

Sensibilisation à la sécurité informatique

Jean-Claude Bordes et Alain Michaud

- Rappeler les grands principes de la sécurité :
 - ☞ du poste de travail
 - ☞ de la messagerie
 - ☞ de la navigation sur internet
- Donner quelques trucs et astuces
- Proposer des outils contribuant à la sécurité
- Donner quelques liens utiles pour approfondir le sujet
 - ☞ <https://www.cybermalveillance.gouv.fr/>
 - ☞ https://www.cybermalveillance.gouv.fr/medias/2023/08/230424_GuideFamilles.pdf
 - ☞ <https://support.microsoft.com/fr-fr/windows/protégez-vous-contre-les-escroqueries-au-support-technique>
 - ☞ Internet sans danger : Le guide du bon sens numérique de Virginie Sellier (Bayard Jeunesse)

- Règles d'or de la prévention
- Sécurité de la messagerie
- Sécurité des données
- Sécurité de la navigation sur Internet
- Sécurité de l'utilisation des réseaux sociaux

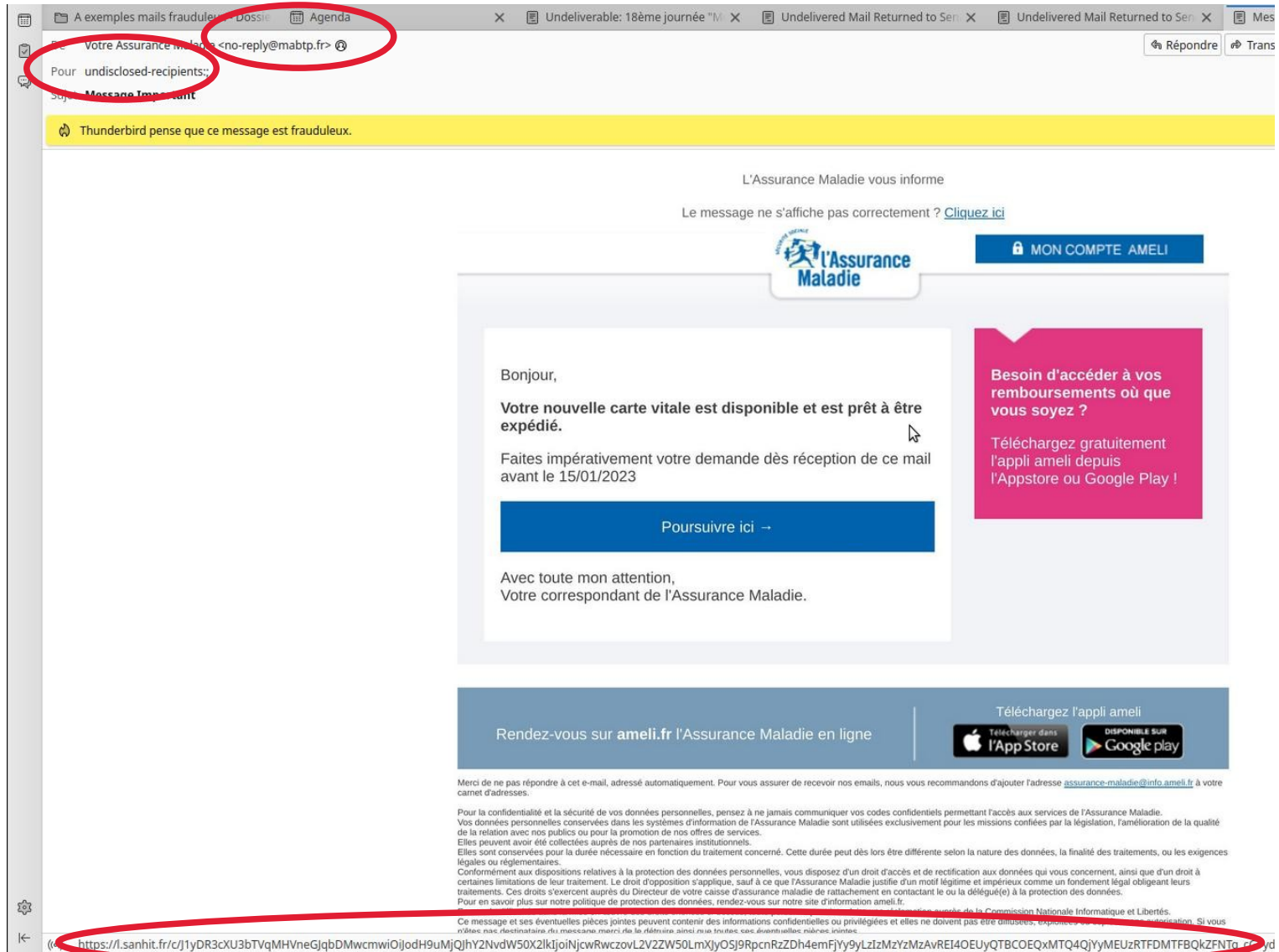
- Il faut mettre à jour régulièrement ses outils numériques
- Il faut protéger ses accès par des mots de passe complexes
- Il faut prendre soin de ses informations personnelles en ligne
- Il ne faut pas faire confiance aux réseaux non maîtrisés
- Il faut être « un peu » paranoïaque
- Confort d'utilisation et sécurité sont rarement compatibles
 - ☞ Enregistrement des identifiants/mots de passe dans le navigateur
 - ☞ Enregistrement des identifiants de carte bancaires sur des sites marchands
 - ☞ Conservation de l'historique et des cookies à la fermeture du navigateur
 - ☞ Case à cocher « Rester connecté »

