

Sous légide

Royaume du Maroc
Ministère de l'Industrie,
de l'Investissement, du Commerce
et de l'Economie Numérique



المملكة المغربية
وزارة الصناعة
والاستثمار والتجارة
والاقتصاد الرقمي

En partenariat

ROYAUME DU MAROC - MINISTRE DE LA FAMILLE, DE LA SOLIDARITE, DE L'EQUALITE ET DU DEVELOPPEMENT SOCIAL



المملكة المغربية
وزارة الأسرة والشؤون
والمساواة والتنمية الاجتماعية

ROYAUME DU MAROC - MINISTRE DE L'EDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



المملكة المغربية
وزارة التربية الوطنية
والتكوين المهني
والتعليم العالي والبحث العلمي



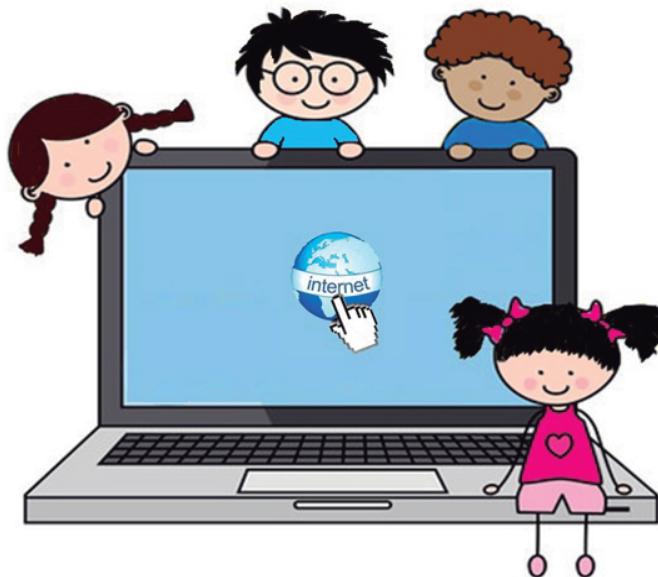
المملكة المغربية
ROYAUME DU MAROC
CNAP
الجهة الوطنية المغربية المختصة بالتحقق من الامتثال
Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel



Centre Marocain de Recherches Polytechniques et d'Innovation

MÉFIE-TOI SUR INTERNET

Guide de bonnes pratiques de sécurité Internet



Enfants de moins de 12 ans

MÉFIE-TOI SUR INTERNET



Guide de bonnes pratiques de sécurité Internet pour enfants de moins de 12 ans

Ce guide est le fruit de collaboration des partenaires de la Campagne Nationale de Lutte Contre la Cybercriminalité (CNLCC 2014-2017), menée sous le parrainage du Ministère de l'Industrie, de l'Investissement, du Commerce et de l'Economie Numérique, par le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI).

Titre de Guide : MÉFIE-TOI SUR INTERNET

Dépôt Légal : 2017MO3962

ISBN : 978-9954-99-672-0

ISSN : 2550-6196

Imprimerie : Espace Impression - Tél. : 05 37 80 12 69

SOMMAIRE

Préambule	4
Comité d'élaboration et de rédaction du guide	5
1 Je profite d'Internet avec méfiance	6
1.1 Aperçu sur Internet	6
1.2 Avantages d'Internet	7
1.3 Je me méfie sur Internet	8
2 Je suis conscient des dangers d'Internet	9
2.1 Cybercriminalité	9
2.2 Cyber-harcèlement	10
2.3 Arnaque ou escroquerie	11
2.4 Cyber-extorsion	12
2.5 Cyber-pédophilie	13
2.6 Exploitation	14
2.7 Téléchargement sur Internet	14
3 Je me protège sur Internet	15
3.1 Mot de passe.....	15
3.2 Antivirus.....	16
3.3 Partage.....	17
3.4 Applications mobiles / Jeux en ligne	18
3.5 WIFI /LIFI	19
3.6 Données personnelles et vie privée.....	20
3.7 Réseaux sociaux	20
3.8 Sites illicites	21
4 Je me comporte bien sur Internet	22
4.1 Bon usage d'Internet	22
4.2 Addiction à Internet.....	22
5 Je m'adresse à qui ?	24
6 Je retiens	25

Préambule

Ce guide de bonnes pratiques de cyber-sécurité a été élaboré grâce au travail collaboratif des partenaires de la Campagne Nationale de Lutte Contre la Cybercriminalité (CNLCC 2014-2017), menée sous l'égide du Ministère de l'Industrie, de l'Investissement, du Commerce, et de l'Économie Numérique, par le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI).

