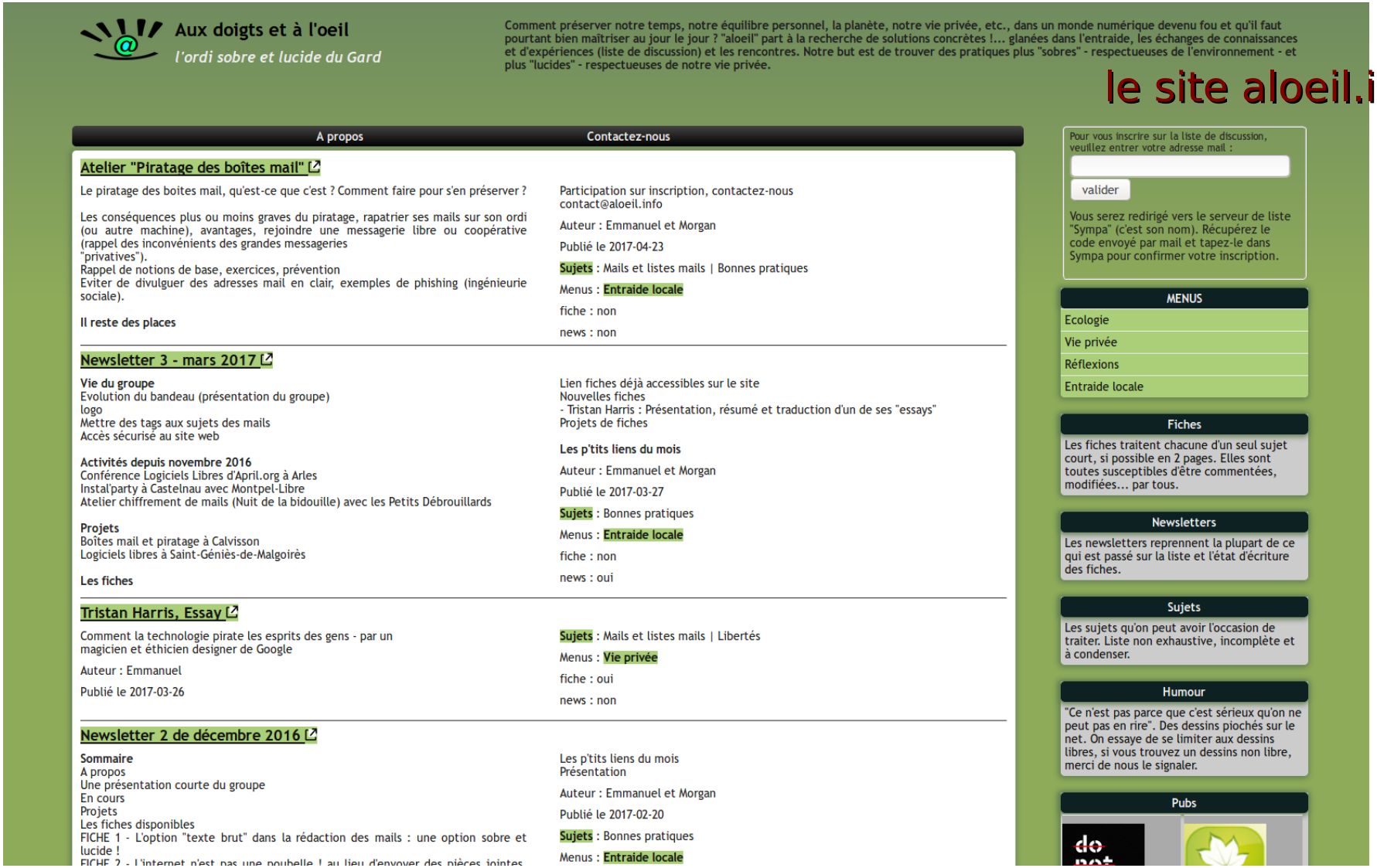
Calvisson 28 avril "le piratage de boites mail"

"aloeil ?"

