Trop confiants et trop exposés : les enfants sont-ils en sécurité en ligne ?

Les enfants passent de plus en plus de temps sur Internet. Mais quelles sont les limites de leur sécurité ? Et qui les aide à se protéger contre les cyber menaces ?

Un rapport de Kaspersky
Mars 2023

Contenu

Aperçu :

"L'éducation est l'arme la plus puissante dont nous disposons pour changer le monde"

Nelson Mandela

La sécurité des enfants fait partie du top 10 de l'agenda politique des pays occidentaux depuis de nombreuses années. Ces 10 dernières années, il est devenu de plus en plus facile de se procurer des appareils connectés, tandis que les usages d'Internet se sont accélérés et développés. Moralité, les enfants sont de plus en plus exposés au risque cyber, pas uniquement à cause du contenu sensible ou pouvant les heurter disponible en ligne, mais aussi à cause des arnaqueurs et des fraudeurs qui y rôdent.

Alors que le Digital Service Act de l'Union Européenne œuvre à fournir des règles plus claires et uniformisées pour le contenu numérique, le gouvernement du Royaume-Uni continue de sanctionner les dirigeants d'entreprises du numérique de peines minimales de 2 ans de prison s'ils continuent d'ignorer les règles de l'Ofcom et échouent à protéger les enfants des contenus sensibles. En parallèle, le gouvernement français a rédigé un projet de loi rendant obligatoire l'installation d'un système de contrôle parental, facilement accessible et compréhensible, sur les appareils connectés à internet vendus en France, et ce afin de lutter contre l'exposition des enfants à des contenus violents ou pornographiques. Des associations telles que e-enfance se sont également spécialisées dans l'assistance et l'accompagnement des enfants face aux violences numériques, notamment le cyber-harcèlement ou les arnaques en ligne.

Malgré ces initiatives, les alertes et les nombreuses actions de sensibilisation menées par les professionnels du secteur depuis de nombreuses années, une large proportion de parents s'assure quelques instants de tranquillité grâce aux écrans. Les dangers sont pourtant bien présents : une minute votre enfant peut être en train de regarder un épisode de Peppa Pig et la minute suivante, se voir proposer un contenu propagandiste indiquant que la terre est plate, une vidéo de Lady Gaga qui "twerke" ou bien pire !

De façon tout aussi alarmante, le contenu consommé par les enfants n'est pas le seul facteur de risques en ligne. A partir du moment où ils ont une présence en ligne, ils sont exposés au cybercrime via des menaces allant d'attaques par phishing au ransomware. Jusqu'à présent, la majorité des débats publics autour des dangers du monde numérique pour les enfants s'est focalisée sur le contenu ou sur l'attitude des enfants en ligne (le cyber harcèlement notamment). Hélas, les jeunes doivent tout autant être sensibilisés et accompagnés pour être en mesure de se protéger contre les arnaques en ligne.

Les enfants sont très vulnérables en ligne, et largement exposés aux risques d'arnaques et de cyber attaques.

Pendant la pandémie de Covid-19, les écoles du monde entier ont été forcées de digitaliser leurs cours et leurs processus éducatifs, imposant aux enfants d'être connectés, et ce qu'ils soient prêts ou non. Des sessions de cours par visioconférence à la création d'adresses emails pour les élèves, en passant par les tutoriels Youtube, des centaines de milliers d'enfants sont arrivés sur Internet – s'ils n'y étaient pas déjà. Et si ces possibilités numériques ont indubitablement aidé à maintenir un programme d'éducation, quelqu'un s'est-il vraiment arrêté une minute dans cette course à l'école digitale, pour poser les bases de l'éducation au numérique, à la fois pour les enfants, mais aussi pour leurs parents ? Ont-ils été sensibilisés aux nombreuses escroqueries en ligne, loin d'être anecdotiques, et aux contenus nuisibles ?

