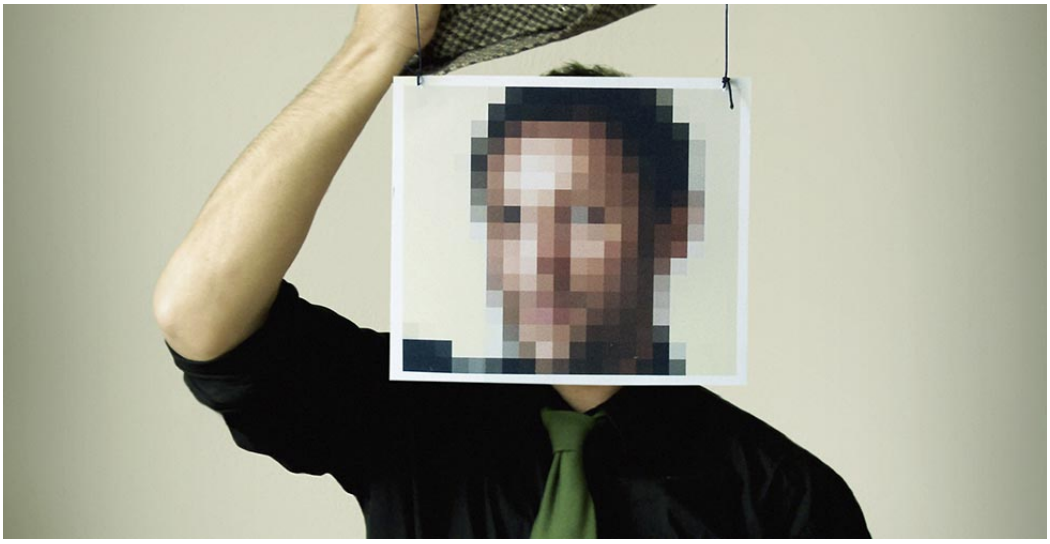
4 réflexes pour mieux protéger votre identité en ligne

19 octobre 2017

A l'occasion du mois de la cyber-sécurité, la CNIL vous propose une série de bonnes pratiques à mettre en place pour protéger votre identité en ligne. Au menu : quelques précautions techniques, un peu de connaissances juridiques et surtout, une pincée de bon sens !



En dire le moins possible lors d'une inscription en ligne

Pour quoi faire ?

Limiter le risque de voir vos données revendues à des acteurs tiers.

Se protéger en cas de fuite de données chez l'organisme à qui vous avez confié vos données.

Les conseils

Masquez votre adresse mail et votre numéro de téléphone lors d'une inscription ou au moment où vous déposez une annonce en ligne. Certains arnaqueurs scrutent et exploitent vos coordonnées pour tenter - via un message personnalisé - de vous soutirer des informations personnelles ou de l'argent dans un autre contexte.

Utilisez des pseudos lors de l'inscription à vos comptes et une adresse non-nominative (type toto35@email.com) pour vous inscrire en ligne. En cas de fuite de données, votre nom et prénom a moins de risques d'être compromis.

Utilisez des alias de messagerie si votre messagerie le permet. Les alias permettent de gérer plusieurs adresses mails virtuelles qui arrivent dans votre boîte aux lettres. Cela vous permet d'une part de détecter et d'identifier tout usage non autorisé d'un de vos alias, et d'autre part de supprimer un alias qui aurait été compromis. Si vous souhaitez y associer une photo, utiliser des photos différentes pour limiter les possibles réidentifications entre plusieurs comptes.

Remplissez le moins de champs possible : un formulaire d'inscription comporte beaucoup de champs facultatifs et demande parfois des informations sensibles (religion, origine ethnique, opinions ...). Méfiez-vous des cases qui vous proposent de réutiliser vos données pour des objectifs qui vous échappent !

Paramétrer ses réseaux sociaux

Pour quoi faire ?

