Un peu plus loin avec nos données

LA SECURITE INFORMATIQUE

La sécurité de nos données

- La sécurité de nos données **dépend de plusieurs critères** :

- **La machine** sur laquelle nos données sont traitées (ordinateur, tablette, smartphone)
- **Le support** qui conserve nos données dans le temps
- **Notre volonté** de sécuriser nos données ou non
- **Notre propre comportement** face aux pièges de la digitalisation (ventes forcées, arnaques, appartenance à un public-cible non spécialiste, curiosité, etc.)

La sécurité de nos machines

- La plus simple à mettre en place: **la sécurité de nos machines**

- Dès le moment où un ordinateur, une tablette ou un smartphone se raccorde à **Internet**
- En cas **d'acquisition ou échange** de données par USB, cartes, DVD, etc.
- Un programme **ANTIVIRUS** est indispensable pour lutter contre les menaces de plus en plus spécialisées (prise en otage de données)

La sécurité de nos machines

- Simple à mettre en place: **un programme antivirus adapté**

- Sous Windows 10, le système abrite un **ANTIVIRUS** efficace
- Actuellement **inutile** sous MAC OSX et sous LINUX
- **Conseillé** sous la forme d'une **solution gratuite** sous Android (smartphones et tablettes)
- Un programme **ANTIVIRUS** ne pardonne cependant pas les comportements à risques

La sécurité de nos supports

- **Sécurisation** de nos supports (disques durs, cartes SD, ou mini-cartes SDHC, etc.) par un programme assurant la copie sur un support supplé-mentaire (Backup)

- Un **programme de copie** des données crée une copie conforme (exacte) du contenu d'un premier support sur un autre. En cas de panne, de dispa-rition de données ou de contamination par un virus, il suffit de repartir de la sécurité la plus récente pour tout retrouver.

La sécurité de notre matériel : facile !

- Le matériel, nous l'avons vu, est facile à sécuriser au moyen de l'installation d'un programme **ANTIVIRUS** et par la mise en **sécurité périodique de nos données** en les recopiant sur un autre support adapté (disque dur externe supplémentaire, stockage dans le nuage)
- Ce qui reste le plus difficile à maîtriser :

NOS PROPRES COMPORTEMENTS FACE AUX PIÈGES DE LA DIGITALISATION

Nous et la sécurité informatique

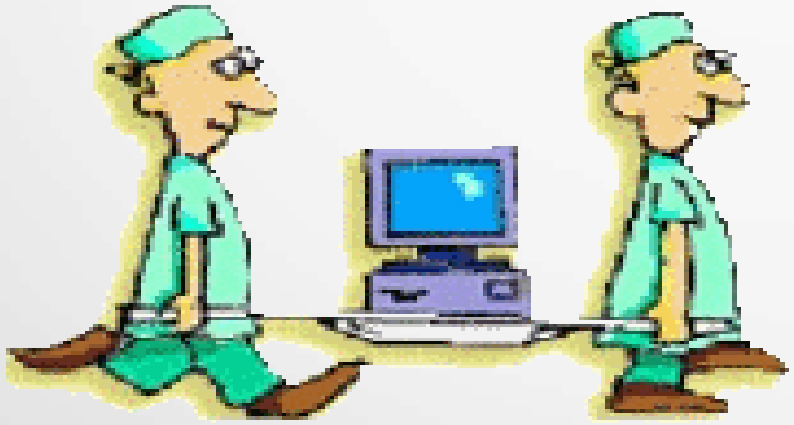
Des farceurs, ces informaticiens !

Les professionnels du dépannage informatique aiment à plaisanter en disant que, dans 99 % des cas, le problème informatique à résoudre se trouve entre la chaise et le clavier !

Affreuse plaisanterie ! Vraiment ?

L’absence de mesures de sécurité

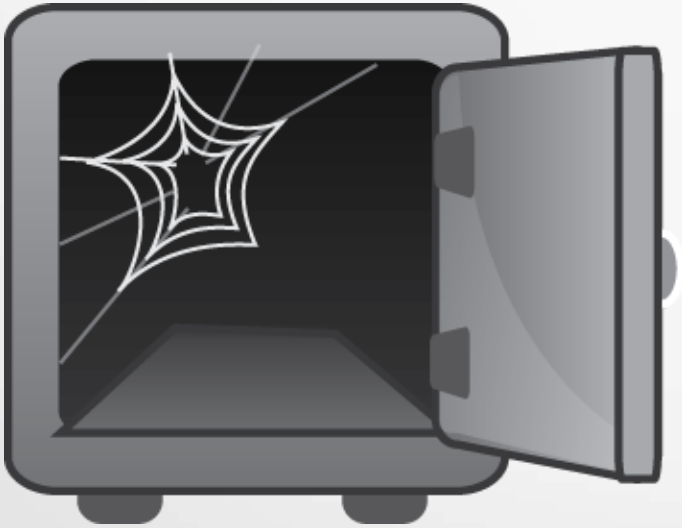
- Trop souvent encore, des personnes confrontées à une panne informatique **majeure** constatent que leur problème sera grave en raison de l’absence de mesures de sécurité.



