Formation: lutter contre le cyber-harcèlement

kaspersky

emc
فضاء مغرب الثقة السيبرانية
Espace Maroc Cyberconfiance
Morocco Cyberconfidence Space

Lutter contre les violences en ligne : un travail complexe

kaspersky

Différents types de harcèlement en ligne – des victimes majoritaires : les enfants et les femmes

- **Le doxing :** « Doxing » est l'abréviation de « dropping dox », dox étant une variante du mot « docs » pour documents, et signifie « fournir des preuves » ou encore « lâcher des infos ». D'une manière générale, le doxing est un acte malveillant utilisé contre des personnes avec lesquelles le cybercriminel est en désaccord ou en mauvais termes. Le doxing (aussi écrit doxxing) est l'acte de révéler des informations qui permettent d'identifier quelqu'un en ligne, comme le véritable nom, l'adresse, le lieu de travail, le numéro de téléphone, des informations financières ou personnelles. Ces informations sont ensuite transmises au public sans l'autorisation de la victime

Lutter contre le doxing

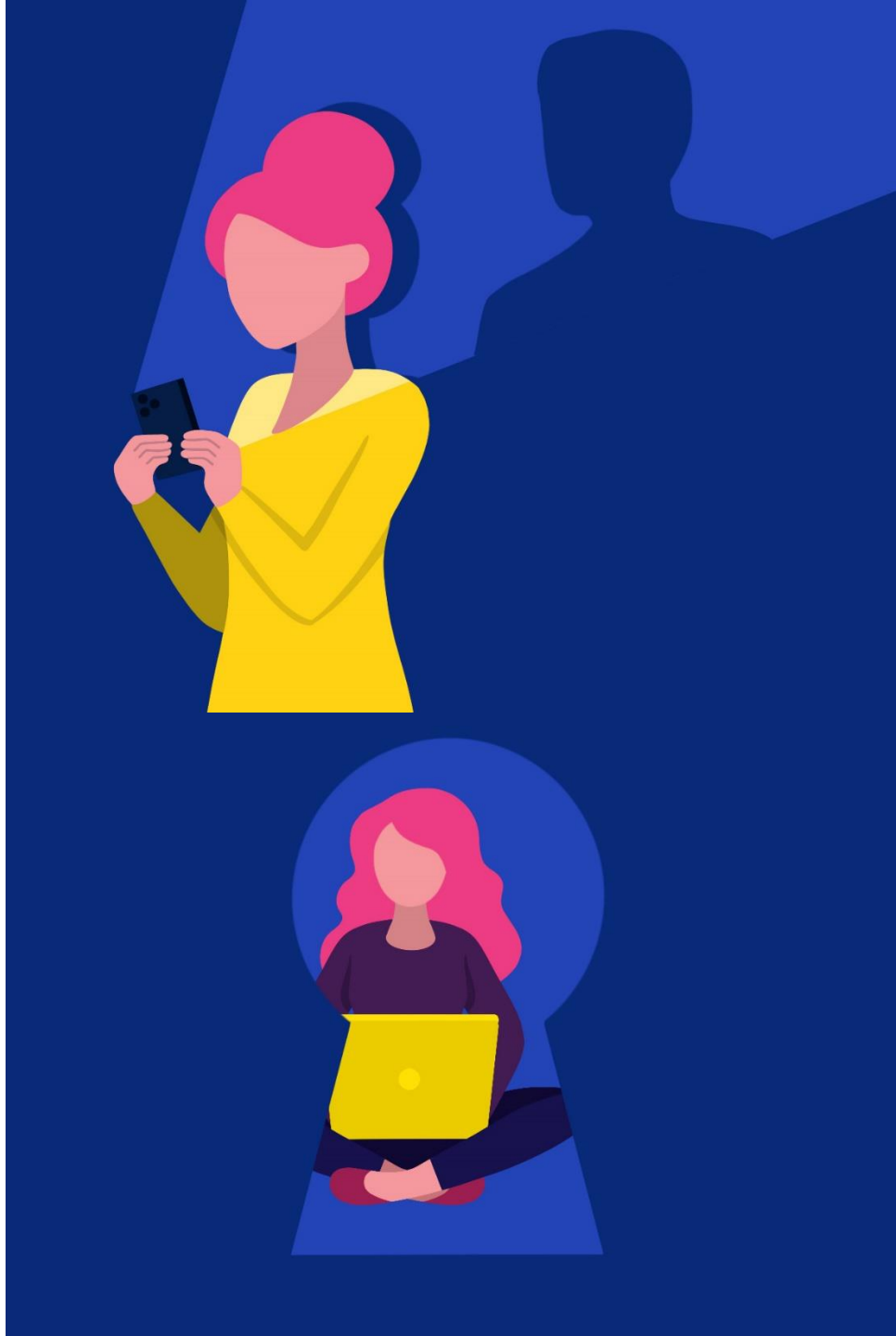
Plateforme anti-doxing checklist.

