guide parental

Protégez vos enfants en ligne

BEE SECURE

ins@fe

LIBERTYGLOBAL

TABLE DES MATIERES

A. Comment utiliser ce kit p. 4

B. Guide pour les parents et les éducateurs: p. 5

1. Surfer en toute sécurité p. 6
2. La communication p. 10
3. Le cyber-harcèlement p. 15
4. Divertissement & téléchargement p. 17

C. Solutions proposées pour les activités p. 21

1. Surfer en toute sécurité p. 21
2. La communication p. 24
3. Le cyber-harcèlement p. 26
4. Divertissement & téléchargement p. 27

D. Glossaire p. 29

E. Adresses utiles p. 39

A. Comment utiliser ce kit

Si vous prévoyez pour un an, semez du riz.
Si vous prévoyez pour dix ans, plantez des arbres.
Si vous prévoyez pour cent ans, éduquez votre enfant.
Proverbe chinois

Cher parent, cher éducateur,

Vous tenez en main le kit de sécurité en ligne destiné aux familles ayant des enfants entre 6 et 12 ans. Cette ressource pédagogique a été créée avec la ferme conviction que les nouvelles technologies ne doivent pas séparer les générations mais plutôt les réunir. Elle a été réalisée grâce à l'expérience d'Insafe, le réseau paneuropéen de centres de contact nationaux travaillant à une sensibilisation plus aiguë aux thèmes de la sécurité sur Internet. La mise au point et la production de ce kit de sécurité en ligne a été soutenue par les partenaires suivants : CASES du Ministère de l'Economie et du Commerce Extérieur, Guichet Unique, Ministère de l'Education et de la Formation Professionnelle, Ministère de la Famille et de l'Intégration, Ministère de la Santé, Service National de la Jeunesse.

Tout comme il peut être dangereux de jouer sur une aire de jeux ou de traverser la route si l'on ne fait pas attention, l'utilisation d'Internet et des technologies mobiles peut se révéler périlleuse pour les imprudents. Heureusement, il existe des outils permettant de conférer aux

utilisateurs d'Internet les connaissances nécessaires des avantages et des risques du Web.

Utilisez votre nouveau kit pour soutenir vos enfants dans leur apprentissage d'une utilisation sûre et efficace d'Internet. Le kit offre plus de cinquante conseils de sécurité et exercices pour vous aider à informer vos enfants d'une façon ludique sur la sécurité en ligne. Il comporte:

- deux brochures sur la sécurité en ligne : une partie amusante pour toute la famille et un guide parental;
- les règles d'or;
- un certificat de famille;
- des autocollants;
- 12 cartes de situation à découper pour les enfants.

Les deux brochures, celle pour la famille et le guide parental, sont marquées avec des couleurs différentes pour souligner les quatre thèmes-clés de la sécurité en ligne: la sécurité, la communication, le divertissement & le téléchargement et le cyber-harcèlement. La brochure destinée aux parents sert de référence pour la partie ludique: elle contient des informations de fond, des remarques sur les activités ainsi que des solutions proposées pour les exercices et les cartes de situation.

La brochure pour la famille est destinée à être utilisée de manière commune par les parents et les enfants. Les quatre thèmes sont abordés à travers l'histoire de deux jeunes, Pit et Claire, leurs parents et Laura, le génie de l'informatique. Chaque chapitre contient des activités pédagogiques, y compris des exercices en ligne, des quiz, des règles d'or et des liens utiles.

Lisez l'histoire à voix haute à vos enfants et parcourez ensemble les activités proposées. A la fin de chaque chapitre, vous pourrez utiliser la carte de situation correspondante pour déclencher une discussion avec vos enfants en vue d'améliorer leur compréhension du contenu.

Lorsque vos enfants auront parcouru avec succès tout le kit, récompensez-les en établissant un ensemble de règles d'or et en signant ensemble le certificat de famille. En dernier lieu, les enfants pourront décorer les brochures avec les autocollants.

Vos remarques nous sont très importantes. N'hésitez pas à contacter votre centre Insafe local (www.bee-secure.lu) si vous avez des questions ou des commentaires. Nous vous souhaitons beaucoup de plaisir dans l'apprivoisement d'Internet…, en famille!

Surfez en toute sécurité,

Safe surfing,

1. Surfer en toute sécurité

UN ORDINATEUR @ LA MAISON

Un ordinateur à la maison peut être une excellente source pédagogique et récréative pour toute la famille. Installez l'ordinateur dans une pièce commune de la maison et établissez des règles spécifiques en ce qui concerne les conditions et la durée de son utilisation; vous ferez ainsi déjà un premier pas important pour assurer la sécurité des jeunes membres de votre famille.

Rappelez-vous que vos enfants peuvent accéder à **Internet** chez des amis, dans des cyber-cafés, etc. Voilà pourquoi il est important d'établir un code de conduite qu'ils pourront appliquer à tout moment et partout.

LA PROTECTION DE VOTRE ORDINATEUR

La sécurité peut être assurée par une compréhension élémentaire des dangers éventuels et une connaissance des solutions simples pour les contrer. Ces remèdes incluent des outils technologiques utiles, mais aussi le bon sens des utilisateurs. Comme tout le reste, celui-ci évolue avec l'âge et la pratique.

Les choses que vous et vos enfants ferez probablement sur votre ordinateur, comme utiliser des **clés USB (clés mémoire)** ou des **CD-ROM**, ouvrir des **pièces jointes** et **télécharger** des **fichiers**, peuvent présenter des menaces. Ces menaces se composent principalement de **programmes informatiques** malicieux (**logiciels malveillants**), mis au point pour endommager votre ordinateur, voler des données personnelles ou vous envoyer des publicités non désirées.

Différents types de logiciels malveillants sont présentés aux enfants: des **virus**, des **vers**, des **chevaux de Troie** et des **logiciels espions**. Les enfants apprennent également à reconnaître les symptômes d'un ordinateur infecté. Ils apprennent à prévenir une infection en n'utilisant Internet que sur des ordinateurs protégés par des programmes antivirus et **anti-espion** mis à jour. On leur conseille également d'être prudents en ouvrant les pièces jointes d'e-mails d'expéditeurs inconnus, en téléchargeant des programmes sur Internet et en utilisant des clés USB ou des CD-ROM.

LA LUTTE CONTRE LE SPAM

80 % des e-mails circulant sur Internet sont des **spams** (e-mails non désirés) susceptibles d'influencer facilement vos enfants. La publication par mégarde d'une adresse e-mail sur le **Web** en utilisant un **groupe de nouvelles**, un site de **chat**, un **forum** public, un site de **réseau social** ou un **forum en ligne** peut produire des spams. Des logiciels spéciaux peuvent recueillir les adresses e-mail du Web pour composer des listes de mailing; celles-ci sont ensuite utilisées pour distribuer des quantités énormes de spams. Les entreprises recourant à de telles activités sont souvent implantées dans des pays où il n'existe pas de législation pour se protéger contre les e-mails non désirés!

Les e-mails non désirés (spams) sont souvent liés à la pornographie, aux médicaments, aux transactions financières douteuses, etc. De plus, le spam peut également être la source de programmes malveillants. Dans la plupart des cas, les e-mails non désirés (spams) sont distribués avec des intentions frauduleuses. Voici quelques conseils pour protéger votre famille:

- Utilisez des « **filtres anti-spam** ». Votre fournisseur d'e-mail propose normalement des options anti-spam que vous pouvez activer dans votre programme e-mail. Contactez votre fournisseur d'email ou d'accès pour obtenir de plus amples informations. Contrôlez régulièrement votre **dossier** « **junk** » ou « **spam** » pour vérifier si des e-mails innocents n'y ont pas atterri. La technologie n'est pas infaillible.
- Apprenez à vos enfants à ne pas ouvrir les e-mails de personnes inconnues. Le spam contient presque toujours des offres et des pièces jointes prometteuses. Montrez-leur comment ils peuvent bloquer l'expéditeur d'un e-mail ou demandez-leur de supprimer les e-mails suspects.

SURFER SUR LE NET

Même les très jeunes enfants peuvent profiter d'Internet pour s'amuser et pour consulter des **sites Web** pédagogiques. Internet offre néanmoins aussi toutes sortes de contenus qui ne sont pas toujours appropriés à leur âge.

Les moteurs de recherche sont d'une grande aide pour trouver des contenus sur Internet. Toutefois, comme la recherche dépend du choix de mots-clés, il est facile de tomber sur des contenus non désirés. Un simple mot-clé anodin peut mener vers un site Web moins innocent contenant le mot-clé en question. Ci-dessous, vous trouverez quelques conseils pour aider vos enfants à surfer à moindre risque sur Internet:

• Créez un compte d'utilisateur spécial pour votre enfant en utilisant un **système d'exploitation** (Windows, Linux, Mac OS) sur lequel vous pouvez activer des fonctions de **contrôle parental**.
• Examinez les fonctions de contrôle parental de votre **navigateur Internet** et du moteur de recherche. Assurez-vous que vous connaissez les choix offerts par les **paramètres familiaux** de ces outils.
• Proposez des **moteurs de recherche** adaptés aux enfants et aux jeunes utilisateurs d'Internet dont vous vous occupez, comme *www.takatrouver.net*.
• Sauvegardez les adresses des sites Web **dont** vos enfants se servent le plus dans leur dossier de **favoris** (une option du navigateur). Ainsi, vous pouvez leur permettre d'utiliser leurs sites web favoris plusieurs fois sans devoir passer par le moteur de recherche.

Outre l'activation des fonctions de contrôle parental dans votre navigateur et dans le moteur de recherche, vous pouvez utiliser un **filtre** supplémentaire, un logiciel visant à protéger les mineurs des contenus non appropriés sur le Web. Demandez conseil à votre distributeur ou recherchez des logiciels d'essai sur Internet. Rappelez-vous que rien ne peut remplacer les conseils des parents ou des éducateurs. Les outils techniques ne sont pas infaillibles et peuvent parfois créer un faux sentiment de sécurité, sauf si vous les utilisez en combinaison avec votre bon sens.
Les logiciels de filtrage peuvent être tellement restrictifs qu'ils bloquent des contenus innocents. Ils peuvent par exemple empêcher les enfants de chercher des informations pour un exposé historique sur la Deuxième Guerre mondiale, parce que la recherche mène vers des sites Web décrivant la violence. De plus, chaque filtre qui peut être enclenché peut également être désactivé par des jeunes ingénieux, souvent experts dans la couverture de leurs traces. Vous ne vous en rendrez compte que si vous apprenez vous-même à utiliser l'ordinateur et les logiciels.