Notre rôle en tant que groupe local d'entraide et de réflexion est de décortiquer les problèmes posés par le numérique et de chercher à y apporter des solutions pratiques. Notre but n'est pas de nous "adapter" à un monde numérique devenu fou ! Mais "d'adopter" les pratiques qui convient à nos vies (pratiques "lucides") ainsi qu'à la planète ("sobres").



le mail "sobre et lucide"

le mail pose deux problèmes, de sécurité et de manipulation des échanges et de croissance incontrôlée qui engloutit d'énormes énergies

le mail sobre ?

le mail est un outil dangereux : on peut d'un seul clic envoyer de gros volume de pièces attachées à de nombreux destinataires, les fichiers vont rester sur des serveurs pendant parfois des années "pour rien" !

Selon Internet Actu, le rapport le plus sérieux (dont les données datent de 2012) estime que **notre niveau de consommation électrique lié au numérique serait de 8% de la production d'électricité totale** de cette même année.

On gardera à l'esprit que le mail est aussi un outil dispendieux en énergie si mal utilisé.

voici les pratiques "lucides" et parfois "sobres" qu'on proposera ici…

1) installer des mots de passe "forts" ou "blindés" ; éviter ensuite de se faire voler son mot de passe (même blindé)

2) laisser le moins possible de contenu sur internet (dit aussi "le cloud"). Pour cela, rapatrier les mails sur son ordi avec un "logiciel de messagerie" comme thunderbird

3) choisir un "service de messagerie" "vertueux" de type messagerie associative fondé sur des principes de respect des données et à échelle humaine

4) enfin prendre quelques précautions et éviter quelques pièges...

questions à l'assemblée

quel matériel utilisez vous (PC de bureau, portable, smartphone,

quel(s) systèmes ? windows, linux, mac, androïd...

quelle messagerie gmail, yahoo... ouvaton, lautre.net, etc.

comment consultez vous vos mails ? navigateur, une appli

vos comptes ont-ils déjà été piratés ?

vocabulaire avant de commencer

logiciel (sur un ordi fixe) = **appli** (sur un smartphone) – suite d'instructions (recette ou partition)

mail ou courrier électronique ou email

boîte mail, un **espace dans un serveur** ; boîte de courriers électroniques, boîte aux lettres électronique (abonnement à un service de messagerie)

adresse mail ou adresse électronique

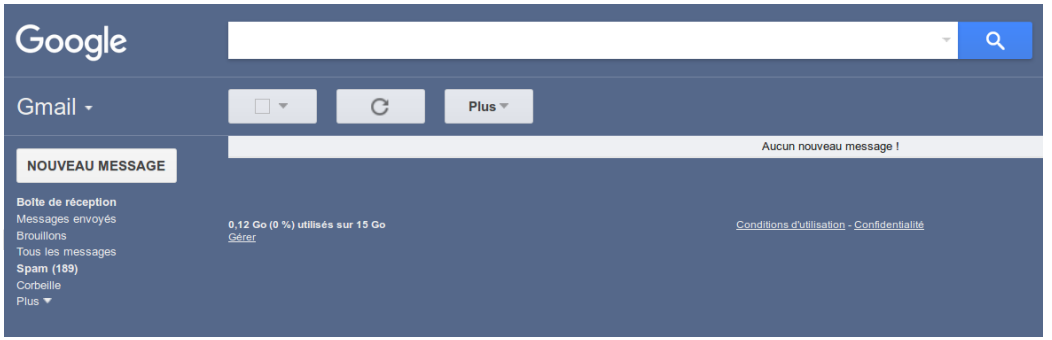
site web : Techniquement, un site web est un logiciel écrit pour le web et installé sur un serveur. Accessible depuis un navigateur à une adresse http:// ou https://

système : windows, MacOS, Linux (et variantes), Androïd, etc.

service de mail ou service de messagerie ou **mailer** : gmail, yahoo, laposte, ouvaton, lautre.net, etc. (service gratuit ou payant)