Il s'agit d'un guide de sensibilisation aux diverses facettes de la cybercriminalité et aux mesures de base, en matière de cyber-sécurité, nécessaires pour aider l'internaute à une navigation plus sécurisée.

Basés essentiellement sur une Webographie variée, certains contenus de ce guide sont des extraits partiels des articles publiés sur Internet. Ce guide, d'aspect de sensibilisation et non commercial, est conçu d'une façon simple et avec un langage adapté, même aux non spécialistes dans le domaine de la sécurité d'Internet ou des systèmes d'information. Le lecteur est sensé approfondir ses connaissances sur les sujets et thèmes abordés. Le guide reste certainement non complet et ne peut en aucun cas être considéré comme une référence dans un domaine assez vaste, tel que celui de la cyber-sécurité.

Le guide est le fruit du travail d'un comité mis en place à ce sujet, constitué des partenaires suivants :

- Ministère de l'Industrie, de l'Investissement, du Commerce et de l'Économie Numérique;
- Ministère de l'Éducation Nationale, de la Formation Professionnelle, de l'Enseignement Supérieur et de la Recherche Scientifique;
- Ministère de la Famille, de la Solidarité, de l'Égalité, et du Développement Social;
- Direction Générale de la Sûreté Nationale;
- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel;
- Centre Marocain de Recherches Polytechniques et d'Innovation;
- Association Bayti.

Comité d'élaboration et de rédaction du guide

- M. Noureddine LASFAR
- Mme. Mahjouba BOUFDAILA
- M. Hamid HABTI

Ministère de l'Industrie, de l'Investissement,
du Commerce et de l'Économie Numérique

- Mme. Halima BENRAMDANE

Ministère de l'Éducation Nationale, de la Formation
Professionnelle, de l'Enseignement Supérieur et de la
Recherche Scientifique

- Mme. Hayat ATMANE

Ministère de la Famille, de la Solidarité, de l'Égalité,
et du Développement Social

- Mme. Layla EZZOUINE

Direction Générale de la Sûreté Nationale

- M. Salim ALAMI

Commission Nationale de Contrôle de la Protection
des Données à Caractère Personnel

- Mme. Houda ADLI

- M. Youssef BENTALEB

Centre Marocain de Recherches Polytechniques et
d'Innovation

- M. Taib BELGHITI

- M. Omar EL BOUNAGUI

- M. Abderrahaman BOUNAIM

Association Bayti

Avec l'appui de :

M. Badr Boubker SEDDIK

ex Directeur de l'Économie Numérique (MICCEN)

Mme. Samia CHAKRI

Directrice de l'Économie Numérique (MICCEN)

Mme. Ilham LAAZIZ MALTI

Directrice du Programme GENIE (MENFPESRS)

M. Mohamed AIT AZIZI

Directeur de la Protection de la famille, de
l'Enfance et des Personnes Agées (MFSEDS)

1.2 Avantages d'Internet



Internet est un outil de communication et d'information très important notamment pour l'enfant.

Aujourd'hui, Internet présente aux enfants plusieurs possibilités, à savoir :

- **Apprendre** grâce à une diversité d'informations et de connaissances disponibles sur Internet.
- **Communiquer** avec les amis ou la famille grâce à des applications permettant d'échanger (audio, vidéos, fichiers, etc.).
- **Jouer et s'amuser** avec un ensemble de jeux éducatifs et d'intelligence ou encore des vidéos et également des livres, etc.

L'ensemble des activités qui peuvent être exercées sur l'ordinateur ou sur des petits appareils mobiles, comme les smartphones et les tablettes, rendent d'Internet un moyen incontournable, permettant à l'enfant d'avoir un accès rapide aux informations pour comprendre, voire apprendre certaines connaissances nécessaires pour le développement de sa personnalité et son éducation.

1.3 Je me méfie sur Internet

Internet est un outil formidable, mais il faut bien en faire attention, comme dans la rue ! Tu peux y rencontrer des personnes inconnues ou des méchants, ou recevoir des informations, des photos, ou des vidéos inappropriées. N'oublie pas que, même si tes parents ne sont pas des spécialistes en Internet, or ils peuvent t'aider pour surfer tranquillement, surtout si tu rencontres des soucis.



