Vulnérabilité numérique face à la cybercriminalité

Par Frédéric Monceau

Synthèse de la conférence du vendredi 24 mars 2017 organisée par l'APELGC et l'API

Il ne s'agit pas ici de transcrire la totalité des propos de M. Monceau, mais à partir de quelques notes, de donner en peu de traits tout à la fois les risques de l'environnement numérique dans lequel nous baignons, et quelques pistes pour s'en prémunir.

1- Les échanges de données numériques sont de plus en plus nombreux, par nos ordinateurs, nos téléphones portables, nos objets connectés, nos cartes bancaires ou commerciales, nos badges d'accès…

2- Ces échanges se font directement, avec une liaison filaire ou une connexion, dont nous sommes conscients, mais aussi par Wifi, bluetooth, ou simple contact (type RFID), parfois à notre insu.

3- Les informations qui circulent intéressent :

   a. Le « secteur marchand » comme Google qui utilise nos pérégrinations sur le net pour déterminer nos profils de consommateurs.

   b. Certains états (les informations de Google et les mails peuvent être analysés par le FBI et la NSA aux Etats Unis. Il est certain que d'autres « puissances étrangères » tentent aussi de maitriser les contenus numériques. Dans ce but, la Russie et la Chine ont développé leurs propres réseaux sociaux).

   c. Des délinquants du NET :
      - Pédopornographie : les enfants peuvent être contactés avec de fausses identités sympathiques, avant d'être approché directement par des prédateurs qui auront enregistré, au travers d'échanges (anodins au début), leurs photos, leur adresse et leurs gouts.
      - Chantage à « l'e-réputation » : après quelques échanges avec une correspondante complaisante, et quelques moments compromettants partagés par vidéo, une menace de diffusion est faite, à défaut de paiement.
      - Rançons demandées après avoir crypté (« chiffré ») le contenu des disques durs, par des petits logiciels contenus dans des pièces jointes (comme les PDF) : après le blocage de l'ordinateur, un mail est envoyé à la victime pour lui demander une rançon (5000€, en *bitcoin*, qui peuvent doubler…)
      - Tentatives de capter les mots de passe ou les numéros de cartes bleues par des mails imitant la forme de sites officiels fiables.
      - Possibilité d'exploitation de commentaires de vacances pour cambrioler le domicile principal, repéré par des informations parcellaires glanées dans les pages des réseaux sociaux.
      - Etc…

4- La législation est très éparpillée et parfois contradictoire, mais l'article 323-2 du Code Pénal punit de 5 ans d'emprisonnement et 75 000 euros d'amende le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données.

Quelques conseils utiles :

Ne pas utiliser le moteur de recherche Google, qui mémorise toutes vos requêtes, mais plutôt Ixquick.eu (qui sert d'écran entre vous et Google) ou même Qwant.com qui ne gardent pas la traces de vos recherches.

N'utilisez pas d'autres **clés USB** que les vôtres, et jamais une clé trouvée par hasard ! Vous ne savez pas ce qu'elle contient et c'est mieux pour vous. A ce titre, enfermez vos données dans des containeurs de chiffrement (type « *ZED !* »)

N'ouvrez pas de pièces jointes venant d'un destinataire inconnu, mais vérifiez auparavant :

1- L'adresse mail développée afin de s'assurer qu'elle n'est pas « exotique »,
2- La cohérence des propos, la langue utilisée, la bonne syntaxe, etc,
3- La nécessité réelle d'ouvrir la PJ.

Sur les **réseaux sociaux**,

1- Limitez la publication de vos données personnelles, en particulier votre adresse,
2- N'acceptez comme amis que ceux que vous connaissez dans la vraie vie,
3- Utilisez des pseudos, pour vous et vos vrais amis.
4- Avant de transmettre des photos personnelles, vérifiez et si besoin effacez les EXIF ou métadonnées (par clic droit / propriétés /détails) qui peuvent contenir des informations de localisation, surtout si elles sont prises par un smartphone (nécessité de passer par un ordinateur pour cette toilette).
5- Sur son téléphone portable, ne pas avoir en permanence le Wifi et le bluetooth connecté.
6- Ayez une méthode de **création de mot de passe de 12 caractères minimums**, utilisant simultanément chiffres, lettres minuscules et majuscules, symboles. Nota : Le Journal Officiel n°0023 du 27 janvier 2017 a publié un texte portant sur l'adoption d'une recommandation relative mots de passe. Temps de déchiffrage par force brute à l'aide de logiciels spécifiques (légaux): environ 4 000 ans.(la surface d'attaque peut-être réduite en fonction des moyens humains/matériels/financiers qui seront engagés….). Bannir prénoms, dates, et personnes trop célèbres que vous appréciez notoirement. Préférez une procédure permettant de créer des mots de passe de 12 caractères tous différents (combinant chiffres, symboles et lettres majuscules et minuscules) avec l'identification du site ou du compte, et au centre une combinaison unique pour tous vos mots de passe : par exemple, pour un compte gmail, récupérez « gm », et « l », et insérez par exemple le nom d'un prof que vous aviez en 2005, Michel Fournet, cela peut donner :

pour gmail	gmMic#05Foul
pour votre adresse Bbox	bbMic#05Foux
pour Amazon	AmMic#05Foun

Videz les historiques de navigation

Créez **plusieurs adresses mails** chez plusieurs fournisseurs, toutes avec des mots de passe différents.

Conservez dans **un étui métallique les cartes** contenant des puces RFID ou NFC pour paiement sans contact ou les badges d'identification.

Conservez le moins possible de données sur le disque dur interne de votre ordinateur, transférez tout sur des **disques externes** que vous ne connectez qu'au moment d'utiliser ces données ; le disque de l'ordinateur ne devrait contenir que les programmes de traitement des données.

Consultez les sites de **l' ANSSI et la CNIL** qui proposent des plaquettes de conseils

- l'ANSSI (Agence nationale de la sécurité des systèmes d'information) https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
- la CNIL (Commission nationale de l'informatique et des libertés) https://www.cnil.fr/fr/maitriser-mes-donnees

En cas d'intrusion dans vos données numériques, **déposez plainte** au Commissariat de Police Nationale, ce qui vous donne ensuite la possibilité de contacter des services spécialisés de la Police, pour éventuellement récupérer vos données (sans certitude, tout dépend si le hackeur est déjà connu des « services », auquel cas sa clé de chiffrement serait peut-être déjà connue….) ….. sinon il faut considérer que le *déchiffrement* de vos données ne sera probablement pas réalisable.

Conclusion : Le principal maillon faible de la « chaine numérique », c'est l'utilisateur. C'est donc par une prise de conscience et en faisant évoluer nos pratiques (et celles de nos enfants) que nous réduirons les risques cités plus hauts, et ceux qui pourraient advenir.