PROTECTION DES DONNÉES PERSONNELLES ET PROFESSIONNELLES

Au-delà du RGPD: quels sont les risques encourus ? comment se protéger ?

PRÉSENTATION

- Nicolas Hochet – URFIST Nice
- nicolas.hochet@univ-cotedazur.fr

- Tour de table
- Attentes et niveau de connaissances

AU-DELÀ DU RGPD ?

Qu’est ce que le RGPD ? (en quelques mots…)

- Le Règlement général sur la protection des données (RGPD) est le nouveau cadre juridique de l’Union européenne qui gouverne la collecte et le traitement des données à caractère personnel des utilisateurs. Il est entré en vigueur le 25 mai 2018

Qui concerne-t-il ?

- **Tout organisme quels que soient sa taille, son pays d’implantation et son activité, peut être concerné.**
- En effet, le RGPD s’applique à toute organisation, **publique et privée**, **qui traite des données personnelles pour son compte ou non, dès lors** :
  - qu'elle **est établie sur le territoire de l’Union européenne**
  - ou que son activité cible directement des **résidents europ**

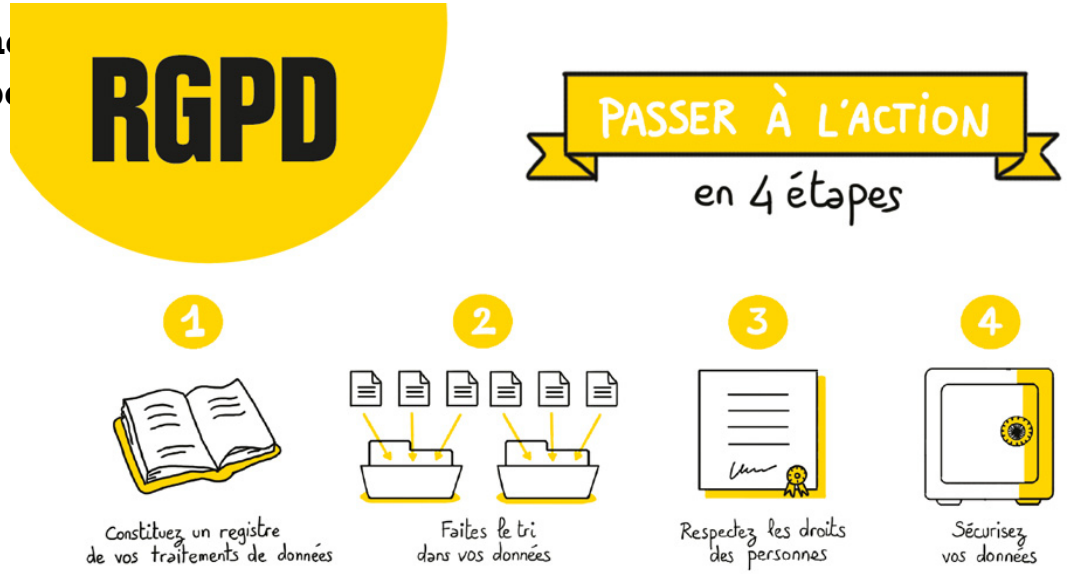
Contre quoi me protège-t-il ?

- Vidéo de présentation

Qu’est-ce qu’il ne couvre pas ?

- Hors union européenne attention avec vos données

Carte interactive CNIL



DE QUELLES DONNÉES PARLE-T-ON ?

- Qu'est ce qu'une « donnée personnelle » ?

Selon la loi Informatique et Libertés (1978), *« constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »*

- Distinction entre données personnelles et professionnelles
  - Responsabilité engagée dans le domaine professionnel ?
- Les données « évidentes » : fichiers, mails, informations bancaires, d'identité…
- … et celles qui le sont moins :
  - Objets connectés
  - Données de santé…
  - Où sont stockées vos données ? (perso et pro ?)
  - Etes-vous prêts à :
    - Les exposer publiquement ?
    - Les perdre ?

LES DONNÉES A CARACTÈRE PERSONNEL SELON LA LOI

- **La nature de la donnée n'a pas d'importance**
  - Exemple : la consommation électrique d'un logement
- Dès lors **qu'il y a un lien vers une personne**
  - Lien direct : conso électrique + nom
  - Ou lien indirect : conso électrique + numéro client fournisseur énergie

RGPD

Cas particulier des « données sensibles » (origines raciales, ethnique, opinions politiques, philosophiques, religieuses ou syndicales ou relatives à la santé ou vie sexuelle…) NE PEUVENT PAS ETRE COLLECTEES ET TRAITEES (hors exceptions définies type professionnels de santé, urgences…)

SÉPARER VIE PRIVÉE ET PROFESSIONNELLE

- Une grande partie des incidents survenus dans les entreprises sont causés par la négligence des employés *(les chiffres varient selon les études mais on parle généralement de 50%)*.
- Les pirates exploitant régulièrement les liens que chacun entretient entre vie privée et professionnelle. Il y a donc lieu d'**édifier une barrière entre ces deux mondes**. La consultation d'emails personnels ou de réseaux sociaux sur son lieu de travail s'avère une source de risques, de même que l'utilisation de mots de passe identiques pour s'identifier à la fois dans son entreprise et chez soi.
- Le **développement du télétravail** ajoute une couche de risque supplémentaire, les espaces en dehors de l'entreprise pouvant être vecteurs d'inoculation de **malwares**. C'est par exemple le cas lorsqu'un collaborateur recharge son mobile professionnel sur un ordinateur d'un espace de travail partagé, ou lorsqu'il utilise sa clé USB personnelle pour transférer des données sur le serveur de l'entreprise.

