

Risques sur Internet

PRÉVÉNIR, IDENTIFIER ET RÉSISTER



GUIDE

BEESECURE



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'éducation nationale,
de l'enfance et de la jeunesse
Service national de la jeunesse

TABLE DES MATIÈRES

INTRODUCTION	3
1. Piratage	4
2. Configurations et bien-être	6
3. Attaque d'hameçonnage (« phishing »)	8
4. Supports de stockage	10
5. Diffusion d'informations	12
6. Escroquerie	16
7. Désinformation	18
8. Contenus illégaux	20
9. Sexting	22
10. Cyberharcèlement	24
MOTS CROISÉS : QU'AVEZ VOUS RETENU ?	26
POINTS DE CONTACT	27
SOLUTIONS	30
INFORMATIONS ET MATÉRIELS SUPPLÉMENTAIRES	32
BIBLIOGRAPHIE	33

INTRODUCTION

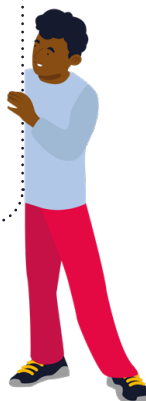
Sur Internet, vous pouvez rencontrer des personnes bienveillantes, des personnes qui n'ont pas vraiment d'impact sur votre vie, tout comme des opportunités. Malheureusement, vous pouvez aussi rencontrer des difficultés, des personnes ayant de mauvaises intentions et, parfois même, recevoir des menaces pouvant avoir un impact sur votre vie quotidienne.

Au cours de cette publication, vous rencontrerez différents personnages dans des situations spécifiques confrontés à des risques sur Internet. Nous comptons sur vous pour les guider vers une utilisation sûre et responsable des technologies de l'information et de la communication ! Après chaque « *sauvetage* », vous trouverez des conseils comment gérer le risque en question. Vous pourrez alors les implémenter dans vos propres habitudes d'utilisation afin de renforcer votre sécurité et votre bien-être et éventuellement aussi ceux de vos proches.

COMMENT UTILISER CE GUIDE ??



Munissez-vous d'un crayon et utilisez le rabat pour cocher les réponses aux solutions proposées !



 LYNN

28 ans



1. PIRATAGE

CONTEXTE



Lynn a l'habitude d'utiliser quasiment les mêmes mots de passe partout.

Jamais elle ne pourrait les retenir autrement !

(exemple : 12345Gmail, 12345Garage, 12345TV, 12345Ordi, 12345Amazon, etc.)

Un soir, en rentrant à la maison, elle constate qu'elle s'est fait cambrioler ! Bizarrement, son système d'alarme n'a pas été déclenché et il n'y a aucun signe d'entrée par effraction.

Lors de l'enquête, on constate que les cambrioleurs ont piraté ses comptes, ce qui leur a permis de désactiver l'alarme et d'ouvrir la porte de garage en toute simplicité.

.....

Aidez Lynn à réagir adéquatement en choisissant parmi les actions ci-dessous :

- 1 changer tous ses mots de passe (un mot de passe sûr et différent pour chaque service)
- 2 changer uniquement le mot de passe de son adresse e-mail
- 3 activer l'authentification à double facteur
- 4 bloquer les accès aux cartes de crédit
- 5 se renseigner sur les informations qui la concernent qui circulent en ligne et exiger la suppression des contenus privés





CONSEILS

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE.

Cela vous permettra de :

- ▶ garder tous les mots de passe à un endroit.
- ▶ générer des mots de passe solides que vous ne serez pas obligé de retenir.
- ▶ choisir parmi deux possibilités pour stocker vos données :
 - **un gestionnaire en ligne¹** : les données sont stockées sur un serveur interne ou un cloud⁴
 - **un gestionnaire hors ligne⁵** : les données sont enregistrées sur l'ordinateur de l'utilisateur

Veillez à choisir un mot de passe sûr et unique pour votre gestionnaire et ne le partagez pas. Activez la double authentification !

CRÉEZ UN MOT DE PASSE SÛR EN 2 ÉTAPES :

- ▶ choisissez une phrase facilement mémorisable et sans informations personnelles
- ▶ utilisez au moins 12 caractères

(exemple : 2dinosaurshabitentsurmars)



Testez la fiabilité de votre mot de passe :

<https://pwdtest.bee-secure.lu>

Vérifiez si un de vos comptes a été piraté :

<https://haveibeenpwned.com>

¹ Méthode d'authentification qui force un utilisateur à présenter deux preuves d'identité distinctes (p.ex. mot de passe plus « token » ou empreinte). | ² Pour le Grand-Duché de Luxembourg : appelez immédiatement (+352) 49 10 10 pour bloquer vos cartes de crédit 24h/24, 7 jours/7 et informez votre banque. | ³ P.ex. : LastPass, Sticky Password | ⁴ Plus d'informations sur le système cloud p.11 | ⁵ P.ex : KeePassX.

 LARA

14 ans

2. CONFIGURATION ET BIEN-ÊTRE

CONTEXTE

Lara veut éviter au maximum les effets négatifs liés au temps d'écran sur son bien-être. Pour ce faire, elle a décidé de :

- ▶ éviter les écrans pendant les repas
- ▶ désactiver les notifications sur son smartphone
- ▶ désactiver le wifi de 21:30 à 07:00
- ▶ désactiver la fonction « *lecture automatique* » sur les plateformes de vidéo⁶

Essayer de réguler le temps d'écran est une bonne base, mais il faut également tenir compte de la :

C É
 T Q U !





