Ne m'imprimez pas !
Lisez-moi sur un écran.

Guide du net « trankil »

Internet n'est pas un terrain de jeux qui s'affranchit des dispositions légales mises en place par la société : le législateur y a transposé des règles issues, essentiellement, du code pénal.

Le simple fait de s'approprier le compte de messagerie ou d'un réseau social d'une autre personne, sans l'accord formel de celle-ci, peut entraîner une plainte déposée auprès du procureur de la République.

Article 226-4-1 du code pénal : Le fait d'**usurper l'identité** d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

De la corruption de mineur au recel de fichiers téléchargés illégalement, les sanctions peuvent être particulièrement lourdes :

Article 227-22 du code pénal : Le fait de **favoriser ou de tenter de favoriser la corruption d'un mineur** est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende lorsque le mineur est âgé de moins de quinze ans (Loi n° 98-468 du 17 juin 1998) "ou lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un **réseau de télécommunications**, ou que les faits sont commis à l'intérieur d'un **établissement scolaire ou éducatif** ou, à l'occasion des entrées ou des sorties des élèves, aux abords d'un tel établissement".

Les mêmes peines sont notamment applicables au fait, commis par un majeur, d'organiser des réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe.

BY NC ND

Article 321-1 du code pénal : Le **recel** est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit. Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende.

Internet présente des risques au quotidien qui peuvent être limités ou supprimés en utilisant des outils ou une stratégie adaptée à ces risques :

1. **Contrôlez régulièrement votre e-réputation** : 31% des 18-34 ans ne sont pas conscients des résultats d'une recherche sur Internet portant sur leur nom (source Internetsanscrainte.fr). Votre futur employeur réalisera probablement une « googlelisation » sur votre personne et beaucoup d'informations anodines regroupées peuvent vous être préjudiciables (photos intimes, liked, opinions religieuses, opinions politiques, faiblesse en orthographe, anciens CV ou autres…). Si vous estimez que certaines informations vous sont préjudiciables, vous disposez du droit à l'oubli (déréférencement par les principaux moteurs de recherche). La commission nationale informatique et liberté vous propose un document intégrant les principaux critères à retenir sur vos droits dans ce domaine :

   https://www.cnil.fr/sites/default/files/typo/document/Droit_au_dereferencement-criteres.pdf

Vous voulez testez votre e-réputation ? Rendez-vous sur l'application co-éditée par la mairie de Paris et la MAIF : http://ereputation.paris.fr/les-fiches-pratiques/.

2. **Choisissez un mot de passe complexe** et ne retenez, en aucun cas, un mot de passe issu de votre profil (date d'un événement, lieu de naissance, nom du chat, nom d'un chanteur…). Si la plupart des applications informatiques testent la solidité de votre mot de passe (mixité majuscule, minuscule, chiffre et ponctuation), il y a encore des mots de passe qui ne résistent pas à des logiciels utilisés par des pirates qui utilisent, par exemple, des dictionnaires et des combinaisons de lettres.

L'agence nationale de la sécurité des systèmes d'information vous propose une page consacrée à la solidité des mots de passe :

Cliquez ici pour tester la "force" de votre mot de passe

BY NC ND

Cette agence propose, par ailleurs, huit recommandations pour la gestion de votre mot de passe (http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf) :

Consolidez votre mot de passe en utilisant les fonctions messagerie de secours, numéro de téléphone portable et phrase secrète.

R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

Pour 2016, le journal 20 minutes avance le chiffre d'un milliard de comptes piratés. Vous voulez vérifier vos comptes : rendez-vous sur HaveIBeenPwned.

3. Vérifiez, sur Internet, les dispositions concernant les **droits d'auteur** mises en œuvre par les propriétaires d'œuvres, des ressources en ce qui concerne le téléchargement ou la copie totale ou entière des ressources. De plus en plus, certaines ressources numériques font l'objet d'une licence qui précise les conditions d'utilisation de ces œuvres en ligne. Vous trouvez sur le portail Internet Creative commons des exemples de réutilisation de ressources numériques. Plusieurs sites Internet vous proposent des ressources libres de droit (logiciels, photographies, œuvres artistiques) : n'hésitez pas à vous y rendre car la gratuité n'exclue pas la qualité ! Rendez-vous, par exemple, sur framasoft ou sur eduscol pour des banques d'images.

4. **Ne vous laissez pas manipuler ! Assurez-vous de la qualité des informations** diffusées sur les sites Internet mais aussi que le site consulté est celui que vous recherchez et que la personne à qui vous vous adressez sur un réseau social n'est pas un « pirate ».

Des « complotistes » aux opinions sectaires, religieuses et politiques, Internet c'est aussi de la « désinformation » organisée ou non. Un expert informatique peut mettre en œuvre une stratégie qui vise à tromper les moteurs de recherche les plus courants et à insérer un site Internet au meilleur positionnement. L'adresse du site peut apporter des précieuses informations sur sa ligne éditoriale (en qualité d'informations, choisissez les sites « gouv.fr » plutôt que les sites « org ». Enfin, vérifiez si les adresses sont cohérentes aux raisons sociales des services ou entreprises (les tentatives de phishing utilisent des adresses proches mais inexactes et concernent des sites qui endorment la méfiance : impôts, CAF, EDF mais aussi Amazon et autres…).

Analysez l'adresse du site (URL).

Exemple de stratégie de positionnement qui a mis en échec le ministère :

IVG : le gouvernement lutte contre les sites anti-avortement

Alors qu'un site anti-avortement, géré par l'association SOS Détresse, s'était glissé en première place sur les pages de recherche Google, Marisol Touraine a lancé le 7 janvier 2016, sur Twitter, une campagne invitant les internautes à cliquer sur ivg.gouv.fr, afin de repositionner le site institutionnel en tête. Il aura finalement fallu recourir au référencement payant pour atteindre l'objectif.