RESPONSABILITÉS PROFESSIONNELLES

- Si vous disposez d'une délégation de pouvoir, votre responsabilité peut être engagée pénalement en cas d'infraction relative au traitement des données à caractère personnel (l'employeur conservant la responsabilité civile et l'entreprise la responsabilité pénale de la personne morale) . Vous engagez également votre responsabilité civile à l'égard du tiers victime de l'infraction, en cas de faute qualifiée (au sens de l'article 121-3 du Code pénal) et ce même si l'infraction et commise dans l'exercice de vos fonctions. *A noter : La réalité et la portée de la délégation de pouvoirs relèvent de l'appréciation souveraine des juges, toutefois il peut être utile de se rapprocher d'un avocat spécialisé avant d'accepter une délégation de pouvoir (exemple d'infraction des salariés : EDF).*
- la copie, l'usage ou la modification d'un logiciel sans licence est illégal et engage la responsabilité du salarié et de l'employeur. Le salarié risque le licenciement pour faute grave.

LES RISQUES SONT-ILS RÉELS ?

Les faits et exemples :

- La France serait le 2nd pays le + touché par les vol de données (étude Symantec 2016)
- Piratages et vol de données Google, Facebook, Uber… : Le stockage de + en + courant de données dans le cloud (information personnelles détenues par des sites internet, messageries, photos, sauvegardes, disques virtuels…) implique une exposition toujours plus importantes de vos données personnelles à des risques que vous ne maitrisez par (ou peu) :
- Vols de données importants :
  - BRITISH Airways (Août 2018) : 380.000 comptes clients (dont données bancaires) piratés.
  - UBER (2016) : 1,4 million de comptes français volés
  - YAHOO (2013) : 3 milliards de comptes touchés !
  - ASHLEY MADISON (2015) : Un groupe de pirates rend public 30Go de données du site de rencontres adultères (nom, mail, préférences sexuelles…)
  - CAMBRIDGE ANALITICA (devenu scandale FACEBOOK) : 87 millions de compte récupérés sans consentement (comptes des « amis » et « amis d'amis » des participants à un questionnaire Facebook. Ces données ont ensuite été traitées afin de faire du profilage et notamment influer sur la campagne américaine de Donald Trump.