2 interfaces entre boite mail et utilisateur

Un **webmail** ou **messagerie web** est un site accessible depuis le navigateur, pour accéder boîte mail, consulter, envoyer, manipuler nos



logiciel de messagerie ou **client de messagerie** (ex. Mozilla Thunderbird) est un logiciel installé sur l'appareil (pc, smartphone...) pour accéder à sa boîte mail. On peut y faire tout ce qu'on fait sur un webmail.

vocabulaire

saisie adresse mail + mot de passe

adresse mail
jean.bombeur@gmail.com
mot de passe
12345

accès au service de messagerie (ou mailer, gmail, hotmail, yahoo...)

connexion à la boite mail ou compte de messagerie

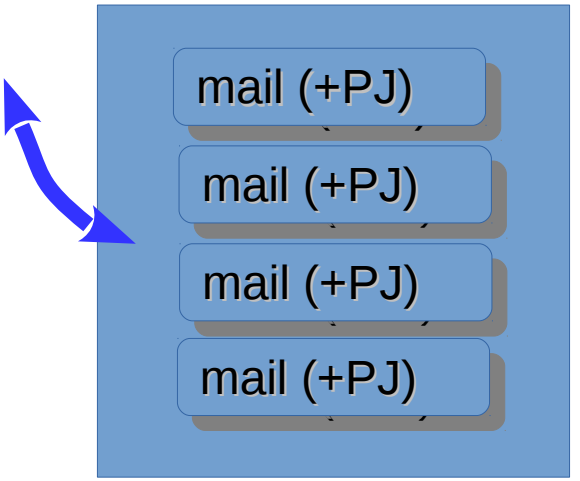
"webmail"
(site web qui donne accès au compte)

navigateur
(ex. **firefox**)

client de messagerie
(logiciel qui donne accès au compte
ex. **thunderbird**)

mails reçus

lecture des mails, envois



connexion via le site web

connexion directe

ordi, smartphone, etc.

les piratages
piratage par vol de mot de passe

Une fois l'adresse mail et le mot de passe connus, n'importe qui peut s'introduire dans une boite mail.

Mais comment le mot de passe a-t-il été découvert ?

"usurpation de chaise" : la manière la plus simple d'entrer dans une boite aux lettres est de s'asseoir au poste dont personne s'est absentée en laissant sa boite ouverte...
-->vidéo « Boîte mail restée ouverte » **(5 minutes) sur le site aloeil.info**

...ou de mettre la main sur un smartphone dont la messagerie reste (en général) toujours ouverte...

...ou encore : en utilisant un réseau wifi, un pirate peut accéder à la messagerie ouverte d'un autre utilisateur connecté sur le même réseau (ça marche avec une boîte mail orange sur une box orange)...

Mais le cas de loin le plus répandu est le **vol de mot de passe** (ou décryptage du mot de passe ou "**crackage**") par un "robot" (un programme informatique) qui teste automatiquement des milliers de mots de passe préparés à l'avance et finit par tomber sur le bon, d'autant plus facilement qu'il ressemble à quelque chose de connu (prénoms, dates de naissances...). Si le mot de passe est suffisamment "fort" (s'il ne peut pas être découvert par essais successifs), le robot abandonnera généralement ses tentatives.

Des méthodes expertes... (**phishing, "ingéniérie sociale"**)

Vidéo « Vol de mot de passe » sur le site aloeil.info
Voir le site d'origine : hack-academy.fr (le chargement du site est un peu long)

se faire voler un mot de passe même très fort
exemple de "phishing" naïf...

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

impots.gouv.fr

un site de la Direction générale des Finances publiques

Cher (e) Client (e)

Apres les derniers calculs annuels de l'exercice de votre activité,
nous vous déterminons que vous admissible a recevoir un remboursement de 120.80 Euro

Veuillez nous soumettre s'il vous plait la demande de remboursement d'impôt

pour nous permettre de la traiter dans un plus bref délai
(le délai du traitement est de 10 jours ouvert).