Consultez le site Web de **SIP-Bench**, une enquête soutenue par la Commission européenne ayant testé 30 outils de contrôle parental et d'anti-spam afin de mesurer leur efficacité pour protéger les enfants de 6 à 16 ans contre les contenus pernicieux dans les différentes applications d'Internet: la **navigation**, l'e-mail, le **transfert de fichiers**, le chat et les **messages instantanés**.

Outre le fait d'éviter les **contenus pernicieux**, assurez-vous que vos enfants ne croient pas tout ce qu'ils voient ou lisent sur Internet. Dans la brochure ludique pour toute la famille, nous suggérons de consulter pour toute recherche d'information, au moins trois sites Web afin de comparer les contenus trouvés. On conseille également aux enfants de mentionner systématiquement la source des informations à chaque fois qu'ils les utilisent pour un devoir scolaire.

REGLES D'OR POUR LES PARENTS

• Assurez-vous que votre ordinateur est protégé par un pare-feu correctement paramétré, ainsi que par un logiciel antivirus et anti-espion. Maintenez ces derniers à jour et faites attention aux **alertes** qu'ils génèrent. Vérifiez si votre fournisseur d'accès à Internet propose des outils antivirus et anti-espion dont vous pourriez vous servir.

• Utilisez un filtre anti-spam dans votre programme e-mail et gardez votre adresse e-mail aussi privée que possible, en évitant de la publier sur le Web. N'ouvrez pas les e-mails d'expéditeurs inconnus et scannez les pièces jointes avant de les ouvrir.

• Maximisez les options de contrôle parental de vos logiciels : système d'exploitation, navigateur Internet, moteur de recherche et programme d'e-mails. Créez des comptes d'utilisateurs séparés pour vos enfants. Assurez-vous que les paramètres de protection des données sont réglés au niveau le plus élevé (voir le menu « Options » dans votre navigateur).

• Envisagez d'utiliser des logiciels de filtrage supplémentaires.

• Contactez votre fournisseur d'accès ou un expert dès que votre ordinateur affiche un comportement bizarre ; il est peut-être infecté. Votre fournisseur devrait également être en mesure de vous donner des conseils.

• Mettez-vous à côté de vos enfants lorsqu'ils sont en train de surfer. C'est une excellente façon d'encourager la discussion et d'augmenter la confiance mutuelle. Proposez-vous le défi d'apprendre ensemble.

• Si vous, ou votre enfant, vous trouvez confrontés sur Internet à des contenus qui semblent illégaux (images d'abus sexuel sur mineurs, racisme, discrimination par exemple), vous pouvez en référer à www.lisa-stopline.lu.

• Rappelez-vous que ces règles de sécurité s'appliquent aussi bien à vous qu'à vos enfants. Encouragez-les à vous raconter tout ce qui leur paraît bizarre.

LIENS UTILES

Pour pouvoir surfer sur l'Internet en toute sécurité, l'essentiel est la connaissance: savoir quels sont les risques, savoir comment se protéger et développer ses connaissances. Vous trouverez d'avantage d'informations sur le site Internet
www.bee-secure.lu
De l'information actuelle, astuces et liens concernant la sécurité en ligne pour les parents, professeurs, enfants et adolescents sont disponibles également ici.

Pour favoriser le développement d'un Internet plus sûr en offrant des solutions qui protègent les mineurs des contenus inappropriés, consultez le site
http://www.sip-bench.org

Si vous trouvez des images d'abus sexuel sur mineurs ou rencontrez des contenus racistes, discriminatoires ou révisionnistes, signalez-les sur
www.lisastopline.lu.

2. La Communication

LES PIECES DU PUZZLE

Vous rappelez-vous combien il était important pour vous de garder le contact avec vos amis quand vous étiez petit ? Internet fournit une multitude de nouveaux endroits pour rencontrer des amis et propose de nouvelles voies servant à s'exprimer et à garder contact avec ses amis grâce à l'envoi d'e-mails, au partage de fichiers, au blogging et au réseau social (p. ex. MySpace, Netlog, Facebook, Hi5, Habbohotel) etc. Les adolescents d'aujourd'hui utilisent les nouvelles technologies de l'information et de la communication pour faire de nouvelles expériences et pour se socialiser dans un nouvel espace dont ils croient qu'il est privé et hors de portée de la surveillance parentale.

Le chapitre sur la communication initie les parents et les enfants au concept des **données personnelles**, de la **vie privée**, des interactions positives en ligne et de la gestion des risques tels que le contact avec les étrangers. La vie privée est étroitement liée aux concepts des **comptes** & **profils**. Un compte est ce qui rend possible l'accès aux services en ligne.

Hors ligne, un abonnement de bus, une carte de gym ou une carte de membre contiennent des informations personnelles. Les comptes et les services en ligne sont identiques. Vous ne pouvez pas les utiliser si vous ne fournissez pas quelques informations personnelles qui forment votre « profil d'utilisateur ». Il est important de savoir que vous pouvez choisir les informations personnelles que vous souhaitez rendre accessibles et avec qui vous voulez les partager.

Dans la protection de votre vie privée, il s'agit de gérer les informations que vous souhaitez révéler aux autres et non de mentir sur votre identité. Les jeunes sont enthousiastes à l'idée de communiquer en ligne avec des amis et d'y créer leur image. Ils ne se rendent toutefois pas toujours compte des conséquences que la publication de leurs données privées peut avoir.

LA CREATION DU PROFIL DE CLAIRE

Le premier pas dans la protection des informations personnelles est de créer un profil plus sûr en réfléchissant prudemment aux données qu'il reprendra et aux paramètres de protection de la vie privée.

Créez plusieurs comptes e-mail pour les différents contextes en ligne. Par exemple, en utilisant des services en ligne tels que le chat, les messages instantanés, le blogging, etc., incitez votre enfant à utiliser une adresse e-mail neutre et un **nom d'écran (pseudo)**. Ainsi, votre enfant n'utilisera pas d'adresse e-mail révélant son nom entier.
Gardez toujours vos **mots de passe** secrets. Assurez-vous que vos enfants comprennent qu'ils ne doivent pas partager leurs comptes personnels avec des amis qui peuvent abuser de leur confiance.

Pensez à personnaliser les **paramètres de protection de la vie privée** de votre profil/compte en choisissant l'option privée et non publique. Ainsi, vous avez la possibilité de contrôler qui pourra le voir et avec qui vous pouvez avoir contact. Un profil privé signifie que vous pouvez gérer votre **liste de contacts**. Prenez aussi en considération que ces plateformes sont mises en place par des firmes qui ont des intérêts commerciaux bien ciblés. De plus, ces logiciels présentent souvent des lacunes de sécurité qui peuvent être exploités par des personnes malveillantes. Apprenez à vos enfants à n'accepter le contact qu'avec des personnes qu'ils connaissent déjà hors ligne.

Si vos enfants utilisent des salons de chat, vérifiez:

- s'il y a de vrais modérateurs. L'absence de modérateurs signifie que le chat n'est pas protégé;
- s'il y a des outils permettant d'ignorer ou de bloquer les chatteurs non désirés;
- s'il y a une fonction d'aide ou de signalisation sur le site Web qu'ils peuvent utiliser en cas de problème;
- si les règles du service sont clairement et visiblement stipulées.

PHOTOS ET WEBCAMS

Les enfants doivent comprendre qu'une photo d'eux appartient à leur vie privée et que les images numériques sont extrêmement puissantes. Elles sont faciles à diffuser et à **modifier** et il est très difficile de les effacer une fois qu'elles ont été envoyées par ordinateur ou par téléphone portable – elles peuvent rester en ligne pour toujours ! Les webcams doivent être utilisées avec prudence et les enfants ne devraient pas les utiliser sans surveillance. Vous et vos enfants ne devriez envoyer vos photos personnelles qu'à des personnes que vous connaissez et auxquelles vous faites confiance. Aussi demandez toujours la permission avant de publier une photo de quelqu'un d'autre. Si vous publiez la photo d'un mineur (moins de 18 ans), il faut demander en plus l'autorisation aux parents. Ne laissez pas vos enfants utiliser un ordinateur et une webcam seuls dans leur chambre.

LE CONTACT AVEC DES INCONNUS

Les personnes que vous rencontrez en ligne ne sont pas toujours ce qu'elles prétendent être. Apprenez à vos enfants à protéger leur vie privée en ligne, tout comme ils le feraient hors ligne. Vous établissez bien les règles de leur comportement par rapport à des étrangers dans le monde réel, pourquoi ne suivraient-ils pas les mêmes règles sur Internet ?

Vos enfants peuvent établir une relation profonde avec des amis en ligne et peuvent être amenés à faire facilement confiance à des personnes qui se montrent intéressées et compréhensives, même s'ils ne les connaissent pas vraiment. Par conséquent, ils peuvent être tentés de rencontrer ces nouveaux amis hors ligne sans vous en informer. Les enfants ne se rendent souvent pas compte du danger potentiel de telles rencontres et les considèrent peut-être comme insignifiantes. Les prédateurs sexuels utilisent les moyens de communication d'Internet pour trouver leurs proies ! Des études révèlent que de nombreux enfants se rendent seuls à des rendez-vous avec des « amis » rencontrés en ligne, sans en informer leurs parents. Parlez-en à vos enfants. Apprenez-leur à toujours fixer un rendez-vous dans un endroit public et à s'y rendre accompagné d'une personne de confiance. La communication est essentielle !!

NETIQUETTE

La **netiquette** concerne les bonnes manières sur Internet et le fait de traiter les autres personnes sur le net de la façon dont on aimerait être traité soi-même. Les enfants ne se rendent peut-être pas compte qu'ils peuvent par mégarde blesser quelqu'un en ligne. Malheureusement, certaines personnes utilisent Internet et/ou le téléphone portable pour contrarier ou harceler d'autres gens. Appelé le cyber-harcèlement, ce phénomène peut toucher un enfant sur quatre (voir le chapitre en question pour de plus amples informations).