Les nouvelles générations d'utilisateurs sont plutôt très au fait des technologies et il serait absurde d'insinuer le contraire. Ayant été exposés aux innovations technologiques dès leur plus jeune âge, ils sont souvent plus au courant que leurs parents du fonctionnement des appareils, du contenu auquel ils peuvent accéder et de ce qui leur est proposé en ligne.Mais sont-ils au courant de ce qu'est une attaque d'hameçonnage ? Savent-ils s'ils y ont déjà été exposés ? Ont-ils déjà partagé leurs informations personnelles, ou celles d'un proche, en ligne ? Peuvent-ils faire la différence entre un email réel et une arnaque ? Ont-ils conscience de la manière dont leurs données sont utilisées par les entreprises légitimes ?

Kaspersky est une entreprise internationale composée d'experts en threat intelligence actifs dans toutes les régions du monde. L'entreprise a profité de cette expérience unique pour entreprendre des recherches approfondies sur la sécurité des enfants en ligne et sur leur compréhension des cyber menaces, telles que les attaques par phishing (ou hameçonnage).

Les résultats de notre recherche révèlent que près de 2 enfants sur 5 en Europe, s'estimant pourtant informés en matière de sécurité en ligne, ont en fait été victimes d'arnaques par phishing. Cela ne souligne pas uniquement le fossé existant entre le fait de comprendre et d'utiliser des technologies et celui de comprendre les menaces qui les accompagnent, mais aussi le fait que les enfants sont très exposés aux différentes escroqueries et menaces en ligne. L'analyse des différences de perception de la menace, mais aussi de l'estimation des connaissances en matière de sécurité numérique entre les différents pays d'Europe est particulièrement intéressante également, car elle révèle notamment que les Français font partie des jeunes européens s'estimant les moins informés en matière de sécurité numérique.

Ce rapport explore la vulnérabilité des enfants aux cybermenaces malgré leur perception de sécurité, mais également leur manière de se comporter en ligne. Il met en évidence le fait que les parents et les systèmes éducatifs doivent jouer un rôle pivot dans l'éducation et la protection des enfants contre les dangers en ligne. Les résultats révèlent que, lorsqu'on les confronte à des emails authentiques et des emails d'arnaques, la majorité des enfants ont des difficultés à les distinguer, démontrant que même s'ils se sentent confiants, ils ont encore beaucoup à apprendre.

6382 enquêtes en ligne auprès d'enfants

âgés de 11 à 15 ans, menées par Censuswide à travers 8 pays.

6655 enquêtes en ligne auprès d'adultes

menées par Censuwide à travers les mêmes pays.

Méthodologie

6382 enfants âgés de 11 à 15 ans ont été interrogés en ligne par Censuswide entre le 3 janvier 2023 et le 10 février 2023 à travers 8 pays : le Royaume-Uni (1003), la France (1001), l'Espagne (1000),le Portugal (507), la Grèce (501), les Pays-Bas (501), l'Allemagne (1002) et l'Italie (1013). Les sondés ont été questionnés sur leurs connaissances en matière de cybersécurité, s'ils avaient déjà été ciblés par une attaque par phishing, s'ils avaient déjà été aidés par un adulte pour identifier une potentielle arnaque par phishing et s'ils pouvaient voir la différence entre un faux et un véritable email.

En parallèle , 6665 adultes ont été interrogés en ligne par Censuswide entre le 3 janvier 2023 et le 10 février 2023, à travers les mêmes 8 pays : Royaume Uni (1001), France (1000), Espagne (1000), Portugal (503), Grèce (650), Pays-Bas (501), Allemagne (1000) et Italie (1000). Les sondés ont également été interrogés à propos de leur exposition aux attaques par phishing, de leurs connaissances en matière de cybersécurité et s'ils avaient déjà aidé des plus jeunes ou des enfants à identifier des arnaques par phishing. Censuswide respecte et emploie des membres de la Market Research Society, qui est basée sur les principes ESOMAR.