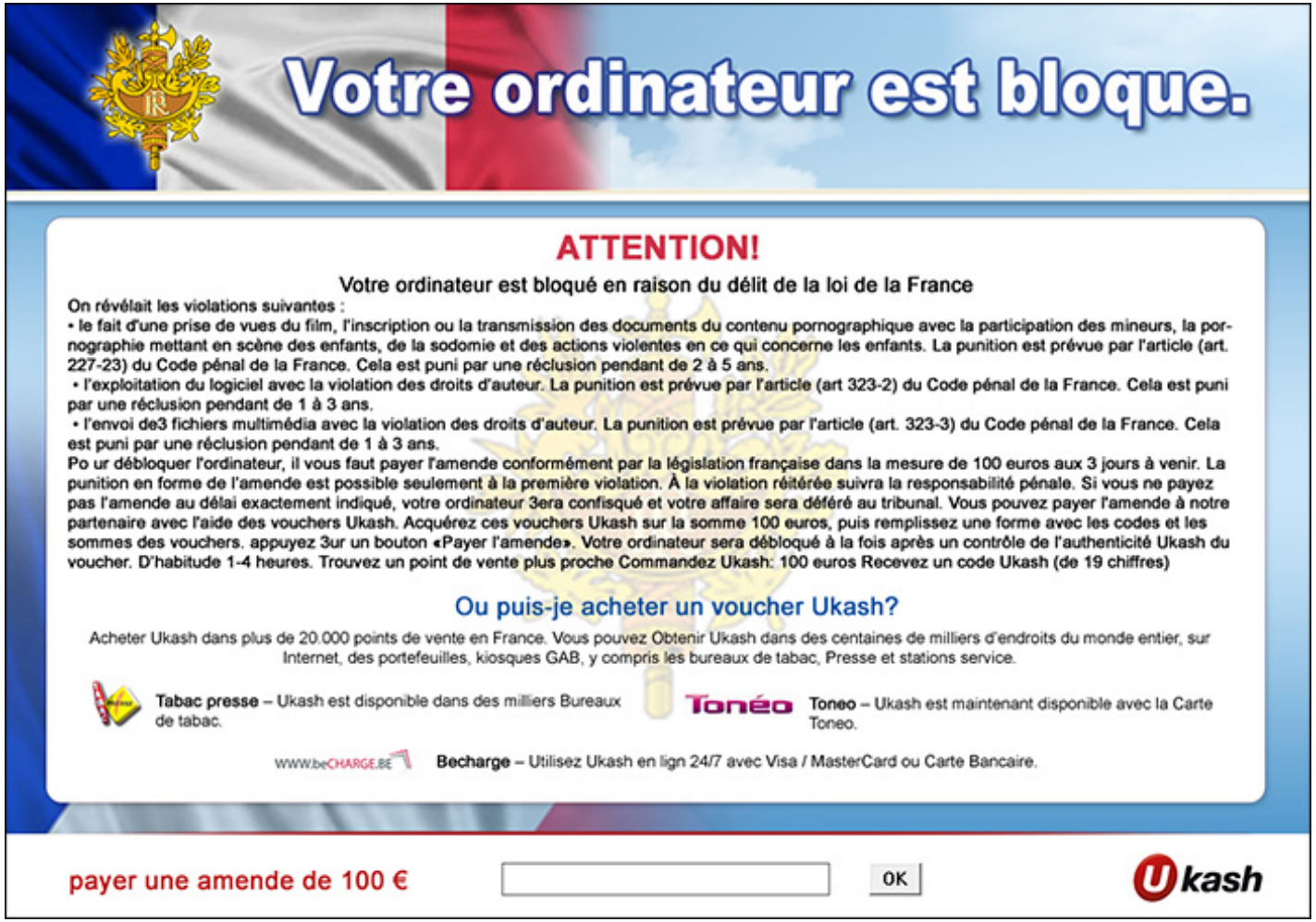
L'EXEMPLE DE LA CAMPAGNE TRUMP

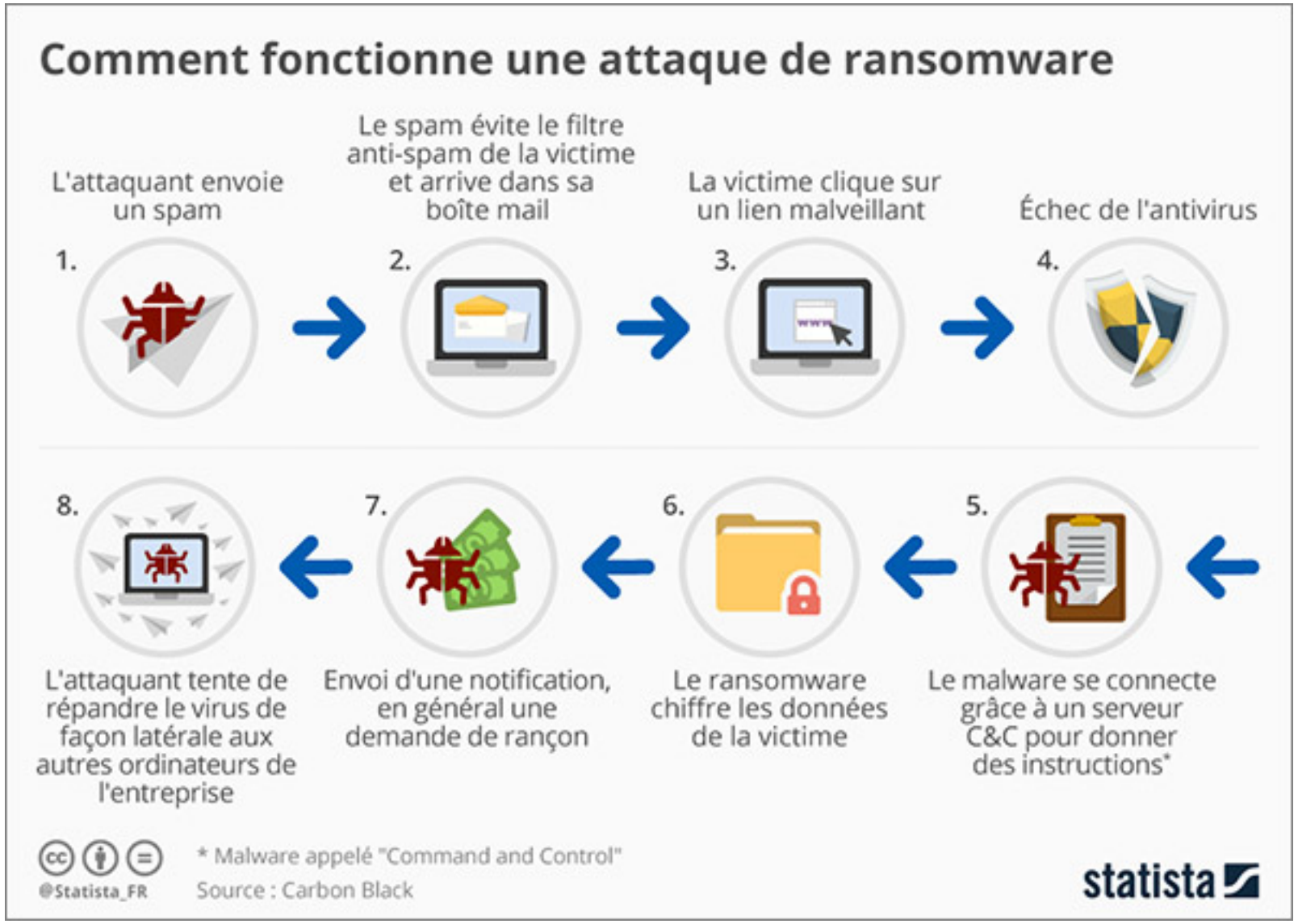
- L'enquête de Thomas Huchon « Comment Trump a manipulé l'Amérique » (Arte – 9/10/18) présente un point de vue inquiétant sur la campagne de 2016 arguant que sans le soutien de Cambridge Analytica, Trump n'aurait probablement pas gagné l'élection :
  - Le rôle de Robert Mercer (soutien initial de Ted Cruz)
  - Le soutien financier, les comités d'action politique et l'équipe Steve Bannon
  - L'achat de données auprès de Facebook, Google, organismes de crédit, banques…
  - La récupération de données non consenties (Facebook/Cambridge Analytica)
  - Les algorithmes du trading appliqués aux profilage psychologique
  - Le ciblage de profils et d'électeurs indécis dans les états clef pouvant faire basculer l'élection
  - Le principe des « dark posts » et des fake news ciblées
  - La victoire de D. Trump malgré 3 millions de voix en faveur de H. Clinton : 77.000 voix « stratégiques »