En lisant ce guide attentivement, tu vas découvrir que sur Internet il y a des « méchants » qui essaient toujours de te tromper. Il faut donc connaître les risques d'Internet afin d'éviter d'être victime d'actes de ces malveillants qui peuvent te créer de graves problèmes ainsi qu'à ta famille, ou qui aussi peuvent nuire à ton ordinateur, ta tablette ou smartphone.

2 Je suis conscient des dangers d'Internet

2.1 La Cybercriminalité



Comme il existe des malfaiteurs dans l'espace réel, appelés criminels, il en existe dans l'espace virtuel (sur internet); on les appelle des cybercriminels. Ils cherchent à t'espionner, à accéder à tes informations secrètes enregistrées sur ton ordinateur, ta tablette ou smartphone, à voler ton identité, à endommager tes données et applications, et même t'harcéler à travers Internet, et bien d'autres actes dangereux.

2.2 Cyber-harcèlement

«Certains élèves s'insultent par SMS, et finissent par se battre dans les couloirs de l'école.»

- Faire circuler sur Internet des photos ou vidéos, d'un ami ou copain de la classe, en se moquant de lui ou en propageant des rumeurs sur lui;
- Déranger ou menacer une personne sur Internet;
- Insulter ou menacer sur Internet ou par messagerie instantanée.

Ce sont des exemples de ce qu'on appelle cyber-harcèlement, qui consiste à profiter d'Internet pour agresser ou menacer les autres par la publication de leurs données et informations intimes.

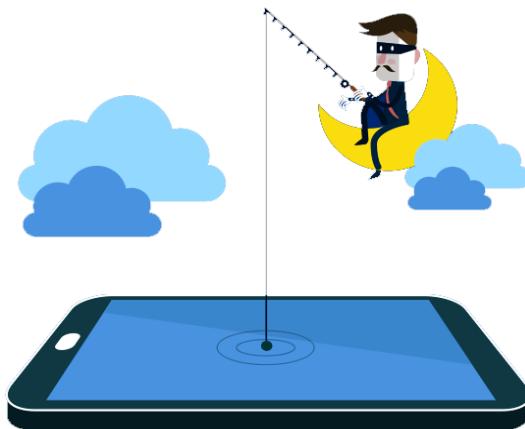


Dans le cas où tu es victime d'un cyber-harcèlement, il faut être courageux et « briser » le silence en s'adressant, sans hésitation, à tes parents, tes tuteurs, tes enseignants ou tes éducateurs, afin de mettre fin à une telle souffrance.

2.3 Arnaque ou escroquerie

Il se trouve sur Internet qu'il y a des personnes qui essaient de t'induire, intelligemment, en erreur par des propos, mensongers ou exploite ton erreur, pour obtenir un profit quelconque ou informations personnelles sur toi ou sur tes proches.

L'arnaqueur, est une personne qui donne l'impression qu'il est de confiance, alors que ce n'est jamais le cas, utilise de faux noms, de fausses photos pour te convaincre qu'il est devenu un ou une amie intime et de confiance. Une fois tu lui fais confiance et tu commences à communiquer avec lui, tu lui donne l'occasion pour arriver à ses buts pour t'attaquer ou attaquer tes proches.



Pour éviter d'être victime d'une arnaque, il faut être vigilant en navigant sur Internet, et ne jamais faire confiance aux inconnus et de ne pas communiquer tes informations et données personnelles à quiconque, sauf si tu le connais ou tu l'as déjà vu ou contacté par téléphone. Si cela est nécessaire, il faut le faire en présence de tes parents, tes tuteurs ou tes enseignants.

2.4 Cyber-extorsion

Dans l'espace virtuel (Internet), comme dans l'espace réel, tu peux rencontrer des difficultés ou des problèmes causés par des utilisateurs d'Internet qui sont en réalité des criminels, et qui profitent de multiples possibilités d'Internet pour attaquer leurs victimes par divers moyens comme l'extorsion (cyber-extorsion). Cette dernière consiste à obtenir une information secrète, un bien ou une somme d'argent par des menaces, d'intimidations ou de chantage.



Il arrive par exemple que quelqu'un peut t'arnaquer et réussit à obtenir tes informations ou celles de tes proches (photos, vidéos, etc), et commence à te menacer pour publier ces informations.

Dans cette situation, il faut alors s'adresser à tes parents, tuteurs, enseignants, éducateurs ou à quelqu'un de confiance, pour qu'ils interviennent afin de te protéger contre ce genre de cybercriminalité.