LANGAGE DE CHAT

En chattant en ligne, les jeunes utilisent un langage unique plein d'émoticones et d'acronymes ! Jetez un coup d'œil sur le tableau ci-dessous pour vous familiariser avec ce langager

Liste indicative d'acronymes de chat:

@+: à plus tard (à bientôt)	OUÈ, OÉ: ouais, oui
@12C4: à un de ces quatre (à bientôt)	PI: pas intéressé(e)
ASV: age, sexe, ville	PTR: pété de rire
AMHA: à mon humble service	PK: pourquoi
ATTA: attend	PSK, PQ, PRK : parce que
ABS: absent	P-T: peut-être
BJR: bonjour	PTAFQM: pas tout à fait quand même
BIZ, BSX: bise, bisou	PV: (en) privé, message privé
BCP: beaucoup	QQ1, KK1, QQN: quelqu'un
BG: belle ou beau gosse	RAB: rien à battre, rien à dire
BB: bye bye	RAF: rien à foutre
CPG: c'est pas grave	RAZ: remise à zéro
DAC/DAK: d'accord	RGD: rire à gorge déployée
DSL: désolé	SLT, SLU: salut
IRL: dans la vie réelle, « in real life »	SPD: « sois pas dèg »
JMEF: je m'en fous	SPJ: sois pas jaloux

JRE: je reviens

JTA, JDR, JTD: je t'adore

KESTUF: qu'est-ce que tu fais

KOI: quoi

KI: qui

MDP: mot de passe

MDR: mort de rire
(traduction de LoL: laughing out loud)

MPM: même pas mal

NRV: énervé

NN, NAN, NA: non

OSEF: on s'en fout

TFK: tu fais quoi

TG, TAGGLE: ta gueule

TJRS: toujours

TKT: t'inquiète

TLM: tout le monde

TMQ: tu me manques

TSÉ: tu sais

VTFF: va te faire foutre

YX: yeux ou je n'en crois pas mes yeux

2M1: demain

2RI1, DR: de rien

Vous pouvez créer des émoticones en combinant des signes de ponctuation et des lettres. En voici quelques exemples:

Un smiley (avec ou sans nez)	**:)** ou **: -)** Deux points, (tiret), parenthèse
Un visage triste (avec ou sans nez)	**:(** ou **:-(** Deux points, (tiret), parenthèse
Un clin d'œil (avec ou sans nez)	**;)** ou **;-)** Deux points, (tiret), parenthèse
Un visage surpris (avec ou sans nez)	**: o** ou **:-o** Deux points, (tiret), petit o
Un grand sourire (avec ou sans nez)	**:-D** ou **: D** Deux points, (tiret), grand D
Une langue tirée (avec ou sans nez)	**: p** ou **:-p** Deux points, (tiret), petit p

RÈGLES D'OR

- Prenez le temps de découvrir comment vos enfants passent leur temps en ligne et demandez-leur de vous montrer comment ils communiquent avec leurs amis.
- Apprenez-leur à protéger leur vie privée en ligne et à respecter celle des autres:
  - en créant des profils sûrs avec des paramètres de sécurité activés;
  - en protégeant leurs mots de passe;
  - en contactant seulement les personnes qu'ils connaissent hors ligne et en ne répondant qu'à celles-ci;
  - en demandant toujours l'accord des parents avant de télécharger des photos d'eux-mêmes ou de votre famille, de la maison, de leur école, etc.;
  - en ne publiant des photos ou des vidéos d'autres personnes qu'avec leur autorisation, voire l'autorisation des parents s'il s'agit de mineurs;
  - en ne communiquant des informations personnelles telles que leur numéro de téléphone, leur adresse, leur école, leur équipe de sport etc., qu'à des personnes qu'ils connaissent dans la vie réelle;
- Installez l'ordinateur dans une pièce commune de la maison afin d'avoir un œil sur leurs activités en ligne.
- Ensemble assurez-vous:
  - de savoir comment refuser des contacts ou bloquer des personnes sur une liste de contacts;
  - de connaître les fonctions de sécurité et de signalisation disponibles sur les sites Web que vous utilisez.
- Créez un climat de confiance en assurant à vos enfants qu'ils peuvent vous parler de leurs expériences ou de leurs erreurs pour que vous puissiez trouver des solutions ensemble! Les erreurs font partie de l'apprentissage..

LIENS UTILES

Le site *www.bee-secure.lu* vous offre plus d'informations sur la manière de communiquer de façon sûre et responsable. Vous y trouverez des conseils ciblés pour les enfants, les jeunes ou les adultes. Vous trouverez également toutes les bonnes pratiques pour sécuriser vos activités en ligne ici.

La Commission européenne organise chaque année une enquête Eurobarometer, qui offre un panorama de l'utilisation d'Internet par les enfants et les jeunes. Consultez le rapport sur: *http://ec.europa.eu/information_society/activities/sip/eurobarometer*

3. Cyber-harcelement

UN CAS DE CYBER-HARCELEMENT

La communication par Internet et par téléphone portable comporte de nombreux avantages. Malheureusement, elle a également certains inconvénients – vos enfants reçoivent ou envoient peut-être des messages avec des contenus qui blessent leurs sentiments ou ceux des autres. Il est important que vous appreniez à vos enfants un comportement socialement acceptable – même nos propres enfants ne sont pas toujours des anges ;-)

Le **cyber-harcèlement**, également appelé cyberbullying, consiste à utiliser les nouveaux appareils et services d'information et de communication pour tyranniser, harceler ou intimider un individu ou un groupe. Les e-mails, le chat, les messages instantanés, les téléphones portables ou autres outils numériques peuvent être utilisés. Dans les environnements de jeux virtuels, les tyrans peuvent attaquer l'**avatar** de votre enfant en tirant dessus, en volant ses possessions virtuelles ou en forçant l'avatar à se comporter d'une façon non voulue. Quelqu'un peut aussi publier leur photo privée ou leurs données personnelles sur un forum ou un site Web public.

Comme le **harcèlement** à l'école ou sur l'aire de jeux, un tel comportement est inacceptable. Les enfants victimes de harcèlement réel ou/et virtuel éprouvent souvent beaucoup de difficultés à en parler. Les parents, les éducateurs et les enfants doivent être attentifs et prêts à réagir. Contrairement au harcèlement traditionnel, le cyber-harcèlement peut encore toucher l'enfant même s'il n'est déjà plus en présence de ses agresseurs. Par exemple, les tyrans peuvent à tout moment envoyer des messages menaçants aux adresses e-mail de la maison et aux téléphones portables.

Les parents peuvent aider à promouvoir un environnement dans lequel le harcèlement n'est pas toléré – apprenez à vos enfants que le fait d'être anonyme sur Internet ne leur permet pas d'agir de façon irresponsable. Ils doivent connaître leurs propres droits et responsabilités et savoir comment respecter les droits des autres.

Ayez toujours un dialogue ouvert avec vos enfants pour pouvoir parler de chaque situation inquiétante.

REGLES D'OR:

- Prenez des précautions contre les expériences négatives en vous assurant que vos enfants savent comment protéger leur vie privée et respecter celle d'autrui.
- Apprenez à vos enfants à ne pas répondre aux messages de harcèlement.
- Aidez vos enfants à comprendre quel genre de messages et de comportement pourrait mettre d'autres personnes mal à l'aise et comment les éviter.

- Assurez-vous qu'ils savent comment bloquer des expéditeurs de leur liste de contacts.
- Gardez les messages offensants, ils peuvent vous servir de preuves.
- Informez-vous sur les stratégies anti-harcèlement mises en place par l'école de vos enfants. Travaillez ensemble avec d'autres parents et enseignants pour empêcher harcèlement et cyber-harcèlement.
- Restez en contact avec l'environnement de vos enfants, rencontrez leurs amis, les parents de leurs amis, leurs enseignants et leurs camarades de classe.
- Encouragez vos enfants à tout vous raconter sur leurs expériences perturbantes hors ligne et en ligne. Rassurez-les, même s'ils font une bêtise, vous serez là pour les aider à trouver une solution!
- Assurez-vous que vos enfants comprennent que ce n'est jamais de leur faute si quelqu'un les harcèle.

LIENS UTILES

Le site *www.bee-secure.lu* fournit des explications sur le cyber-harcèlement et propose aux parents et aux enseignants des solutions pour traiter ce phénomène.

Des enfants victimes de harcèlement peuvent s'adresser au 116 111 (Kannerjugend-Telefon). Les parents peuvent s'adresser au Elterntelefon (26 64 05 55) ou à la BEE SECURE Helpline (26 64 05 44).

4. Divertissements & Telechargements

SUR INTERNET, TOUT CE QUI BRILLE N'EST PAS OR

Internet est un espace virtuel proposant une multitude d'activités, y compris des activités commerciales. Si vous ne permettez pas à vos enfants d'avoir tout ce qu'ils voient dans les publicités à la télévision, ni tout ce qui les impressionne dans les magasins, vous devez également leur apprendre à ne pas croire ni vouloir tout ce qu'ils voient en ligne, par exemple de la musique, des jeux, des **sonneries** et autres accessoires.

Passer du temps avec vos enfants sur Internet vous donne l'occasion de leur expliquer que des produits comme des sonneries, des **fonds d'écran**, des **mp3**, des **avatars** etc. sont rarement gratuits. Lorsque vous trouvez de telles publicités, montrez-leur les petits caractères pour démontrer qu'ils ne doivent pas prendre pour argent comptant tout ce qu'ils trouvent sur le net.

Pour vous abonner à un service (gratuit ou non), vous devez remplir en règle générale un f**ormulaire en ligne** contenant des informations personnelles importantes. Ne complétez ces formulaires que si vous savez comment vos données personnelles seront utilisées, et dissuadez vos enfants de remplir de tels formulaires, sauf si vous le faites ensemble.

Les **fenêtres pop-up** servent souvent à vendre des produits sur Internet. Elles ne sont toutefois pas toujours utilisées à cet effet – cela dépend si elles viennent d'un site Web fiable ou non. En général, si vous faites confiance au site, vous pouvez faire confiance au pop-up. Toutefois, certaines fenêtres pop-up sont utilisées pour lancer des produits peu fiables, pour diffuser des programmes malveillants ou pour amener l'utilisateur vers des questionnaires en ligne recueillant des données personnelles. Apprenez à vos enfants à fermer les fenêtres pop-up non fiables en cliquant sur la croix rouge dans le coin supérieur droit.

JOUER EN LIGNE

Les jeux jouent un rôle important dans l'évolution d'un enfant, étant donné que les aptitudes sociales et l'esprit stratégique se développent dans un environnement régi par des règles. Nombre de jeux numériques sont attrayants et interactifs et sont utilisés à des fins éducatives.

Toutefois, les jeux numériques ne sont pas tous de bonne qualité. Vous devez décider quel genre de jeux est le plus approprié pour vos enfants et en établir les règles. Vous pouvez

vous assurer que le temps que vos enfants utilisent pour jouer en ligne ne le sera pas au détriment d'autres activités.