LES RISQUES POSSIBLES

- Les messageries en ligne (et/ou non cryptées)
  - Que contiennent vos mails (stockés… on ne sait pas où…) ? Y avez-vous attachés des pièces jointes (photos, impôts, carte identité, attestations, justificatifs, courriers juridiques, professionnels, administratifs…)
  - Si mon mail est piraté que vont devenir ces documents ?
  - Auriez-vous envoyé la même chose sur une carte postale ?
- Les ransonwares et cryptolockers : ciblent particuliers et entreprises, blocage de fichiers, de sites web, demande de rançon…
- Le vol de données bancaires (CB)
- Les smartphones
- Usurpation d'identité numérique…
- Etes-vous certains de votre e-reputation ?
  - Savez-vous que 85% des recruteurs effectuent une recherche sur internet avant d'embaucher un candidat *(Enquête 2017 Regionjob auprès de 324 recruteurs)*
  - Que peut-on trouver sur vous sur internet ?
    - Généralités
    - Outils et essais

LES RANSOMWARES




Comment fonctionne une attaque de ransomware
1.
L'attaquant envoie un spam
2.
Le spam évite le filtre anti-spam de la victime et arrive dans sa boîte mail
3.
La victime clique sur un lien malveillant
4.
Échec de l'antivirus
5.
Le malware se connecte grâce à un serveur C&C pour donner des instructions*
6.
Le ransomware chiffre les données de la victime
7.
Envoi d'une notification, en général une demande de rançon
8.
L'attaquant tente de répandre le virus de façon latérale aux autres ordinateurs de l'entreprise
@Statista_FR
* Malware appelé "Command and Control"
Source : Carbon Black
statista

SE PROTÉGER DES RANSOMEWARES

- Sauvegarder ses fichiers (au minimum ses fichiers sensibles) : Disque dur externe, station de sauvegarde, en ligne (Google drive, Dropbox, iCloud…), Time machine…
- Maintenir à jour son système (OS) et ses logiciels
- Sur Windows 10 : activer la protection des fichiers
- Utiliser un antivirus à jour
- Se méfier des pièces jointes
- En cas d'infection :
  - Débranchez l'ordinateur infecté du réseau, des disques externes…
  - Si l'ordinateur n'est pas bloqué utilisez un logiciel de désinfection
  - Si tout est bloqué utilisez un CD/clef bootable
  - Dans le pire des cas réinstallez le système et restaurez vos fichiers sauvegardés… Mais ne payez jamais !

LES CARTES BANCAIRES

- + 1 millions de victimes en France en 2016 (Observatoire national de la délinquance et des réponses pénales (ONDRP))
- + 18.000 plaintes en 3 mois recensées par la nouvelle plate-forme en ligne PERCEVAL (signalement officiel sur « service-public.fr » des fraudes à la CB) lancée en Juin 2018 !
- De multiples techniques de vol : physique, copie/clone (faux distributeur, chez le commerçant, espionnage à distance du code…), usurpation d'identité, technique de phishing, piratage d'un site internet détenant vos coordonnées bancaires, virus (malware) sur votre ordinateur…
- Se protéger : Installer un firewall, un anti-malware, ne payer que sur des sites sécurisés (https), préférer les paiement à double authentification, sécuriser son compte mail, éviter les sites « douteux », vérifier régulièrement ses comptes bancaires.

LES SMARTPHONES

Soyons clairs : la plupart d'entre nous détenons dans nos téléphones une grande partie de notre vie numérique… Et souvent également celle de notre entreprise. Même si ils n'ont pas l'apparence d'un ordinateur, ils en sont pourtant. Les risques encourus sont donc similaires mais accentués par la mobilité :

- **Divulgation de données** suite au vol ou à la perte de l'appareil : le smartphone est perdu ou volé et sa mémoire n'est pas protégée, ce qui permet à quiconque d'y accéder.
- **Divulgation non intentionnelle de données :** lorsque l'utilisateur du smartphone divulgue lui-même des données, sans le vouloir : par exemple, par la géolocalisation de photos ou le partage public d'informations sur les réseaux sociaux…
- **Attaque sur un smartphone déclassé** : un smartphone est donné, revendu, mais il n'est pas correctement «nettoyé », de sorte qu'un pirate peu facilement accéder aux données.
- **Attaques de phishing** : un pirate peut récupérer des données de connexion ou un numéro de carte de crédit grâce à de fausses applications ou de messages qui semblent crédibles. En outre, **les filtres anti-phishing ne fonctionnent pas** sur les smartphones.
- **Attaques par Spyware** : si un Spyware a été installé sur votre smartphone, il peut collecter ou même modifier une grande quantité de données. Les spywares peuvent atteindre toute forme de donnée personnelle.
- **« Network Spoofing »** : un pirate peut déployer un point d'accès WiFi ou GSM pour que des utilisateurs s'y connectent en pensant que c'est un point d'accès légitime. Il pourra ensuite librement intercepter les données qui circulent entre le point d'accès et les smartphones des utilisateurs connectés. Ces données lui permettront de mener des attaques ultérieures, comme par exemple l'appel de numéros surtaxés.