Les découvertes

Les enfants savent qu'ils sont ciblés par des arnaques par phishing de manière régulière et pourtant, ils continuent de transmettre des informations personnelles via les réseaux sociaux ou des jeux en ligne :

- 26% des enfants européens interrogés (15 % des français) indiquent avoir été victimes d'arnaques par phishing, avec plus d'un tiers (35 %) rapportant être au courant d'être la cible de tentatives de ce genre au moins plus d'une fois par mois.
- Cependant, malgré cela, près de la moitié des enfants français interrogés (48 %) et plus de la moitié des européens (55 %) admettent partager des informations personnelles telles que leur nom et leur ville sur les réseaux sociaux. 44 % des français et 54 % des européens donnent ouvertement le nom de leur animal de compagnie et le nom de leur rue dans des quiz sur les réseaux sociaux.
- En outre, à peu près 2 enfants sur 5 interrogés (39%) indiquant avoir des connaissances en matière de sécurité en ligne ont déjà été victimes d'arnaques par phishing, contre seulement 1 enfant sur 10 (11%) estimant « ne rien y connaître » en cybersécurité.

Plus les enfants s'estiment informés à propos des menaces en ligne, plus ils sont susceptibles d'être victimes d'arnaques en ligne.

- En effet, les enfants ayant déjà été victimes d'arnaques en ligne sont encore plus susceptibles (79%[1]) de partager des informations personnelles pour s'aider à se rappeler d'un mot de passe que ceux qui n'ont pas été victimes (47%[1]).
- Les enfants interrogés ont admis avoir plus tendance à ouvrir des liens contenus dans un message WhatsApp (30%) que des liens contenus dans des SMS (11%).
- Plus alarmant encore, 83% des enfants interrogés ayant déjà été victimes d'une arnaque par phishing estiment qu'ils ont des chances d'être de nouveau piégés. En comparaison, 2 enfants sur 5 n'ayant jamais été victimes d'arnaques estiment pouvoir se faire piéger[3].

Si les jeunes ont conscience d'être exposés aux arnaques par phishing et en sont inquiets, les adultes entreprennent peu d'actions pour leur enseigner les manières de rester en sécurité en ligne :

- Seuls 2 adultes interrogés sur 5 (42 %), et 1 adulte français sur 3 (33 %) indiquent avoir aidé les plus jeunes à identifier des arnaques de phishing.
- Certains adultes (27%[3]), qui avouent ne pas s'y connaître en matière de cybersécurité, tentent d'enseigner à la jeune génération la sécurité en ligne et la manière de repérer une attaque par hameçonnage : un cas classique d'aveugle guidant l'aveugle.
- Géographiquement, 71% des adultes interrogés au Royaume Uni, 67% en France et 53% en Allemagne admettent ne jamais aider les plus jeunes à identifier les arnaques, contre 65% des Grecs et 51% des Portugais ayant déjà aidé les jeunes.
- Plus inquiétant en France : plus de la moitié des adolescents (54%) et près d'un tiers des adultes indiquent ne pas savoir ce qu'est une arnaque par phishing. Cela en fait le pays avec les habitants les moins au fait des arnaques en ligne en Europe.
- Pourtant, malgré ces chiffres, 71% des enfants français sont certains de n'avoir jamais été victimes d'arnaques par phishing – chiffres à relativiser donc puisqu'ils ne sont pas en mesure de les identifier (seuls 12% admettent ne pas savoir s'ils ont été victimes ou non).

Seuls 2 adultes interrogés sur 5 (42 %), et 1 adulte français sur 3 (33 %) indiquent avoir aidé les plus jeunes à identifier des arnaques de phishing.

[1] Combinaison des réponses "Oui, plus d'une fois" et "Oui, une fois".

[2] 'Très bien informé, je suis un pro' et 'Assez bien informé, j'en sais plus que la plupart des gens' combinées.

[3] 'Pas très bien informé, je pense être en dessous de la moyenne' et 'Pas du tout bien informé, je ne comprends pas tout' combinées

L'excès de confiance, un facteur de risque

Les enfants pensent en savoir plus que les adultes mais attention à l'excès de confiance, qui les expose parfois à des risques en ligne.