CONSEILS

IL EST ÉGALEMENT ESSENTIEL DE SÉCURISER LES APPAREILS À L'AIDE D'UNE CONFIGURATION ADÉQUATE :

- ▶ avoir des comptes utilisateurs verrouillés⁷ pour tous les services et les appareils
- ▶ bloquer les publicités pop-up et désactiver les achats intégrés (« in-app »)
- ▶ activer les mises à jour automatiques
- ▶ activer le verrouillage automatique en cas d'inactivité
- ▶ désactiver les permissions inutiles afin de limiter le partage de données

(informations personnelles, données de géolocalisation, enregistrements audio/vidéo, reconnaissance vocale)

- ▶ se protéger au mieux contre les virus et les menaces :
 - installez un antivirus sur vos ordinateurs, PC portables et macs
 - assurez-vous que l'antivirus reçoive des mises à jour régulières
 - faites régulièrement des scans manuels pour l'entièreté de votre disque dur

PROTÉGEZ VOS DONNÉES TRANSMISES SUR LE RÉSEAU WI-FI

Pour cela, utilisez :

- ▶ un mot de passe sûr pour la connexion au réseau
- ▶ le WPA3 comme mode de chiffrement pour votre routeur (protocole le plus récent et le plus sécurisé actuellement disponible)

Si votre appareil ne supporte pas le WPA3, utilisez le WPA2.

⁶ YouTube, Disney+, Netflix, etc. | ⁷ Comptes protégés par des mots de passe, codes, reconnaissances faciales et/ou empreintes digitales

 **DENNIS**

25 ans



3. ATTAQUE D'HAMEÇONNAGE (« PHISHING »)

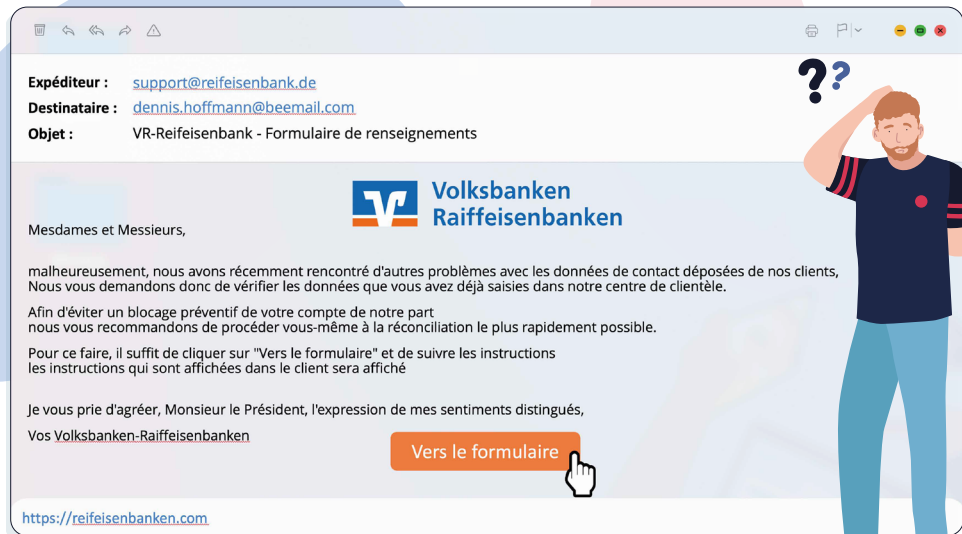


CONTEXTE

Denis est ciblé par une attaque d'hameçonnage.

Aidez Dennis à identifier les risques :

- 1 le lien redirige sur un site web falsifié qui par la suite invite à saisir des informations personnelles*
- 2 le lien redirige sur un site web authentique et invite à saisir des informations personnelles





CONSEILS

AVANT DE RÉAGIR À UN E-MAIL QUE VOUS NE RECONNAISSEZ PAS IMMÉDIATEMENT, SOYEZ CRITIQUE :

- ❶ Disposez-vous d'un compte auprès de ce service ?
- ❷ L'expéditeur...
 - Est-ce que vous le connaissez ?
 - L'adresse électronique correspond-elle à celle de l'expéditeur ?
 - S'agit-il de l'adresse électronique officielle ?
- ❸ Le lien vous conduit-il au site officiel du service ?

Si vous répondez négativement à une ou plusieurs de ces questions, soyez prudents :

- ▶ contactez uniquement le **service officiel de l'éventuel prestataire** en question afin de vous renseigner (pour Dennis, il s'agirait de l'**helpdesk** de sa banque)
- ▶ signalez l'e-mail auprès du **CIRCL**⁹ (**C**omputer **I**ncident **R**esponse **C**enter **L**uxembourg) ou via **SPAMBEE**¹⁰, un plug-in gratuit pour votre navigateur Web
- ▶ n'ouvrez pas la pièce jointe, elle pourrait contenir **un logiciel malveillant**



Les logiciels malveillants, visant à espionner en toute discrétion les données personnelles, ne sont pas annoncés par e-mail et les correctifs de sécurité ne sont JAMAIS distribués par e-mail !

Si vous êtes victime d'hameçonnage, réagissez au plus vite à cette violation de données !¹¹

⁹ Mots de passe, numéros de compte, cartes de crédit, etc. | ⁹ www.circl.lu/report/#report-an-incident |

¹⁰ www.spambee.lu | ¹¹ Cf. question sous « piratage » p. 4.

 **JULIE**

23 ans



CONTEXTE

Julie est en pleine rédaction de son mémoire de fin d'études. Pour l'instant, ses fichiers sont enregistrés localement sur son PC mais, comme tout support de stockage, celui-ci n'est pas sûr à 100 % !

Aidez Julie à diversifier son système de sauvegarde :

- 1 clé USB
- 2 impression papier
- 3 cloud
- 4 disque dur externe





CONSEILS

Le cloud permet d'accéder à vos documents, photos, vidéos ou tous types de fichiers où que vous soyez, sur n'importe quel appareil ou terminal. Cela vous facilite la vie, mais veillez à protéger vos données :

- ▶ utilisez un mot de passe sûr et si possible la double authentification
- ▶ protégez tous les appareils qui y sont connectés¹²
- ▶ chiffrez¹³ les documents ou données sensibles stockées sur le cloud (p.ex : Vera-Crypt¹⁴, Cryptomator¹⁵)

Soyez attentifs aux conditions d'utilisation et aux garanties offertes par les différents services :

- ▶ Qui a accès à vos données ?
- ▶ Quelle utilisation le prestataire de cloud peut-il en faire ?
- ▶ Quelles sont les garanties offertes quant à la protection des données ?
- ▶ Qu'en est-il en cas d'interruption ou de cessation du service ?
- ▶ La destruction de vos données est-elle garantie lorsque vous les effacez ?