Pour les infos que vous pouvez contrôler :

- Soyez conscient de ce que vous partager, tout peut être utilisé et sorti de son contexte
- C'est le cas aussi pour tout ce qui peut constituer « votre profil » en ligne : êtes vous sûr d'assumer ce post sur les réseaux sociaux ou vous donnez votre avis sur la politique ?
- Ayez le contrôle des sites sur lesquels vous publiez des informations pour être à même de changer vos mots de passe en cas d'information sur des leaks.
- Attention aux géotags (infos sur la localisation). Qui peut tirer profit d'une information sur votre position ? Des criminels intéressés par vos habitudes, celles de vos enfants.
- Attention aux données d'identification sur les photos partagées : peut-on voir une pièce ID officielle ? Un document confidentiel ?
- Utiliser des messageries chiffrées
- Utiliser des sites de shopping officiels pour éviter l'exfiltration de données.

Différents types de harcèlement en ligne – des victimes majoritaires : les enfants et les femmes

- **Le stalking :** le stalking consiste à espionner une personne sans son consentement. Dans le cadre des activités en ligne, le stalkerware (outil d'espionnage) est un appareil invisible, installé sur le téléphone d'une victime, souvent par une personne proche et qui traque toutes ses activités, ses messages, sa localisation à son insu. Ces outils sont souvent utilisés dans le cadre de violences conjugales. Si ces outils sont pernicieux et faits pour être invisibles sur un téléphone il existe heureusement des manières de les détecter, ou de les soupçonner.




NUISIBLE NUMÉRIQUE
Pourquoi devrais-je lui faire confiance si je peux l'espionner... et la piéger ?
COMMENT SAVOIR SI TON PARTENAIRE T'ESPIONNE
MODERNA DE PUEBLO & kaspersky


Chérie, tu me prêtes ton téléphone une minute ?
Le mien n'a plus de batterie et j'ai besoin d'envoyer un message urgent...
Oui bien sûr, le mot de passe c'est...
LE "STALKERWARE"
cela consiste à espionner une personne à travers un dispositif mobile qui scannera ses conversations, accèdera à ses photos, vidéos et réseaux sociaux, permettra sa géolocalisation en temps-réel...


Ce type de pratique est particulièrement courant au sein du couple, car il n'est pas très difficile d'accéder au téléphone de l'autre à tout moment.
Je ne lui fais pas confiance, toute la journée à chater sur WhatsApp...
Et hier... elle est restée si longtemps chez sa mère ? Je n'y crois pas une minute...
Application Parasite
Téléchargement
Installation
Les plus utilisées sont vendues légalement en se faisant passer pour des applications de sécurité, de contrôle parental ou d'antivol.


Malheureusement, c'est assez facile d'installer en secret un outil stalkerware dans le téléphone d'une victime.
Et voilà, merci mon amour...
Ces applications d'espionnage restent cachées (ne montrent aucune icône ou notification) des yeux de la victime.


Mais même si vous ne remarquez rien d'inhabituel sur votre téléphone, il est possible de le remarquer dans le comportement de votre partenaire...
Hey, il faut qu'on s'organise pour le mariage de ton cousin
Oh, oui... il m'a envoyé un message hier avec l'invitation
C'EST BIZARRE, J'AURAIS JURÉ NE PAS LUI AVOIR ENCORE DIT...