Le monde n'a jamais été aussi connecté qu'aujourd'hui. On estime que 4.9 milliards de personnes sont connectées à Internet – cela représente 62% de la population mondiale. Parmi ces internautes, 1 sur 3 est un jeune de moins de 18 ans.

Considérant ces chiffres, il est impossible de ne pas se préoccuper de la sécurité des jeunes et des enfants en ligne. Apprentissage en ligne, jeux, réseaux sociaux et méthodes de socialisation numériques… les enfants passent de plus en plus de temps derrière des écrans. Contrairement aux générations précédentes, ils n'ont pas connu autre chose, ils sont nés avec des tablettes, des ordinateurs, un accès instantané à l'information, au divertissement, aux échanges illimités… Les jeunes d'aujourd'hui vivent dans un monde connecté au rythme effréné qui ne ralentit pas.

En tant qu'adultes, nous avons appris à nous adapter aux écrans mais nous n'avons pas encore intégré l'éducation au numérique de la même manière que nous apprenons à nos enfants à marcher, à écrire, à traverser la route. Ainsi dans notre étude, on constate qu'encore trop peu d'adultes accompagnent leurs enfants dans leur apprentissage des risques et des manières de se protéger en ligne. La problématique est globalement que le niveau de compétence en cybersécurité n'est pas beaucoup plus élevé chez les adultes que chez les enfants. Si les uns sont parfois trop confiants, les autres ne vont pas se sentir légitimes à enseigner des méthodes qu'ils ne maîtrisent que peu. En France, 34% des jeunes estiment s'y connaître en cybersécurité contre un peu moins de la moitié des adultes (49,8%). Pour autant, seuls 33% des adultes admettent avoir déjà aidé des enfants à reconnaître des arnaques en ligne.

L'ennui, c'est qu'estimer s'y connaitre en cybersécurité ne nous épargne pas du risque, voire tend à nous faire prendre plus de risques. L'étude indique que près de 2 enfants sur 5 (39%) qui pensent s'y connaître sont en fait déjà tombés dans le piège d'une arnaque par phishing. En comparaison, 11% seulement des enfants qui s'estiment « ignorants » en matière de cybersécurité indiquent avoir déjà été victimes d'une arnaque par phishing. Sont-ils plus prudents parce qu'ils s'estiment trop peu informés? Ou ignorent-ils avoir été la cible de phishing car ils n'ont pas su reconnaître une arnaque? Considérant que 72 % des enfants en Europe (75% en France) se sont trompés au moins une fois dans l'identification de faux emails, on peut imaginer qu'il y a un peu des deux.

Qu'ils soient trop confiants ou pas du tout informés, le résultat semble identique : les enfants sont trop exposés aux risques en ligne et notamment aux tentatives de phishing et d'escroqueries en tout genre. Lorsqu'on les confronte au fait qu'ils n'ont pas su reconnaître un certain nombre d'arnaques, les enfants français sont préoccupés par le niveau de sophistication des arnaques, mais ils craignent également de tomber de nouveau dans le piège. 46% s'estiment surpris de s'être trompés.

Le cybercrime est en croissance. Les attaques par phishing ont augmenté de 61% en 2022 et on ne voit aucun signe d'amélioration. Les attaques et les arnaques sont plus nombreuses, mais également de plus en plus sophistiquées, avec de nouveaux outils tels que les IA qui les rendent plus difficiles à identifier et ce, quel que soit l'âge de la victime.

Alors, comment faire en sorte que les enfants soient moins vulnérables aux arnaques par phishing, et de manière générale aux risques en ligne ?

26% des enfants européens interrogés (15 % des français) indiquent avoir été victimes d'arnaques par phishing

Une Génération Z trop connectée

Bien que les jeunes Européens se disent bien informés des enjeux de cybersécurité, 75% des jeunes Français, et 72 % des jeunes européens n'ont pas été capables d'identifier 1 ou plusieurs exemples d'arnaques par phishing. Si les Français reconnaissent en majorité (54 %) leur ignorance sur le sujet, ils apparaissent aussi comme les moins avertis d'Europe quant à la cybersécurité. Pour autant, en termes de pratiques, ils ne sont pas les plus mauvais élèves, mais suivent la tendance européenne : les jeunes dans leur globalité partagent consciemment beaucoup trop d'informations personnelles sur les réseaux sociaux.