EN RÈGLE GÉNÉRALE :

- ▶ lors d'une connexion à un compte via l'appareil d'un tiers, utilisez le mode « navigation privée¹⁶ » (données personnelles / mots de passe ne sont pas stockés)
- ▶ évitez les clés USB inconnues qui peuvent contenir des logiciels malveillants
- ▶ quant aux œuvres (littérature, art, musique, films, jeux vidéo, etc.), vérifiez si elles sont protégées par le droit d'auteur
 - téléchargez vos contenus vidéo ou audio uniquement depuis des sites légaux
 - citez toutes les sources que vous avez utilisées pour la rédaction d'un travail



**Les lois s'appliquent aussi sur Internet.
L'ignorance ne protège pas de la sanction !**

¹² Cf p.5 sous « Configurations et bien-être » | ¹³ Les données sont codées sous une forme qui les rend impossible à lire sans la clé adéquate. | ¹⁴ www.veracrypt.fr/en/Home.html | ¹⁵ <https://github.com/cryptomator/cryptomator> | ¹⁶ CTRL-MAJ-P pour Firefox ou Internet Explorer, CTRL-MAJ-N pour Chrome

 **LISA**

25 ans



5. DIFFUSION D'INFORMATIONS



CONTEXTE

Lisa est en safari en Afrique du Sud avec un ami et partage un selfie avec un rhinocéros sur les réseaux sociaux.

Quelles informations pourraient être lues par un tiers avec cette photo :

- | | |
|---------------------------------|------------------------------|
| 1 le lieu | 8 l'orientation de la caméra |
| 2 les coordonnées géographiques | 9 la focale |
| 3 l'heure | 10 l'exposition |
| 4 le type de vacances | 11 l'ouverture |
| 5 les noms | 12 le flash |
| 6 les prénoms | 13 la valeur ISO |
| 7 le modèle de la caméra | |

Partager toutes ces données n'est pas sans risques. Quels sont les dangers potentiels ?

- 1 Surveillance
- 2 Mise en danger du rhinocéros
- 3 Perte de l'autodétermination informationnelle
- 4 Vente des données





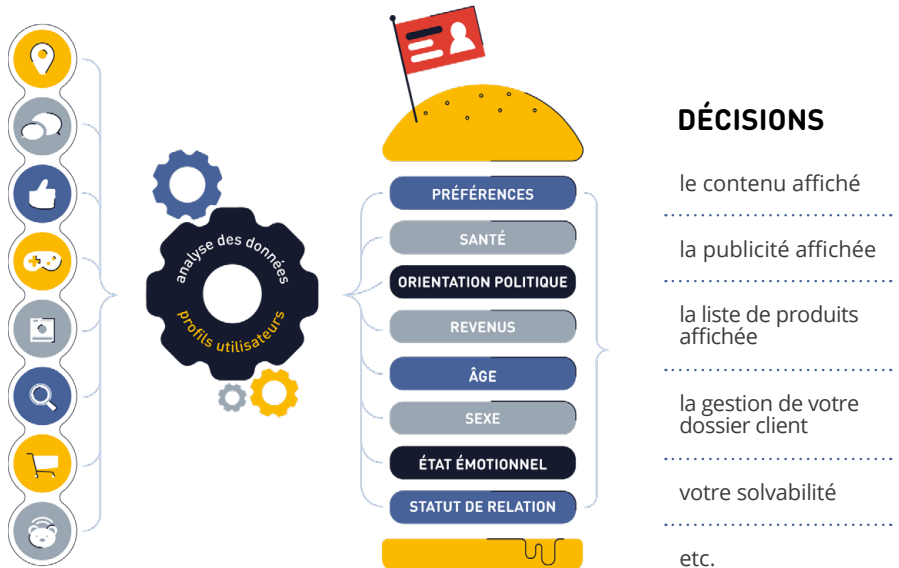
CONSEILS 1/2

LIMITEZ LE PARTAGE DE VOS DONNÉES.

Chaque activité sur Internet (clic, j'aime, publication, discussion, recherche, achat, inscription, etc.) est une trace numérique sous forme de données.

Sans limitation de partage, ces informations permettent :

- ▶ aux personnes avec de mauvaises intentions de suivre vos activités ainsi que votre localisation
- ▶ aux entreprises de créer des profils virtuels et de traiter eux-mêmes ces données ou encore de les vendre à des tierces personnes





CONSEILS 2/2

COMMENT LIMITER LE PARTAGE DE DONNÉES ?

- Soyez attentifs aux conditions d'utilisation et aux garanties offertes par les différents services¹⁷.
- Désactivez les permissions inutiles¹⁸.
- L'art d'en dire moins sur soi : tout le monde ne doit pas tout savoir.
- Utilisez une adresse électronique principale pour les relations de confiance et une adresse électronique secondaire (ou un alias) pour les contacts publics.
- Adaptez les paramètres de confidentialité et vérifiez-les en fonction de l'évolution du service.
- Supprimez les comptes qui ne sont plus utilisés.
- Refusez les cookies non-essentiels.
- Utilisez des outils plus économes en données (p.ex : Privacy Badger, Startpage).
- Supprimez les métadonnées d'une photo/vidéo avant de la publier¹⁹.