Les enfants peuvent jouer à des jeux sur un CD/DVD, sur des sites Web, **sur des consoles de jeux ou sur un téléphone portable ou d'autres appareils mobiles. Les jeux en ligne se distinguent des jeux numériques plus anciens parce qu'ils ont besoin d'une** connexion réseau **en direct. Ces jeux en ligne** vont de jeux simples et bien connus comme Pacman et Tetris, aux jeux mettant en scène une réalité virtuelle où plusieurs utilisateurs jouent ensemble en ligne en créant des contenus et des histoires. Nombre de ces **jeux multi-joueurs** proposent à leurs participants des communautés virtuelles. On doit donc tenir compte des mêmes règles de sécurité que pour la communication avec des inconnus sur Internet. (voir chapitre sur la communication).

Il existe un système de classification paneuropéen pour les jeux électroniques, PEGI, où les jeux sont classés selon l'âge des différents publics et les contenus. Ce système est soutenu par plusieurs fabricants, y compris PlayStation, Xbox et Nintendo, ainsi que par des éditeurs et des concepteurs de jeux interactifs à travers toute l'Europe. Tenez compte, à chaque fois que vous achetez un jeu, de ces pictogrammes que vous trouverez sur le dos de chaque boîte, mais rappelez-vous toutefois que tous les enfants de 12 ans ne sont pas identiques. Pour les jeux en ligne, un système de classification « PEGI ONLINE » est en cours d'élaboration.

LE PARTAGE DE FICHIERS & LES DROITS D'AUTEUR ©

Les jeunes considèrent Internet comme un trésor inépuisable de films, de musique et de jeux à télécharger, à regarder, à écouter et à jouer. Ils téléchargent souvent des documents sur des réseaux de « peer » (réseaux de partage de fichiers) sans se rendre compte que l'œuvre originale de l'artiste, du créateur/de l'auteur est protégée par des droits. Cela inclut les films, les chansons, les livres, les logiciels et les images.

Est-ce illégal ?

Le partage de fichiers n'est pas illégal s'il s'agit de fichiers dont vous avez créé vous-même le contenu (mais vous ne pouvez pas partager des fichiers que vous avez seulement adaptés). En général, le **téléchargement** en amont et en aval de musique et de films sans permission préalable du détenteur des **droits d'auteur** est illégal partout dans le monde (même si chaque pays a sa propre législation sur les droits d'auteur). Comme règle approximative, considérez que le partage de musique et de films est **illégal** et soyez prudent avec les applications **peer-to-peer**.

Est-ce risqué ?

Le **partage de fichiers** expose votre ordinateur à des risques en ouvrant des ports par lesquels des programmes et des logiciels malveillants peuvent entrer ; ceux-ci peuvent empêcher votre ordinateur de fonctionner correctement. Il est également possible que d'autres personnes accèdent à vos données personnelles ou utilisent votre ordinateur pour l'envoi de spams ou de contenus illégaux. Le partage de fichiers est légal quand il s'agit de fichiers dont on est soi-même l'auteur.

Où puis-je trouver de la musique légale ?

Des centaines de sites Web dans le monde entier proposent de la musique légale (voir Liens utiles), parfois même gratuitement ! Il s'agit par exemple de sites Web de musiciens qui aimeraient que leurs fans jugent leur musique et où ceux-ci peuvent s'informer de leurs concerts et albums.

REGLES D'OR

Assurez-vous que vous utilisez un site légal pour télécharger de la musique et des films sur Internet:

- Encouragez vos enfants à utiliser des sites Web offrant des contenus légitimes, et expliquez-leur que tout ce qui brille n'est pas or sur Internet.
- Expliquez les risques associés au téléchargement imprudent de contenus du net.
- Protégez votre ordinateur en utilisant un pare-feu correctement paramétré, un antivirus actualisé au moins une fois par jour et en mettant régulièrement à jour vos programmes.
- Apprenez à vos enfants à sauvegarder les fichiers téléchargés sur le disque dur et à les scanner AVANT de les ouvrir.
- Lisez toujours la déclaration de confidentialité et les conditions d'utilisation avant d'installer quelque chose. Vérifiez (sur Internet) si le logiciel que vous souhaitez télécharger est fiable.
- Fermez les fenêtres pop-up non fiables en cliquant sur la croix rouge dans le coin supérieur droit. Ne cliquez jamais à l'intérieur.

ENFANTS & JEUX:

- Etablissez des règles concernant la durée pendant laquelle votre enfant peut jouer.
- Placez l'ordinateur ou la console de jeu dans une pièce commune. Vous pourrez ainsi garder vos enfants à l'œil.
- Surveillez les habitudes de jeux de vos enfants – si vous les surveillez sur une aire de jeux, pourquoi pas lorsqu'ils jouent dans des endroits virtuels?
- Parlez des contenus de jeux et des éléments qui ressemblent à la réalité, de ceux qui n'y ressemblent pas et de ceux qui amusent vos enfants.
- Avant d'acheter un jeu à votre enfant, assurez-vous que le contenu est approprié à son âge (système PEGI paneuropéen ou tout autre système de classification national).

Si vos enfants jouent à des jeux en ligne avec plusieurs utilisateurs :

- Choisissez des sites avec des règles strictes et de vrais modérateurs.
- Prévenez-les qu'ils ne doivent pas révéler leurs données personnelles à d'autres joueurs.
- Recommandez-leur de ne pas rencontrer d'autres joueurs hors ligne, sauf si vous les accompagnez.
- Encouragez vos enfants à s'adresser à une personne de confiance en cas de harcèlement, de menaces ou de langage inacceptable, d'affichage de contenus désagréables ou d'invitations à se rencontrer en dehors du contexte du jeu.
- Si de telles situations problématiques vous sont révélées, utilisez les moyens de signalement des abus de la plateforme de jeux.
- Retirez votre enfant du jeu ou changez son identité en ligne, si quelque chose dans le jeu ou dans la façon dont il évolue vous met mal à l'aise.

LIENS UTILES

Pour tout ce qui concerne les achats en ligne ou les arnaques sur Internet, vous pouvez vous adressez à l'Union Luxembourgeoise des Consommateurs (www.ulc.lu) ou au Centre Européen des Consommateurs du Luxembourg
www.cecluxembourg.lu

Pour plus d'informations et de conseils utiles sur les questions de droits d'auteur ou sur la suppression de pop-up par exemple, consultez le portail luxembourgeois de la sécurité Internet:
www.bee-secure.lu

Apprenez-en plus sur les jeux en ligne et le système de classification PEGI:
http://www.pegi.info/fr

1. Surfer en toute sécurité

COMMENTAIRES SUR LES ACTIVITÉS

Attribue les images aux mots correspondants : la tour de l'ordinateur, le tapis de souris, l'écran, les haut-parleurs, la webcam, l'imprimante, la clé USB (ou clé mémoire), la souris, le CD-Rom.

Un exercice d'échauffement pour familiariser vos enfants avec les différentes parties de l'ordinateur et le reste du matériel hardware. Vous pouvez élargir l'exercice comme bon vous semble.

Demande à tes parents de t'envoyer un e-mail avec une pièce jointe, ou envoie t'en un toi-même. Exerce-toi à effectuer les étapes suivantes : un clic droit sur la pièce jointe pour l'enregistrer sur le bureau de ton ordinateur. Va vers le bureau, clique sur le document avec le bouton droit et sélectionne scanner. Lorsque tu sais que le document est sûr, tu peux l'ouvrir. Rappelle-toi : clic droit et ENREGISTRER – SCANNER – OUVRIR.

Envoyez un e-mail à l'adresse e-mail de vos enfants ou à vous-même en joignant un fichier. Laissez vos enfants suivre les instructions de l'exercice en sauvegardant le document d'un clic droit sans l'ouvrir. Après avoir sauvegardé le fichier sur le bureau ou dans un dossier de l'ordinateur comme « Mes Documents », montrez à vos enfants comment cliquer encore

une fois d'un clic droit sur le fichier pour le scanner avant de l'ouvrir. Ainsi, vous les encouragez à prendre des habitudes de sécurité.

Suis le conseil de Laura et apprends à décrire ton adresse e-mail à chaque fois que tu dois vraiment la publier en ligne. Tu pourras ainsi éviter que ton adresse e-mail ne soit automatiquement captée et utilisée par des spammeurs.
cyberchat.schmid@monmail.com = cyberchat point schmid arobase monmail point com
Pour t'entraîner, décris les adresses e-mail de ta famille: ton adresse e-mail, l'adresse e-mail de ta famille, l'adresse e-mail de ta mère, l'adresse e-mail de ton père

Pour éviter que l'adresse e-mail soit automatiquement recueillie par un logiciel dans le but d'envoyer du spam, décrivez-là au lieu de l'écrire. Laissez vos enfants s'entraîner à cette technique comme décrit ci-dessus. Pensez toutefois au fait que vos enfants devraient éviter de publier leur adresse e-mail sur Internet ; s'ils le font, ils doivent utiliser une adresse qui ne révèle pas leur vrai nom (voir le chapitre sur la communication).

Pour aider Claire à mieux comprendre avant que Laura ne continue son explication, jette un coup d'œil sur les activités dans le cadre ci-dessous et entoure celles que tu ne peux faire que lorsque tu es connecté à Internet.

Les très jeunes enfants ne comprendront peut-être pas exactement quelles activités requièrent une connexion au réseau. Pour écrire un texte, l'ordinateur ne doit pas obligatoirement être connecté, mais pour chatter il doit l'être. Vous pouvez écouter de la musique sur votre ordinateur en utilisant un CD ou un fichier de musique sauvegardé sur votre ordinateur, mais vous pouvez aussi directement écouter de la musique en ligne. Vos enfants ne doivent indiquer que les activités pour lesquelles une connexion au réseau est absolument indispensable.

Avec tes parents, tape www.takatrouver.net dans le navigateur. Recherche des informations sur le tyrannosaure et essaie de découvrir quand ce dinosaure a vécu sur terre. Essaie aussi de trouver une bonne image représentant un tyrannosaure. N'oublie pas de vérifier ces informations sur trois sites Web différents.

Apprenez à vos enfants de bonnes habitudes de recherche, en leur rappelant de ne pas faire confiance à tout ce qu'ils voient en ligne. Rappelez-leur de chercher et de comparer les informations sur au moins trois sites et de toujours mentionner leurs sources lorsqu'ils rédigent un exposé pour l'école.