Plus de la moitié des enfants interrogés en Europe (55 %) admettent avoir mentionné en ligne des informations personnelles telles que leur nom, leur date de naissance ou leur ville. C'est un peu moins en France avec 48 % des répondants admettant l'avoir fait. En plus de ces informations en apparence anodines, 54% des enfants européens, et 44% des jeunes Français admettent avoir déjà répondu à des quiz en ligne les interrogeant sur le nom de leur animal de compagnie, de leur rue ou de leur série TV préférée.

Ce qu'on n'a pas toujours en tête, c'est que ce genre de « quiz » en ligne sont bien souvent des stratagèmes mis en place par des acteurs malveillants pour récupérer des informations personnelles, et leur permettre de construire un « profil social et numérique » de leur victime, utile pour perpétrer des attaques en ligne, telles que des piratages de compte ou des fraudes financières.

Bien sûr, tout le monde peut être la cible d'attaques, indépendamment des informations partagées en ligne. Néanmoins, les données issues de nos recherches indiquent que plus nous partageons d'informations personnelles en ligne auprès de sources inconnues et non vérifiées, plus nous sommes susceptibles d'être ciblés par des cyberattaques telles que le phishing. Selon notre enquête, les enfants ayant davantage tendance à devenir victimes d'arnaques en ligne sont ceux qui ont :

- Utilisé des informations personnelles pour se souvenir d'un mot de passe
- Indiqué des informations personnelles sur les réseaux sociaux
- Répondu à des quizz sur les réseaux sociaux

Les recherches démontrent un problème croissant, celui du partage excessif d'informations personnelles de la part des générations Z et Alpha. Plus ils partagent, moins ils se méfient, et plus ils tendent à être victimes de cybercrime.

> Le plus ils partagent, le moins ils se méfient, et le plus ils ont tendance à être victimes de cybercrime.

"L'éducation au numérique est un processus, et pas une fin en soi. Informer, sensibiliser aux risques en ligne est une chose, mais adopter les bons réflexes, être capable de prendre du recul et d'adresser la question de la sécurité lorsqu'on navigue sur internet, c'est différent. C'est comme pour conduire une voiture, on peut maîtriser le code de la route, mais cela ne fait pas de nous des conducteurs prudents pour autant. Les bonnes pratiques au numérique sont relativement simples (utiliser des mots de passe forts, ne pas cliquer sur les liens contenus dans des emails indésirables/non sollicités, etc.) mais il faut qu'elles deviennent des réflexes.

La sécurité en ligne est un mélange de connaissances techniques, de compréhension de la nature humaine, et d'expérience vis-à-vis de ses dérives… C'est à force d'actions communes, de communication et de sensibilisation constante mais aussi de coopération entre les différents acteurs, les pouvoirs publics et les entreprises privées qu'on parviendra à intégrer la culture du numérique, l'hygiène cyber comme on l'appelle, au sein des usages et ce, quels que soient les utilisateurs et leurs âges"

Bertrand Trastour - DG France de Kaspersky

Le niveau de sensibilisation est actuellement insuffisant et nous devons faire plus pour éduquer les enfants sur la manière d'être en sécurité en ligne… mais à qui en revient la responsabilité ?

