## Checklist

## « Protéger ses données et sa réputation en ligne »

**Spécialisé dans la gestion de la réputation sur Internet et la sécurité de l'information, Stéphane Koch* nous livre quelques conseils simples en matière de protection des données et de gestion de la réputation en ligne.**

### ✓ Recherche régulière sur son nom

Pour protéger efficacement sa réputation en ligne, il est primordial de connaître les contenus en ligne associés à votre nom. En cas de contenu indésirable, il est possible dans certains cas d'effectuer une demande de retrait de contenu auprès du webmaster du site ou du moteur de recherche qui recense le site, ou de demander le déréférencement du contenu concerné de l'index des principaux moteurs de recherche.

### ✓ 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 (likes). Vérifiez les publications dans lesquelles vous êtes identifiés. N'acceptez comme amis que des personnes que vous connaissez effectivement. Le nombre d'« amis en commun » n'est pas un critère fiable.

### ✓ 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 en général, ne cliquez pas dessus et téléphonez à votre ami pour le prévenir. Il en va de même pour les messages privés, y compris ceux reçus par l'intermédiaire de WhatsApp. Veillez à ne pas cliquer directement sur les liens qui vous sont indiqués dans les messages, et qui vous redirigent sur un contenu ou une plateforme (tels que les documents « Google Docs », ou toute autre action qui vous demande de vous identifier sur l'un de vos services web, comme « Connectez-vous à Facebook pour voir cette vidéo. »).

✓ **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 physique.

✓ **Effacement des données**

Lorsque 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 l'effacement ; le simple fait de les effacer, c'est-à-dire de les mettre dans la « corbeille », ne suffit pas. Il faut procéder à un effacement sécurisé des données.

✓ **Mots de passe**

Sécurisez vos appareils et comptes en ligne avec des mots de passe sûrs. Chaque compte doit bénéficier d'un mot de passe spécifique et unique. Il est utile d'utiliser un gestionnaire de mots de passe (uniquement si l'on utilise aussi l'authentification forte, à deux facteurs). Des outils comme Keepass, Dashlane et LastPass et 1Password fonctionnent aussi avec les smartphones Android ou Apple.

✓ **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 potentiellement localiser celui-ci, le bloquer et effacer son contenu. Il est important de conserver l'identifiant IMEI de l'appareil pour le communiquer à votre opérateur de télécommunication ainsi qu'à votre assurance, en cas de vol de votre mobile. Cet identifiant figure généralement sur la facture, sur l'emballage de l'appareil ou dans les paramètres de celui-ci.

✓ **Antivirus et firewall**

Ayez un antivirus à jour sur tous vos appareils (smartphone, tablette et ordinateur). Les versions gratuites de Sophos ou d'Avast, par exemple, offrent une protection de base. Néanmoins, les versions payantes de G Data, Kaspersky ou Bit Defender ont généralement

un taux de détection de virus plus élevé, et intègrent une suite complète d'outils de sécurité (tels que Firewall et protection contre les *ransomwares*, l'accès à la webcam, ou les intrusions). Si vous surfez sur des réseaux Wi-Fi publics, prévoyez également un VPN et pensez à sécuriser la réception de vos emails.

✓ **Applications**

Ne téléchargez des logiciels et des applications que depuis des sites en 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**

Dans les paramètres de votre navigateur, il est possible d'activer la navigation sécurisée, afin d'éviter que les entreprises puissent récolter des informations sur vos comportements en ligne, et génèrent des prix de manière dynamique lors de vos actes d'achats, en fonction de votre niveau de revenu perçu. Il faut aussi que la fonction « Ne pas me pister » soit activée dans les paramètres du navigateur. Mais il reste essentiel de vérifier la fiabilité des sites que vous visitez, ou encore de bloquer les publicités en ligne. Les sites qui proposent une navigation sécurisée (que l'on peut identifier par le « HTTPS » au début du lien Internet) sont considérés comme étant généralement plus sûrs. Différents types de navigateurs disponibles.

✓ **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. De manière générale, nous vous conseillons de

vous appuyer sur deux sources d'informations différentes, et de vérifier que les contenus de ces deux sources soient similaires.

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

Notre rubrique Sécurité & protection des données fournit des informations complémentaires et souligne les risques possibles. Elle donne également des conseils pour le quotidien, pour rester dans la légalité, et indique des ressources pour les enfants et les adolescents, pour les parents et pour 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 la Plateforme nationale 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. Le site 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