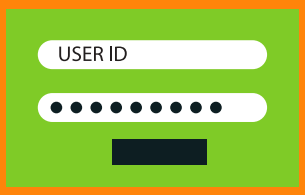
CYBERSÉCURITÉ : 10 CONSEILS POUR PRÉVENIR LE PIRATAGE DE VOTRE ORDINATEUR

CI-CERT

CONTACTS:
CÔTE D'IVOIRE - COMPUTER EMERGENCY RESPONSE TEAM

Tel : +225 20 34 43 73 / 74
Mail : info@cicert.ci
Site web : http://www.cicert.ci/
Marcory Anoumanbo, Abidjan – Côte d'Ivoire

SOMMAIRE



CÔTE D'IVOIRE - COMPUTER EMERGENCY RESPONSE TEAM

Tel : +225 20 34 43 73 / 74
Mail : info@cicert.ci
Site web : http://www.cicert.ci/
Marcory Anoumanbo, Abidjan – Côte d'Ivoire

ATTENTION!

Vous pensez être anonyme sur le web ? Que personne ne trouvera votre mot de passe ? Que votre code wifi vous protège amplement ?

Faux ! Si vous souhaitez mettre toutes les chances de votre côté pour éviter de vous faire pirater ou espionner, voici exactement ce que vous devez faire !

1

Choisissez avec soin votre mot de passe

Utilisez des mots de passe de qualité, sans quoi vous risquez de faciliter l'accès à vos données personnelles.

- **Privilégiez les mots de passe longs, comprenant des majuscules et des minuscules, des chiffres, et des caractères spéciaux. Exemple : Wejd*25ipO%Ram.**

Nombre de pirates disposent en effet de logiciels leur permettant de générer toutes les combinaisons du dictionnaire, voire des formules plus complexes. Des mots de passe tels que « voiture », votre date d'anniversaire ou le nom de votre chien sont donc à proscrire.

- **Changez votre mot de passe régulièrement**
- **Choisissez-en un différent pour chacun de vos comptes.**

En effet, une fois qu'un hacker (cyberpirate) a trouvé l'un de vos mots de passes, il va essayer d'accéder à vos autres comptes avec celui-ci. Si vous avez reçu un nouveau mot de passe par courriel, n'oubliez pas de vous débarrasser de ce message.

2

Faites régulièrement les mises à jour de votre système et logiciels installés

On l'oublie trop souvent : **les mises à jour régulières sont impératives**, celles-ci contiennent **les dernières sécurités du marché, adaptées aux nouveaux virus informatiques**.

Alors, même si l'installation peut prendre un peu de temps, lancez-vous… ce seront dix minutes de perdues mais beaucoup de piratages qui seront évités !

Les dernières mises à jour vous permettent de bénéficier des dernières avancées de la sécurité de l'informatique et de lutter contre une nouvelle génération de virus et de malware, à la pointe du piratage informatique !
Ce n'est pas accessoire...

3

Optez pour une clé WIFI WPA2, dans les paramètres de votre compte auprès de votre fournisseur internet

Il existe plusieurs types de clés wifi.
La clé WEP est la plus courante, car elle reste habituellement le choix par défaut des fournisseurs d'accès. Mais c'est également la moins sécurisée. **Les clés WEP peuvent être décryptées par des pirates en moins de cinq minutes, contre une quinzaine d'heures pour une clé WPA 2**.

Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur Internet ou accédez directement aux paramètres de votre wifi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès.

4

Faites attention aux liens figurant dans un mail ou sur une page web

Ne cliquez pas trop vite sur les liens, même ceux qui vous paraissent familiers.

Une des attaques les plus classiques vise à **tromper l'internaute en l'incitant à cliquer sur des liens figurant dans un e-mail ou une page web**. Ce lien peut-être malveillant.

En cas de doute, abstenez-vous et préférez écrire vous-même l'adresse voulue dans la barre d'adresses de votre navigateur.

5

Sauvegardez régulièrement vos données

À défaut d'anticiper un vol de données, la sauvegarde de votre ordinateur vous permettra d'**éviter leur perte définitive**. Rien de pire que perdre vos fichiers professionnels ou vos souvenirs personnels…

Investissez donc dans **l'achat d'un bon disque dur externe pour effectuer régulièrement des sauvegardes**. Cette solution ne se substitue pas à un anti malware ou un logiciel de sécurité, mais elle permettra de conserver une trace de vos données.