2.5 Cyber-pédophilie



Sur Internet, il se peut que des personnes te demandent de faire des gestes que tu ne dois jamais faire devant les gens, comme des attouchements inappropriés sur ton corps, ou encore de faire des bizous ou te déshabiller. Ces personnes sont des pédophiles, qui essaient souvent de te piéger par la Webcam et capturer tes photos ou te filmer.

Les pédophiles essaient parfois de te montrer des enfants ou des adultes avec corps nus ou en positions ou gestes inhabituels et inacceptables. Il arrive qu'un pédophile t'invite via Internet pour se rendre à un lieu pour une raison ou une autre.

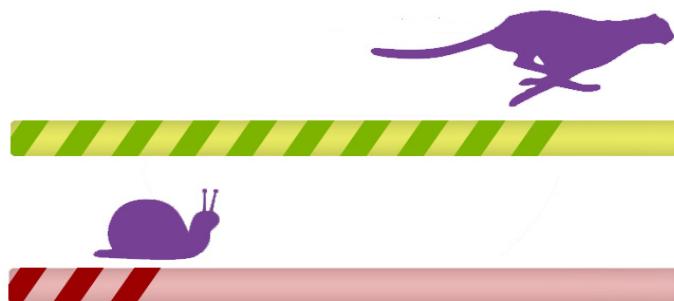
Si jamais tu as le moindre doute d'une telle personne, connue ou non, il ne faut jamais obéir à cette personne, éteindre immédiatement l'ordinateur ou tablette ou smartphone et en parler immédiatement à tes parents, tuteurs, enseignants ou éducateurs.

2.6 Exploitation

Il arrive sur Internet que des personnes souhaitent t'exploiter sans que tu sois conscient, souvent ça commence par te demander des échanges de photos, d'activer ta Webcam, jouer en ligne, recevoir des cadeaux ou des récompenses, se rendre sur un lieu, et ceci n'est qu'un début pour t'exploiter.

L'exploitation des enfants sur Internet commence par s'amuser, mais termine souvent par une agression. Si tu vois que quelqu'un ne cesse de te demander de lui exécuter des choses qui te paraissent bizarres, il faut en parler à tes parents, tuteurs, enseignants ou éducateurs.

2.7 Téléchargement sur Internet



Il arrive que tu aies besoin de télécharger des fichiers (images, vidéos, jeux, documents, etc.), ce qui est possible et facile à faire une fois connecté à Internet. Il faut se méfier; car une telle opération présente des vrais risques.

En effet, les fichiers téléchargés à partir des sites Internet ou à partir des applications mobiles, ces fichiers peuvent contenir des virus qui endommagent ton ordinateur, ton

smartphone ou ta tablette.

Le téléchargement ne doit pas se faire à partir de n'importe quel site. En fait, les sites de téléchargement doivent être des sites de confiance.

Afin d'éviter les dangers liés au téléchargement, à chaque fois que tu as besoin de télécharger un jeu, une vidéo ou autre, tu demandes l'autorisation et l'accompagnement de tes parents ou tuteurs.

3 Je me protège sur Internet

3.1 Mot de passe



« Un mot de passe, c'est comme une brosse à dent !!
on ne le prête à personne, même à ton/ta meilleur(e) ami(e) »

Pour garder la confidentialité et protéger nos informations sur Internet, on utilise souvent un login et un mot passe. qui peuvent être malheureusement piratés (volés) par des cybercriminels.

Voici quelques règles de bonnes pratiques à suivre pour mieux se protéger contre le piratage de ton mot de passe.

- Un bon mot de passe doit être composé d'au moins 12 caractères;
- Pour le retenir facilement, utilise par exemple une phrase : « J'arrive à 8 heure à l'ÉCOLE »;
- Un mot de passe doit être difficile à deviner pour ne pas être piraté facilement;
- Il doit être régulièrement changé pour éviter qu'il soit piraté;
- Ne jamais communiquer ton mot de passe sur Internet et ne le donne à personne;
- N'écrit pas ton mot de passe sur n'importe quel support (papier ou autre);
- Ne pas utiliser ton nom ou celui des membres de ta famille ou amis, ta date de naissance, etc. comme mot de passe.

3.2 Antivirus

Un antivirus est un logiciel destiné à défendre l'ordinateur, le smartphone, ou la tablette contre les virus informatiques. Ces derniers sont des programmes indésirables qui s'infiltrer discrètement dans la machine à travers, par exemple les téléchargements, et causent parfois des dégâts énormes, comme la perte des données, ou ils espionnent ce que nous faisons sur notre ordinateur, smartphone ou tablette.