- Définitions et précautions générales
- Comment reconnaître un mail frauduleux
- Quelques exemples de mails frauduleux

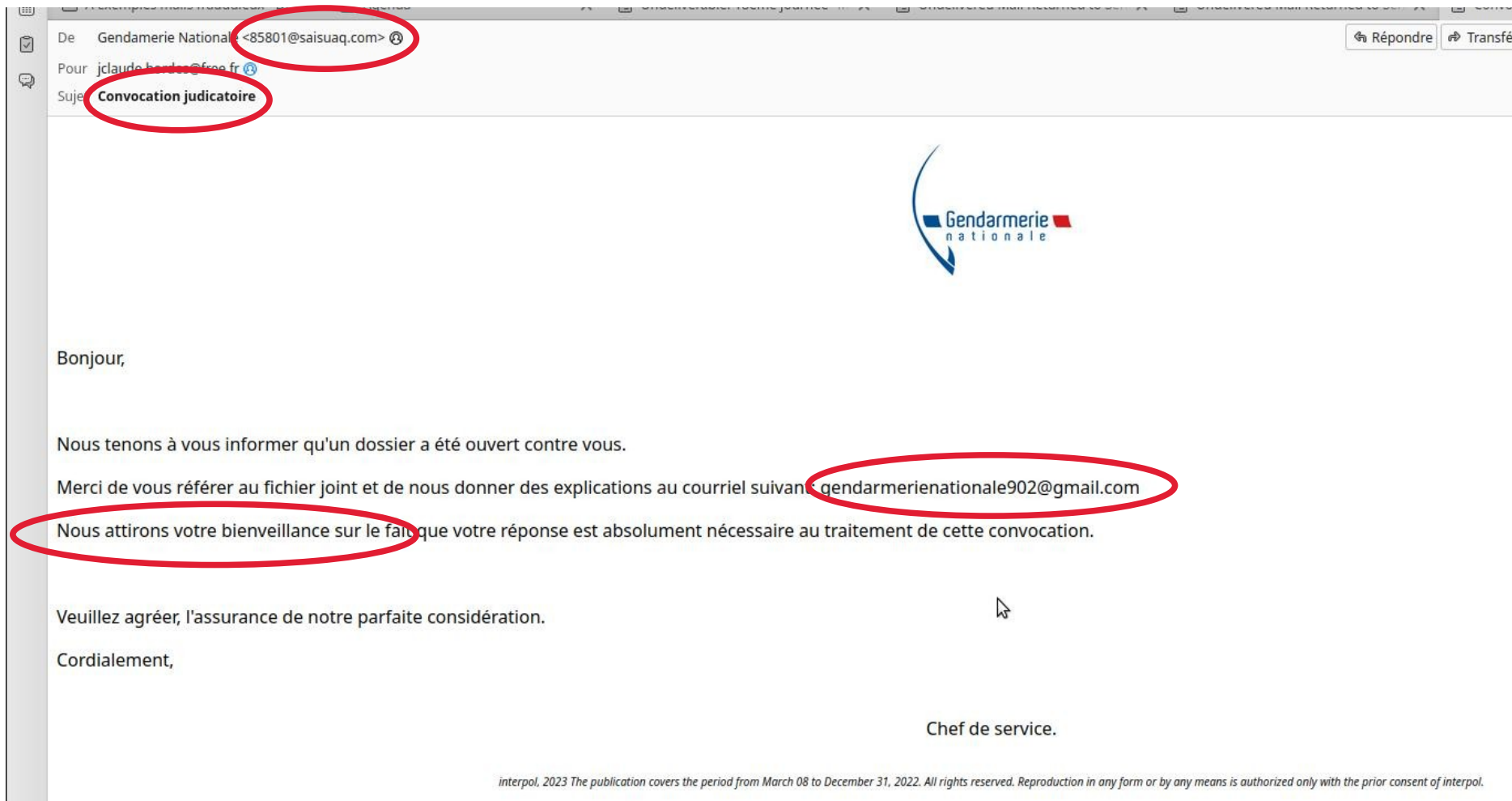
- Menace : phishing ou hameçonnage
- Un individu se fait passer pour une banque, une administration, une entreprise de livraison... pour :
 - ☞ se faire communiquer des informations personnelles ou bancaires,
 - ☞ inciter à ouvrir une pièce jointe contenant un logiciel malveillant (virus, ransomware...),
 - ☞ cliquer sur un lien malveillant pour rediriger vers un site frauduleux.
- Précautions à prendre si on reconnaît un mail suspect (cf. diapo 6)
 - ☞ Ne jamais répondre
 - ☞ Ne jamais cliquer sur un lien
 - ☞ Ne jamais ouvrir une pièce jointe
 - ☞ Effacer le mail