- Il peut s’agir d’**une volonté délibérée** de la part de l’utilisateur (je n’ai rien de précieux sur ma machine et je n’ai ni le temps ni l’envie de faire des sécurités)
- Par **ignorance du danger** menaçant nos données (je ne savais pas et personne ne m’en avait parlé auparavant)

L’absence de mesures de sécurité

- Mesures volontairement non prises : en supporter les conséquences, à savoir perdre ses photos, ses courriers et autres documents



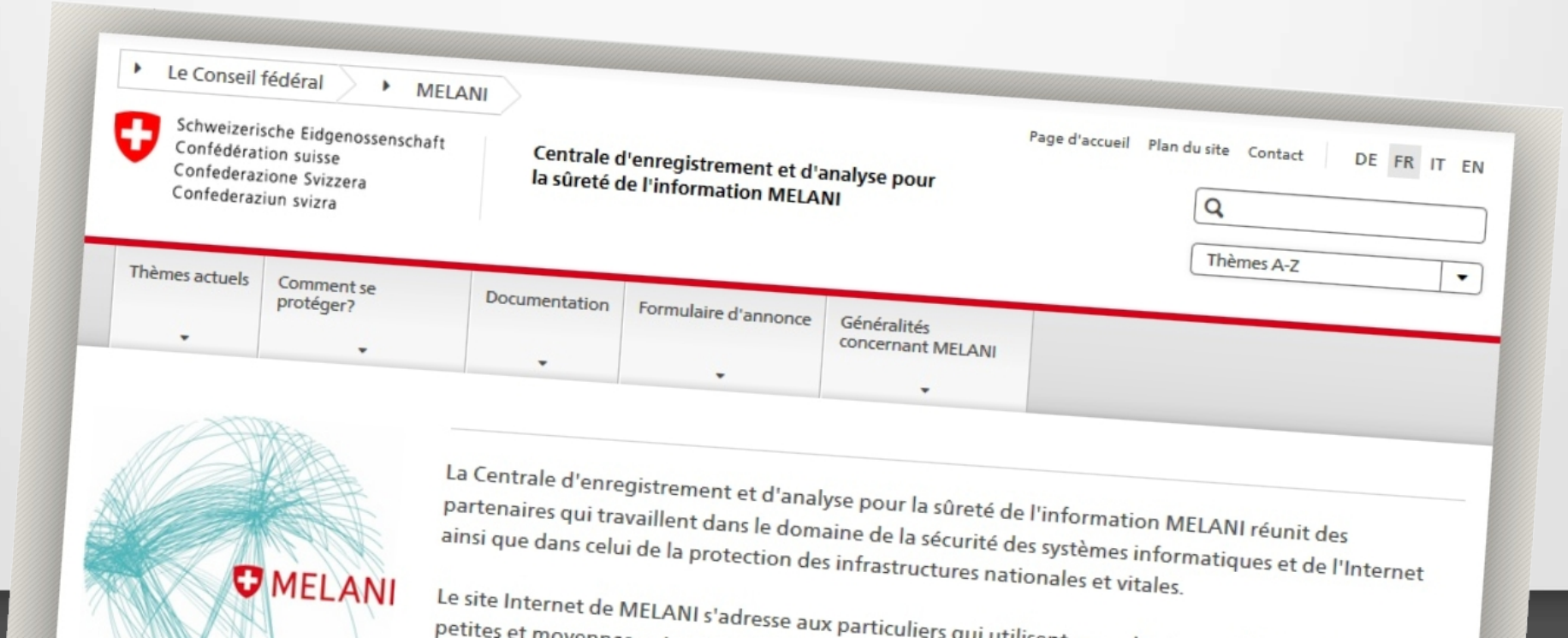
- Par ignorance, les conséquences seront les mêmes mais la triste expérience servira de leçon.

ON PEUT VOULOIR NE PAS EN ARRIVER LÀ EN PRENANT DES MESURES DÈS MAINTENANT.

C’est une bonne idée de sécuriser ses données et de veiller à ne pas cliquer sur n’importe quel lien provenant d’internet

Avant d’aller plus loin

- En Suisse, un organe officiel nommé MELANI est chargé de répertorier les menaces affectant les particuliers et les petites entreprises. Des spécialistes dépendant des organes de la Police fédérale traquent tous les jours les escrocs en puissance. Chacun peut signaler à cette centrale les attaques dont il a été l’objet.



Les comportements à risques.

- Tous les courriels que nous recevons ne sont pas bien intentionnés.
- Certains proviennent de personnes que nous ne connaissons pas.
- Les fournisseurs de boîtes à lettres électroniques procèdent à une détection en amont (spams ou courriers indésirables). Toutefois, des messages passent entre les gouttes.
- Essayons de repérer ces messages en restant attentifs.