Pour assurer sa sécurité sur Internet, se protéger contre les menaces informatiques les plus courantes, il est indispensable de posséder un logiciel antivirus.

L'antivirus est similaire en quelque sorte à un vaccin : une fois installé sur la machine, il identifie les virus, s'ils existent, et les éjecte ou les supprime. Or, afin d'identifier les virus, l'antivirus doit être mis à jour : c'est-à-dire rafraîchir sa mémoire afin de reconnaître les derniers virus mis en ligne par les cybercriminels.

Il existe des antivirus gratuits ou payants, l'essentiel c'est de les installer et de les mettre à jour pour une navigation sécurisée.



3.3 Partage

Le partage est une opération qui permet d'échanger sur Internet ou tout autre réseau informatique des photos, des vidéos ou des informations, etc. stockées sur notre ordinateur, tablette ou smartphone.

Bien qu'il a des avantages, le partage présente aussi des dangers comme la propagation de virus, logiciels malveillants ou d'espionnage.

Il est indispensable d'être très vigilant en partageant des fichiers ou informations. Il faut demander l'assistance de tes parents, tuteurs, enseignants ou éducateurs.



Pour tout téléchargement ou partage, il est recommandé de demander l'assistance de tes parents ou un adulte avant de commencer à télécharger ou partager un fichier.

3.4 Applications mobiles / Jeux en ligne

En utilisant les applications mobiles ou les jeux en ligne, il faut être vigilant parce qu'ils peuvent contenir des virus susceptibles d'endommager ton ordinateur, ta tablette ou ton smartphone.

Avant de télécharger et installer une application ou un jeu, il est indispensable d'être accompagné de tes parents, tuteurs, enseignants ou éducateurs. Souvent les applications gratuites imposent l'accès libre et l'exploitation des données stockées telles que, tes photos, tes vidéos et tes conversations.



3.5 WIFI / LIFI

Aujourd'hui, il est devenu possible de se connecter à Internet de n'importe où ! restaurants, domiciles, aéroports, gares, parcs, etc. et ceci grâce à la connexion sans fil Wifi (technologie basée sur les ondes) ou encore Lifi (technologie basée sur l'utilisation de la lumière). Toutefois, cette facilité de connexion présente également des risques pour la sécurité de nos connexions, nos données personnelles et nos ordinateurs.



Le Wifi ou le Lifi, présente également des dangers et risques. En effet, des pirates ou cybercriminels peuvent accéder à ton ordinateur, ou à ta tablette ou smartphone si le

wifi/lifi et activé.

En général, la connexion à partir d'un réseau public (restaurant, grandes surfaces, café, hôtel, etc.), est non sécurisée. Évite alors d'introduire tes identifiants en se connectant à partir de tels lieux.

3.6 Données personnelles

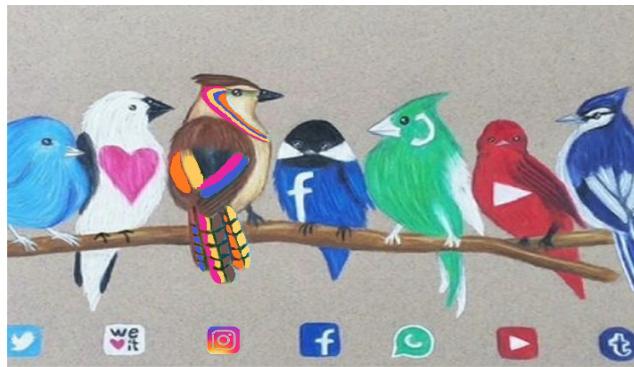
Toute information qui peut te faire connaître (ton nom, ton prénom, ta photo ou encore ta date de naissance et celles d'autrui), est l'appelée une donnée personnelle, et elle fait partie de ta vie privée. Il faut être alors très vigilant lors de la communication de ces données :

- Ne pas répondre aux questions sur ta vie personnelle qu'en présence et qu'après l'accord de tes parents ou tuteurs;
- Ne jamais communiquer tes informations personnelles sur Internet : il risque d'être utilisées à des fins mal intentionnés;
- Une fois publiées, ces informations risquent toujours d'être présentes même après les avoir supprimées.