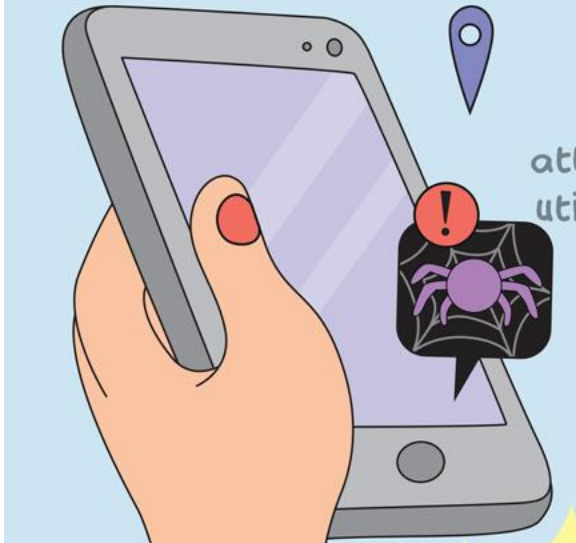

Selon les experts des ONG qui viennent en aide aux victimes de violences conjugales, le stalkerware est également une forme de violence.
Pourquoi n'es-tu pas rentrée directement après le travail ?
OU ÉTAIS TU ?
Oh, c'est juste que j'ai croisé Marta sur le chemin et nous avons été boire un verre pour papoter.
Un agresseur peut utiliser la surveillance pour prendre le contrôle total de sa victime.

SI VOUS SOUPÇONNEZ D'ETRE ESPIONNE :

Surveillez votre batterie et vos données :
ces applications consomment des ressources parce qu'elles envoient des transmissions en permanence

Vérifiez quelles applications ont accès à quoi :
attention si certaines applications inconnues utilisent des autorisations spéciales ou de la géolocalisation

Installez un antivirus
qui vous identifie et vous prévient en cas de stalkerware.