6

Soyez vigilant avant d'ouvrir les pièces jointes d’un mail

Les pièces jointes contenues dans les e-mails peuvent contenir un malware qui récupérera vos informations personnelles et notamment votre mot de passe. Le simple fait de cliquer sur une pièce jointe peut suffire à l'activer.

- **Ne consultez une pièce jointe que si l'émetteur est de confiance et le contenu du mail cohérent**. *Si vous avez un doute, contactez l'émetteur de l'e-mail (si vous le connaissez) qui vous confirmera ou non l'envoi de la pièce jointe ;*

- ***Souvenez-vous* que votre antivirus (qui doit être à jour) n'est pas infaillible, même s'il analyse les fichiers et pièces jointes de votre ordinateur.** *Pour une vérification exhaustive, vous pouvez effectuer une analyse complète de vos fichiers et URL en ligne grâce à cet outil https://www.virustotal.com/fr/ ;*

- N'ouvrez jamais les fichiers dont les extensions sont **.VBS**, **.JBS**, **.SHS**, **.PIF** ;
- N'ouvrez jamais les fichiers dont les extensions sont multiples, comme **NOM.BMP.EXE** ou **NOM.TXT.VBS**, ou **NOM.PIF** ;
- N'ouvrez jamais les fichiers aux noms attrayants comme **SEXY_NUDE.VBS** ;
- Méfiez-vous des fichiers dont les extensions sont **.EXE**, **.BAT** ou **.COM**.

7

Naviguez sur le web depuis un compte utilisateur sur votre ordinateur, et non un compte administrateur

Ne naviguez pas depuis un compte administrateur.

L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l'utilisation d'un compte utilisateur, qui vous permet également de naviguer sur le web sans entraves.

8

Évitez de divulguer vos informations confidentielles et personnelles sur internet

Il est très important de contrôler la diffusion d'informations personnelles. Internet est loin d'être ce lieu d'anonymat qu'on imagine.

Évitez de fournir vos coordonnées ou d'autres données sensibles dans les forums ou sur des sites n'offrant pas toutes les garanties requises.

Un conseil : le symbole https:// au début de l'adresse web et l'image d'un petit cadenas est gage de site web certifié et sécurisé, mais dans le doute, mieux vaut s'abstenir.

9

Combiner un antivirus et un pare-feu, pour augmenter votre protection

Aucun ordinateur n’est imprenable.

Ne facilitez pas la tâche aux hackers. Mieux vous serez protégé, plus rude et dissuasive sera la tâche pour les personnes malveillantes.

Le pare-feu permet de limiter un certain nombre de connexions entrantes et sortantes. Si malgré tout, le pirate trouve une faille dans votre ordinateur, un antivirus peut l’empêcher de nuire.

10

Méfiez-vous des messages étranges envoyés par vos contacts, ils peuvent avoir eux-mêmes été piratés

L'envoi de liens malveillants peut-être **indépendant de la volonté de leurs expéditeurs**, même de ceux que vous connaissez !

Si un correspondant avec lequel vous échangez régulièrement vous adresse par exemple un message dans une langue étrangère, ou que sa manière de s'exprimer est différente, n'ouvrez pas les pièces jointes contenues dans son message et ne cliquez pas sur les liens qui y figurent. En cas de doute, passez-lui un coup de fil !

Check-list

- [ ] Choisissez avec soin votre mot de passe
- [ ] Faites régulièrement les mises à jour de votre système et logiciels installés
- [ ] Optez pour une clé WIFI WPA2, dans les paramètres de votre compte auprès de votre fournisseur internet
- [ ] Faites attention aux liens figurant dans un mail ou sur une page web
- [ ] Sauvegardez régulièrement vos données
- [ ] Soyez vigilant avant d'ouvrir les pièces jointes d'un mail
- [ ] Naviguez sur le web depuis un compte utilisateur sur votre ordinateur, et non un compte administrateur
- [ ] Évitez de divulguer vos informations confidentielles et personnelles sur internet
- [ ] Combiner un antivirus et un pare-feu, pour augmenter votre protection
- [ ] Méfiez-vous des messages étranges envoyés par vos contacts, ils peuvent avoir eux-mêmes été piratés

Côte d'Ivoire - Computer Emergency Response Team
Tel : +225 20 34 43 73 / 74
Mail : info@cicert.ci
Site web : http://www.cicert.ci/
Marcory Anoumanbo, Abidjan – Côte d'Ivoire