SMARTPHONES & RISQUES « CONSENTIS »

Outre les risques de piratage évoqués, les smartphones sont également les meilleurs agents de renseignement vous concernant. Ils sont en effet équipés d'une multitude de capteurs souvent ignorés par les utilisateurs : *GPS, appareils photo, micro, puce NFC, accéléromètres, gyroscopes… ,*

Dans le pire des cas ces capteurs peuvent être piratés et permettre de vous espionner mais très souvent vous donnez (ou vos collègues, amis, famille), plus ou moins consciemment, l'accès à votre localisation, votre activité physique, vos contacts, vos centres d'intérêt… à de nombreuses compagnies privées le plus souvent étrangère : Facebook, Google, Instagram, Snapchat, Apple…

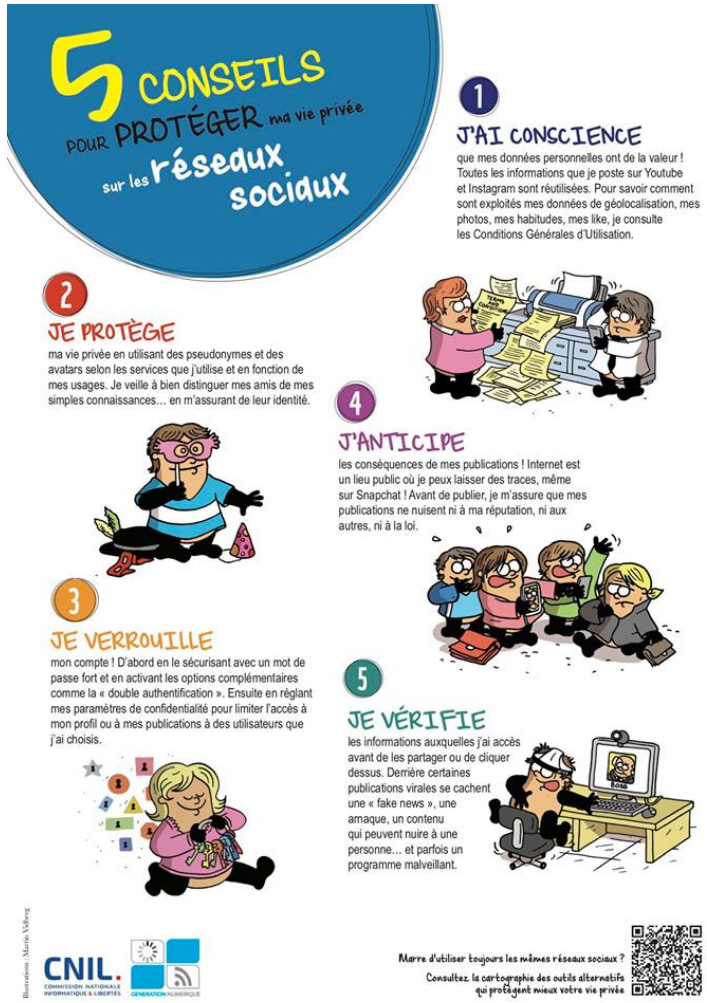
- Lisez-vous toujours, et tenez-vous compte, des avertissements « j'autorise l'application à utiliser mon appareil photo, ma position… ??? –

Les applications et l'intrusion dans la sphère privée sont en constante augmentation du fait notamment de l'explosion du marketing géolocalisé et ciblé qui vise à vous proposer un produit selon votre position, la météo, vos habitudes… (Waze, Maps…) mais également d'applications qui collectent vos données sans votre consentement (et sans nécessité).

LIMITER L'EXPOSITION DE SES DONNÉES

Protéger son compte Google et limiter la collecte de données :

- **Astuce n°1**
  Supprimer les annonces Google est impossible. Mais vous pouvez néanmoins empêcher que celles-ci soient basées sur vos centres d'intérêt.
  Où ça ? Dans "mon compte" > "paramètres des annonces".
- **Astuce n°2**
  Désactiver la collecte de vos données de géolocalisation par Google Maps se fait en quelques clics.
  Où ça ? Dans "mon compte" > "vos informations personnelles" > "accéder aux commandes relatives à l'activité" > désactivez l'onglet "historique des positions".
- **Astuce n°3**
  Effacer votre historique de navigation dans Chrome n'empêche pas Google de collecter des informations sur votre activité (recherches et sites visités). Les supprimer prend 15 secondes.
  Où ça ? Dans "mon compte" > "accéder à mon activité" > "supprimer des activités par" > sélectionnez "toute la période" et "tous les produits" > "supprimer".
- **Astuce n°4**
  Depuis la page compilant l'ensemble des applications ayant accès à certaines de vos données Google, vous pouvez supprimer les droits d'accès que vous ne jugez plus pertinents.
  Où ça ? Dans "mon compte" > "applications et sites connectés".