>> Pour acceder au formulaire pour votre remboursement d'impôt , cliquez ici .

Un remboursement peut être retarde pour diverses raison . Par exemple

la soumission du dossier non valides ou inscriptions après une certaine limite

Le Conciliateur fiscal adjoint
Philippe BERGER

Vous étés tenu de fournir un numéro de téléphone ou notre conseil pourra vous joindre .

Nous vous prions d'accepter nos excuses .

--> Pour tester un formulaire
imitant celui d'un pirate et voir que les infos peuvent être conservées

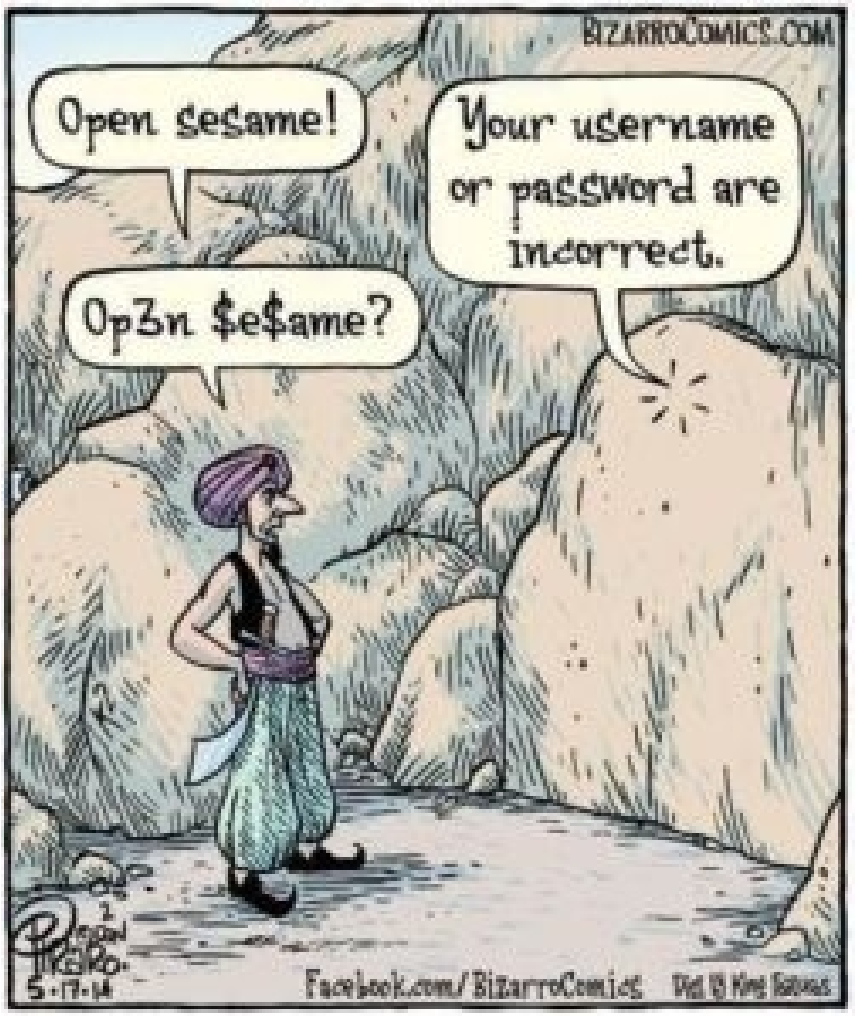
Les informations n'iront pas plus loin que la base de données de mon compte chez Ouvaton.coop

Mais

ne mettez pas de vraies informations, c'est juste un exemple.

les conséquences

Une fois introduit dans la caverne d'Ali Baba,
le pirate peut faire quelques dégâts.



les conséquences possibles

L'ancien mot de passe n'est plus reconnu !