L'éducation est un droit humain fondamental et, dans la plupart des pays du monde, elle est garantie pour tous sans discrimination. Parallèlement, l'agenda de l'éducation ne cesse d'évoluer et de s'adapter aux besoins de la société. Par exemple, au début de l'année 2023, le Premier ministre britannique, Rishi Sunak, a annoncé qu'il était prévu que tous les élèves étudient les mathématiques sous une forme ou une autre jusqu'à l'âge de 18 ans, dans le but d'améliorer les connaissances en calcul dans tous les domaines. En France, le Ministre de l'Education Nationale Pap N'Diaye a annoncé à l'occasion du Safer Internet Day 2023 qu'un cours sur le cyber-harcèlement serait bientôt obligatoire en classe de 6e alors que les cas de harcèlement scolaire aux conséquences dramatiques se multiplient à travers l'Europe. C'est une avancée, mais est-ce suffisant ? Enseigner l'impact du comportement humain en ligne est certes indispensable, mais quid des bons réflexes techniques numériques ? Comment reconnaître un mail de phishing, comment garder la maîtrise de ses données personnelles ?

On peut saluer les améliorations constantes apportées aux programmes éducatifs, mais notre rapport semble pointer du doigt certaines lacunes dans l'éducation aux bonnes pratiques de sécurité en ligne. Est-ce que suffisamment de temps y est consacré ? Il n'y a tout simplement pas assez de cours soulignant les dangers auxquels exposent les différentes menaces, ni de cours sur la manière de rester en sécurité sur la toile. Les enfants comptent donc sur leurs parents et leurs tuteurs pour leur apprendre ces bonnes pratiques, mais qui se charge d'enseigner la cybersécurité à ces derniers?

Moins de la moitié des adultes européens, et à peu près un tiers des adultes français interrogés indiquent avoir déjà aidé un enfant ou un adolescent à identifier des arnaques par phishing. Pourtant, 40 % des adultes à travers l'Europe admettent ne pas être suffisamment au fait des enjeux de cybersécurité. Ce chiffre atteint même 49 % en France. Un adulte sur 5 (19 % en Europe, 20 % en France) admet même s'être déjà fait avoir par une arnaque de phishing.

L'absence de cours sur la sécurité en ligne dans les écoles ainsi que le manque de compréhension ou de volonté des parents et adultes de transmettre leur savoir en matière de sécurité à la jeune génération révèlent des lacunes au niveau de l'éducation à la sécurité en ligne, lacunes qu'il est capital de combler.

En France, et en Europe, des initiatives encourageantes ont vu le jour, telles que **l'association e-enfance**, qui accompagne les jeunes victimes de violences en ligne et œuvre à sensibiliser les plus jeunes aux bonnes pratiques en ligne. Par ailleurs, le groupement d'intérêt public d'aide aux victimes de cyber malveillances, cybermalveillance.gouv.fr a **récemment lancé un guide** à destination des familles pour donner les conseils de base pour une meilleure hygiène numérique au quotidien.

> Les pays européens ne consacrent pas assez de temps à l'enseignement de la sécurité en ligne à l'école.

Pourquoi avons-nous besoin d'éducation à la cybersécurité

Les enfants sont l'avenir, donc éduquons-les à la cybersécurité.

Les résultats de cette étude pointent tous dans la même direction : qu'importe l'âge, tout le monde est exposé au risque d'arnaques en ligne. Un acteur malveillant ne se préoccupe pas de votre âge ni d'où vous venez, pour lui, tout le monde est une proie potentielle. L'unique manière d'y mettre un terme est de renforcer et d'améliorer l'éducation afin que chacun, jeune ou moins jeune, ait la possibilité de détecter et éviter les arnaques du quotidien.

Les adolescents et les enfants ne font pas exception et il est dangereux de leur laisser penser que parce qu'ils se sentent intouchables, ils le sont vraiment. Qu'ils soient informés ou non sur la sécurité en ligne, ils restent vulnérables aux cyberattaques tant qu'ils ne changent pas leurs comportements.

Internet a ouvert le monde à la jeune génération et lui a offert une multitude de possibilités, mais la vitesse et les taux d'adoption ont été si rapides que personne ne s'est arrêté pour prendre du recul et voir à quel point nous sommes tous exposés aux dangers bien réels qui existent et trompent des adultes tous les jours. Il est tout simplement irréaliste de penser que la génération qui a grandi avec les tablettes et les smartphones saura instinctivement ce qu'il faut éviter et ce sur quoi il ne faut pas cliquer.