Avec tes parents, tape www.takatrouver.net dans le navigateur. Recherche des informations sur un certain sujet, par exemple le tyrannosaure, et enregistre les trois sites qui te semblent les plus intéressants en cliquant sur le menu Favoris dans la partie supérieure du navigateur et en les ajoutant à tes sites favoris. Tu peux également créer ton propre dossier.

Sauvegarder et organiser des sites intéressants dans le dossier des favoris (choisir Options sur la barre du navigateur) est une bonne façon de réduire le besoin de vos jeunes enfants de rechercher des informations sur Internet.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (protégé) 2: (virus), (inconnus), (téléchargeant), (clé mémoire), (infectés), (non protégé) 3: (bizarrement) 4: (connais), (pièces jointes), (titres), (spams) 5: (seule), (spams) 6: (première), (trois), (compare), (chaque personne), (publier) 7: (antivirus), (anti-espions) 8: (parles), (parents) 9: (informe)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 1. Ne surfe jamais sur Internet si ton ordinateur n'est pas protégé par un programme antivirus et anti-espion mis à jour. Ce serait comparable à une frontière sans garde-frontière, ton ordinateur pourrait être infecté par des programmes nuisibles tels que des virus, des chevaux de Troie, des vers ou des logiciels espions.

SITUATION 2. Sois attentif aux e-mails envoyés par des personnes que tu ne connais pas et qui contiennent des pièces jointes ou des e-mails qui promettent « monts et merveilles » – il s'agit très probablement de spams ! Le spam pourrait infecter ton ordinateur avec des programmes nuisibles tels que des virus, des chevaux de Troie, des vers ou des logiciels espions. N'ouvre pas ces e-mails. Bloque l'expéditeur en cliquant d'un clic droit de la souris sur le mail et en sélectionnant « bloquer l'expéditeur », ou supprime tout simplement ces messages.

SITUATION 3. Si tu cherches des informations sur Internet, ne fais pas confiance à la première bonne page que tu trouves. Consulte au moins trois sites différents et compare les informations que tu trouves. Rappelle-toi : tout le monde ayant accès à Internet peut y créer et y publier des informations.
Si tu prépares un exposé ou que tu rédiges un devoir, tu dois toujours mentionner la source des informations et des illustrations que tu as utilisées…, voilà comment un vrai scientifique procèderait.

2. La communication

COMMENTAIRES SUR LES ACTIVITÉS

Indique à quel point tu considères les renseignements suivants comme privés: ton numéro de téléphone, ta couleur de cheveux, ton nom, le pays dans lequel tu habites, le nom de ton école, ton adresse, le nom de ton animal domestique, la profession de tes parents, ton adresse e-mail, tes photos, ton âge.

Est-ce que vos enfants ont la même perception de la confidentialité que vous ? Les trois couleurs représentent « très privé » (rouge), « assez privé » (orange) et « moins privé » (vert).

Aide Claire à créer un super mot de passe en suivant les conseils de Laura.

Les bons mots de passe contiennent une série aléatoire de différents caractères (chiffres, lettres et signes de ponctuation) et doivent toujours être gardés secrets.

Suis l'exemple de Claire et crée un profil sûr. Crée ensuite un exemple de profil dangereux.

Laissez vos enfants créer un profil sûr et ensuite un profil qui l'est moins révélant des informations privées. Rappelez-leur que la création d'un profil sûr ne les protège pas s'ils ne continuent pas à protéger leur vie privée lors de leurs communications en ligne.

Analyse cette photo en détail et note ce que tu peux dire de cette personne.

Quelles informations personnelles peuvent être déduites d'une photo ? Les enfants ne se rendent souvent pas compte du pouvoir des images.

Suis l'idée de Claire et trouve trois conseils que « Pit, le petit chaperon rouge », pourrait recevoir de Laura pour se protéger contre les « loups du Web ».

Vérifiez si vos enfants se rendent compte que le contact avec des étrangers en ligne peut comporter des risques.

Comment aimerais-tu être traité par les gens en ligne? (1….. 2….. 3…..)

Assurez-vous que vos enfants comprennent qu'ils doivent traiter les autres comme ils aimeraient être traités eux-mêmes…

DECHIFFRE LE CODE: Trouve le sens des acronymes de chat les plus fréquents en les reliant à leur signification:

Améliorez votre compréhension des acronymes en consultant le chapitre Communication – Netiquette, langage de chat.

Utilise des combinaisons de touches pour représenter les émoticones suivantes : Un smiley - Un visage triste - Un clin d'œil - Un visage surpris - Un grand sourire - Une langue tirée.

Voir le chapitre Communication/Netiquette, langage de chat pour plus d'informations.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (profil) 2: (vie privée), (responsable) 3: (personnes que tu ne connais pas), (informes-en) 4:(netiquette), (traité) 5: (émoticone) 6: (mot de passe), (ponctuation) 7: (secret) 8: (refuse) 9: (connais).

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 4. Lorsque tu utilises Internet, ton profil ou les informations que tu révèles peuvent atteindre des dizaines, des centaines, des milliers et même des millions de personnes. Voilà pourquoi il faut choisir prudemment les informations que tu veux bien révéler sur ta personne. Ne donne des informations personnelles qu'aux personnes auxquelles tu fais confiance et que tu connais déjà bien hors ligne.

SITUATION 5. Michel a probablement donné son mot de passe à son copain qui a décidé de se venger en envoyant des e-mails insultants de sa part. Garde toujours tes mots de passe pour toi, sauf si ça ne te dérange pas que d'autres personnes lisent tes e-mails ou se fassent passer pour toi pour dire des choses que tu ne dirais pas!

SITUATION 6. Rencontrer un inconnu n'est pas une bonne idée. Mais si tu penses vraiment pouvoir faire confiance à un ami en ligne qui veut te rencontrer, informes-en tes parents pour qu'ils puissent t'accompagner. Aucun véritable ami ayant de bonnes intentions n'y verra d'inconvénient. Cela ne posera problème qu'aux personnes ayant quelque chose à cacher.

3. Cyber-harcelement

COMMENTAIRES SUR LES ACTIVITÉS

Dessine une image de l'invitation que Pit a reçue de ses enseignants. Imagine le logo et le slogan contre le harcèlement que l'école utilisera pour la semaine « anti-harcèlement ».

Laissez libre cours à la créativité de vos enfants et laissez-les dessiner dans le cadre vide.

Suis l'exemple de Pit et indique cinq raisons pour lesquelles tu donnerais un « carton rouge » à quelqu'un.

Discutez avec vos enfants des genres de comportement qu'ils trouvent inacceptables.

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (correctement), (gâchent) 2: (parle) 3: (BONNE) 4: (cyber-harcèlement) 5: (bloque) 6: (connais) 7: (répondrais)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 7. Ce n'est vraiment pas une façon appropriée d'utiliser ton téléphone portable. Ne transmets pas de messages, d'images ni d'autres documents pouvant blesser un tiers. Traite toujours les autres comme tu aimerais être traité toi-même. Dans une telle situation, parles-en à tes parents ou à un adulte de confiance.

SITUATION 8. Pit doit dire à son ami qu'il ne peut rien au mauvais comportement du tyran. Il ne doit pas répondre aux messages du tyran, mais les garder comme preuves et les montrer à ses parents ou à ses enseignants. Pit doit également parler avec ses parents, qui peuvent l'aider à soutenir son ami.

SITUATION 9. La netiquette indique que tu dois traiter les autres sur le Web comme tu aimerais être traité toi-même. Tu en as certainement appris assez sur ce sujet pour aider Claire.

4. Divertissements & Telechargements

COMMENTAIRES SUR LES ACTIVITÉS

Ouvre ton moteur de recherche préféré. Tape « sonneries gratuites » ou « jeux gratuits » et jette un coup d'œil sur les résultats. Analyse quelques sites Web. Peux-tu en détecter les pièges?

Entraînez-vous en effectuant une recherche avec les mots-clés indiqués et cherchez des pièges de marketing sur les sites Web que vous trouvez. Vous verrez comment l'information en petits caractères est omise des slogans de publicité.

Quel est ton jeu d'ordinateur préféré ? Vérifie si tes parents le connaissent et peuvent le décrire. S'ils n'ont aucune idée, explique-le leur d'abord et demande-leur ensuite d'en faire une petite description. Est-ce qu'ils ont réussi ? Combien de points leur donnerais-tu sur dix ? …/10 Un des parents décrit le jeu préféré de l'enfant. L'enfant dessine une image du jeu.

Savez-vous vraiment à quel genre de jeux vos enfants jouent en ligne et connaissez-vous leur jeu préféré? Laissez-les vous tester !

AS-TU TROUVÉ LA BONNE RÉPONSE?

1: (gratuits) 2: (formulaires) 3: (pièges) 4: (illégales) 5: (croix) 6: (ignorer) 7: (vie privée) 8: (partager), (toi-même) 9: (télécharge)

SOLUTIONS PROPOSÉES POUR LES CARTES DE SITUATION

SITUATION 10. La plupart des chansons et des films disponibles sur Internet sont des copies illégales. En outre, les sites Web sur lesquels des chansons et films sont partagés contiennent habituellement un grand nombre de programmes nuisibles tels que des virus, des chevaux de Troie, des vers et des logiciels espions. La meilleure solution pour Claire serait l'option b) ou c). Le téléchargement de sa chanson préférée sur un site fiable et légal lui coûtera bien sûr moins cher que l'achat du CD entier. Claire doit demander l'avis et la permission de ses parents.

SITUATION 11. Il existe des services gratuits sur Internet, mais les sonneries, les fonds d'écran, les mp3, les avatars et autres le sont rarement. Si Pit y regarde de plus près, il découvrira sans doute de petits caractères révélant les frais réels de ces services. Les sonneries, les jeux en ligne, etc. sont tous d'excellents moyens d'inciter les gens à s'abonner à des services soi-disant « gratuits », mais qui leur coûteront en réalité de l'argent.

SITUATION 12. Pit doit se rappeler de garder son identité cachée quand il joue en ligne avec des partenaires qu'il ne connaît pas dans la vie concrète. Il ne doit pas révéler d'informations concernant son nom de famille, son adresse ou son école, etc. Il doit aussi informer ses parents des jeux auxquels il joue en ligne et ne doit jamais télécharger un jeu sur Internet sans d'abord demander leur permission, parce que leur ordinateur pourrait être endommagé.

D. Glossaire

Abonner: s'enregistrer volontairement à un service (service de nouvelles) qui envoie directement des informations dans votre boîte de réception personnelle.

