educa.Guides

Safersurfing
Sécurité sur les réseaux sociaux

En collaboration avec

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité

École et TIC

Mentions légales

Éditeur educa.ch
Auteur Prévention Suisse de la Criminalité www.skppsc.ch
Photos büro z {grafik design}, Berne

© educa.ch CC BY-NC-ND (creativecommons.org)
Novembre 2011

Prévention Suisse de la Criminalité → 4

Situation initiale → 6

Tchats → 6
Plateformes sociales → 7
Nouvelles règles de prévention → 7

Messages centraux → 8

Thèmes centraux → 12

Cyber-intimidation → 12
Abus sexuel sur Internet → 15
Cyberaddiction → 18

Ce guide dispose d'une page Internet sur educa.ch. Vous trouverez à cet endroit un fichier PDF du guide, que vous pouvez également consulter en ligne, ainsi que des informations complémentaires et des liens vers des sites proposant du matériel pédagogique. Ces informations et liens sont mis à jour régulièrement. La date de publication ainsi que celle d'une éventuelle actualisation sont indiquées sur le PDF.

→ Page Internet

Les « réseaux sociaux privés », également appelés « communautés en ligne », tels que Facebook, Netlog ou MySpace, sont très prisés autant par les adultes que par les adolescents. Ces sites proposent aux utilisateurs de créer des profils personnalisés, de discuter avec des amis, de nouer de nouveaux contacts et de former des communautés d'intérêt. Bien que toutes ces possibilités soient très intéressantes, elles comportent aussi certains risques.

Prévention Suisse de la Criminalité

Dans ce contexte, la Prévention Suisse de la Criminalité (PSC) et la rédaction d'educa.ch ont conçu un dossier consacré à la sécurité sur les réseaux sociaux. Ce dossier reprend les éléments principaux de la campagne en ligne de la PSC : « Netlog, Facebook & Co : sûr et certain ! ». Cette campagne s'adresse aux enfants, adolescents, parents et autres responsables de l'éducation.

Liens

→ Prévention Suisse de la Criminalité
→ « Netlog, Facebook & Co : sûr et certain ! »

Situation initiale

La campagne en ligne de la Prévention suisse de la criminalité (PSC) s'inscrit dans la continuité de la campagne Safersurfing de la PSC. Safersurfing contient des messages de prévention s'adressant aux enfants et aux adultes qui leur sont proches en vue d'améliorer la sécurité sur les tchats. Or aujourd'hui, les enfants et les adolescents utilisent de moins en moins les tchats et sont davantage présents sur les plateformes sociales (telles que Facebook, Netlog, Myspace, etc.).

Tchats

Les messages de prévention en relation avec les tchats reposent principalement sur les moyens de protection contre les abus sexuels commis sur des mineurs par des adultes qui les ont rencontré par Internet. L'objectif consiste à faire comprendre aux enfants et adolescents qu'ils doivent garder leur anonymat sur les tchats, qu'ils ne doivent ni envoyer de photos d'eux ni révéler des informations personnelles à des inconnus, et qu'ils apprennent à réagir adéquatement s'ils font une mauvaise expérience.

Plateformes sociales

Les plateformes sociales fonctionnent différemment des tchats. Les profils, pièces maîtresses des plateformes, doivent comporter un maximum d'informations et de photos. Les personnes ayant mis en ligne un profil veulent être reconnues, nouer de nouvelles amitiés et se présenter aux autres de la façon la plus originale possible pour se démarquer des autres.

Nouvelles règles de prévention

Dans le cadre du travail de prévention, les messages existants ont perdu leur impact. La simple protection contre les risques en gardant l'anonymat doit être remplacée par la gestion de ceux-ci grâce au renforcement des compétences médiatiques des internautes. Cette gestion doit faire référence à l'autoreprésentation, à la communication, et de manière plus générale, à la transmission des informations.

Lien
→ Safersurfing

Messages centraux

Plusieurs messages centraux sont au coeur de la campagne de la Prévention suisse de la criminalité. Un aspect important est celui du réglage des paramètres de sécurité sur les plateformes sociales en ligne en vue de protéger davantage les données personnelles.

L'Internet n'oublie jamais rien
Les enfants et adolescents doivent prendre conscience que les informations – principalement les fichiers images – qu'ils mettent en ligne ne pourront plus être effacées de la toile. Bien des années plus tard, elles seront toujours accessibles, et ce même quand les jeunes seront devenus adultes et ne voudront peut-être plus les défendre.