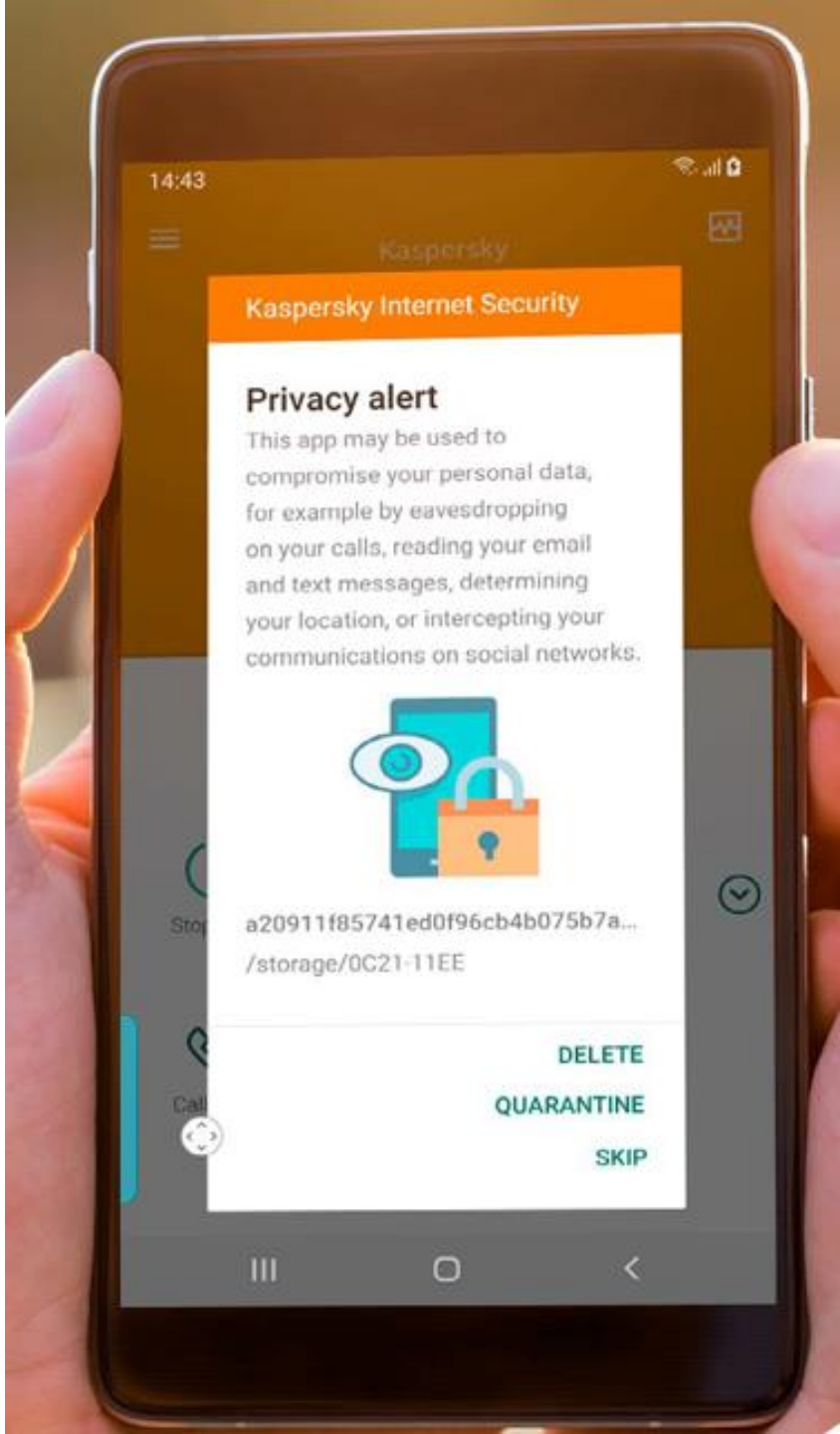


Ne les laissez pas vous contrôler, demandez de l'aide pour faire sortir les cyber intimidations de votre vie.

MODERNA DE PUEBLO & kaspersky

Lutter contre les stalkerwares / comment s’en prémunir ?

- La Coalition contre les stalkerwares
- Outils type TinyCheck à disposition des associations de lutte
- Ne pas partager son mot de passe à son conjoint
- Vérifier la batterie et son épuisement
- Vérifier les paramètres : est-ce que des applications ne tournent pas en arrière plan
- Utiliser une solution de sécurité : même gratuite, elle permet de détecter les logiciels indésirables type stalkerware