Première conséquence, qui pourrait être fatale : impossible de se reconnecter, l'ancien mot de passe n'est plus reconnu (le pirate l'a remplacé). **Le compte de messagerie peut être à ce stade définitivement perdu** (et son contenu pourra continuer d'être exploité par le pirate…).

Certaines messageries permettent de créer un nouveau mot de passe. Est-ce possible sur votre messagerie ? Mais la plupart du temps le pirate préfère rester discret et le mot de passe n'est pas changé.

Les contacts sont perdus !

Le pirate récupère la liste de contacts et peut l'effacer !

Le pirate peut utiliser les contacts ou la boite mail pour envoyer des messages compromettants

Le pirate peut utiliser la boite mail et envoyer des messages compromettants.

Il peut utiliser l'adresse mail pour inonder les contacts de spams. Ne pas s'étonner si des messages suspects continuent d'être envoyés même une fois le mot de passe changé.

L'envoi de **messages loufoques** aux contacts (du genre "j'ai besoin de ton aide...") permet de tester que les comptes de messageries sont bien "actifs" et accessoirement de récupérer des sous…

Les traces de vos achats sur l'Internet récupérées !

Quand vous faites des achats sur Internet, on vous demande de créer un compte avec identifiant et mot de passe. Très nombreux sont ceux qui, pour gagner du temps, donnent comme mot de passe celui de la boite mail. Or, l'adresse et le mot de passe sont entre les mains du pirate...Il peut donc se rendre sur le compte d'achat (par ex. chez Amazon.fr), changer l'adresse de livraison,commander ce qu'il veut. Arrivé au paiement, il pourra même parfois payer... si le moyen de paiement est resté actif depuis la dernière transaction (ce qu'il ne faut jamais faire bien sûr, et que beaucoup de sites incitent pourtant à faire (paiement rapide "en 1 click").

Conséquence gravissime mais rarissime : L'usurpation d'identité, gravissime, mais heureusement rarissime, il n'empêche qu'on ne doit pas laisser des copies de son état-civil en pièces attachées.

mesures préventives pour limiter les problèmes

Blinder son mot de passe !

Assécher sa messagerie sur Internet

Migrer vers un service de messagerie "vertueux"

blinder son mot de passe

Top 10 des mots de passe les plus piratés en 2016

1	**123456**
	(Numéro un pour la énième année consécutive...)
2	**123456789**
3	**qwerty (ou azerty en français)**
4	**12345678**
5	**111111**
6	**1234567890**
7	**1234567**
8	**password**
9	**123123**
10	**987654321**

faire un mot de passe **fort**

voir aussi fiche "mots de passe" aloeil

Nombre de caractères et "alphabets" recommandés

D'après le site de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) il ne faut pas moins **de 16 caractères utilisant un alphabet de 90 symboles** pour obtenir un mot de passe réellement "**fort**". Exemple : **`Aeg$ai9oow*ahk>u`**

le site de l'ANSSI pour tester la force des mots de passe :
http://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

D'autre part il est conseillé de ressaisir régulièrement son mot de passe voire de se déconnecter systématiquement à chaque fin de session (ne pas accepter que les comptes restent ouverts ou le mot de passe enregistré par un navigateur ou autre logiciel).

En pratique

Il peut être trop difficile de retenir des mots de passe aussi compliqués au quotidien ou trop contraignant de les utiliser.
Pour retenir un mot de passe on peut avoir recours à une phrase mnémotechnique

<L28Ao@adtdcàC!]

le 28 avril on a appris des tas de choses à Calvisson !