GÉRER SA PRESENCE SUR RÉSEAUX SOCIAUX

USURPATION D'IDENTITÉ EN LIGNE

- « L'usurpation d'identité consiste à utiliser, sans votre accord, des informations permettant de vous identifier. (…) (nom, prénom, mail, photos, identifiants…). Ces informations peuvent ensuite être utilisées à votre insu, notamment pour souscrire sous votre identité un crédit, un abonnement, pour commettre des actes répréhensibles ou nuire à votre réputation. » *(www.cnil.fr)*
- L'usurpateur peut soit se faire passer pour vous en créant de faux comptes Twitter, Facebook… Soit utiliser vos vrais comptes si vos identifiants ont été piratés… Dans les 2 cas vous ne maitrisez plus votre « e-reputation » (de nombreux sites ont mis en ligne des procédures de récupération de compte usurpés et de signalement des imposteurs).

Figure 1. L'identité numérique (d'après www.buschini.com)

GÉRER SON IDENTITÉ NUMÉRIQUE

- Quelles sont les traces que je laisse sur internet ?
- Quels éléments permettent de m'identifier ?
- Ces informations sont elles exactes ?
- Suis-je d'accord pour les diffuser publiquement ?
- Ceux qui les diffusent ont-il obtenu mon consentement éclairé ?
- Puis-je facilement modifier ou supprimer ces informations ?

GÉRER SA PRÉSENCE NUMÉRIQUE

E-RÉPUTATION

- Qu'est-ce-que la "e-réputation " ?

L'e-réputation est l'image numérique d'une personne sur Internet. Elle est constituée par tout ce qui est accessible en ligne lié à cette personne : réseaux sociaux, blogs, plateformes vidéos, commentaires sur des sites…

- Est-ce important ?

La recherche d'informations sur une personne est de plus en plus utilisée à la fois sur un plan personnel (famille, amis, connaissances…) mais également dans le domaine professionnel (recruteurs, employeurs, collègues, clients, relations…); il devient donc essentiel de **contrôler** et de **maîtriser** son image numérique accessible par tous.

- Est-ce maitrisable ?

Si vous pouvez (plus ou moins) contrôler les contenus mis en ligne par vous même, il peut être compliqué de gérer l'image qui ne dépend pas de vous car publiée par d'autres (bienveillants ou non) : « tags », citations, photos, usurpation, dénigrement…

E-RÉPUTATION

- Comment la contrôler ?

La première démarche consiste à effectuer une enquête sur vous-même :

- Le minimum vital : un mini audit sur Google (ne pas oublier la recherche par images…)
- Les réseaux sociaux : déconnectez-vous de tous vos comptes et regardez ce qu'un anonyme peut voir sur vous. Si possible, effectuez la même recherche avec un compte « ami d'ami ».
- Soyez cohérent : Evitez d'afficher des informations variées ou contradictoires entre vos différents profils, notamment professionnels.
- Testez-là : https://www.nothing-to-hide.fr

- Que faire en cas de contenu négatif nuisant à votre réputation ?

- La loi informatique et libertés permet à toute personne présentant des motifs légitimes de demander la suppression de données la concernant diffusées sur internet.
- La demande s'effectue auprès du site à l'origine de la publication. En cas de refus il faudra porter l'affaire en justice ; en cas de de non-réponse sous 2 mois la CNIL pourra intervenir.

QUELS SONT VOS DROITS ?

Le droit d'accès

Vous pouvez demander directement au responsable d'un fichier s'il détient des informations sur vous, et demander à ce que l'on vous communique l'intégralité de ces données.

Le droit à la portabilité

Vous pouvez récupérer une partie de vos données dans un format lisible par une machine. Libre à vous de stocker ailleurs ces données portables ou de les transmettre d'un service à un autre.

Le droit au déréférencement

Vous pouvez saisir les moteurs de recherche de demandes de déréférencement d'une page web associée à votre nom et prénom.

Le droit de rectification

Vous pouvez demander la rectification des informations inexactes vous concernant.
Le droit de rectification complète le droit d'accès.

Le droit d'opposition

Vous pouvez vous opposer, pour des motifs légitimes, à figurer dans un fichier. Vous pouvez vous opposer à ce que les données vous concernant soient diffusées, transmises ou conservées.

Le droit d'accès aux fichiers de police, de gendarmerie, de renseignement, FICOBA

Lorsque vous ne pouvez pas demander directement aux services de police, de gendarmerie ou de renseignement, ou à l'administration fiscale d'accéder aux données qui vous concernent, le droit d'accès s'exerce de manière indirecte par l'intermédiaire de la CNIL.