3.7 Réseaux sociaux

Les réseaux sociaux, comme Facebook, permettent aux gens de se connaître, de former des groupes d'amis et de se partager des informations.

Pour protéger les enfants contre les arnaques, l'harcèlement, la violence, les réseaux sociaux ne sont autorisés, en principe, qu'à partir de 13 ans.



3.8 Sites à contenus illicites

En surfant sur Internet, il se peut que tu accèdes à des sites dont le contenu est illicite ou inapproprié, par exemple des sites présentant des images ou vidéos de violence, corps nus ou portant atteinte à la dignité humaine ou incitant à la haine, etc.

Ces sites sont interdits et tu ne dois ne jamais les consulter. En plus, si jamais au hasard tu te trouves sur de tels sites, il faut que tu en parles à tes parents, tuteurs, enseignants ou éducateurs, afin de les signaler et les bloquer.



4 Je me comporte bien sur Internet

4.1 Bon usage d'Internet

Internet est un formidable moyen de communication, d'échange et d'accès à la connaissance. Mais il présente également des dangers et risques. C'est pourquoi il est important de savoir comment se protéger, et surtout comment se comporter sur Internet. Un mauvais usage d'Internet impacte négativement, entre autres, sur ta santé et ta scolarité. Il faut limiter, voire diminuer le temps passé sur Internet.

4.2 Addiction à Internet

Il faut faire attention de ne pas être accro et dépendant d'Internet : passer assez de temps devant l'écran conduit à l'addiction à Internet. Ci-après un test qui pourra t'aider à avoir une idée sur ton degré d'addiction. Il faut faire participer tes parents ou tuteurs à mieux s'organiser pour un usage modéré et équilibré d'Internet.



Test d'addiction

Réponds par oui ou non aux questions suivantes :

	Oui	Non
Passes-tu plus de temps que fixé initialement sur Internet ?		
Limiter le temps passé sur Internet te dérange-t-il ?		
Des amis ou des membres de ta famille se sont-ils plaints du temps que tu passes sur Internet ?		
Est-ce que le rendement scolaire ou tes enseignants ont souffert à cause du temps que tu passes sur Internet ?		
Est-ce que tu trouves difficile de rester quelques jours sans te connecter à Internet ?		
Est-ce qu'il y a des zones d'Internet, des sites particuliers que tu trouves difficiles à éviter ?		
As-tu essayé, sans succès, d'écourter l'usage d'Internet ?		
Est-ce que tu dévies beaucoup de tes préoccupations à cause d'Internet ?		

Évaluation

- De 1 à 3 réponses affirmatives : petite tendance à devenir addictif à Internet.
- Entre 4 et 6 réponses affirmatives : possibilité de développer une conduite addictive.
- Entre 7 à 9 réponses affirmatives : forte tendance à devenir dépendant.

5 Je m'adresse à qui ?



Dans le cas où tu es victime d'une arnaque, d'un harcèlement, du vol de ton compte ou de tes informations et données personnelles ou de toute sorte d'attaque cybercriminelle, tu ne dois jamais garder le silence. Au contraire, tu dois t'adresser à tes parents, tuteurs, enseignants, éducateurs, à quelqu'un de confiance ou à une autorité compétente pour t'aider à résoudre ce problème.

6 Je retiens

Pour une meilleure protection sur Internet, ci-après quelques règles à respecter :

Quand je navigue

- Je ne communique jamais mes informations personnelles (nom, date de naissance, adresse, numéro de téléphone, etc.);
- Je ne communique mes mots de passe à personne. Je choisis mes mots passe un peu « compliqués », par exemple en mélangeant des lettres et des chiffres;
- Les Informations publiées sur Internet, ne sont pas toujours fiables, je demande conseil à un adulte;
- En cas d'un contenu illicite, je quitte le site et j'en parle à un adulte;
- Ne jamais répondre à des inconnus pour éviter d'être victime d'un acte de cyber-harcèlement ou cyber-extorsion;
- Je choisis des sites adaptés à mon âge.

Quand je communique en linge

- Je n'oublie pas que l'on ne peut jamais savoir qui se cache derrière un pseudo;
- Je n'accepte pas d'inconnus sur mes listes de contact.

Quand je joue en ligne

- Je choisis des jeux adaptés à mon âge que j'utilise avec modération.



www.cmrpi.ma

MÉFIE-TOI SUR INTERNET

Guide de bonnes pratiques de sécurité Internet

Enfants de moins de 12 ans