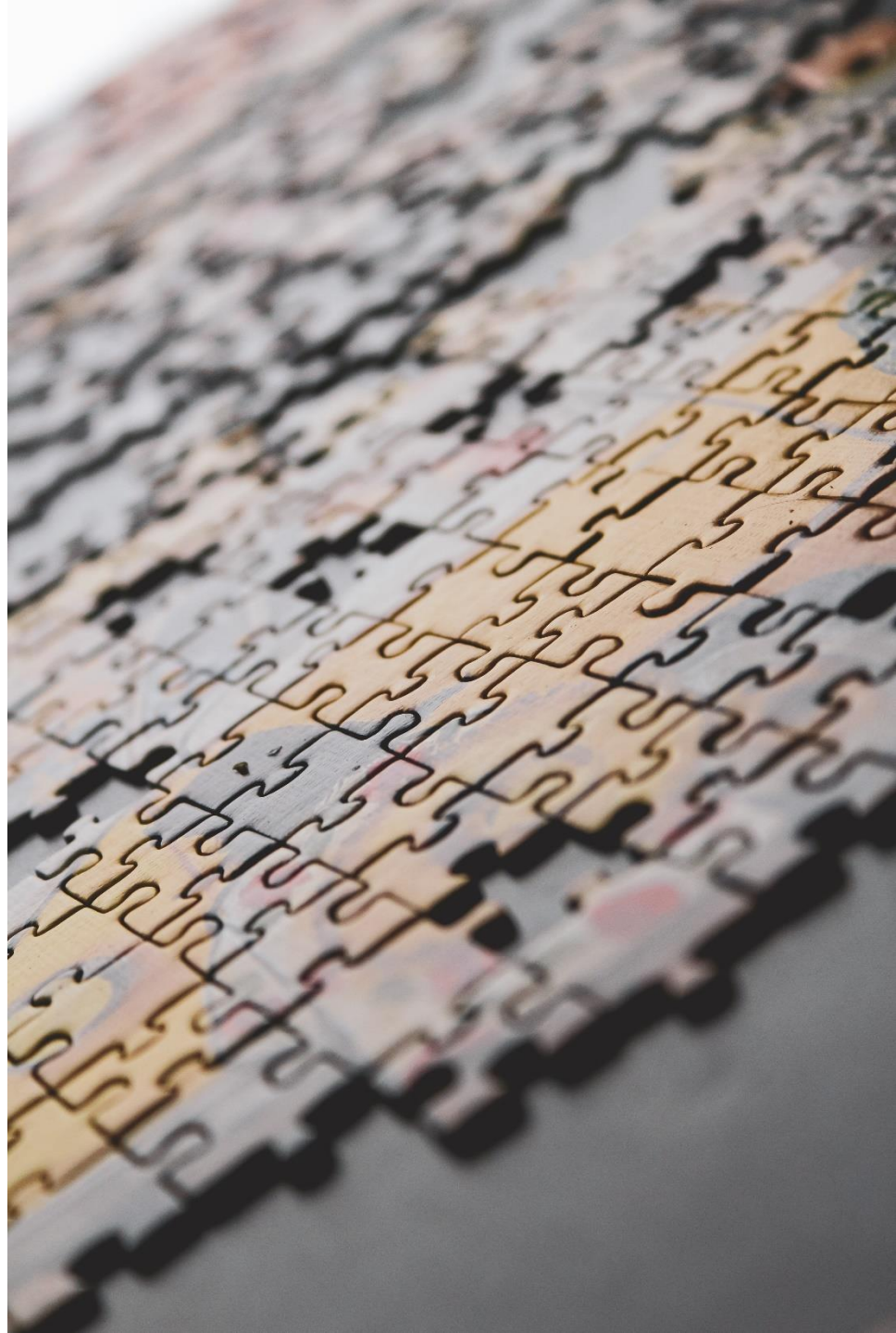


Différents types de harcèlement en ligne – des victimes majoritaires : les enfants et les femmes

- **Le revenge porn, ou la sextorsion :** La sextorsion, ou le chantage sexuel, consiste à faire chanter une victime en révélant ses informations intimes, si elle ne paye pas son extorqueur. Dans ce monde connecté, qui est l'ère numérique, nos informations peuvent être dévoilées en envoyant des sextos, des photos intimes et même des vidéos. Les escrocs demandent habituellement de l'argent, mais parfois font du chantage sur des choses plus compromettantes lorsque vous refusez de les payer plus. La majorité des victimes sont des adolescentes.

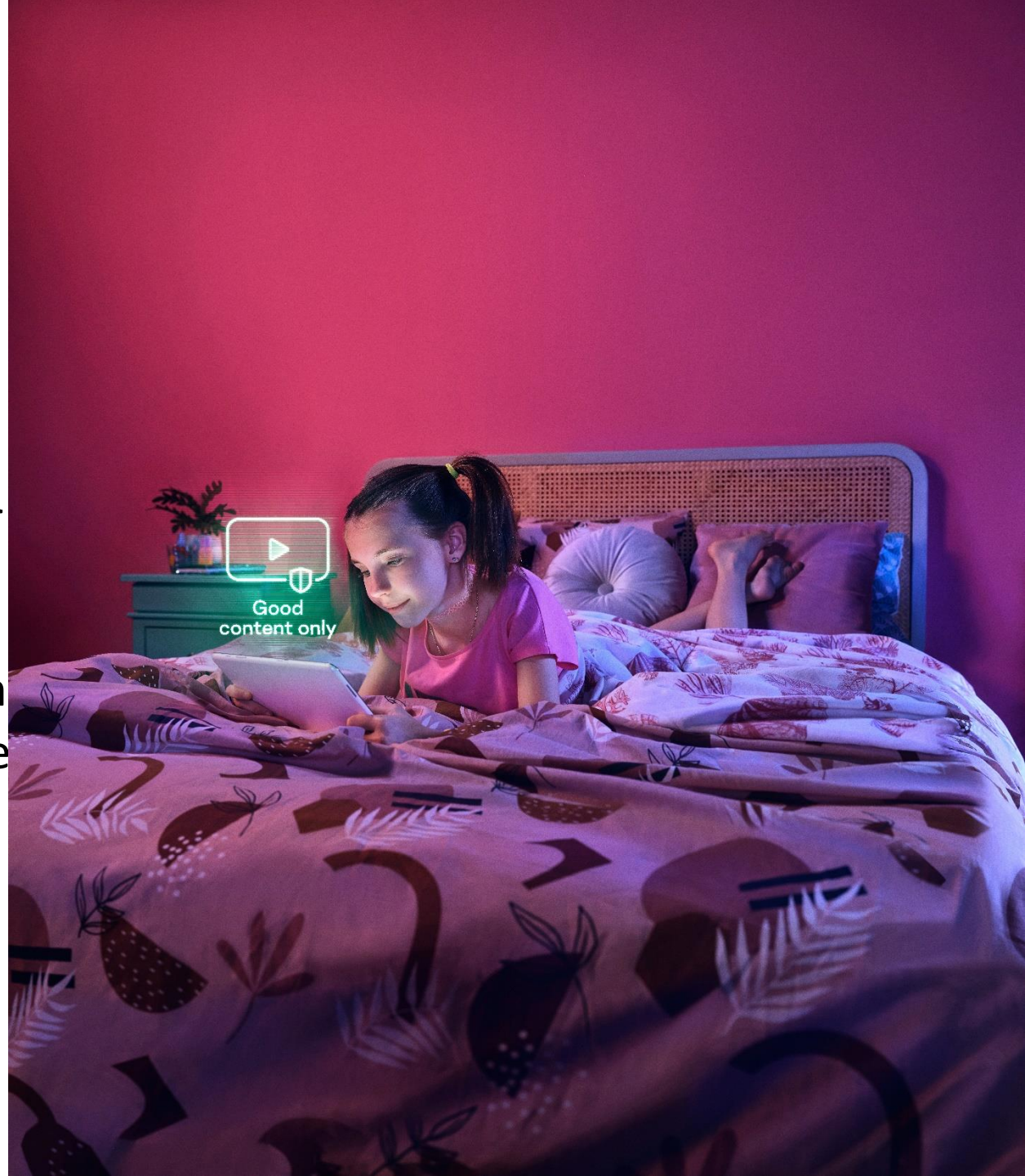
Lutter contre le revenge porn et le chantage en ligne : prendre le contrôle de ses données