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES DE L'UNION EUROPÉENNE (RGPD) :

- ▶ protège les données personnelles des utilisateurs sur Internet (toute information qui permet d'identifier une personne ou de la rendre identifiable)
- ▶ prévoit une série d'obligations et de droits pour les professionnels et les utilisateurs afin d'assurer la transparence quant à la conservation, le transfert et la manière dont les données sont utilisées²⁰

Si vos droits ne sont pas respectés :

- contactez le responsable de traitement (« DPO »)
- si votre démarche reste sans suites :
 - ◇ introduisez une réclamation auprès de la CNPD²¹
 - ◇ consultez un avocat et ouvrez une action en justice²²

¹⁷ Cf. p.11 questions à poser avant de s'inscrire à un service | ¹⁸ Informations personnelles, géolocalisation, enregistrements audio/ vidéo, reconnaissance vocale | ¹⁹ www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to | ²⁰ Pour plus d'informations, consultez www.bee-secure.lu/rgpd | ²¹ <https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html> | ²² Assurez-vous au préalable d'avoir pris toutes les autres mesures. Un procès peut être couteux et fastidieux.



 **SASHA**

16 ans

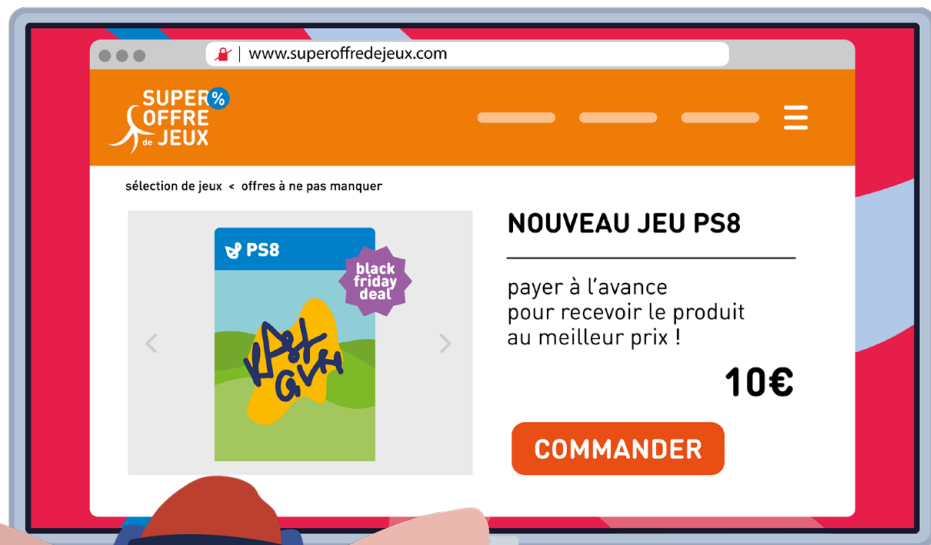


6. ESCROQUERIE

CONTEXTE

Sasha veut s'acheter un jeu vidéo pour sa nouvelle console. Il a attendu le Black Friday en espérant tomber sur une bonne offre.

Aidez Sasha à comprendre qu'il s'agit d'une arnaque ! Quels sont les indicateurs visibles sur le site ?





CONSEILS

VÉRIFIEZ LA FIABILITÉ DU SITE.

- ▶ Le prix de vente est-il réaliste ?
- ▶ Le site Internet comprend-il des mentions légales ?
- ▶ Les conditions de vente sont-elles transparentes ?
- ▶ Les données transmises sont-elles chiffrées (présence de HTTPS) lors de l'achat ?
- ▶ Comment les autres acheteurs évaluent-ils le vendeur ?
- ▶ Le site propose-t-il des modes de paiement sécurisés (facture, à la livraison, système de paiement électronique) ?
- ▶ Est-il possible de contacter le vendeur ?

POUR TOUTE TRANSACTION EN LIGNE, UTILISEZ :

- ▶ une authentification à double facteur²³
- ▶ un mot de passe sécurisé
- ▶ un accès Wi-Fi privé (pas de réseau public)
- ▶ une connexion sécurisée HTTPS

HTTPS, un protocole de transfert sécurisé : grâce à lui, l'échange de données est chiffré entre l'utilisateur d'un site Web et le serveur qui héberge le site. Cela permet d'éviter que vos données ne soient interceptées ou lues par des tiers²⁴.

Installez le plugin HTTPS everywhere dans votre navigateur Web !

Méfiez-vous des connexions Wi-Fi sans mot de passe (public) : toute communication peut être visible pour les autres appareils connectés ce qui permet le vol des mots de passe, noms d'utilisateur et/ou d'autres données.

²³ Cf. page 4 | ²⁴ Un certificat SSL/TLS accompagnant https est primordial pour les sites sur lesquels vous entrez des données personnelles, telles que des données bancaires ou des cartes de crédit. Pour vérifier, cliquez sur le « cadenas » dans la barre d'adresse.

7. DÉSINFORMATION

 **PIERRE**

13 ans



CONTEXTE



Après quelques recherches, Pierre découvre que la photo provient d'un site satirique²⁵ qui communique clairement à ses utilisateurs qu'aucune de leurs informations publiées n'est vraie. L'auteur de la publication sur le réseau social a sciemment propagé une information satirique sans le mentionner. Cela devient donc de **la désinformation**.

Aidez Pierre à comprendre les risques de la désinformation:

- 1 la désinformation peut avoir de réelles conséquences sociales et politiques
- 2 la désinformation rend tous les internautes de plus en plus bêtes



CONSEILS

ÉVITEZ DE CONTRIBUER À LA PROPAGATION DE LA DÉSINFORMATION, DE FAUSSES NOUVELLES OU DE CANULARS !

- ▶ Remettez en question l'information :
 - Qui se cache derrière ?
 - La source est-elle digne de confiance ?
 - Comment le sujet est-il présenté par d'autres entités ?
- ▶ Prévenez vos contacts s'ils propagent une désinformation.
- ▶ Signalez la désinformation sur la plateforme.
- ▶ Les e-mails et messages qui vous invitent à les diffuser à tous vos contacts (lettres en chaîne) sont presque toujours des canulars ou des arnaques.