Acronyme: abréviation constituée des premières lettres de chaque mot d'une phrase ou d'une expression. Les acronymes sont souvent utilisés par les chatteurs pour communiquer plus rapidement, p. ex. LoL, @+, BIZ (voir le chapitre sur la Communication).

Adresse e-mail: lieu virtuel vers lequel les messages e-mail peuvent être envoyés. Les adresses e-mail se composent de deux parties séparées par le symbole @.

Alerte: une petite boîte apparaît à l'écran pour donner des informations ou vous avertir d'un processus potentiellement nuisible, p. ex. l'arrivée d'un nouveau mail ou l'état de votre protection antivirus.

Anti-espion: programme qui lutte contre les logiciels espions. Le programme scanne toutes les données entrantes pour détecter les logiciels espions et bloque les menaces trouvées, ou fournit une liste d'entrées suspectes à supprimer.

Antivirus: programme informatique tentant d'identifier, d'isoler, d'obstruer et d'éliminer les virus informatiques et autres logiciels malveillants. L'antivirus scanne d'abord les fichiers pour chercher les virus connus et identifie ensuite les comportements suspects des programmes informatiques qui indiquent une infection.

Auteur: créateur d'une œuvre littéraire ou audiovisuelle, d'un logiciel, etc. Les droits d'auteur protègent les créations des auteurs contre la reproduction illégale.

Avatar: profil d'un utilisateur représenté par un nom d'utilisateur et une image, une icône

ou un personnage 3D dans les jeux d'ordinateur en ligne et les mondes virtuels.

Barre d'outils: série d'icônes ou de boutons qui font partie de l'interface du programme d'un logiciel. La barre d'outils sert d'interface en étant toujours disponible et facile à utiliser pour effectuer les fonctions courantes.

Blog: abréviation de weblog : site Web pour lequel un individu ou un groupe génère du contenu, normalement tous les jours, consistant en des textes, des images, des fichiers audiovisuels et des liens.

Blogging: fait d'écrire ou de mettre à jour votre blog.

CD-ROM: acronyme de « Compact Disc read-only memory ». Il s'agit d'un disque compact non enregistrable contenant des données lisibles par un ordinateur. Les CD-ROM sont très appréciés pour la distribution de logiciels informatiques.

Chat: communication synchrone par Internet à l'aide de messages écrits, en utilisant des applications de chat et de messagerie instantanée (p. ex. MSN).

Cheval de Troie: code malicieux, logiciel malveillant qui peut entrer dans votre ordinateur par le biais de procédures semblant inoffensives, comme des jeux ou même des programmes de recherche de virus. Les chevaux de Troie ne se multiplient pas d'eux-mêmes mais sont normalement créés pour accéder à des données délicates ou pour détruire des données, ils peuvent effacer les informations d'un disque dur ou voler des informations confidentielles.

Clé mémoire/USB: appareil de stockage de données pourvu d'un connecteur USB (universal serial bus). Une clé mémoire est normalement petite, légère, amovible et réinscriptible.

Compte: un compte vous permet d'être authentifié et autorisé à utiliser les services en ligne grâce à un nom d'utilisateur et à un mot de passe. Vous pouvez utiliser votre système d'exploitation pour créer des comptes d'utilisateur séparés pour chaque membre de la famille.

Connexion Internet: fait référence au moyen grâce auquel les utilisateurs se connectent à Internet. Les méthodes courantes d'accès à Internet incluent la connexion via une ligne téléphonique, des T-Lines, un Wi-Fi, un satellite et des téléphones portables.

Contenu illégal: un contenu en ligne illégal viole la législation nationale. Les contenus les plus courants de ce genre sont des images d'abus sexuel sur enfants, des activités illégales dans les salons de chat, la haine en ligne et les sites Web xénophobes.

Contenus pernicieux: images, textes, documents, etc. dont le contenu peut causer des dommages, p. ex. des images montrant de la violence sont inappropriées et pernicieuses pour les enfants et les adolescents.

Contrôle parental: voir définition des paramètres de famille.

Cookies: fichier placé dans votre navigateur par un site Web. Chaque fois que vous accédez à nouveau au site Web, le cookie est renvoyé au serveur sur lequel le site Web est stocké. Les cookies témoignent de vos préférences en matière de sites et sont utilisés par des établissements de vente en ligne. Le rejet de cookies peut rendre certains sites Web inutilisables.

Corbeille: répertoire informatique dans lequel des fichiers supprimés sont temporairement

stockés avant que les utilisateurs ne les suppriment définitivement. Vous devez régulièrement supprimer les anciennes données non désirées de la corbeille pour libérer de la place sur le disque dur, la mémoire interne de votre ordinateur.

Cracker (n.m): personne qui accède illégalement à des systèmes informatiques.

Cracker (v): copier illégalement des logiciels commerciaux en violant les droits d'auteur.

Cyber-harcèlement: fait référence au harcèlement par les médias électroniques, normalement par l'envoi de messages instantanés et d'e-mails. Il peut inclure des attaques, des menaces, des remarques sexuelles et des paroles péjoratives. Les cyber-tyrans publient par exemple des informations personnelles sur leurs victimes, ils usurpent même leur identité pour publier des documents à leur nom dans l'objectif de les diffamer ou de les ridiculiser.

Données personnelles: toute information pouvant être liée à une personne. Si des données personnelles doivent être recueillies, traitées et stockées, les raisons doivent être explicitement déclarées.

Dossier: entité dans un système de fichiers qui contient un groupe de fichiers et/ou d'autres répertoires. Les dossiers peuvent contenir une multitude de documents et sont utilisés pour organiser les informations.

Dossier junk/spam: dans une boîte e-mail, l'endroit où les mails considérés comme spam ou junk sont stockés.

Droits d'auteur: série de droits exclusifs réglant l'utilisation d'une idée, d'un travail ou d'informations. Les droits d'auteur sont représentés par le symbole « © ».

E-mail: moyen de communication écrite et électronique qui permet d'envoyer des messages accompagnés de tout type de fichier informatique en pièce jointe – texte, image, audio et autres.

Emoticone: image - icône - utilisée pour exprimer des sentiments et des émotions, p. ex un smiley. Elle peut être symbolisée en utilisant des caractères standards de clavier et des signes de ponctuation, ou en utilisant des caractères préétablis et proposés par les salons de chat, les salons de jeux, les services de messagerie instantanée, les téléphones portables, etc.

Favoris: fichier du navigateur à personnaliser pour sauvegarder les liens/signets. Les signets peuvent être organisés dans des sous-dossiers et/ou marqués par un mot-clé pour faciliter la recherche.

Fenêtre pop-up: fenêtre qui apparaît soudain lors d'une visite sur un site Web ou en appuyant sur une touche spéciale. D'habitude, la fenêtre pop-up contient un menu d'options et reste sur l'écran jusqu'à ce qu'on sélectionne l'une des options ou qu'on la ferme en cliquant sur la croix située dans le coin supérieur droit.

Fichier informatique: archive/collection d'informations liées (documents, programmes, etc.) enregistrée sur un ordinateur sous son propre nom de fichier. Les fichiers d'ordinateur peuvent être considérés comme l'homologue moderne des documents papier qui étaient conservés dans les dossiers de bureau et les bibliothèques.

Filtre: application réglant l'accès aux informations ou aux services spécifiques d'Internet,

vous avertissant des sites Web problématiques, retenant la navigation de l'utilisateur, bloquant les sites Web à risque et pouvant même éteindre l'ordinateur. Les systèmes de filtrage sont installés sur des ordinateurs individuels, des serveurs, des téléphones avec accès à Internet, etc.

Filtre anti-spam: application bloquant les messages de spam de façon à ce qu'ils n'arrivent pas dans votre boîte de réception.

Flaming: interaction hostile et insultante entre des utilisateurs d'Internet. Cela a normalement lieu dans des forums de discussion, dans la discussion relayée par Internet (Internet Relay Chat – IRC) ou même par e-mail.

Fond d'écran: dessin, image ou autre représentation graphique qui forme l'arrière-plan de l'écran d'ordinateur.

Formulaire (formulaire en ligne): document formaté contenant des champs vides pour vous permettre d'y entrer des données. La forme électronique peut être remplie avec des textes libres ou en choisissant des alternatives dans des listes préétablies (liste déroulante). Après l'envoi, les données sont directement envoyées à une application de traitement qui entre les informations dans une base de données.

Forum: groupe de discussion en ligne où les participants ayant des centres d'intérêt communs peuvent ouvertement échanger des messages sur des sujets divers.

Groupe de nouvelles: voir définition du forum.

Hacker: terme populaire pour designer une personne qui s'adonne au cracking informatique (voir « cracker »). Est parfois utilisé dans les cercles informatiques pour désigner une personne passionnée par les ordinateurs.

Harcèlement: attaques, menaces, remarques sexuelles, paroles péjoratives et assauts physiques perpétrés par un ou plusieurs tyrans.

Inscription: abonnement à un service en ligne: newsletter, forum de discussion, e-mail, plate-forme de chat, etc. Normalement, les utilisateurs devraient avoir la possibilité de se désinscrire à tout moment.

Internet: réseau mondial de réseaux d'ordinateurs interconnectés, publiquement accessible, permettant la transmission et l'échange de données. Il comprend des réseaux académiques, commerciaux et gouvernementaux ainsi que des réseaux domestiques plus petits proposant de nombreux services tels que l'information, les e-mails, le chat en ligne, le transfert de fichiers, etc.

Jeux en ligne massivement multijoueurs: jeux proposant un vaste monde 3D, peuplé de milliers de joueurs jouant des rôles à caractère fictif et se faisant concurrence. Les jeux de rôle, où les participants créent ou suivent ensemble une histoire, dominent cette catégorie.

Jeu numérique: jeu créé par des concepteurs de jeux et joué sur un ordinateur. Un jeu en ligne est défini comme étant un jeu numérique nécessitant une connexion réseau directe pour pouvoir être utilisé. Les jeux en ligne peuvent soutenir l'interaction entre une multitude de joueurs.

Junk mail: messages e-mail non désirés, quasi identiques, qui sont envoyés aux adresses e-mail de plusieurs personnes. Étant donné qu'Internet est public, le junk mail et le spam

sont difficiles à éviter.

Lien: référence à un document disponible en ligne (page Web, document écrit, image, etc). Lorsque vous cliquez sur le lien, vous êtes dirigé vers une nouvelle page ou un autre site Web. Les liens écrits sont normalement bleus et soulignés, mais ils peuvent également être d'une autre couleur et non soulignés. Des images peuvent aussi servir de liens vers d'autres pages Web.