- Share Aware > comprendre que tout ce qui est posté peut être utilisé
- Privacy Checker
- Paramètres de confidentialité
- Mots de passe uniques > utilisation de gestionnaires de mots de passe.
- Antivirus qui protègent les webcams, micros etc.



Accompagner ses enfants pour ne pas qu'ils deviennent des agresseurs ou des victimes de harcèlement

- La communication sur les risques encourus & sur les données à ne pas partager en ligne
- S'intéresser à leurs centres d'intérêt en ligne
- Les accompagner vers de meilleurs usages en ligne plutôt que les priver > outils de contrôle parentaux



Quels conseils de Kaspersky ?

- Etablir des règles à la maison et s'y tenir ! Une récente étude européenne montre que 68% des parents ne parviennent pas à suivre les règles qu'ils imposent à leurs enfants à la maison.
- Utiliser des logiciels de contrôle parental comme par exemple Kaspersky Safe Kids si possible sur l'ensemble des appareils numériques auxquels l'enfant a accès
- Ouvrir le dialogue et communiquer avec son enfant en s'intéressant à ses activités en ligne, à ses centres d'intérêts, aux influenceurs qu'il suit par exemple.
- Ne pas hésiter à utiliser des outils ludiques pour échanger autour des dangers d'Internet en réalisant des quiz en ligne par exemple, comme le propose Kaspersky sur son site Internet dédié aux bons gestes numériques.
- Sensibiliser sur le fait que les actions en ligne ont des répercussions dans la vie réelle. Une insulte, une menace en ligne peut avoir des conséquences dévastatrices pour celui qui en est la cible, et entraîner une condamnation pour son auteur dans la « vie réelle ».
- Kaspersky a mis à disposition des outils en ligne à destination des éducateurs pour les aider à former les enfants à la cybersécurité.
- Suivre les recommandations du CSA et des réseaux en termes d'âges requis pour accéder à un contenu.

Quelques outils de sensibilisation mis à disposition par Kaspersky

- Livre Midori Kuma
- Plateforme « tools for educators » avec des vidéos, des contenus pédagogiques et ludiques pour intégrer l'éducation numérique au parcours éducatif de l'enfant
- La plateforme « share aware » avec des conseils d'utilisation de chaque plateforme de réseau social et notamment en rappelant les fonctionnalités proposées par chacune des plateformes pour sécuriser ses comptes et ses données.
- Une formation en collaboration avec Skill Cup pour apprendre les bonnes pratiques du numérique de manière ludique. Une formation à la fois pour les enfants, les parents et quiconque souhaite obtenir les bases de la sécurité informatique.
- Un quizz avec Midori qui permet d'obtenir un « certificat numérique »

Construire un monde plus sûr

Kaspersky s’est donné pour mission d’accompagner l’avenir, et de le sécuriser. Tant dans les outils que dans les usages.

Des outils à disposition des familles, des éducateurs et des jeunes : un contrôle parental, des outils de sensibilisation adaptés au public (livre Midori etc.)

Une compréhension de la réalité des besoins, des usages, en matière de numérique > études terrain

Des partenariats public/privé et du travail avec d’autres acteurs sans qui, la construction du monde plus sûr serait impossible

Nous protégeons les utilisateurs contre les menaces numériques depuis

25 ans

L'excellence technologique
Fournisseurs de cybersécurité primés depuis 1997

Innovation permanente
De nouvelles solutions et fonctionnalités sont créées pour répondre à l'évolution des besoins des utilisateurs

Une confiance accrue
400M de clients et 250K partenaires nous font confiance dans le monde entier

Une interface utilisateur de premier ordre
nous simplifions les choses complexes en nous appuyant sur des années de savoir-faire