En cas de doute, vérifiez les informations reçues via des sites comme p. ex. www.hoaxbuster.com ou www.mimikama.at.

²⁵ Source : Der Postillon. Erstes Baby mit Maske geboren, 2020. Capture d'écran: www.der-postillon.com/2020/09/baby-maske.html

 **PIT**

35 ans



8. CONTENUS ILLÉGAUX

CONTEXTE

Pit consulte son fil d'actualités sur un réseau social et participe à la publication de commentaires haineux, en lien avec des demandeurs d'asile et des réfugiés qui rejoignent la Grande-Bretagne en camion :

**Zozo_78**

Une bonne kalachnikov avec assez de munitions ferait des miracles. Une mauvaise kalachnikov serait encore mieux car elle arroserait plus!!! 🤪

 J'aime  Commenter  Partager

18:52

**Sonix-2002**

Le napalm ne coûte même pas la moitié! ;)

 J'aime  Commenter  Partager

19:05

**Lablagueatoto**

Faudrait injecter des gaz d'échappement dans la remorque. 🤖

 J'aime  Commenter  Partager

19:12

.....

Est-ce ce que ce genre de comportement en ligne est punissable par la loi ?

- 1 Oui
- 2 Non



CONSEILS

DERRIÈRE CHAQUE ÉCRAN SE CACHE UN ÊTRE VIVANT, RAISON POUR LAQUELLE IL EST IMPORTANT DE :

- ▶ rester poli et respectueux
- ▶ respecter les autres opinions et avis
- ▶ ne jamais écrire la rage au ventre
- ▶ ne jamais appeler à la violence

CONTRIBUEZ À LA LUTTE CONTRE LES CONTENUS ILLÉGAUX EN LES SIGNALANT AUPRÈS DES PLATEFORMES CONCERNÉES ET DE MANIÈRE ANONYME, SUR :



Cela concerne :

- ▶ les contenus racistes, révisionnistes et discriminants (y compris les discours de haine)
- ▶ les représentations d'abus sexuels sur mineurs
- ▶ les contenus terroristes



Afin de rendre encore plus agréable le vivre-ensemble sur Internet, la plupart des communautés et sites Web mettent à disposition un code de conduite. Veillez à respecter les bases de la « **netiquette** »²⁶ !

²⁶ www.bee-secure.lu/netiquette

8. PASCAL

16 ans

SAM 18 ANS



9. SEXTING

CONTEXTE



Pascal hésite à envoyer un selfie intime à Sam pour leur anniversaire de rencontre. Il commence à réfléchir au **pour** et au **contre** :

POUR

- il lui fait confiance, il ne pense pas qu'il partagerait la photo avec d'autres personnes
- au cas où il aurait enregistré la photo, il la supprimerait s'il le lui demandait
- c'est excitant d'envoyer une photo intime

CONTRE

- si Sam ne sécurise pas bien ses données²⁷, la photo pourrait être partagée à leur insu
- si un jour ils se quittaient en mauvais termes, Sam pourrait décider de partager la photo avec d'autres personnes ou sur un site Web

Pascal ne dispose pas encore de toutes les informations pour pouvoir prendre une décision éclairée. D'un point de vue légal, est-ce que Pascal peut partager une photo intime de lui-même ?

- 1 **Oui**, seul Sam commet une infraction en partageant la photo de Pascal sans son accord.
- 2 **Non**, Pascal a moins de 18 ans et commet donc une infraction en produisant, possédant et partageant une photo intime de lui.
- 3 **Oui**, Pascal a 16 ans et ne commet donc pas d'infraction en produisant, possédant et partageant une photo intime de lui.
- 4 **Oui**, Pascal peut faire ce qu'il veut avec sa photo.





CONSEILS

UN CONTENU INTIME²⁸ DE VOUS CIRCULE SUR INTERNET ?

Parfois, il suffit d'informer immédiatement et gentiment mais fermement la personne, qu'elle enfreint votre droit à l'image et qu'elle doit donc supprimer le contenu. Si elle refuse et/ou qu'elle exige d'autres contenus sous forme de chantage :

- ▶ ne réagissez plus à ses messages
- ▶ rassemblez des preuves
- ▶ déposez plainte, au plus vite, auprès de la police

Si vous êtes mineur et que vous avez partagé votre image intime, ne vous laissez pas décourager par le fait que vous avez commis une infraction ! Vous serez informés des faits et la police fera tout son possible pour vous aider.

- ▶ utilisez les fonctions « signaler » et « bloquer » du réseau social
- ▶ ne restez pas seul

Gratuits, anonymes et confidentiels, les services d'assistance téléphonique et en ligne constituent également un bon point de départ pour trouver l'aide adaptée :



Online Help (www.kjt.lu)

Consultation par écrit, en ligne, pour les enfants et les jeunes

Chatberodung (www.kjt.lu)

Consultation par discussion en direct, pour les enfants et les jeunes



Pour plus d'informations sur le cadre légal, le dépôt d'une plainte et comment agir lors de confrontations : www.bee-secure.lu/sexting-guide.

²⁷ Mots de passe faibles, pas de mises à jour régulières, pas de double authentification, etc. | ²⁸ Vidéo ou photo

10. CYBERHARCÈLEMENT

 ALEX

13 ans



CONTEXTE



 Que
dois-je
faire...?

Lors d'un tchat, Alex a reçu des insultes et des messages désagréables de la part de ses camarades de classe, suite à une photo embarrassante de lui, qui a été partagée sur les réseaux sociaux.

Dennis ne sait pas quoi faire. Que lui conseillerez-vous ?

- 1 « Demandes à la personne qui a partagé la photo de la supprimer. »
- 2 « Fais comme si de rien n'était, demain ils rigoleront de quelqu'un d'autre. »



CONSEILS

Activez la fonction permettant d'approuver manuellement les tags sur les publications, dans les paramètres sur les réseaux sociaux.