On peut aussi réduire le nombre de caractères , 12 semblant être un minimum.
Le mot de passe doit être d'autant plus fort que le contenu de la boite mail est plus convoité et qu'une attaque personnalisée risque de se produire (personnalité, militant, journaliste, etc.)

fabriquer autant de mdp que l'on veut avec un programme de type pwgen (*)

pwgen 16 -B -y

```
Thu~eghox4iuc9ca    uje*oKe9Tai~xahv    UaL9quaiNg`ee)s9    Phoh4ietohy'eivo
Aid9hai[nooy4io4    Xooxae}jie9tieTi    aej9uya_ne"a4Xie    EiWu;uH7ahgh{e[y
ahj{oF3eiWie7quo    Li9xooh"ei4eij.o    nahs_ee7eih3aKoo    een"ahqu7ohCho@e
bieK-oxiX4eijien    shu!f7ki9chae7aj    Xue7gahng7phox_e    Aeg$ai9oow*ahk>u
eeT9Xeu;thohr<a3    eeKie9Uk7je~hoe&    gooth4Ahyuu?pahy    nie7oowae~n7aech
```

(*) programme installé sur son ordi, ne pas utiliser de "service" en ligne sur internet !

une dernière méthode...

Roger Buffle Jr. supplies his father with yet another computer password.

pour info : comment sont protégés les mots de passe ? le "hashage" ou "hachage"

Les mots de passe doivent être stockés par les sites dans des bases de données pour pouvoir être reconnus quand on s'y connecte.

Nos mots de passe pourraient être volés par quelqu'un qui aurait accès à la base de données du site, si elle n'était pas protégée.

Pour éviter ces fuites, nos mots de passe ne sont pas stockés en clair, mais "hashés".

faire un essai de hashage

https://zetm.ouvaton.org/HacheAloeil.php

Résultat :

"12345" haché avec "Des" :

1rzvaeZ5J$LzPUgjsxY4A8vJoNzLEzp.

Inversement il est impossible de retrouver le mot de passe à partir du résultat du hachage 1rzvaeZ5J$LzPUgjsxY4A8vJoNzLEzp. Des robots qui seraient arrivés jusqu'à la base de données n'ont pas d'autre solution que de tester des milliers de mots de passe comme "12345" jusqu'à trouver le bon hachage

les piratages (2)
la collecte des contenus

certains "mailers" (gmail, yahoo...) **collectent et manipulent les contenus des mails**

CGU Google (actuelles)

https://www.google.fr/intl/fr/policies/terms/regional.html

Nos systèmes automatisés analysent vos contenus (y compris les e-mails) afin de vous proposer des fonctionnalités pertinentes sur les produits, ***telles que*** *des résultats de recherche personnalisés, des publicités sur mesure et la détection des spams et des logiciels malveillants.* ***Cette analyse a lieu lors de l'envoi, de la réception et du stockage des contenus.***

le contenu des mails est analysé en vue de leur traitement pour établir des profils, pour faire du ciblage comportemental – cette manipulation massive en autorise d'autres comme le marketing par mail qui alimente entre autres le spam (Louise Merzeau) (très mal profilé ! mais gaspillant d'énormes quantités d'énergie et d'attention).

...la plupart des utilisateurs ignorent cette collecte (cette information est "largement en deçà d'un horizon de visibilité", Louise Merzeau, chercheuse)

...l'utilisateur n'a pas d'autre choix que d'accepter que ses propres données soient utilisées quand il ouvre un compte sur ces messageries.

...s'il refuse la logique de marketing par mail et de coût écologique de ces pratiques, la seule solution est de choisir une messagerie qui ne collecte pas les "data" personnelles. (voir plus loin)

les piratages (3)
piratage massif de type yahoo

exemple de yahoo : 1 milliard de comptes "piratés"

4 experts dont 2 agents secrets russes ont piraté le compte d'un employé de yahoo à partir duquel ils ont eu accès au stockage de l'ensemble des mails de yahoo.

Le "pillage" aurait duré 2 ans… attaque soutenue et constante…

Dans ce cas, l'employé aurait donné à son insu des détails qui ont permis de deviner son mot de passe après une longue approche "d'ingéniérie sociale"

https://www.nextinpact.com/news/103704-piratage-yahoo-quatre-russes-inculpes-dont-deux-agents-fsb.htm

Un autre type est l'espionnage par les grandes agences de surveillance américaines, russes, NSA*, etc. Elles entrent par des "portes dérobées"** ou "back doors" dans les serveurs (des services de messagerie entre autres), principalement les grandes pour avoir accès à plus de comptes d'un seul coup. Espionnage de toutes nos communications.