- **Contenu du mail**
 - ☞ L'orthographe et la syntaxe laissent « à désirer »
 - ☞ Je n'ai pas de compte dans la banque ou l'organisme de crédit
 - ☞ On me demande de mettre à jour mes données personnelles et/ou bancaires en cliquant sur un bouton ou un lien contenu dans le message
 - ☞ On me demande de payer une somme modique en cliquant sur un bouton ou un lien contenu dans le message
 - ☞ Un correspondant figurant dans mon carnet d'adresse me demande de répondre à son mail car on ne peut pas le joindre
- **Adresse mail de l'expéditeur**
 - ☞ L'adresse de correspond pas à l'expéditeur supposé
 - ☞ L'affichage du code source du message montre une différence entre l'adresse affichée dans le champ « De : » et l'adresse réelle

- **Adresse mail du destinataire**
 - ☞ Le message est adressé à « Undisclosed-recipients » ou à l'expéditeur
 - Mon adresse mail est en copie cachée (Cci) et fait partie d'une liste d'adresses
- **Adresses internet associées aux liens et boutons**
 - ☞ Quand je passe le pointeur de la souris sur un lien ou un bouton, l'adresse affichée est « bizarre » ou est exactement la même pour tous les liens et boutons
 - L'adresse pointe vers un site frauduleux ou un logiciel malveillant




A screenshot of a web browser displaying a fraudulent email from 'L'Assurance Maladie'. The browser's address bar shows 'A exemples mails frauduleux' and several tabs for 'Undeliverable: 18ème journée "M...'. The email header shows the sender as 'Votre Assurance Maladie <no-reply@mabtp.fr>' and the subject as 'Message Important'. A yellow warning bar from Thunderbird states 'Thunderbird pense que ce message est frauduleux.' The email content features the 'L'Assurance Maladie' logo and a blue button labeled 'MON COMPTE AMELI'. The main text reads: 'Bonjour, Votre nouvelle carte vitale est disponible et est prêt à être expédié. Faites impérativement votre demande dès réception de ce mail avant le 15/01/2023'. Below this is a blue button 'Poursuivre ici ->'. To the right, a pink box asks 'Besoin d'accéder à vos remboursements où que vous soyez ?' and promotes downloading the 'ameli' app. At the bottom, there is a footer with a URL 'Rendez-vous sur ameli.fr L'Assurance Maladie en ligne' and logos for the App Store and Google Play. A long, complex URL is visible at the bottom of the page, circled in red.



De Gendarmerie Nationale <85801@saisuaq.com>

Pour jclaude.bardos@free.fr

Sujet **Convocation judiciaire**



Bonjour,

Nous tenons à vous informer qu'un dossier a été ouvert contre vous.

Merci de vous référer au fichier joint et de nous donner des explications au courriel suivant gendarmerienationale902@gmail.com