Demandez la permission des personnes représentées sur des photos avant de les publier. Les lois sur le droit à l'image, au Luxembourg comme dans d'autres pays, s'appliquent !

Le droit à l'image n'est pas éphémère, on a le droit à tout moment de la vie d'exiger la suppression d'un contenu !

ÊTES-VOUS VICTIME DE CYBERHARCÈLEMENT ?

- ▶ Ne répondez pas aux messages.
- ▶ Rassemblez des preuves (vous pouvez porter plainte !).
- ▶ Utilisez les fonctions « signaler » et « bloquer » du réseau social.
- ▶ Ne restez pas seul.

Gratuits, anonymes et confidentiels, les services d'assistance téléphonique et en ligne constituent également un bon point de départ pour trouver l'aide adaptée :



Online Help (www.kjt.lu)

Consultation par écrit, en ligne, pour les enfants et les jeunes

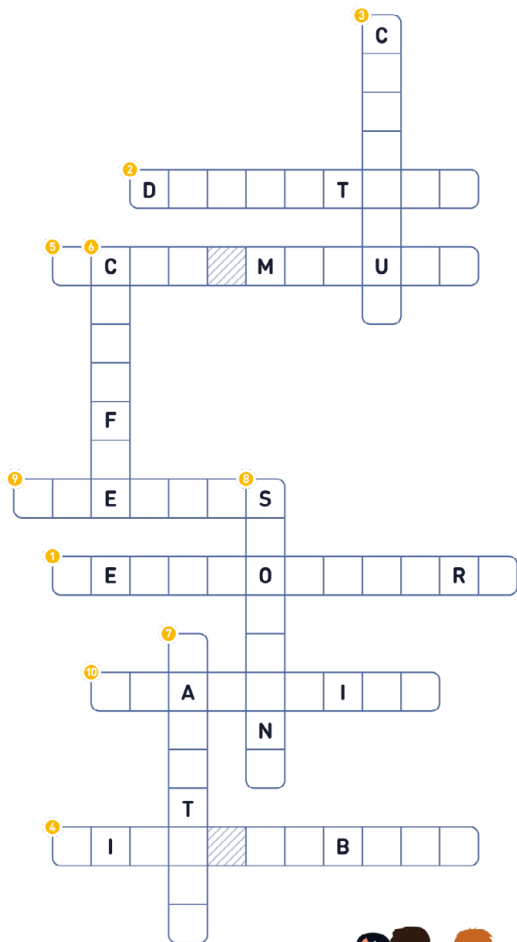
Chatberodung (www.kjt.lu)

Consultation par discussion en direct, pour les enfants et les jeunes



Pour plus d'informations sur le cadre légal, le dépôt d'une plainte et comment agir lors de confrontations : www.bee-secure.lu/cyberharcèlement-guide.

MOTS CROISÉS : QU'AVEZ VOUS RETENU ?



1 J'utilise un pour rassembler mes mots de passe à un même endroit de manière sûre.

2 Je toutes les permissions inutiles afin de protéger mes données.

3 Je garde un esprit face aux e-mails inconnus et aux informations en ligne.

4 J'évite les transactions en ligne sur un

5 Même si j'ai activé les mises à jour automatiques et que je dispose d'un antivirus, je fais régulièrement un de mon disque dur.

6 Je les documents ou données sensibles stockés sur le cloud.

7 L'ignorance ne protège pas de la

8 Je contribue à la lutte contre les contenus illégaux en les signalant sur la BEE SECURE

9 Si je suis victime de partage d'un contenu intime, je rassemble des afin de pouvoir porter plainte.

10 Je vérifie la du site avant d'y acheter un produit ou un service.

POINTS DE CONTACT

SOUTIEN ET CONSEILS

BEE SECURE Helpline

Ligne d'assistance téléphonique gratuite. Tout citoyen de tout âge peut y poser des questions sur l'utilisation sûre, responsable et positive des technologies de l'information et de la communication (TIC), comme dans le contexte du cyberharcèlement, des réseaux sociaux, des droits à la vie privée, de la sécurité technique et bien plus.

La BEE SECURE Helpline est le premier point de contact pour ces questions et offre une consultation anonyme et confidentielle.



KJT

Le KJT conseille et soutient les enfants et les jeunes, ainsi que les personnes qui s'occupent d'eux, dans leurs préoccupations et leurs questions quotidiennes, leurs craintes, leurs problèmes et aussi leurs crises.

« Personne ne doit rester seul. »

Chaque enfant, chaque adolescent peut s'adresser directement à des conseillers spécialement formés. Les parents et les personnes en relation avec les enfants, ainsi que les professionnels du domaine pédagogique et psychologique, ont également accès à ce service de conseil simple et direct.



- Kanner-Jugendtelefon **116 111**
- Online Help (www.kjt.lu)
- Chatberodung (www.kjt.lu)
- Ecoute parents **26 64 05 55**

Anonym Glécksspiller a.s.b.l.

Le service de conseil « *game over* » de Anonym Glécksspiller est l'interlocuteur pour les questions concernant l'utilisation saine des médias à écran numérique. Outre l'éducation et l'information des parents et des jeunes, le service comprend un diagnostic en cas de suspicion d'utilisation pathologique, des conseils éducatifs et familiaux spécifiques aux médias, ainsi que la possibilité d'un soutien psychothérapeutique.

<https://gameover.lu>

Union luxembourgeoise des consommateurs (ULC)

L'ULC est une association sans but lucratif qui a pour objet social la protection, la défense, l'information et l'éducation des consommateurs luxembourgeois. En tant qu'organisation représentative, elle représente également les consommateurs auprès des instances publiques et politiques.

www.ulc.lu

SIGNALEMENTS ET RÉCLAMATIONS

BEE SECURE Stopline

Contribuez à la lutte contre les contenus illégaux en ligne en les signalant de manière anonyme sur <https://stopline.bee-secure.lu>. Cela concerne les représentations d'abus sexuels sur mineurs, les contenus racistes, révisionnistes et discriminants (y compris les discours de haine) et les contenus terroristes.