LES DONNÉES MOINS « ÉVIDENTES »

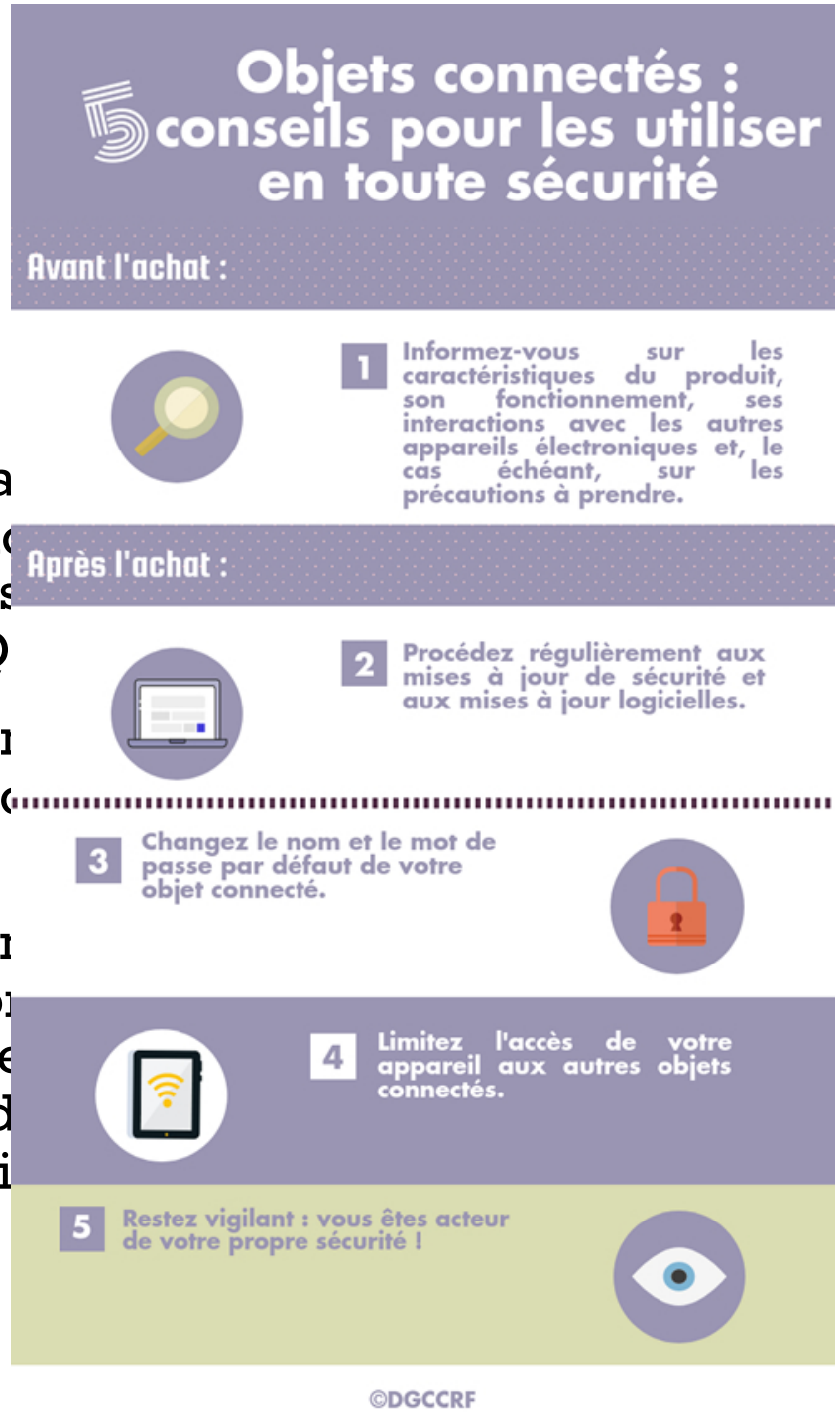
… Mais vulnérables

LES DONNÉES DE SANTÉ

- Des données sensibles mais convoitées :
  - Sensibles car relevant de la vie privée et soumises au secret professionnel mais convoitées par de multiples acteurs (laboratoires, assureurs, industriels…)
  - Vulnérables car insuffisamment protégées : matériels vieillissant, obsolescence du matériel informatique, manque d'audits de sécurité, failles de sécurité… A ce sujet par exemple la CNIL à récemment mis en demeure l'Assurance maladie.
  - Exposées car le système de santé est nécessairement ouvert à de multiples acteurs (150.000 structures, + 1 millions de personnels de santé) et à des objets connectés qui se banalisent (tablettes, applications mobiles…, cloud…) parfois peu sécurisés.
  - Des données protégées (en France et en Europe) mais exposées aux Gafa : Les données bénéficient en France d'une protection juridique importante mais la montée en puissance du big data (risques de piratage) et l'omniprésence des gafa dans le domaine des objets connectés (au travers de capteurs notamment) menacent la confidentialité de celles-ci.

LES OBJETS CONNECTES

- Quelles données ? → Surveiller son rythme cardia
  tester sa glycémie, surveiller à distance son domic
  d'énergie, remplir son frigo, poser un question à s
  Alexia, Siri… Où sont stockées c(s)es données ? Q
- Quels risques ? → Utilisation commerciale des don
  : comment garantir l'anonymat des données collec
  Comment se prémunir du piratage ?
- Comment se protéger ? → Avant l'achat il convien
  caractéristiques, le fonctionnement, le type de don
  d'anonymisation… Après l'achat il faut sécuriser le
  paramètres de partage, veiller aux mises à jour (d
  les mots de passe par défaut et les modifier réguli



COMMENT SE PROTÉGER ?