Les informations circulent et peuvent être transformées en un rien de temps
En règle générale, il est facile de copier, de déformer et de diffuser à grande échelle des données et des images qui ont été mises en ligne. L'auteur des informations perd ainsi le contrôle de ses données et se retrouve sans pouvoir intervenir ni sur leur diffusion ni sur leur utilisation.

L’expérience virtuelle est aussi une réalité
La frontière entre le monde virtuel et le monde réel est très claire dans certains domaines et plus obscure dans d’autres. Aujourd’hui, l’univers virtuel comporte aussi des informations et des photos de personnes bien vivantes et qui peuvent être consultées par un large public, bien réel lui-aussi. Les informations virtuelles peuvent donc entraîner des conséquences réelles, par exemple dans le cadre de nouvelles connaissances faites sur le Web et que l’on souhaite rencontrer dans la vraie vie. Les mesures de prévention habituelle, comme une saine méfiance, ne doivent donc pas être négligées dans le monde virtuel.

Sur Internet, on n’est jamais « rien qu’entre soi »
L’utilisation de l’internet dans une chambre offre une certaine forme d’intimité privée qui peut s’avérer particulièrement traitre. Les conversations dans les espaces publics des tchats peuvent être suivis par d’autres personnes. Les profils insuffisamment sécurisés postés sur les plateformes sociales peuvent être consultés, voire copiés pour être transformés ensuite. Dans les réseaux sociaux, les amis des amis des amis ne sont pas toujours des gens en qui on peut avoir confiance. Pourtant, c’est souvent ainsi qu’ils sont traités en ce qui concerne la divulgation d’informations.

Lien
→ Comment configurer les paramètres de sécurité sur facebook!

Safari
Ablage
Bearbeiten
http://www.facebo
facebook
Du
Verb
Besuch

arstellung Verlauf Lesezeichen Fenster Hilfe

Willkommen bei Facebook - anmelden, registrieren oder mehr erfahren

ok.com/index.php?lh=d97f9c55cec7f95c686f41f5541b1810

E-Mail

Passwort

Angemeldet bleiben

ziehst weiter? Bleibe in
indung
ne facebook.com auf deinem Handy.

Hol dir Facebook-Handy

Registrieren

Facebook ist und bleibt ko

Vorname:

Nachname:

Deine E-Mail:

E-Mail nochmals eingeben:

Neues Passwort:

Ich bin:

Thèmes centraux

Dans sa campagne, la Prévention suisse de la criminalité associe les quatre messages centraux – traités dans le chapitre précédent – à des thèmes concrets en matière de criminalité. Si l'internaute ne tient pas compte des messages centraux, il s'expose directement ou indirectement à la cyber-intimidation, aux abus sexuels et aux problèmes d'addiction.

Cyber-intimidation

On parle de cyber-intimidation (ou cybermobbing) si, pendant un certain temps, une personne se fait importuner, brimer, harceler, voire carrément terroriser sur Internet par d'autres personnes, pour la plupart des enfants et des adolescents. La méthode de cyber-mobbing la plus fréquemment rencontrée est la suivante : la victime est harcelée et humiliée par autrui qui diffuse des photos ou des vidéos gênantes et osées, voire des informations blessantes sur le Web ou les envoie par SMS ou MMS sur les téléphones portables. De même, des profils falsifiés sur des sites sociaux ou communautaires peuvent embarrasser les victimes et leur créer des ennuis considérables.

Prévenir

La PSC propose quelques conseils aux parents sur comment réduire au maximum le risque pour que leur enfant ne devienne pas victime de cyber-intimidation :