Institut Luxembourgeois de Régulation (ILR)

L'ILR supervise le marché de l'électricité et donc les acteurs qui y sont actifs. On distingue notamment les producteurs, les fournisseurs et les gestionnaires de réseau.

Vous pouvez faire appel à l'ILR en cas de :

- difficultés à régler un problème avec un fournisseur ou avec un gestionnaire du réseau pour une procédure de médiation ou, dans certains cas, une procédure de règlement de litige

- pour toutes questions sur le marché de l'électricité (guichet unique)

<https://web.ilr.lu>

Centre Européen des Consommateurs Luxembourg (CEC Luxembourg)

Le CEC Luxembourg fait partie d'un réseau de 29 Centres Européens des Consommateurs dans l'Union européenne, ainsi qu'en Islande et en Norvège (European Consumer Centre Network – ECC-Net).

L'ECC-Net remplit avant tout les tâches suivantes :

- information du consommateur à propos du droit européen de la consommation et de la politique européenne dans le domaine de la consommation
- conseil pour le consommateur dans les litiges de consommation à caractère transfrontalier
- assistance du consommateur dans ses litiges transfrontaliers de consommation avec une entreprise située dans un autre pays de l'Union européenne, en Islande ou en Norvège

www.cecluxembourg.lu

Computer Incident Response Center Luxembourg (CIRCL)

Le CIRCL est une initiative gouvernementale conçue pour recueillir, examiner, signaler et répondre aux menaces et incidents de sécurité informatique.

Signalez les attaques d'hameçonnage (phishing) :

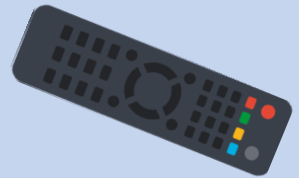
<https://circl.lu/report/#report-an-incident>

Commission nationale pour la protection des données (CNPD)

Etablissement public chargé de vérifier la légalité des fichiers et de toutes collectes, utilisations et transmissions de renseignements concernant des individus identifiables et d'assurer dans ce contexte le respect des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée.

Si vous désirez introduire une réclamation :

<https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html>



SOLUTIONS

1. PIRATAGE : 1, 3, 4, 5

2. CONFIGURATIONS ET BIEN-ÊTRE : sécurité technique

3. ATTAQUE D'HAMEÇONNAGE (« PHISHING ») : 1 (le nom n'est pas écrit correctement) ; de manière générale, il est également déconseillé d'ouvrir les pièces jointes des e-mails douteux.

4. SUPPORTS DE STOCKAGE : 1, 3, 4

5. DIFFUSION D'INFORMATIONS :

• **Quelles informations pourraient être lues par un tiers avec cette photo ?**

1 - 13 Les photos contiennent des métadonnées, c.-à-d. des informations sur la photo et l'appareil qui peuvent être lues à l'aide d'un programme de traitement d'images.

• **Partager toutes ces données n'est pas sans risques. Quels sont les dangers potentiels ?**

1 - 4 Les braconniers se servent des réseaux sociaux pour planifier leurs meurtres d'espèces en voie d'extinction. Les rhinocéros sont particulièrement menacés en raison de la valeur de leur corne.

6. ESCROQUERIE :

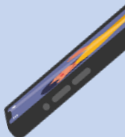
- le site ne dispose pas d'une connexion sécurisée HTTPS
- le prix de vente n'est pas réaliste
- il faut payer à l'avance pour recevoir l'offre

7. DÉSINFORMATION : 1 - www.bee-secure.lu/desinformation-politique

8. CONTENUS ILLÉGAUX : oui - <https://stopline.bee-secure.lu/fr/illegalcontent>²⁹

9. SEXTING : 2

10. CYBERHARCÈLEMENT : 1





MOTS CROISÉS : QU'AVEZ VOUS RETENU ?



- 1 J'utilise un **gestionnaire** pour rassembler mes mots de passe à un même endroit de manière sûre.
- 2 Je **désactive** toutes les permissions inutiles afin de protéger toutes mes données.
- 3 Je garde un esprit **critique** face aux e-mails inconnus et aux informations en ligne.
- 4 J'évite les transactions en ligne sur un **WIFI public**.
- 5 Même si j'ai activé les mises à jour automatiques et que je dispose d'un antivirus, je fais régulièrement un **scan manuel** de mon disque dur.
- 6 Je **chiffre** les documents ou données sensibles stockées sur le cloud.
- 7 L'ignorance ne protège pas de la **sanction**.
- 8 Je contribue à la lutte contre les contenus illégaux en les signalant sur la BEE SECURE **stopline**.
- 9 Si je suis victime de partage d'un contenu intime, je rassemble des **preuves** afin de pouvoir porter plainte.
- 10 Je vérifie la **fiabilité** du site avant d'acheter un produit ou un service.

²⁹ Contenus basés sur une histoire vraie: ces commentaires ont été publiés en 2015 ; les auteurs ont chacun été condamnés à payer une amende entre 1000 et 1500€ en 2017. www.rtl.lu/news/national/a/1036740.html

INFORMATIONS ET MATÉRIELS SUPPLÉMENTAIRES

PUBLICATIONS

BEE SECURE publie régulièrement des contenus sur des thèmes liés à une utilisation sûre et responsable d'Internet par les enfants et les adolescents dont, des guides, des fiches thématiques, du matériel pédagogique ainsi que des rapports. Ces publications sont disponibles sur www.bee-secure.lu/publications.

.....

FORMATIONS

BEE SECURE propose diverses formations de sensibilisation pour les enfants et les adolescents, des formations continues pour les enseignants et les éducateurs ainsi que des soirées pour les parents.

Plus d'informations sur www.bee-secure.lu.