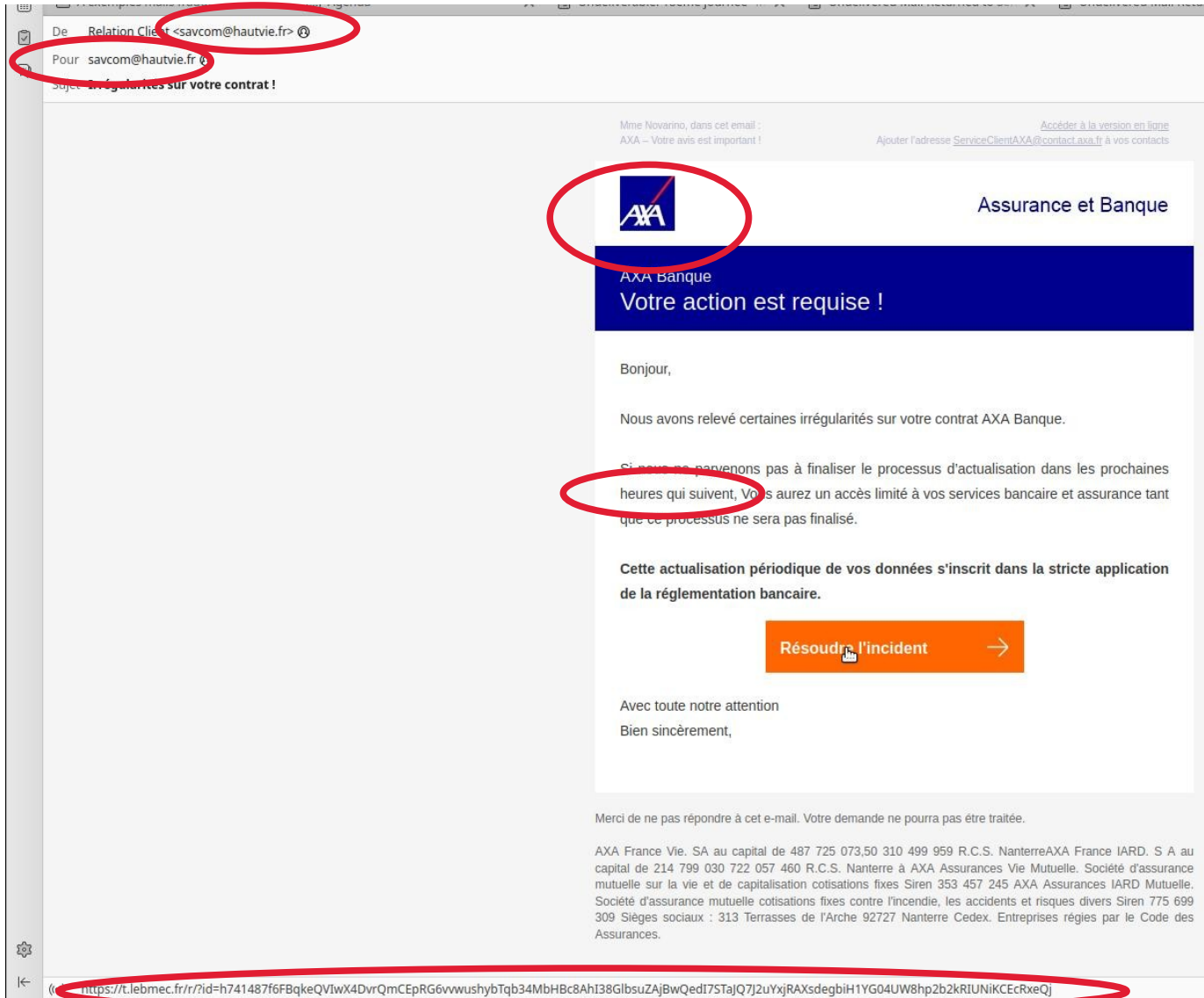
Nous attirons votre bienveillance sur le fait que votre réponse est absolument nécessaire au traitement de cette convocation.