Les enfants sont notre avenir et il faut faire davantage dans les écoles comme à la maison pour leur apprendre à se protéger en ligne. Même s'ils pensent avoir les connaissances et les compétences nécessaires pour se protéger, il arrive toujours qu'ils tombent dans le piège de certaines attaques de phishing, même les plus simples. C'est sans compter que les menaces deviennent de plus en plus sophistiquées, au fur et à mesure que le nombre d'informations personnelles mises en ligne croît. Nous vivons dans un monde régi par les données et, que vous ayez 11 ou 111 ans, votre empreinte numérique s'étend chaque jour, offrant aux criminels toujours plus d'opportunités et de contenus à voler.

[4] Répondants de tous les pays étudiés, Royaume-Uni, France, Espagne, Portugal, Grèce, Pays-Bas, Italie et Allemagne.

Quelques conseils et ressources

Bien entendu, il existe des solutions de sécurité pour les mobiles ou ordinateurs à l'image de **la nouvelle gamme Kaspersky Premium** qui protège la confidentialité, l'identité et garantit la sécurité des appareils comme des données des utilisateurs. Mais au-delà des outils, voici quelques recommandations simples à mettre en place pour améliorer sa résilience en ligne :

- **Ignorer systématiquement** tous les emails qui vous demandent d'entrer des données confidentielles ou personnelles.
- Lorsque vous recevez un email de la part d'une institution officielle, connectez-vous directement sur le site en tapant l'adresse dans votre barre de recherche de navigateur et **ne cliquez pas sur le lien présent dans l'email**. S'il y a des informations à fournir, cela sera précisé sur votre espace personnel. Sinon, c'est qu'il s'agit d'une tentative d'arnaque.
- Idem si vous recevez des offres promotionnelles ou des emails de la part de marque vous faisant part d'offres en cours. **Si c'est trop beau pour être vrai : c'est que c'est sans doute faux**.Et dans le doute, plutôt que de cliquer sur le lien dans l'email, tapez l'adresse du site de e-commerce dans le navigateur. Si des offres existent, elles seront mentionnées.
- Si vous recevez des SMS ou des messages sur les messageries instantanées – et ce, même de la part d'une personne que vous pensez connaître, **ne cliquez pas sur les liens s'ils vous paraissent louches.**
- **Utilisez des mots de passe complexes** et uniques pour chaque site sur lequel vous créez un compte. Utilisez un gestionnaire de mots de passe pour vous aider à les mémoriser.
- **Ne communiquez jamais d'informations confidentielles** sur les réseaux sociaux, par téléphone ou par messagerie instantanée.
- **Paramétrez vos comptes sur les réseaux sociaux** pour qu'ils ne soient pas accessibles publiquement et pour bloquer les messages/ invitations non sollicitées, cela limitera les tentatives d'arnaques.

Pour plus d'informations sur la manière dont enfants et adultes peuvent se protéger contre les menaces en ligne, **rendez-vous ici.**

Ressources utiles

- Le **rapport spam and phishing 2022** de Kaspersky
- Le portail **« Share Aware »** pour comprendre son profil d'utilisateur sur les réseaux sociaux et adopter les bonnes pratiques
- Le **Privacy Checker** de Kaspersky, pour aider à régler les paramètres de confidentialité des réseaux sociaux utilisés et vérifier la robustesse du mot de passe.
- Les solutions **Kaspersky Safe Kids** et **Kaspersky Premium**, pour accompagner techniquement les bonnes pratiques en ligne.
- Le **Cyber Guide Familles**, édité par Cybermalveillance.gouv.fr
- **Conseils de Kaspersky** pour lutter contre le phishing
- Parmi les différentes formes d'arnaques et de risques en ligne, liées notamment à la publication en excès, il existe le doxing. Kaspersky a créé toute une plateforme avec des ressources et des conseils **lutter contre le doxing.**

Kaspersky France
1bis Place de la Défense
92400 Courbevoie
www.kaspersky.fr

kaspersky