Table des matières

Guide de survie #mesdonnees

Le choix de la messagerie

- chiffrer ses e-mails avec http://openpgp.org/ afin que seul votre correspondant y accède. Il existe des extensions pour les principaux clients mails du marché (Outlook, Mail…) comme https://enigmail.net
- si on chiffre ses e-mails, être attentif aux avertissements que le logiciel de cryptage envoie (chaine de signature incorrecte, manque un élément pour le cryptage…)
- éviter les services dont les conditions générales sont peu respectueuses des données personnelles
- utiliser un service d'e-mail sécurisé basé en Suisse: https://protonmail.com/
- utiliser des e-mails "poubelle" en fonction du besoin: http://fr.getairmail.com/, http://www.yopmail.com/
- utiliser les messageries sécurisées mises à disposition (p.ex. pour le télébanking)
- retenir qu'une banque ne demande jamais d'informations personnelles ou sensibles par e-mail
- phishing PayPal: faire attention à l'e-mail de retour (par exemple info@paypa1.com) et aux messages truffés de fautes d'orthographe
- solutions de rechange pour éviter d'utiliser WhatsApp : https://threema.ch, https://www.blackberry.com/us/en/products/bbm-enterprise-bbme, https://prism-break.org/fr/projects/chatsecure/, https://telegram.org/
- se désabonner uniquement de newsletters auxquelles on s'est abonnés

Règle d'or:
Bien choisir sa messagerie en fonction de l'utilisation qu'on va en faire et des besoins qu'on a en matière de confidentialité

Connexion / Facebook login / Google Sign-In

- en créant son profil, éviter d'indiquer une adresse type prenom.nom@...
- ne pas utiliser son adresse professionnelle
- utiliser différentes adresses email : privé, prof, famille, mail "poubelle"
- retenir que naviguer sous pseudo: ce n'est pas vraiment une protection!

Règle d'or:
Etre prudent sur les autres données qu'on dévoile sur nous et réfléchir à la raison pour laquelle on les indique

Guide de survie #mesdonnees

Navigation / mouchards / cookies

- s'assurer que le cadenas est fermé dans la barre de navigation lors d'un échange de données sensibles
- vider les cookies et l'historique après chaque session, surtout si on n'est pas sur notre propre machine, ou automatiser cette tâche
- utiliser un plugin qui analyse les cookies en fonction de leur origine et évite certains traçages: https://www.ghostery.com, https://www.eff.org/fr/privacybadger, https://addons.mozilla.org/fr/firefox/addon/trackmenot/
- utiliser un bloqueur de pubs comme https://adblockplus.org/fr/
- utiliser le mode de navigation privée des navigateurs
- ne donner des infos personnelles que si la demande est pertinente
- ne pas envoyer d'informations sensibles via un wifi public
- utiliser http://www.sheriff-v2.dynu.net/views/home pour vérifier s'il y a discrimination du prix d'un produit
- assurer les mises à jour de son matériel et des programmes
- utiliser un navigateur utilisant le réseau Tor ou passer par un tunnel VPN
- utiliser des alternatives à Google (http://www.duckduckgo.com) et Facebook
- faire une recherche avec son nom dans les moteurs pour vérifier ce qu'on trouve
- utiliser http://www.youronlinechoices.com/ch-fr/ pour désactiver les cookies dévoilant nos données comportementales

Règle d'or:
Penser à ériger des barrières capables de vous protéger des intrusions

Conditions générales des services web

- retenir que si un service est présenté comme étant gratuit, c'est l'utilisateur qui devient le produit

Règle d'or:
Lire les conditions générales avant de valider son inscription

Guide de survie #mesdonnees

Réseaux sociaux

- régler les paramètres de confidentialité dans les paramètres des réseaux sociaux
- régler les paramètres de confidentialité dans les applications mobiles
- régler les paramètres de confidentialité pour les applications liées à Facebook et limiter les droits d'accès s'il y a lieu
- utiliser http://fdvt.org/ pour évaluer ce qu'on rapporte à Facebook
- voir et supprimer tous les contacts que vous avez importés depuis l'application Facebook https://www.facebook.com/invite_history.php
- désactiver dans l'application Facebook le paramètre d'importation continue de vos contacts
- voir et supprimer tous les contacts que vous avez importés depuis Messenger https://www.facebook.com/mobile/messenger/contacts
- interrompre l'importation continue de vos contacts depuis Messenger https://www.facebook.com/help/838237596230667
- contrôler les informations de votre profil auxquelles accèdent les applications installées sur les profils de vos amis https://www.facebook.com/settings?tab=applications&section=friends_share&view
- voir quels sont les centres d'intérêt en lien avec votre profil, liens que Facebook a
- défini pour vous https://www.facebook.com/ads/preferences/
- Instagram: aide pour désactiver la synchronisation des contacts et supprimer ma liste de contacts https://help.instagram.com/236691729788553
- LinkedIn: Gestion des contacts importés : https://www.linkedin.com/help/linkedin/answer/43377?lang=fr
- prendre connaissance de tous les conseils donnés par Stéphane Koch, spécialiste des réseaux sociaux http://www.rts.ch/la-1ere/programmes/on-en-parle/7981254.html/BINARY/OEP-310816-DonneesPerso-RS.pdf

Règle d'or:
Régler finement les paramètres de confidentialité pour chaque réseau social

Guide de survie #mesdonnees

Smartphones / téléphonie / géolocalisation / apps / rencontres

- noter son numéro IMEI (ailleurs que sur le téléphone) en tapant *#06#
- verrouiller son smartphone
- préférer un verrouillage de son smartphone par empreinte digitale à un code
- mettre un scotch sur la caméra
- utiliser de préférence des applications suisses
- ne pas indiquer sa date de naissance réelle, rester dans le vraisemblable
- garder la divulgation d'infos sensibles pour les rencontres en chair et en os
- choisir un lieu public fréquenté pour la première rencontre
- être attentif à l'accès que vous octroyez pour chaque application à vos données personnelles (contacts, photos, GPS…)
- L'app Exif Viewer (iOs) permet de gérer les données EXIF contenues dans ses photos
- deGeo Camera et NoLocation (iOs) permettent de prendre des photos sans donnée EXIF ou de les supprimer ultérieurement

Règle d'or:
Contrôler à quelles données personnelles les applications peuvent accéder (contacts, photos, géolocalisation…)

Les cloud sécurisés

- utiliser un certificat SSL afin de protéger les communications
- utiliser un service où le client est le seul à avoir la clé existante (chiffrement fait sur l'ordinateur)
- utiliser son propre système de cloud chiffré
- stocker les informations sensibles sur un ordinateur non connecté à internet

Règle d'or:
Ne pas mettre de données confidentielles sur le cloud

De qui se protège-t-on sur le net?
- des Etats qui exercent une surveillance
- des entreprises qui abusent commercialement de nos données personnelles
- des criminels
- de nous-même, pour préserver sa réputation

Alexis Roussel - 14 octobre 2015