Les messages frauduleux

- Une personne que l’on ne connaît pas nous **menace de chantage** en prétextant connaître des informations à notre sujet. On transmet le message à MELANI sans l’ouvrir et sans cliquer sur un quelconque lien.
- Le message **semble officiel** (Poste, Banque, fournisseur d’accès comme Swisscom, UPC, etc.). Il nous demande de communiquer notre mot de passe. On transmet le message à MELANI sans l’ouvrir et sans cliquer sur un quelconque lien. **Un fournisseur de service ne demandera JAMAIS un mot de passe par e-mail. Le message est forcément frauduleux.**

Les sollicitations financières

- Un ami ou une amie (une personne de votre carnet d'adresses) prétend être en déplacement à l'étranger et avoir été l'objet d'un vol de ses effets ou avoir besoin de soins hospitaliers urgents. Cette personne vous réclame de l'argent et vous demande de l'envoyer par un intermédiaire fumeux. Transmission immédiate à MELANI.
- Prenez votre téléphone et contactez sans tarder cette personne qui vous confirmera qu'elle n'est pas du tout à l'étranger et qu'elle n'a besoin de rien.
- Cette personne serait bien inspirée d'informer tous ses contacts qu'elle est victime d'un vol des données de son carnet d'adresses, d'une usurpation de son identité et qu'une tentative d'escroquerie par un tiers n'est pas à exclure.

Les sollicitations financières

- Vous apprenez subitement l'existence d'un grand oncle qui a passé toute sa vie en Afrique australe et qui vient de mourir sans testament et sans laisser d'héritiers. Le mail émane d'un organe qui semble parfaitement officiel, intégrant une référence au Consulat de Suisse dans ce pays.
- C'est généralement un avocat qui vous envoie le courrier, indiquant que vous ne pourrez participer à la succession qu'en versant un certain montant lui permettant la prise en charge de ses propres frais. Un capital important est articulé pour vous encourager à procéder au versement.
- Evidemment, tout est faux. Sauf peut-être la personne qui attend votre versement avec impatience et qui, au final, pourrait fort bien être ... un authentique avocat !

Les fausses informations

- Un courrier électronique vous est adressé en vous demandant de verser de l'argent pour venir en aide à un enfant abandonné ou nécessitant des moyens médicaux auxiliaires importants.
- Il y a 99 chances sur 100 pour que cette information figure déjà depuis longtemps sur **le site spécialisé** qui recense tous ces faux messages et les vagues de fausses informations destinées à escroquer les bonnes gens en agissant sur leur corde sensible :

www.hoaxbuster.com

- Copiez simplement la première phrase du texte reçu et collez-là dans la fenêtre de saisie au-dessus de la loupe rouge. Appuyez sur la touche Enter. Votre réponse ne devrait pas tarder.

Les pièges d’internet en résumé

- 1- Ne pas répondre aux e-mails indésirables ou spontanés.
- 2- Ne rien acheter qui a été recommandé par un e-mail indésirable.
- 3- Ne jamais cliquer sur les liens d'e-mails pressants.
- 4- Ne jamais répondre à un e-mail demandant des informations personnelles ou confidentielles.
- 5- Savoir que sa banque ne demandera jamais d'informations personnelles par e-mail.
- 6- Utiliser des mots de passe compliqués (mélanges de chiffres et de lettres, de minuscules et de majuscules).

Les pièges d’internet en résumé

- 7- Utiliser des mots de passe différents pour chacun de ses comptes.
- 8- Ne jamais enregistrer ses mots de passe sur des ordinateurs étrangers.
- 9- Ne pas installer de programmes suggérés dans des mails.
- 10- Ne pas utiliser n'importe quel support USB tombant sous la main.
- 11- Verrouiller l'accès à son ordinateur.
- 12- Protéger l'accès à son smartphone et le configurer pour qu'il s'auto-verrouille.

Les pièges d’internet en résumé

- 13- Considérer comme "spam" toutes les demandes d'inconnus sur les réseaux sociaux.
- 14- Se méfier des bannières sur les sites web clamant que l'on est "le millionième visiteur" ou le vainqueur d'un "prix incroyable".
- 15- Utiliser un antivirus et/ou vérifier que l’antivirus dont on dispose est bien en fonction.

- Ces précieuses informations étaient fournies par AVIRA, fabricant d’antivirus. Elles sont dignes de foi.

Créons notre mot de passe !

- On choisit une phrase dont il est facile de se souvenir :
- La statue de Pestalozzi est sur la place principale d'Yverdon-les-Bains (1400).
- On garde la première lettre de chaque mot et on garde aussi le code postal en entier et entre parenthèses. Cela donne :

LsdPeslppd'Y-l-B(1400)

- Testez votre mot de passe sur le site :

https://howsecureismypassword.net

Pour conclure

- Tout ce qui touche à la sécurité de nos auxiliaires informatiques est à prendre **avec le plus grand sérieux**.
- Le **matériel est très simple à sécuriser**.
- Le plus grand risque provient de **notre comportement** et, très souvent, de notre crédulité ou de notre inexpérience.
- En matière d'informatique, **RIEN N'EST JAMAIS SÛR**. Et encore moins à 100 % !

COSY, Conseil des Séniors d'Yverdon-les-Bains, février 2019