Logiciel: voir définition du programme informatique.

Logiciel d'essai: logiciel que vous pouvez essayer avant de l'acheter. Les versions d'essai de logiciels contiennent normalement toutes les fonctions de la version normale, mais ne peuvent être utilisées que pendant une période limitée.

Logiciel espion: logiciel malveillant secrètement attaché à un fichier téléchargé

d'Internet qui s'installe de lui-même sur le PC et en surveille l'activité. Il envoie des informations à un tiers, souvent des entreprises tâchant d'établir des profils personnels pour envoyer des publicités ou d'autres informations, ou des crackers qui souhaitent accéder à des données privées.

Logiciel gratuit et logiciel partagé: en général, les logiciels sont protégés par les droits d'auteur et ne peuvent donc pas être téléchargés. Un logiciel gratuit est un logiciel dont le détenteur des droits accepte qu'il soit utilisé sans frais par tout le monde. Un logiciel partagé est un logiciel dont le détenteur des droits accepte qu'il soit utilisé par tout le monde pendant une période d'essai. Après cette période, l'utilisateur doit payer une redevance pour continuer à utiliser le service.

Liste de contacts: collection de contacts dans un programme de messagerie instantanée et d'e-mail, dans les jeux en ligne, sur les téléphones portables, etc. Des contacts peuvent être ajoutés, refusés ou supprimés.

Matériel hardware: partie physique d'un ordinateur, contrairement au logiciel, qui agit au sein du matériel hardware. Le hardware peut se trouver à l'intérieur : cartes mères, disques durs et mémoire vive (RAM) – souvent désignés comme composants ; ou à l'extérieur : écrans, claviers, imprimantes, etc. – également appelés périphériques.

Malware: abréviation anglaise de logiciel malveillant, c'est-à-dire un logiciel créé dans le but de s'infiltrer ou d'endommager un système informatique sans l'accord du propriétaire. En font partie les virus informatiques, les vers, les chevaux de Troie, les logiciels espions, les logiciels gratuits malhonnêtes (publiciels) et d'autres logiciels malveillants et non désirés.

Messagerie instantanée (MI): forme de communication instantanée et simultanée entre deux utilisateurs ou plus. MI vous permet de communiquer avec une liste sélectionnée de contacts. Lorsque les personnes de votre liste de contacts sont en ligne, vous êtes immédiatement avertis.

Mobile: appareil de télécommunication électronique, également connu sous les noms de téléphone portable, téléphone cellulaire, GSM, smartphone. Il dispose des mêmes fonctions de base qu'un téléphone fixe normal. Aujourd'hui, la plupart des téléphones portables disposent d'un appareil photo et un bon nombre propose l'accès à Internet (service payant).

Modifier: processus de modification d'une image, d'un fichier, d'une photo ou d'une il-

lustration d'une façon apparente ou non. De nos jours, il existe un grand nombre d'outils pouvant être utilisés pour influencer le contenu ou la forme des données et pour créer un résultat ne correspondant pas à la réalité.

Mot de passe: série de caractères secrets permettant à leur propriétaire d'accéder à un fichier, à un ordinateur, à un compte ou à un programme ; il s'agit d'une mesure de sécurité contre les utilisateurs non autorisés (voir chapitre sur la communication).

Moteur de recherche: outil utilisé pour rechercher des informations contenues sur un site Web. Les plus connus sont Google et MSN Search. Des moteurs de recherche disposent de préférences d'utilisateurs avancées qui peuvent inclure des paramètres de sécurité intéressants.

Mp3: format de codage spécifiquement audio. La taille d'un fichier mp3 correspond à un dixième de celle du fichier audio original, mais le son a presque la qualité de celui d'un CD. En raison de leur taille réduite et de leur haute fidélité, les fichiers mp3 sont devenus populaires pour sauvegarder des fichiers de musique sur les ordinateurs et les appareils portables.

Navigateur: programme utilisé pour visualiser des sites Web. Internet Explorer, Netscape Navigator et Firefox sont trois des navigateurs les plus utilisés pour Windows, Safari est fréquemment utilisé sur les Mac. La plupart des versions récentes des navigateurs offrent des options de contrôle parental.

Naviguer: fait d'utiliser le navigateur pour visualiser des sites Web ou surfer sur le net.

Net: abréviation d'Internet.

Netiquette: étiquette d'Internet qui établit les règles de politesse des communautés en ligne.

Nom d'écran: voir définition du surnom.

Page d'accueil: il s'agit de la page Web qui se charge automatiquement lorsque le navigateur démarre. Le terme est également utilisé pour désigner la première page ou la page principale d'un site Web (voir définition).

Paramètres de famille: aussi appelés contrôle parental : paramètres utilisés pour personnaliser un navigateur ou un autre outil du Web, en vue de le rendre plus adapté aux enfants par l'utilisation d'options telles que le filtrage du contenu, la limitation du temps, le contrôle des jeux, etc.

Paramètres de protection des données: série de détails privés spécifiques au compte que vous pouvez éditer de façon à augmenter la protection des données contre la révélation d'informations personnelles, les cookies, etc.

Paramètres de sécurité (profil): série d'options de sécurité à personnaliser qui est liée à votre profil en ligne (voir définition). D'habitude, ces options sont liées à l'ouverture d'images et de fichiers, à l'identification de fournisseurs d'information de confiance et au niveau de permission pour les contenus adultes.

Pare-feu: partie du matériel hardware (intégré dans votre routeur) ou logiciel (installé sur votre ordinateur) configuré en vue d'empêcher les utilisateurs non autorisés (hackers et crackers) d'accéder à l'ordinateur ou à un réseau d'ordinateurs connectés à Internet.

Partage de fichiers: échange en ligne de fichiers entre des utilisateurs d'ordinateur. Le terme couvre aussi bien le fait d'offrir des fichiers à d'autres utilisateurs (télécharger en amont) que celui de copier des fichiers sur Internet vers un ordinateur (télécharger en aval). Les fichiers sont normalement partagés à travers des réseaux P2P (peer-to-peer).

Pièce jointe: fichier informatique qui est envoyé en même temps qu'un message e-mail. Les vers et les virus sont souvent distribués sous forme de pièces jointes aux e-mails. Les e-mails avec pièces jointes provenant d'expéditeurs inconnus doivent être considérés comme suspects.

Possession virtuelle: série d'objets que chaque joueur d'un jeu reçoit. Chaque joueur les possède virtuellement par le biais d'un terminal informatique montrant ces objets.

Pornographie enfantine: la pornographie enfantine a des définitions légales différentes dans les différents pays. Au minimum, la pornographie enfantine est définie comme étant une image montrant une personne - un enfant – se livrant à des activités explicitement sexuelles ou étant représentée de façon à donner cette impression.

Port: interface sur un ordinateur utilisée pour le connecter à un autre appareil. Les ports peuvent être internes ou externes. Les ports internes établissent une connexion avec un lecteur de disque ou un réseau, tandis que les ports externes se connectent à un appareil périphérique comme une imprimante ou un clavier.

Privé: informations sur un individu ou un groupe qui ne sont pas révélées au public. Quand quelque chose est considéré comme privé pour quelqu'un, c'est généralement considéré comme étant personnel.

Processeur: ou unité centrale de traitement (Central Processing Unit - CPU). C'est la partie d'un ordinateur qui traite les données, génère les signaux de contrôle et stocke les résultats. Avec la mémoire de l'ordinateur, elle en forme la partie centrale.

Profil: informations personnelles des utilisateurs se trouvant sur des sites de réseau social, des systèmes de messagerie instantanée, des applications de chat en ligne, des jeux en ligne, etc. Les profils peuvent être publics ou privés et sont personnalisés par les utilisateurs pour représenter leur personne dans des environnements virtuels.

Profil d'utilisateur: série d'informations décrivant l'utilisateur spécifique d'un logiciel, d'un site Web ou d'un autre outil technique. Typiquement, il inclut des informations telles que le nom d'utilisateur, le mot de passe et d'autres détails (p. ex. la date de naissance, les centres d'intérêt).

Programme informatique: normalement appelé logiciel. Le logiciel se compose d'une séquence structurée d'instructions écrites par des programmeurs informatiques et permettant à l'ordinateur d'effectuer des tâches. Lorsque vous achetez un logiciel, il se trouve souvent sur un CD-ROM (voir définition), un moyen physique de stocker les programmes.

Protection des données: possibilité pour un individu ou un groupe de contrôler le flux d'informations sur leur personne et de ne se révéler que sélectivement. La protection des données est parfois liée à l'anonymat, au souhait de passer inaperçu dans le monde public.

Répertoire: unité d'organisation que votre ordinateur utilise pour classer les dossiers et les fichiers dans une structure hiérarchique, p. ex. Mes Documents, Mes images, etc.

Réseau P2P: un réseau peer-to-peer (P2P) permet à ceux qui y sont connectés d'échanger

des fichiers par le téléchargement en amont et en aval (voir définition). Il ne s'agit que d'une des façons de partager des fichiers sur Internet. Certains services de partage de fichiers sont illégaux.

Réseau social: communautés de membres en ligne partageant des centres d'intérêt et des activités, qui se contactent et se fréquentent en ligne en utilisant des logiciels et des services appropriés (voir sites de réseau social).

Salon de chat: lieu public virtuel destiné à la communication en temps réel. Des personnes de par le monde entier peuvent se rencontrer dans les salons de chat et discuter à l'aide de messages qu'elles tapent sur leur clavier. Si vos enfants utilisent des salons de chat, assurez-vous qu'ils sont adaptés à leur âge et qu'il y a des surveillants et des modérateurs.

Scanner: action ou processus consistant à convertir du matériel imprimé en fichier numérique en utilisant un scanner. Cette conversion vous permet de visualiser ces documents sous forme de fichiers électroniques sur votre ordinateur et de les distribuer en ligne.

Second Life: communauté 3D, bien connue sur le Web, mise à disposition par une entreprise implantée aux Etats-Unis, Linden Labs. Les utilisateurs peuvent se contacter virtuellement à l'aide d'un avatar (voir définition), créer des maisons et de nombreux environnements, échanger et gagner de l'argent virtuel, etc.

Service d'assistance: service assuré par e-mail et parfois par téléphone. Les enfants peuvent y formuler leurs problèmes, souvent liés à des contenus illégaux et pernicieux ou des expériences désagréables ou effrayantes relatives à leur utilisation des technologies en ligne.