* NSA : National Security Agency = Agence Etasunienne de surveillance, née avec le Patriot Act.
** Portes dérobées :"failles de sécurité" tenues secrètes introduites exprès dans un programme pour avoir accès à ses données.

Migrer vers des services de messagerie plus vertueux à échelle humaine
une parade aux piratages "massifs" des grands services de messagerie

Des mailers proposent un service basé sur des logiciels libres et leurs CGU respectent notre vie privée (nos mails), voire même certains se disent "écologiques".

Quelques exemples de mailers :

newmanity.com

protonmail.com

junior.netcourrier.com
et net-c.com (1)

. . .
et d'autres

Voir aussi cet article sur Blog-libre de fin 2016 :
https://www.blog-libre.org/2016/12/16/messagerie-email-ethique-ou-comment-eviter-de-se-faire-braquer-sa-vie-privee/

Des associations proposent des services web complets : espace web, des listes de discussion et des boîtes mail. On peut bien sûr les utiliser pour les mails uniquement.
En général ces services sont payants (mais pas tous), la plupart entre 20 et 30€ par an, associations, coopératives ou micro-entreprises.

Quelques exemples associatifs :

lautre.net

ouvaton.coop

zaclys.com

marsnet.org
... et d'autres

1 : ancien Netcourrier, repris par une équipe de "libristes" français

laisser le moins possible de contenu sur le web "pour rien"

gaspillage d'énergie + risques de sécurité
les transférer avec un "client de messagerie"

thunderbird, logiciel de messagerie ou "client de messagerie" qui est installé sur l'ordinateur. Permet d'envoyer et recevoir des mails avec PJ depuis l'ordinateur au serveur du service de messagerie (sans passer par le site web) et de stocker ses mails sur son ordi.

Avantage : les sauvegardes, classement, nettoyage... sont beaucoup plus simples en "local" ; elles sont pratiquement impossibles en ligne

Deux méthodes ou "protocoles" existent au choix pour télécharger les messages depuis le "service de messagerie" :

IMAP qui est considéré comme plus moderne laisse les messages sur internet et télécharge des copies (de cette manière on peut toujours consulter sa messagerie depuis son portable ou un autre ordi). Conséquence, la boite mail enfle, enfle et devient ingérable...

POP qui télécharge et efface dans la foulée. Les boites sont vidées. Remarque importante : on peut régler le programme pour que les messages ne soient pas effacés tout de suite mais après un délai de 8 jours, 1 mois...

Pour les ordiphones, un équivalent de Thunderbird s'appelle K9-mail.

précautions finales

- 1 mot de passe par compte (amazon, banque, mail…)
- stocker les mots de passe de manière à ne pas les perdre ! pas sur le disque dur, la messagerie, ni dans le navigateur, etc. Sur un calepin ?
- ne jamais afficher en clair des adresses mail lors d'envois groupés. Les mettre en "Cci" (Carbon Copy Invisible) :
- toujours refuser que les mots de passe restent enregistrés par les logiciels ou les services de messagerie (firefox chrome thunderbird...)

plan de l'atelier

Vocabulaire et notions de base

Le piratage des boites mail, qu'est-ce que c'est ?

- piratage par vol de mot de passe

  déroulement, techniques

  se faire voler son mot de passe même très fort (phishing)

  conséquences plus ou moins graves

  parades

  faire un mot de passe fort

  pour info : le hashage
- "piratage" (légal?) du contenu des messages par le service de messagerie
- piratage "industriel" (milliard de comptes) exemple de yahoo

Parades

- rapatrier ses mails sur son ordi (ou autre machine)
- rejoindre une messagerie "vertueuse", libre ou coopérative (rappel des inconvénients des grandes messageries "privatives").
- précautions finales