Francetvinfo 11 janvier 2016

Vérifiez, par l'utilisation de plusieurs moteurs de recherche, la cohérence des résultats de vos requêtes et apprenez à différentier les résultats « naturels » des résultats commerciaux. Vérifiez si l'information recueillie sur le net n'est pas un canular (hoax) ou une théorie complotiste. **L'Etat a mis en place un outil pédagogique pour vous aider à déchiffrer les rumeurs : http://www.gouvernement.fr/on-te-manipule.**

Page d'accueil du site ministériel **« on te manipule »**	Hoax, rumeurs, photos ou vidéos truquées… les fausses informations abondent sur internet. Parfois la désinformatio va plus loin, et prend la forme de pseudo-théories à l'apparence scientifique qui vous mettent en garde : "On te manipule !" A en croire ces "théoriciens" du complot, États, institutions et médias déploieraient des efforts systématique pour tromper et manipuler les citoyens. Il faudrait ne croire personne… sauf ceux qui portent ces thèses complotistes ! Étrange, non ? Et si ceux qui dénoncent la manipulation étaient eux-mêmes en train de nous manipuler ? Oui, #OnTeManipule quand on invente des complots, quand on désigne des boucs émissaires, et quand on demande d'y croir sans aucune preuve. Découvrez les bons réflexes à avoir pou garder son sens critique et prendre du recul par rapport aux informations qui circulent.

A qui avez-vous affaire ? Les hackers utilisent les messageries et les réseaux sociaux pour hameçonner et leurs stratégies sont de plus en plus élaborées et peuvent avoir de lourdes conséquences :

Menacé de chantage sur Skype, un lycéen se suicide - 5 juin 2015 - L ...
tempsreel.nouvelobs.com › Faits divers ▾
5 juin 2015 - Menacé de **chantage** sur Skype, un lycéen se **suicide** ... interlocutrice virtuelle de voir une "vidéo intime" diffusée sur **Internet** s'il refusait de la payer, ... Ce **suicide** rappelle un drame similaire survenu à **Brest** en octobre 2012.

Connaissez-vous le Fingerprinting ? Lui il sait tout de vous : votre identité numérique est bâtie sur les particularités techniques de votre PC, tablette ou Smartphone.

5. **Soyez discrets sur le net.** Les navigateurs, moteurs de recherche, réseaux sociaux et sites Internet sont friands d'informations vous concernant. Si le « cookie » semble être l'outil de recueil de données le plus exploitable à des fins commerciales, les « liked », les requêtes auprès des moteurs de recherche et tout simplement les informations que vous avez échangé sur les réseaux sociaux sont capitalisées sur la « toile » dans un but commercial. Pensez à utiliser un moteur de recherche qui ne vous trace pas (Qwant ou Startpage par exemple mais il en existe quelques autres). Enfin, des utilitaires et même un navigateur (Opéra VPN) peuvent vous protéger de cette collecte de données en modifiant votre adresse IP ou en proposant des applications sur serveurs qui vous rendent invisibles.

6. **Protégez-vous des virus** et ne croyez surtout pas que votre téléphone Android est à l'abri d'attaques virales. Installez au moins un logiciel antivirus gratuit qui intègre un « pare-feu » et n'oubliez pas de les mettre à jour régulièrement. Sauvegardez vos données les plus importantes sur clé USB ou sur le cloud (de préférence, pour le cloud, choisissez une solution nationale ou européenne qui n'a pas la même conception de la propriété qu'aux Etats-Unis).

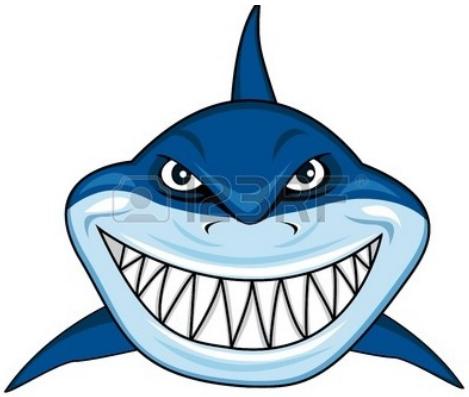
7. **Respectez les autres** et ils vous respecteront. Les dénigrements sur les réseaux sociaux sont source de mal être pour certaines personnes. Si vous êtes témoins de campagnes de dénigrement, parlez-en à une assistance sociale, à l'infirmière de votre établissement scolaire ou au CPE avant qu'il ne soit trop tard.

8. **N'abusez-pas d'Internet** : Internet vous facilite la vie au quotidien et a un impact certain sur l'affiliation sociale. Sa maîtrise constitue un des enjeux de l'appropriation des technologies numériques mais l'addiction présente un danger sous-estimé (car mal mesuré) qui peut avoir un effet nocif sur votre vie sociale et votre santé.

9. Soyez actif sur le net et contribuez à le rendre meilleur :

- **Internet signalement (portail officiel de signalement des contenus illicites de l'Internet :** https://www.internet-signalement.gouv.fr/PortailWeb/planets/ConseilsInternet.action
- **Phishing initiative (portail destiné à signaler les tentatives de phishing) :** https://phishing-initiative.fr/contrib/
- **Signal Spam (portail destiné à signaler les Spams) :** https://www.signal-spam.fr/
- **Signaler un hoax (il existe d'autres solutions : Hoaxbuster, securiser.com…) :** http://www.hoaxkiller.fr/contact/nousecrire.htm

SURFEZ TRANKIL



Droit Putut Handoko