Logiciels libres et protection des données personnelles

Listez vos données personnelles !

exemples :

- mots de passe / codes d'accès
- documents
- informations personnelles (adresse, téléphone...)
- données en ligne (informations liées aux comptes)
- carnets d'adresses
- favoris internet
- historique de navigation internet

La sécurité des données en trois mots : CIA

- confidentialité
- intégrité
- accessibilité

Les risques encourus par nos données personnelles

Au niveau local

perte / destruction ou vol d'ordinateur : perte de données et/ou compromission des données
ransomware : perte des données et extorsion de fonds
compromission de données par des tiers : compromission des données et/ou perte des données
mots de passe : usurpation d'identité / perte et compromission des données

deux aspects de la défense:

1. bonnes pratiques : https://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf
2. Choisir avec soin ses mots de passe -> méthode phonétique ou des premières lettres, mot de passe individualisé, changement régulier, éviter les solutions de stockage des mots de passe (https://www.ssi.gouv.fr/guide/mot-de-passe/
3. Mettre à jour régulièrement vos logiciels -> cela limite les failles de sécurité porte d'entrée de logiciels malveillants
4. Télécharger ses programmes sur les sites officiels des éditeurs -> attention aux liens sponsorisés
5. Effectuer des sauvegardes régulières -> de préférence sur un site distant de confiance,

éventuellement utiliser le chiffrement, à l'inverse attention qux WIFI publics
6. Sécuriser votre accès Wi-Fi -> rendez la borne anonyme et utilisez une clef WPA2, WEP interdit
7. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur -> code pin + schéma
8. Protéger ses données lors de ses déplacements -> sauvegarde pré-déplacement, désactivez le wifi et bluetooth si c'est inutile
    - Être prudent lors de l'utilisation de sa messagerie -> porte d'entrée privilégiée des virus par une pièce jointe ou un lien frauduleux
9. Séparer les usages personnels des usages professionnels
10. Être vigilant lors d'un paiement sur Internet -> contrôlez le chiffrement de la connection (https://) et vérifiez l'adresse du site, privilégiez le paiement indirect ou par validation SMS
11. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique (voir ensemble de la séance)

2. Réponses logicielles

- antivirus / antimalware -> OUI les Apple sont concernés ! A titre indicatif : avast
- parefeu > à titre indicatif comodo ou zonealarm sur Windows / application native Apple OS X
- sauvegarde : à titre d'exemple : synchronisation framadrive par owncloud mais ce n'est pas de la sauvegarde !!

sur internet

exemple des informations recueillies par un compte google

quelles infos sur le web et où ?
réseaux sociaux : exemple de facebook et son panneau de gestion de la confidentialité
applications (mobiles ou ordinateurs)
boîtes email
sites de e-commerce, les cookies
calendriers en ligne
stockage en ligne
historique de navigation
mots de passe firefox !!!
cache !!! videz le avec ctrl+F5

-> concept d'empreinte digitale

Les Ateliers du PicInfos & Astuces de bonne pratique informatique

Gardez ces astuces et ces liens avec vous, afin d'acquérir le bons réflexes !

Les moteurs de recherche : fuyez Google & Yahoo!

- qwant.com (moteur de recheche français qui ne traçe ni ne filtre les contenus)
- duckduckgo.com
- startpage.com (utilise Google à votre place) ou startpage.eu (metamoteur sauf google)
- ecosia.org (moteur de recherche à vocation écologique!)
- lilo.org/fr

Les applications en ligne : framasoft.org en recense des dizaines très pratiques et gratuites. E.g. :

- un éditeur de texte à partager : framapad.org
- un tableur type excel en ligne, à partager également : framacalc.org
- un organisateur de réunion du type Doodle : framadate.org
- un disque dur en ligne, du type Googledrive : framadrive.org
- un outil de partage de photos : framapic.org

Les hébergeurs de messagerie en ligne : être protégé a un prix !

- gandi.net (12euros/an) est le grand classique du webmail alternatif
- posteo.de/en (12euros/an) est allemand, et se veut aussi sécurisé qu'écologique
- protonmail.com (gratuit) est basé en Suisse pour assurer l'anonymat de ses clients
- ovh.com/fr

Améliorer Firefox pour mieux surfer :

- adblockplus.org permet de bloquer la publicité en ligne, mais n'empêche pas la récupération de vos données.
- Google Redirects Fixer & Tracking Remover permet, si on utilise Google d'aller directement sur le site choisi sans passer par le tracker (suiveur) de Google qui enregistre vos clics.
- HTTPS everwhere permet de crypter ses informations en permanence, comme vous le faites lors de paiements en ligne.
- Paramétrez l'historique et les cookies
- ghostery ou Ublock origin
- un peu à part : modifier votre fichier host ! http://someonewhocares.org/hosts/

Quelques réflexes à conserver :

- Ajoutez en favori les sites que vous visitez régulièrement : il n'y a pas de limite de nombre
- Effacez vos historiques régulièrement si ce n'est pas fait automatiquement.
- Lorsque vous vous connectez à un compte (facebook, google), ne faites que ça et n'ouvrez pas d'onglets à côté si vous êtes connectés
- Quittez Facebook et rejoignez Diaspora !
- Souscrivez à un abonnement chez FrenchDataNetwork (association : fdn.fr)