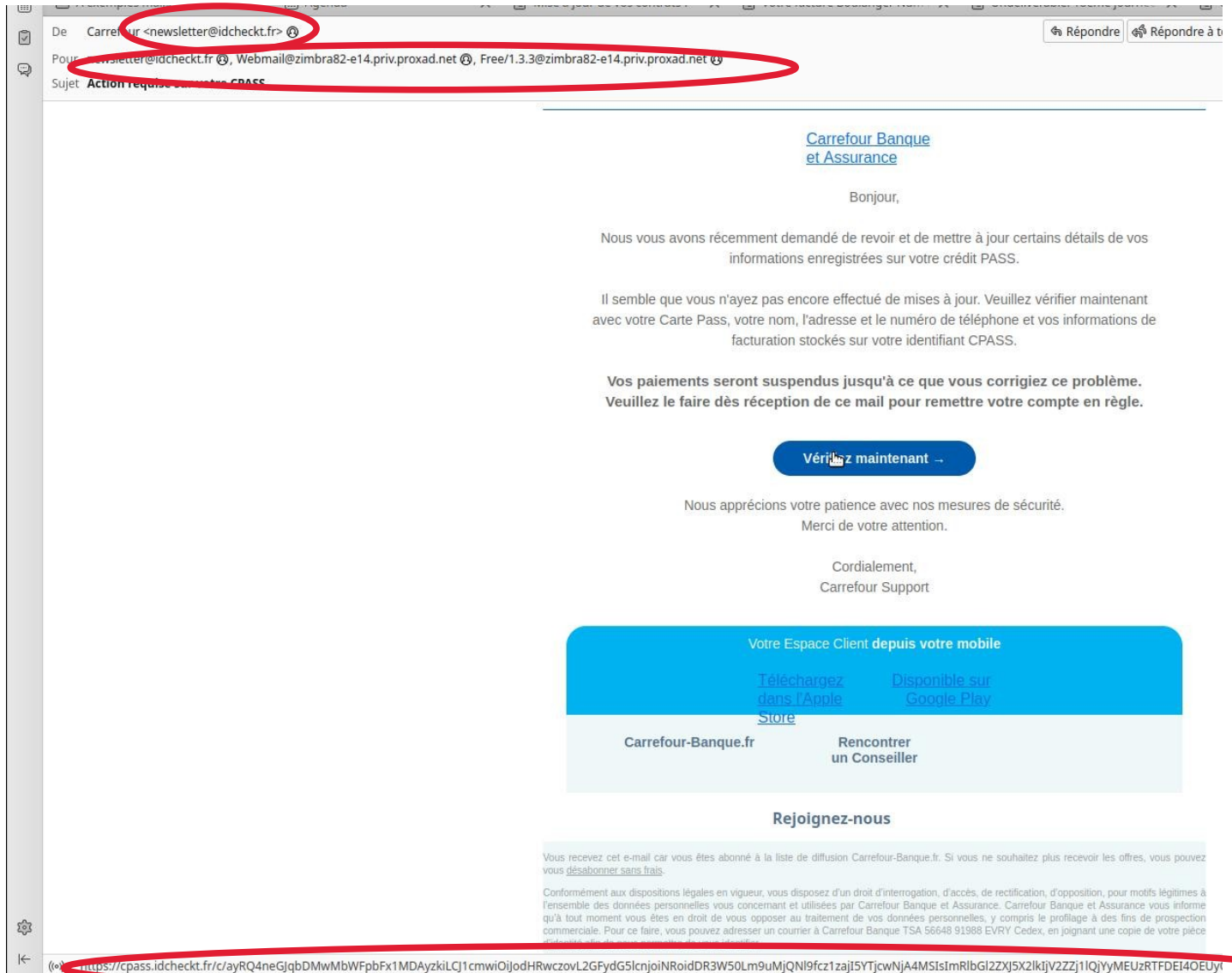
Veillez agréer, l'assurance de notre parfaite considération.

