



Checklist : Protéger ses données et sa réputation en ligne

Comment protéger ses données et sa réputation en ligne ? Spécialiste de l'e-réputation et de la protection des données, Stéphane Koch* nous livre quelques conseils simples.

✓ **Contenus en ligne associés à son nom**

Pour protéger efficacement sa réputation en ligne, il est primordial de connaître les contenus en ligne associés à votre nom en tapant régulièrement celui-ci dans un moteur de recherche. Il est dans certains cas possible d'effectuer une demande de retrait de contenu auprès du webmaster du site ou du moteur de recherche qui recense le site.

✓ **Facebook et réseaux sociaux**

Evitez de publier des contenus sensibles et prenez les mêmes précautions que dans la vie réelle. Apprenez comment [désactiver votre compte et le supprimer](#). Activez les [deux facteurs d'authentification](#). Ne partagez pas [publiquement votre liste d'amis](#) ni [vos intérêts](#) (j'aime). N'acceptez comme amis que des personnes que vous connaissez effectivement.

✓ **Comportements étranges des amis**

Les arnaqueurs peuvent pirater les comptes de vos amis et envoyer des liens à partir de ceux-ci. Si un contenu diffère de ce que votre ami publie ou envoie d'habitude, ne cliquez pas dessus et appelez votre ami sur son numéro fixe ou mobile pour le prévenir.

✓ **Copies de sauvegarde**

Effectuez régulièrement des copies de sauvegarde de vos données importantes. Veillez à protéger vos supports de sauvegarde avec un [mot de passe sûr](#) et à les conserver dans un autre lieu que l'original.

✓ **Effacement des données**

Lors que vous jetez, envoyez en réparation ou revendez un appareil (smartphone, tablette, ordinateur, clé usb, carte SD), veillez à effacer toutes les données. Soyez néanmoins conscient que certaines peuvent subsister même après effacement.

✓ **Mots de passe**

Sécurisez vos appareils et comptes en ligne avec des [mots de passe sûrs](#). Pour aller plus loin, il est possible d'utiliser un [gestionnaire de mots de passe](#), qu'il s'agit de coupler à un second facteur d'authentification (par exemple en utilisant [Google Authenticator](#) ou une clé Yubikey).

✓ **Connexion à partir d'un appareil public ou appartenant à un tiers**

Utilisez un [mot de passe à usage unique](#). Lorsque vous avez terminé, déconnectez-vous manuellement de tous vos comptes en ligne.

✓ **Gestion à distance en cas de vol d'un appareil**

En cas de perte ou de vol d'un appareil, Android Device Manager et iCloud vous permettent, à distance, de localiser celui-ci, de le bloquer et d'effacer son contenu.

✓ **Antivirus et firewall**

Ayez un antivirus à jour sur tous vos appareils (smartphone, tablette et ordinateur). De nombreuses versions gratuites offrent une protection satisfaisante. Si vous surfez sur des réseaux Wi-Fi publics, prévoyez également un firewall et pensez à sécuriser la réception de vos emails.

✓ **Applications**

Ne téléchargez des logiciels et applications que depuis des sites dans lesquels vous avez confiance. En cas de doute, renoncez. Veillez en outre à toujours maintenir votre navigateur et vos autres applications à jour.

✓ **Modules supplémentaires pour sécuriser la navigation**

À l'aide de modules pour votre navigateur, il est possible d'activer la [navigation sécurisée](#) dès que cela est possible, d'éviter que les entreprises puissent [récolter des informations](#) sur vos comportements en ligne, de vérifier la [fiabilité des sites](#) que vous visitez ou encore de [bloquer les publicités](#) en ligne.

✓ **Gratuité et publicité**

Aujourd'hui, la gratuité n'existe pas sur Internet. Les entreprises sont commerciales. Minimisez votre empreinte publicitaire en ne donnant que les [informations obligatoires](#).

✓ **Géolocalisation et publicité**

Veillez à [désactiver la géolocalisation et le suivi publicitaire](#) sur vos différents appareils lorsque vous n'en avez pas l'utilité.

✓ **Formuler les bonnes questions pour obtenir les bonnes réponses**

Nul besoin d'être un expert pour protéger sa vie privée en ligne. Utilisez les moteurs de recherche pour apprendre par exemple à [régler les paramètres de confidentialité](#) des principaux réseaux sociaux, [effacer les données de navigation](#) internet ou encore [désactiver la géolocalisation](#) de votre smartphone.

✓ **Consulter notre rubrique consacrée à la protection des données**

Notre [rubrique](#) propose un [aperçu des risques](#) en la matière, des conseils pour se protéger – [réseaux sociaux](#), [collecte de données](#), [bon sens](#), [stockage dans le nuage](#), [protection des contenus privés](#) – et pour rester dans la légalité – [droit à l'image des tiers](#), [droit d'auteur](#), ainsi que des ressources pour les [enfants et adolescents](#), les [parents](#) et les [enseignants](#).

* Diplômé en Lutte contre la criminalité économique et spécialiste en relations publiques, **Stéphane Koch** est formateur, conseiller et chargé de cours dans le domaine des technologies de l'information et de la communication.

Jeunes et médias est le Programme national de promotion des compétences médiatiques. Son objectif est d'encourager les enfants et les jeunes à utiliser les médias numériques de façon sûre et responsable. Il offre aux parents, aux enseignants et aux professionnels des informations, un soutien et des conseils sur la juste manière d'encadrer les enfants et les jeunes.
www.jeunesetmedias.ch