot-fi-semnalate-la-numarul-de-telefon-unic-national-gratuit-119-numa-rul-este-corelat-cu-112-si-echipe-mobile-pot-intervenii-imediat/>
35. ANITP, Agence nationale roumaine contre la traite des êtres humains.
<https://anitp.mai.gov.ro/contact/>
36. Système national unique d'appels d'urgence 112 (Roumanie).
<https://www.112.ro/>
37. Le programme SMART ONLINE = SAFE OFFLINE.
<https://www.looksmart.ro/nicholas/projects/smart-online-safe-offline.html>
38. La plateforme TRUST // NO TRUST.
<https://www.looksmart.ro/trustnotrust/fr/>

À propos des images

Les illustrations des chapitres proviennent des supports du cours SMART ONLINE = SAFE OFFLINE et ont été créées à l'aide de l'intelligence artificielle. Les captures d'écran de messages frauduleux sont reproduites uniquement dans un but éducatif, pour aider les lecteurs à reconnaître les fraudes ; plusieurs sont de vrais exemples reçus en Roumanie. Les marques et logos visibles appartiennent à leurs propriétaires, qui n'ont aucun lien avec ces messages. Les deux images de l'exercice du chapitre 8 ont été générées par IA pour le module REAL / FAKE / AI de la plateforme TRUST // NO TRUST.



Better **safe** than sorry

Tu as terminé le guide. Maintenant, entraîne-toi : la plateforme **TRUST // NO TRUST** te place dans des situations fictives, inspirées de risques réels, où tu décides toi-même quoi faire.

www.looksmart.ro/trustnotrust

CONTACT

Nicholas Carstoiu

nicholas.carstoiu@gmail.com · +40 743 332 318

www.looksmart.ro/nicholas

Droits d'auteur. © 2026 Nicholas Carstoiu (Nicholas Cârstoiu). Tous droits réservés. Ce guide peut être téléchargé, imprimé et diffusé gratuitement, en intégralité et sans modification, à des fins éducatives non commerciales, en citant la source. La vente, la modification ou la reprise partielle du contenu sans l'accord écrit de l'auteur sont interdites.

À propos de la sécurité. Ce guide a une vocation uniquement informative et éducative. Suivre ses recommandations réduit les risques, mais ne garantit pas une protection contre toutes les menaces en ligne, qui changent sans cesse. Ce guide est une brique de ton éducation numérique, pas un substitut à la discussion avec tes parents, tes professeurs ou des spécialistes. En cas de danger, contacte immédiatement le 112 ou les services d'aide du chapitre 10.