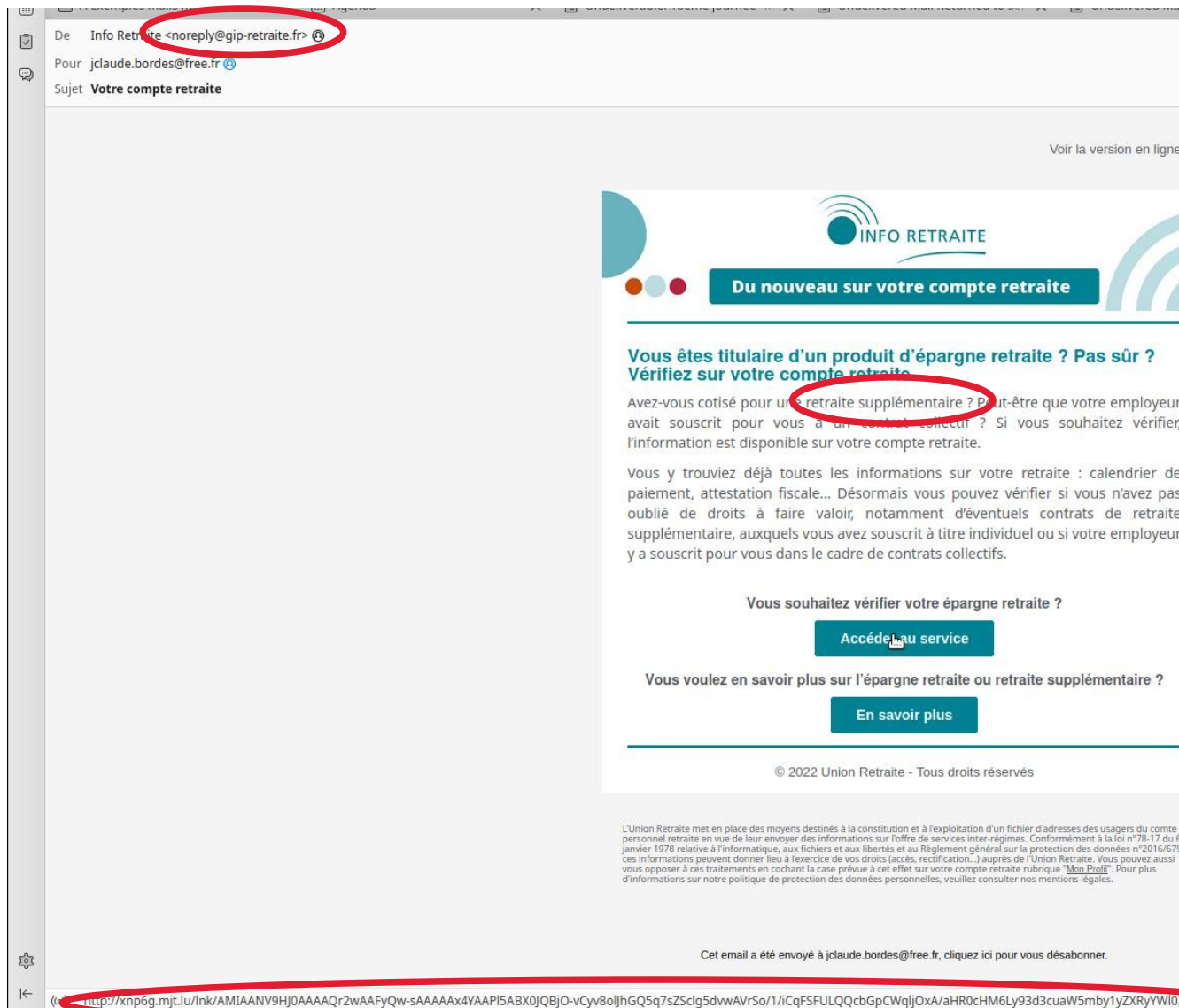
Cordialement,

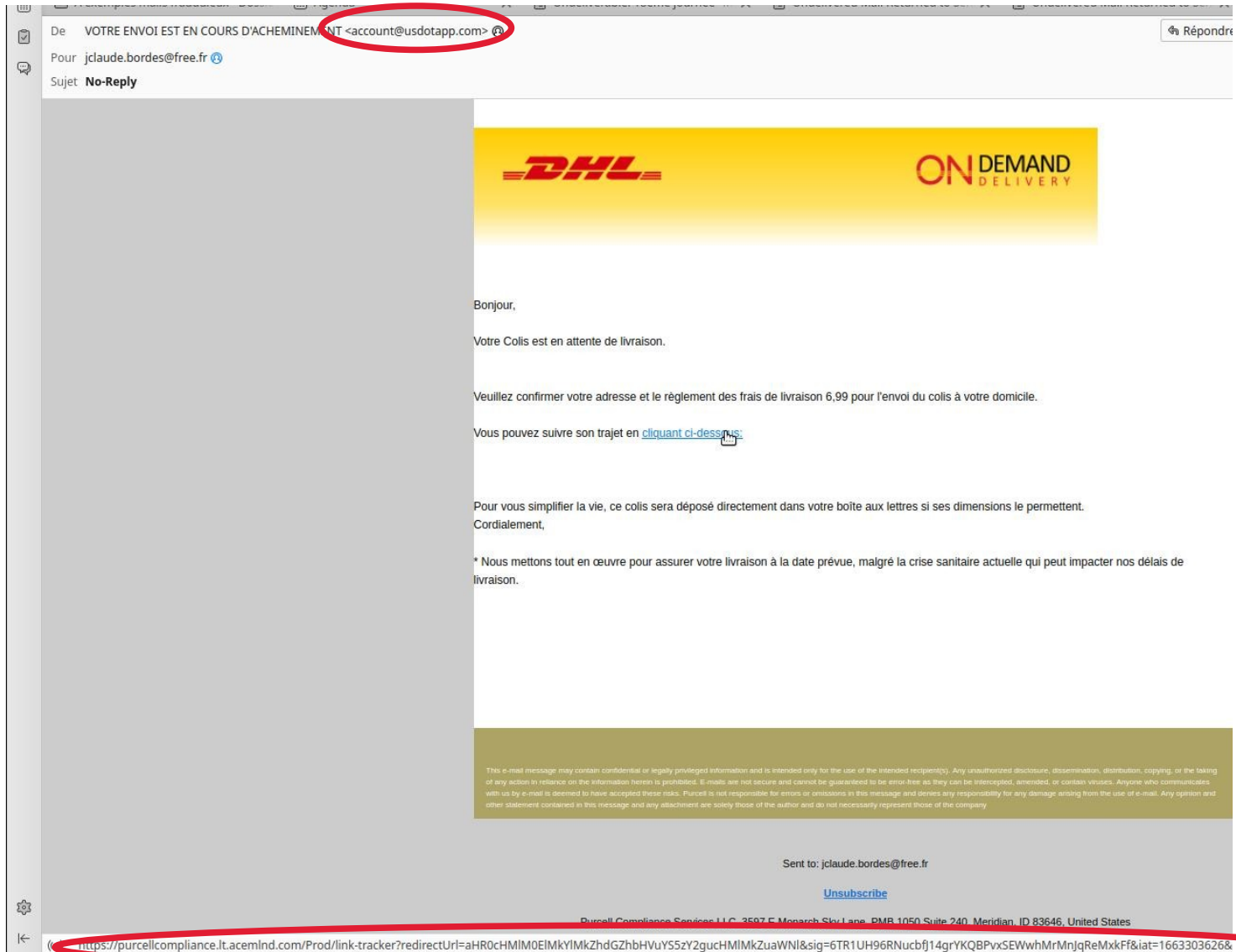
Chef de service.