Service d'assistance téléphonique: service d'assistance téléphonique ou service basé sur le Web qui permet de signaler des contenus supposés illégaux et/ou une utilisation illégale d'Internet. Les services d'assistance téléphoniques sont tenus de mettre en place des procédures transparentes et efficaces pour traiter les plaintes et s'assurer du soutien du gouvernement, de l'industrie, des agences de maintien de l'ordre et des utilisateurs d'Internet dans les pays concernés.

Signaler: fonction qui permet aux utilisateurs des lieux virtuels publics de signaler un problème (technique, comportement inacceptable d'un utilisateur, contenu illégal, etc.) à un modérateur ou au webmaster.

SIP-Bench: enquête soutenue par la Commission européenne ayant testé 30 outils de contrôle et d'anti-spam afin d'évaluer leur efficacité à protéger les enfants contre les contenus pernicieux sur Internet.

Site Web: emplacement sur le World Wide Web. Chaque site Web contient une page d'accueil, le premier document que l'on voit en entrant sur le site. Les sites contiennent normalement des liens vers d'autres fichiers et sites. Les sites Web appartiennent à des individus, des entreprises ou des organisations et sont gérés par ceux-ci.

Sites de réseau social: plates-formes virtuelles abritant des communautés de membres partageant les mêmes centres d'intérêt et activités. Les membres doivent créer des profils d'utilisateur et peuvent partager des outils pour télécharger des textes, des images ou d'autres fichiers, publier des messages et participer à des forums. De nombreux sites de réseau social sont interdits aux enfants de moins de 13 ans et offrent des paramètres de sécurité pour les profils.

Sonnerie: son d'un téléphone portable pour les appels entrants. Une grande variété de sons

et de musique à personnaliser est disponible pour les propriétaires de téléphones portables; ceux-ci peuvent les télécharger, souvent contre paiement, et les utiliser.

Surnom: synonyme de nom d'écran ou pseudonyme. Il représente l'utilisateur d'un service en ligne et est choisi par l'utilisateur lui-même. Il représente les utilisateurs dans les listes de contacts, les salons de chat, etc. Les surnoms peuvent protéger votre anonymat en ligne s'ils sont bien choisis.

Spam: e-mail non désiré, normalement de nature commerciale, envoyé en masse. L'envoi de spam à d'autres personnes est certainement l'une des violations les plus célèbres d'Internet.

Système d'exploitation: programme faisant marcher les fonctions de base d'un ordinateur et permettant à d'autres programmes de tourner. Des exemples bien connus sont Windows, Linux et Mac OS.

Téléchargement: fait référence au processus consistant à copier un fichier d'un service en ligne vers un ordinateur.

Transfert de fichiers: fait de transmettre des fichiers par un réseau informatique. Du point de vue de l'utilisateur, le transfert de fichiers est souvent désigné comme téléchargement en amont ou en aval.

URL (Uniform Resource Locator - localisateur uniforme de ressource): adresse d'un site Web ou d'un fichier spécifique sur Internet. Elle ne contient pas de caractères spéciaux ni d'espaces et utilise des barres obliques pour dénoter les différents répertoires. La première partie de l'adresse indique le protocole à utiliser, la deuxième partie spécifie l'adresse IP ou le nom du domaine où la ressource se trouve.

Vers: type spécial de virus qui se renouvelle de lui-même et peut se propager sans l'intervention du propriétaire de l'ordinateur vers un grand nombre d'ordinateurs ; il peut endommager un réseau, consommer des largeurs de bande énormes, éteindre un ordinateur, etc.

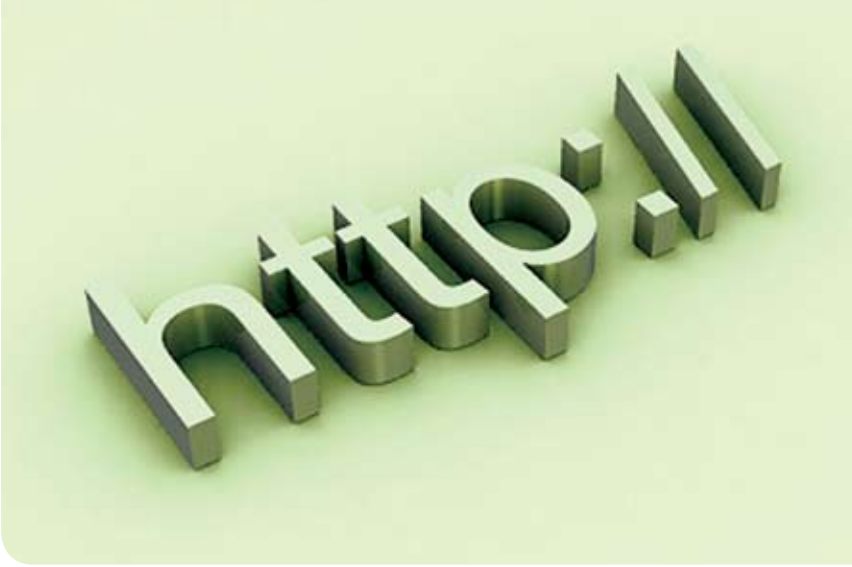
Virus: type de code malicieux, logiciel malveillant créé pour se propager à l'aide de l'intervention des utilisateurs. D'habitude, il se propage par les pièces jointes aux e-mails, mais également par des outils de mémoire externes infectés (clé USB, CD-ROM).

Voix sur réseau IP (VoIP): technologie permettant aux utilisateurs de parler par Internet, souvent après avoir téléchargé un logiciel client. Les appels sont gratuits pour les utilisateurs qui s'appellent avec le même logiciel client VoIP (p. ex. Skype, Voicebuster). De tels logiciels offrent normalement aussi des possibilités de chat et de partage de fichiers.

Vol d'identité: vol d'informations personnelles (p. ex. nom, date de naissance, numéro de carte de crédit) et fait de les utiliser illégalement.

Web: abréviation de World Wide Web : une collection de documents en ligne formatés en HTML (HyperText Markup Language), qui contient des liens vers d'autres documents, des graphiques, des fichiers audio et vidéo. Le Web est une partie d'Internet.

Webcam: caméra qui peut diffuser à travers le Web, dans un système de messagerie instantanée, des applications de conférence vidéo sur ordinateur, des plates-formes de chat, etc. Les caméras ayant accès au Web incluent une caméra numérique qui télécharge des images vers un serveur du Web, en continu ou à intervalles réguliers.



E. ADRESSES UTILES

BEE SECURE – LE CENTRE DE SENSIBILISATION LUXEMBOURGEOISE

BEE SECURE est un projet visant à la promotion un usage plus sûr d'Internet et des nouvelles technologies de la communication par les jeunes. *www.bee-secure.lu*

BEE SECURE-HELPLINE

La BEE SECURE-Helpline offre la possibilité aux enfants, aux jeunes, aux parents ou à toute personne qui s'y adresse de s'informer ou de se faire conseiller personnellement pour toute question touchant l'utilisation de l'Internet ou du mobile. *www.bee-secure.lu*
help@bee-secure.lu ou par téléphone 26 64 05 44

LISA-STOPLINE

Le projet LISA Stopline a pour objectifs de fournir une structure de signalement anonyme des contenus illégaux rencontrés sur Internet, et de traiter ces signalements en collaboration avec les autorités compétentes au niveau national et international. *www.lisa-stopline.lu*

CASES

CASES, le portail luxembourgeois de la sécurité de l'information du Ministère de l'Economie et du Commerce extérieur, offre à l'utilisateur des nouveaux médias une multitude d'informations et de conseils pratiques concernant la sécurité technique et les comportements à adopter pour réduire les risques. *www.cases.lu*

KANNER-JUGENDTELEFON

Les enfants et les jeunes peuvent contacter KJT par téléphone ou par écrit sur le site internet pour toute question ou tout problème qui les tracasse. *www.12345kjt.lu*

AUTRES LIENS:

CEC – CENTRE EUROPÉEN DES CONSOMMATEURS

Le Centre Européen des Consommateurs GIE du Luxembourg a pour tâches d'informer, de conseiller et d'assister les consommateurs dans leurs activités de consommation trans-frontalière. Le consommateur trouvera notamment des lettres-types pour réagir en cas d'arnaque en ligne *www.cecluxembourg.lu*

ECOLE DES PARENTS JANUSZ KORCZAK

L'Ecole des Parents Janusz Korczak de la Fondation Kannerschlass propose des conférences et des séminaires pour les parents *www.kannerschlass.lu/eltereschoul*

ERWUESSEBILDUNG

Développement personnel et compétence médiatique sont les deux axes des activités du service Erwuessebildung. Celui-ci propose notamment des cours d'initiation aux nouveaux médias. *www.erwuessebildung.lu*

GUICHET UNIQUE

"De Guichet" élargit les possibilités d'accès aux administrations et aux services publics. Il permet au citoyen de s'informer et de réaliser ses démarches administratives par voie électronique. *www.guichet.lu*

INSAFE

Insafe coordonne le réseau européen des centres de sensibilisation nationaux. BEE SECURE est membre de Insafe. *www.saferinternet.org*

INHOPE

Inhope est le réseau mondial des sites de signalement de contenus illégaux sur Internet. Inhope a pour objectifs de promouvoir la mise en place de plateformes de signalement, de veiller à la qualité de ces services et de garantir l'efficacité et la rapidité de la lutte contre les contenus illégaux, en particulier les images d'abus sexuel sur enfants. La Lisa-Stopline est membre de INHOPE. *www.inhope.org*

LIFELONG LEARNING

Site dédié à la formation continue des adultes *www.lifelong-learning.lu*

MINISTÈRE DE LA FAMILLE ET DE L'INTÉGRATION, DIVISION IV – ENFANCE, FAMILLE ET JEUNESSE

www.mfi.public.lu

PORTAIL SANTÉ

Portail luxembourgeois d'information sur toutes les questions de santé *www.santé.public.lu*

SNJ – SERVICE NATIONAL DE LA JEUNESSE

Le Service National de la Jeunesse (SNJ) est une administration publique placée sous l'autorité du ministre en charge de la jeunesse. Le SNJ a été créé dans le but de soutenir les jeunes et les structures du secteur jeunesse au Luxembourg. *www.snj.lu*

Titre: Kit familial de sécurité en ligne • Créé par Insafe/Liberty Global-UPC en 2008
Préfixe: 9782959974 • Id 51950 • NUMERO ISBN 9782959974038 • EAN: 9782959974038