Réserver l'accès à vote vie privée à un cercle d'intimes

Garder la maitrise de votre image en ligne (pour accéder à un emploi, une formation, ...).

Eviter d'être victime d'arnaqueurs ou d'usurpateurs.

Les conseils

Cloisonnez vos usages en fonction de votre audience : n'utilisez pas un seul et unique outil pour organiser votre vie sociale en ligne, au contraire essayez de diversifier les outils que vous utilisez pour avoir plus de flexibilité dans vos usages et être moins vulnérable en cas de piratage : une messagerie privée pour vos conversations entre amis, un réseau social professionnel pour dialoguer avec vos collègues, un groupe fermé pour discuter avec votre famille...

Limitez l'audience de vos publications et de votre compte : Afin de ne pas être retrouvé par n'importe qui sur le web, définissez pour chaque message que vous postez les personnes qui pourront le consulter. De nombreuses options permettent de ne pas être

retrouvé depuis les moteurs de recherche, de limiter l'accès à votre liste d'amis, de masquer vos informations de compte, de désactiver la géolocalisation de vos publications ...

Faites régulièrement le ménage dans les applications tierces connectées à votre compte afin de limiter le partage d'informations avec des tiers.

Connaitre ses droits !

Pour quoi faire ?

être autonome dans la maitrise de vos données qui circulent sur le web.

augmenter votre niveau d'exigence vis-à-vis des organismes à qui vous confiez vos données.

Les conseils

Ayez une bonne connaissance de votre droit à l'image. Cela vous permettra de disposer de toutes les clés nécessaires avant d'autoriser la prise de vue d'un photographe/vidéaste qui souhaiterait exploiter votre image sur des supports web ou papier.

Ayez une bonne connaissance de vos droits Informatique et Libertés. Cela vous permettra :
de demander l'effacement de contenus gênants vous concernant,

de mettre à jour des données que vous considérez comme obsolètes,

d'exiger une information lisible et une sécurité optimale pour les données que vous confiez à des tiers,

de porter plainte auprès de la CNIL en cas de manquements à la loi.

Depuis 2014, vous pouvez également demander aux moteurs de recherche de ne plus associer un contenu gênant vous concernant avec votre nom et prénom. Recherchez régulièrement votre nom sur les moteurs de recherche, cela vous permettra d'être alerté lorsque du contenu indésirable est publié sur vous. Vous pouvez également vous abonner à des services d'alerte, qui vous notifieront automatiquement lors de la publication de contenus sur votre nom.

Avoir une bonne hygiène informatique !

Pour quoi faire ?

Eviter d'être la victime d'une arnaque en ligne, d'une attaque ciblée ou d'une usurpation.

Protéger les informations que vous stockez sur votre terminal en cas de perte, vol.

Les conseils

Mettez régulièrement à jour vos systèmes d'exploitation et **installez un antivirus sur vos ordinateurs.** Ce sont des prérequis indispensables pour espérer protéger vos données d'une attaque de rançonciel.

Utilisez des mots de passe solides. Une bonne hygiène en termes de mot de passe et une vigilance accrue vous mettront à l'abri des cyber-risques les moins élaborés. Utiliser l'authentification à deux facteurs et un dispositif d'alerte en cas d'intrusion lorsque c'est possible. Retrouvez nos conseils pour bien protéger votre smartphone, vos boites e-mail.

Maintenez une grande vigilance lorsque vous utilisez un wifi public dont certains n'offrent pas suffisamment de protection contre l'interception de vos données.

Ayez une méfiance systématique vis-à-vis des messages suspicieux reçus dans votre boîte email ou sur votre application de messagerie.

Enfin, chiffrez vos informations les plus sensibles pour les rendre illisibles par des tiers en cas de perte ou de vol de votre terminal.

VOUS ÊTES VICTIME DE CYBERMALVEILLANCE ?

Rendez-vous sur le site www.cybermalveillance.gouv.fr/