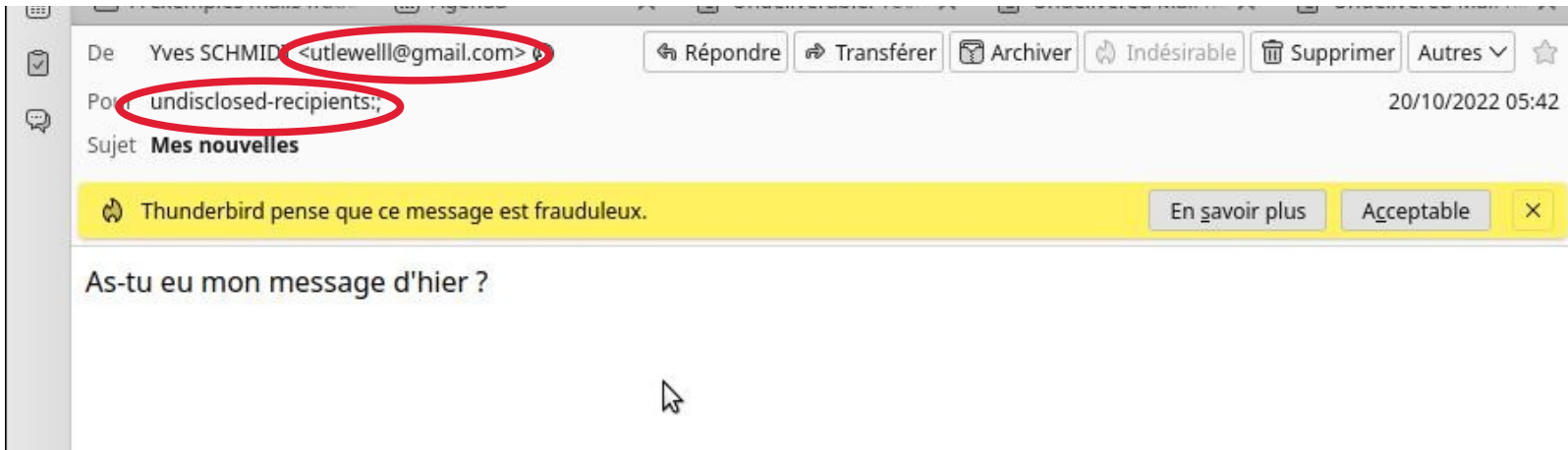
interpol. 2023 The publication covers the period from March 08 to December 31, 2022. All rights reserved. Reproduction in any form or by any means is authorized only with the prior consent of interpol.