- Utiliser un antivirus (et le garder à jour…) → aujourd'hui + fonctionnalités (Phishing…)
- Protéger ses mots de passe !!! (oui 3 !)
  - Faire un test sur pwned : https://haveibeenpwned.com
  - NE PAS UTILISER LE MEME MOT DE PASSE PARTOUT
  - Utiliser les doubles identifications
  - Complexifier ses mots de passe → un méthode simple
  - Utiliser plusieurs adresses des messagerie
    - Adresse professionnelle (et QUE professionnelle)
    - Adresse personnelle
    - Adresse « poubelle »
  - Ne répondez pas, n'ouvrez pas les mails inhabituels et Méfiez-vous !
    - Support@microsft.com n'est pas Microsoft, DHL.fr… n'est pas DHL (.com/fr)
    - Affichez l'adresse mail de l'expéditeur et pas seulement son nom !
    - En cas de doute vérifier systématiquement sur le site « original » (alertes, infos phishing…)
  - **Utiliser un gestionnaire de mots de passe**

Ma fille Emilie est née en 2000 à Nice

↷

MfE&ne2000@N

Non ce n'était pas le radeau de la méduse ce bateau

↷

Ncn'éplr2lmcb

Mnémotechnique… et plus efficace que *123456789* ou *laurent06*…

COMMENT SE PROTÉGER ?

- Il existe de nombreuses alternatives peu intrusives permettant de contrôler l'utilisation de vos données :
- Navigateurs :
  - Surfez en mode « incognito »
  - Utilisez un navigateur moins intrusif :
  - Désactivez les options de pistage, bloquez les cookies (attention nombreux sites ne fonctionnent plus)
- Choisissez un **moteur de recherche différent de Google** (90% des recherches) qui ne collecte pas vos données (pas de pistage ou de stockage de cookies):
  - Qwant (français, code source à disposition de la CNIL)
  - DuckDuckGo (mais US donc attention loi partage de données (PRISM)…
- Naviguez en **Https** *(extension Https Everywhere)*
- Installez un filtre/protection (dans le navigateur) **anti phishing**
- Installez un bloqueur de publicités
- Cryptez vos données sensibles et/ou exposées (dans le Cloud par exemple)

LES OUTILS

- Les bloqueurs de publicité & malwares : Adblock, Adguard, uBlock…
- Les firewall et antivirus : Avast, Bitdefender, Kaspersky
- Les VPN : Hoxx VPN Proxy, Touch VPN…
- Le HTTPS : https everywhere, Smart HTTPS…
- Réputation numérique : NothingtoHide
- Cryptage de fichiers (logiciels libres) : 7-zip, Peazip, **VeraCrypt,** Axcrypt (PC)…
- Créer une identité numérique « validée » : La Poste, France Connect…

LES GESTIONNAIRES DE MOTS DE PASSE

- Nombreuses alternatives sur le marché (libres ou commerciales)
- Renforcent considérablement la dureté des mdp et leur non reproductibilité
- Un seul mot de passe à retenir (mdp « maître »)
- Fonctionnement autonome et/ou extension du navigateur
- Gestion centralisée possible (synchronisation entre tous vos ordinateurs, tablettes et mobiles) → pose la question du stockage « cloud » (cryptage obligatoire)
- Remplissage automatique de formulaires (stockage des identités)
- Stockage de notes sécurisées (+partage sécurisé)
- Génération aléatoire de mdp sécurisés
- Base commune de mdp (sécurisée)

LES DIFFÉRENTES SOLUTIONS POSSIBLES

- intégrées aux navigateurs (Firefox, Chrome, Internet explorer…)
  - Nécessite d'être « connecté » au navigateur (et permet usage « cloud »)
  - Ex. Firefox (similaires autres navigateurs) – Burger/préf./vie privée & sécu (Accès Worpress)
  - Enregistrer mot de passe 1 fois puis automatique ensuite
- Intégrées au système d'exploitation (ex : le Trousseau iCloud chez Apple)
  - Même principe : ex. avec Safari (Accès Unice) → Présentation Trousseau
- Logiciels autonomes (liés à un ordinateur)
  - Ex. KeePass – Logiciel libre, très sécurisé, mono plateforme (pas de stockage Cloud)
- Solutions centralisés (Cloud – mais non obligatoire)
  - Dashlane, 1password, LastPass, Roboform… A vvoir selon sécurité, besoins, fonctionnalités, prix… Nombreux comparatifs disponibles.

RISQUES/AVANTAGES

- Stockage au même endroit de toute sa « vie » numérique
- Possibilité de piratage des éditeurs/hébergeurs (mais les mdp sont cryptés)
- Hors libre et navigateurs, solutions logicielles payantes sous forme d'abonnement
- ATTENTION à la perte de mot de passe maître…

- Renforcement de TOUS vos mots de passe --> il devient inutile de les retenir donc vous pouvez utiliser des mdp « forts »
- Evite le piratage en série → Si on vous pirate un couple mail/mdp (hack d'un site internet par exemple) il ne pourra pas être reproduit sur d'autres sites.
- Intégration multiplateformes et synchronisation via internet

EXEMPLE/ESSAI LASTPASS

- Installation de l'extension sur Firefox
- Connexion au compte test existant :
  - Exemple de stockage du mdp avec Roboform
  - Exemple de sécurisation avec TouchID Mac
- Connexion à un site de test : Wordpress
  - Enregistrer identification dans LastPass
  - Déconnexion
  - Reconnexion : Identification LastPass présente dans zones de mdp
  - Accéder au coffre-fort LastPass : WP présent (modifiable/accessible…)
  - Si changement de mdp : le logiciel détecte changement et propose màj de la base