BIBLIOGRAPHIE

BEE SECURE. BEE SECURE RADAR 2022

www.bee-secure.lu/fr/publication/bee-secure-radar (consulté le 10/03/2022)

_____ . CYBERHARCÈLEMENT

www.bee-secure.lu/fr/risques/cyberharcement (consulté le 11/11/2021)

_____ . DÉSINFORMATION

www.bee-secure.lu/fr/risques/desinformation

_____ . DÉSINFORMATION EN POLITIQUE

www.bee-secure.lu/desinformation-politique (consulté le 11/11/2021)

_____ . LES ÉCRANS EN FAMILLE

www.bee-secure.lu/les-ecrans-en-famille (consulté le 11/11/2021)

_____ . NETIQUETTE

www.bee-secure.lu/netiquette (consulté le 11/11/2021)

_____ . QU'EST-CE QUE LE BIG

DATA ?

www.bee-secure.lu/fr/publication/quest-ce-que-le-big-data-2 (consulté le 11/11/2021)

_____ . RGPD

www.bee-secure.lu/rgpd (consulté le 11/11/2021)

BEE SECURE, CNPD, Cybersecurity Competence Center Luxembourg (C3). SPAMBEE

www.spambee.lu (consulté le 11/11/2021)

BEE SECURE, SCRIPT, Police Lëtzebuerg, Parquet de Luxembourg. Nu(e) sur le net ?

www.bee-secure.lu/sexting-guide (consulté le 11/11/2021)

BEE SECURE, Tactical Tech. Réagir à une violation de données.

www.bee-secure.lu/fr/publication/comment-reagir-a-une-violation-de-donnees (consulté le 11/11/2021)

Commission nationale pour la protection de données. CNPD

<https://cnpd.public.lu/fr/commission-nationale.html> (consulté le 11/11/2021)

_____ . Formulaire de réclamation

<https://cnpd.public.lu/fr/particuliers/faire-valoir/formulaire-plainte.html> (consulté le 11/11/2021)

_____ . Règlement général sur la protection des données

www.cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees.html (consulté le 11/11/2021)

CIRCL. formulaire de réclamation.

www.circl.lu/report/#report-an-incident (consulté le 11/11/2021)

CORE. A knowledge base on children & children in the digital age.

www.core-evidence.eu (consulté le 10/03/2022)

Der Postillon. Erstes Baby mit Maske geboren.

www.der-postillon.com/2020/09/baby-maske.html (consulté le 11/11/2021)

ILR

www.web.ilr.lu (consulté le 11/11/2021)

Livingstone, S. & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE-Children Online: Research and Evidence.

www.doi.org/10.21241/ssolar.71817 (consulté le 10/03/2022)

NBC News. Your safari selfies are cute, but they're a road map for poachers.

www.nbcnews.com/business/business-news/your-safari-selfies-are-cute-they-re-road-map-poachers-n1016031 (consulté le 23/11/2021)

RTL. Geldstrof fir 3 Ugekloten, Parquet hat feste Prisong gefrot

www.rtl.lu/news/national/a/1036740.html (consulté le 11/11/2021)

Tactical Tech. La technologie est stupide : comment choisir la technologie pour le travail à distance ?

www.tacticaltech.org/news/technologie-est-stupide (consulté le 23/11/2021)

ULC. Votre ASBL

www.ulc.lu/fr/presentation/?id=1 (consulté le 11/11/2021)

Selon vous, quelles sont les solutions ?



1. Piratage

Aidez Lynn à réagir adéquatement en choisissant parmi les actions ci-dessous :

- ☐ 1 ☐ 3 ☐ 5
☐ 2 ☐ 4

2. Configurations et bien-être

Essayer de réguler le temps d'écran est une bonne base, mais il faut également tenir compte de la :

____ C ____ É
T ____ Q U ____ !

3. Attaque d'hameçonnage (« phishing »)

Aidez Dennis à identifier les risques :

- ☐ 1 ☐ 2

4. Supports de stockage

Aidez Julie à diversifier son système de sauvegarde :

- ☐ 1 ☐ 3
☐ 2 ☐ 4

5. Diffusion d'informations (1/2)

Quelles informations pourraient être lues par un tiers avec cette photo :

- ☐ 1 ☐ 6 ☐ 11
☐ 2 ☐ 7 ☐ 12
☐ 3 ☐ 8 ☐ 13
☐ 4 ☐ 9
☐ 5 ☐ 10



5. Diffusion d'informations (2/2)

Partager toutes ces données n'est pas sans risques. Quels sont les dangers potentiels ?

- ☐ 1 ☐ 3
- ☐ 2 ☐ 4

6. Escroquerie

Aidez Sasha à comprendre qu'il s'agit d'une arnaque ! Quels sont les indicateurs visibles sur le site ?

Entourez sur la page les zones visibles sur le site !

7. Désinformation

Aidez Pierre à comprendre les risques de la désinformation :

- ☐ 1 ☐ 2

8. Contenus illégaux

Est-ce ce que ce genre de comportement en ligne est punissable par la loi ?

- ☐ 1 ☐ 2

9. Sexting

D'un point de vue légal, est-ce que Pascal peut partager une photo intime de lui-même ?

- ☐ 1 ☐ 3
- ☐ 2 ☐ 4

10. Cyberharcèlement

Dennis ne sait pas quoi faire. Que lui conseillerez-vous ?

- ☐ 1 ☐ 2



Plus d'informations sur **bee-secure.lu**



Éditeur : Service national de la jeunesse (SNJ)

B.P. 707 - L-2017 Luxembourg

www.snj.lu

www.bee-secure.lu



Consultez :

www.creativecommons.org/licenses/by-nc-sa/4.0/deed.fr

Initié par :



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Opéré par :



Service national
de la jeunesse



Cofinancé par :



Cofinancé par le mécanisme pour l'interconnexion
en Europe de l'Union européenne

Version digitale

Risques sur Internet – 03.2022

ISBN : 978-2-919796-46-5

© Conception graphique : Alternatives communication