- Expliquez à votre enfant ce qui peut arriver avec les informations le concernant diffusées sur l'Internet. La plupart des enfants et des adolescents sont particulièrement insouciants en ce qui concerne les informations personnelles sur le Web ; ils les révèlent facilement et mettent des photos en ligne. Ils ne réalisent pas suffisamment que ces informations peuvent être consultées par un très grand nombre de personnes, dont font aussi partie des personnes malintentionnées.
- Même si votre enfant n'est pas victime d'une cyber-intimidation, il est important d'en discuter avec lui. Faites-lui savoir qu'il n'est pas impuissant si cela devait lui arriver. En se défendant et en se confiant à autrui, il a plus de chances de mettre l'auteur des faits devant ses responsabilités. Il faut qu'il sache que les malfaiteurs laissent toujours des traces qui permettent ensuite de les identifier.
- Encouragez votre enfant pour qu'il se confie à vous. De temps à autre, demandez à votre enfant comment ça se passe avec ses contacts virtuels. Restez vigilants si vous remarquez que son comportement change : si votre enfant se renferme sur lui ou ne raconte plus rien sur ses relations avec les autres sur les sites communautaires ni sur ses nouveaux amis de tchat. Ne menacez pas votre enfant de lui supprimer Internet si des problèmes apparaissent. Sinon il ne vous confiera rien si des évènements graves ont lieu.

Réagir

La PSC donne quelques conseils pour réagir si votre enfant est victime de cyber-intimidation :

- En premier lieu, cherchez à savoir ce qui s'est réellement passé. Si les auteurs des attaques de mobbing sont plus ou moins connus, cherchez le dialogue avec les enfants, les adolescents, les parents et, si les intimidations touchent le milieu scolaire, avec les enseignants. Discutez entre adultes des mesures à prendre et y associer aussi votre enfant. Essayez en premier lieu de résoudre le conflit avec les personnes concernées.
- Si vous n'arrivez pas à trouver une solution au problème, adressez-vous à des organismes professionnels. Les services professionnels offrent des conseils sur l'aspect juridique du problème et sur l'intérêt de porter plainte auprès de la police. De plus, la loi protège les citoyens d'attaques morales, d'injures et d'insultes. Les menaces, le harcèlement sexuel ou le chantage sont des faits qui relèvent du droit pénal et, s'ils ont été dénoncés, doivent permettre de confondre les auteurs des délits. Pour cela, rassemblez toutes les preuves d'injures et d'intimidations afin de pouvoir les présenter.
- Modifiez les informations en ligne concernant votre enfant. Changez l'adresse e-mail et, si nécessaire, aussi le numéro de téléphone portable de votre enfant, afin de mettre un terme aux attaques de mobbing. Conseillez-lui également de modifier son pseudonyme sur les sites communautaires et sur les tchats. Signalez les coordonnées de l'auteur aux modérateurs des sites ou des tchats concernés. Exigez d'eux de supprimer les contenus, les photos et les vidéos qui portent atteinte à l'intégrité morale de votre enfant.

Liens

→ Cyber-initimidation
→ Assistance téléphonique 147
→ Tel-jeunes : la cyber-intimidation

Abus sexuel sur Internet

Les sites de réseautage social ou les sites communautaires proposent divers services permettant aux jeunes de créer des groupes et de se présenter aux autres. Les adolescents y communiquent et flirtent entre eux, exposent leurs profils, photos et vidéos, créent des groupes d'intérêt et nouent de nouvelles amitiés. Les personnes qui s'inscrivent sur ces réseaux en vue d'entrer en contact avec des enfants et des adolescents dont ils pourraient ensuite abuser, notamment sexuellement, représentent un réel danger. Sur Internet, nous ne pouvons jamais être sûrs à 100% de la personne qui se cache derrière un profil. C'est pourquoi, les adolescents doivent d'une part rester prudents quand ils font de nouvelles connaissances et, d'autre part, s'habituer à respecter des mesures de prévention.

Prévenir

La PSC propose quelques conseils aux parents sur comment réduire au maximum le risque pour que leur enfant ne devienne pas victime d'abus sexuel :

- Renseignez-vous sur les communautés en ligne fréquentées par votre enfant : créez vous-même un profil et informez-vous sur les possibilités techniques afin de préserver au maximum la sphère privée sur le Web. En règle générale, vous avez la possibilité de protéger l'aspect confidentiel des données dans les sous-menus « Extras » ou « Paramètres » proposés par de nombreux sites. Si vous avez des questions concernant ces paramètres, contactez les modérateurs des sites en question. Sachez que tout profil déposé ne devrait être accessible qu'aux amis que votre enfant connaît personnellement.
- Discutez avec votre enfant du profil qu'il a posté sur un site communautaire. Parlez-lui des informations non appropriées (nom, adresse, téléphone, âge, photos et vidéos gênants ou aguicheurs) et de la manière dont des tiers pourraient s'en servir pour lui nuire.
- Prudence en cas de rendez-vous avec une personne connue sur l'Internet. Si votre enfant a moins de 16 ans, interdisez-lui toute rencontre avec des personnes connues sur l'Internet. Pour les jeunes de plus de 16 ans, il est important de discuter avec eux des dangers qu'une telle rencontre représente et de fixer des limites très claires.
- Contactez les administrateurs des sites communautaires si vous avez des questions concrètes ou si vous souhaitez signaler un abus (abus sexuel, cyber-intimidation, contenus non appropriés, etc.). Utilisez les offres de « l'association pour l'animation jeunesse en milieu ouvert » qui propose aussi des cours spécifiques à l'utilisation « des sites de réseautage social » pour les parents et pour les adolescents.

Réagir

La PSC donne quelques conseils pour réagir si l'enfant est victime d'abus sexuel.

- Si votre enfant a été victime d'un abus sexuel, contactez immédiatement le service de conseils aux victimes de votre canton (vous trouverez l'adresse en fin de document) et portez plainte à la police.
- Proposez votre aide également à des tiers. Si votre enfant ou vous-même avez pris connaissance d'un abus sexuel sur un enfant ou un adolescent, proposez votre aide. Renseignez les personnes concernées sur la manière de s'informer, sur où trouver de l'aide et sur comment mieux se protéger à l'avenir.

Liens

→ Abus sexuels sur l'Internet
→ Stop pornographie enfantine sur Internet
→ Fondation Suisse pour la Protection de l'Enfant
→ Dites le – Pornographie enfantine

Cyberaddiction

Le risque d'addiction à l'Internet existe. Beaucoup de jeunes se connectent à l'Internet ou passent du temps devant l'ordinateur tous les jours. Ils y jouent et communiquent sur les tchats ou les sites sociaux, comme Netlog, Facebook ou autres sites communautaires en ligne. La fascination exercée par l'Internet peut aussi devenir problématique et, dans le cas extrême, entraîner une cyberaddiction.

Prévenir

La PSC propose quelques conseils aux parents et enseignants sur comment réduire au maximum le risque pour que l'enfant ne devienne pas victime de cyberaddiction :

- Regardez la réalité en face: Votre enfant risque-t-il de développer une cyberaddiction ? Préoccupez-vous de savoir combien de temps votre enfant passe sur Internet.
- Intéressez-vous aux activités de votre enfant. Demandez-lui de vous expliquer les jeux auxquels il joue, les profils qu'il a postés sur des sites sociaux et les raisons pour lesquelles il préfère tel jeu plutôt qu'un autre. L'objectif est que votre enfant vous montre son profil, par exemple sur Netlog, et vous présente les personnes avec qui il tchate.
- Imposez des limites. Les enfants et les adolescents ont souvent beaucoup de mal à se discipliner. Vous devez les aider à s'intéresser intelligemment aux activités virtuelles. Décidez avec votre enfant du temps qu'il a le droit de passer devant l'ordinateur et veillez à ce qu'il le respecte.
- Surveillez votre enfant. Il est du devoir des parents ou des responsable de l'éducation de surveiller les jeunes afin qu'ils ne se mettent pas en danger, ni dans le monde virtuel, ni dans le monde réel. Concernant l'utilisation de l'Internet, il vous faut connaître les activités virtuelles pratiquées par votre enfant.

– Proposez de l’aide à votre enfant. Si vous avez l’impression que votre enfant fuit les problèmes quotidiens en se réfugiant derrière des activités virtuelles sur Internet, vous devez lui proposer votre aide.

Réagir

La PSC donne quelques conseils pour réagir si l’enfant est victime de cyberaddiction.

– Si vous craignez que votre enfant ait déjà développé une cyberaddiction et si d’en parler avec lui est trop difficile, adressez-vous à des spécialistes. Diverses organisations proposent des aides compétentes, à vous et à votre enfant, afin de trouver une solution pour sortir des activités nuisibles.

Liens

→ Cyberaddiction
→ Portail d’information Addiction Suisse
→ Cyberdependance
→ Addiction info suisse

educa.ch
Institut suisse des médias pour la formation et la culture
Erlachstrasse 21 | Case postale 612 | CH-3000 Berne 9

Téléphone : +41 (0)31 300 55 00
info@educa.ch | www.educa.ch