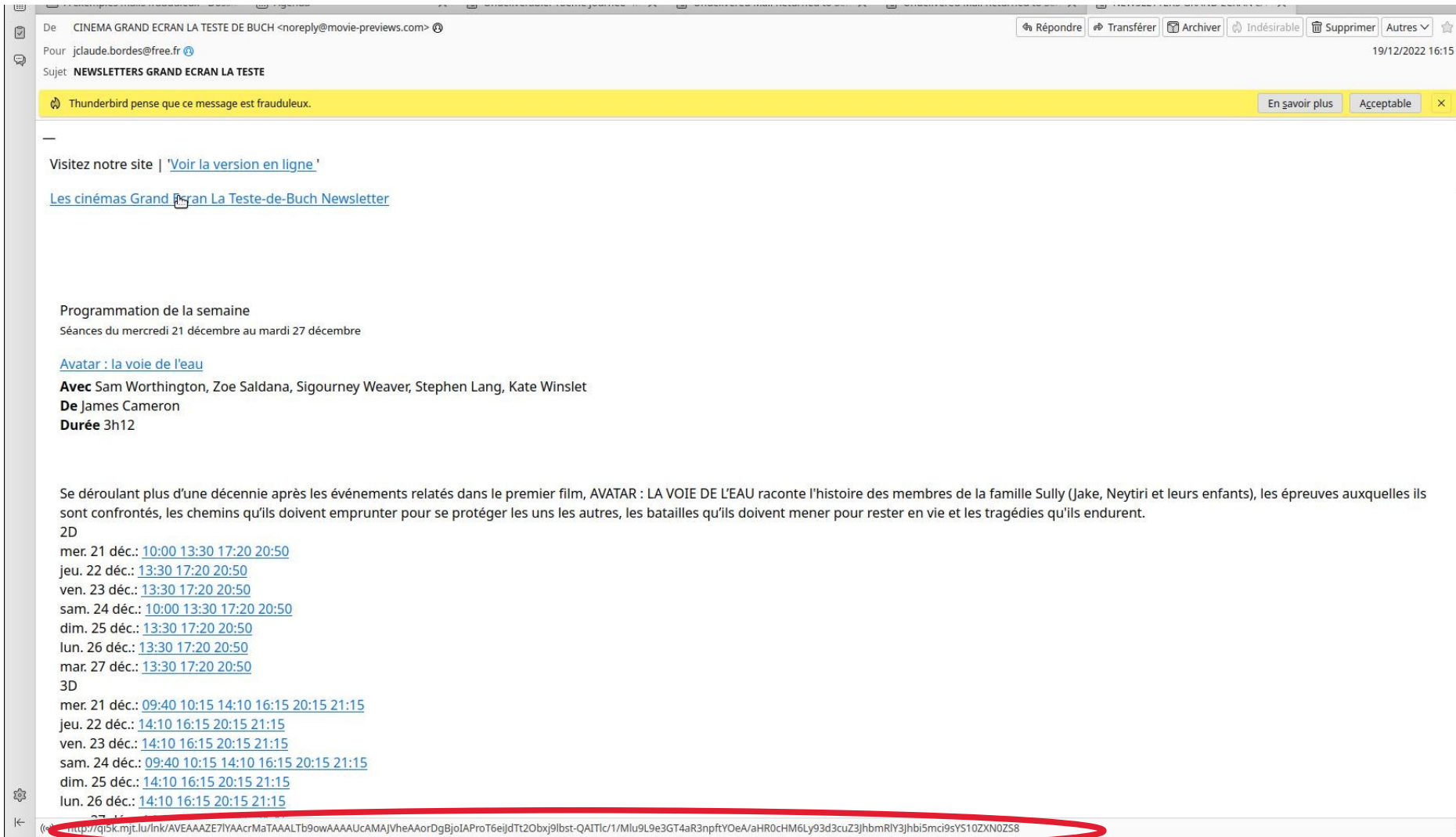














De Disney+ <noreply@disneyplus.com> 

Pour jclaude.bordes@free.fr 

Sujet **Veillez mettre à jour vos informations - 02:27**



```

Source de : mailbox:///home/jcb/thunderbird/0g6v3hww.default/Mail/Local%20Folders/Cl...
Fichier Modifier Affichage Aide

From - Mon Nov 13 08:30:23 2023
X-Account-Key: account2
X-UIDL: 432022.6f+yxyIaSKf,V+0S9q17tACVIw4=
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Return-Path: admin@boulangerie-poitiers.com
Received: from zimbra82-e14.priv.proxad.net (LHLO
zimbra82-e14.priv.proxad.net) (172.20.243.235) by
zimbra82-e14.priv.proxad.net with LMTP; Mon, 13 Nov 2023 02:27:01 +0100
(CET)
Received: from mail.boulangerie-poitiers.com (mx25-g26.priv.proxad.net [172.20.243.
by zimbra82-e14.priv.proxad.net (Postfix) with ESMTTP id 7D39917C6C
for <jclaude.bordes@free.fr>; Mon, 13 Nov 2023 02:27:01 +0100 (CET)
Received: from mail.boulangerie-poitiers.com ([34.90.31.172])
by mx1-g20.free.fr (MXproxy) with ESMTPS for jclaude.bordes@free.fr
(version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256);
Mon, 13 Nov 2023 02:27:01 +0100 (CET)
X-ProxAd-SC: state=HAM score=0
X-ProxAd-Cause: (null)
Authentication-Result: mail.boulangerie-poitiers.com;
auth=pass (plain)
Content-Type: multipart/mixed; boundary="=====0345449350300727770=="
MIME-Version: 1.0
To: jclaude.bordes@free.fr
Subject: =?utf-8?q?Veillez_mettre_à_jour_vos_informations_-_02=3A27?
From: Disney+ <noreply@disneyplus.com>
Received: from localhost (Unknown [127.0.0.1])
by mail.boulangerie-poitiers.com (Haraka/3.0.2) with ESMTPS id BB122E31-FC9E-4
envelope-from <admin@boulangerie-poitiers.com>

```

Cher(e) abonné(e),

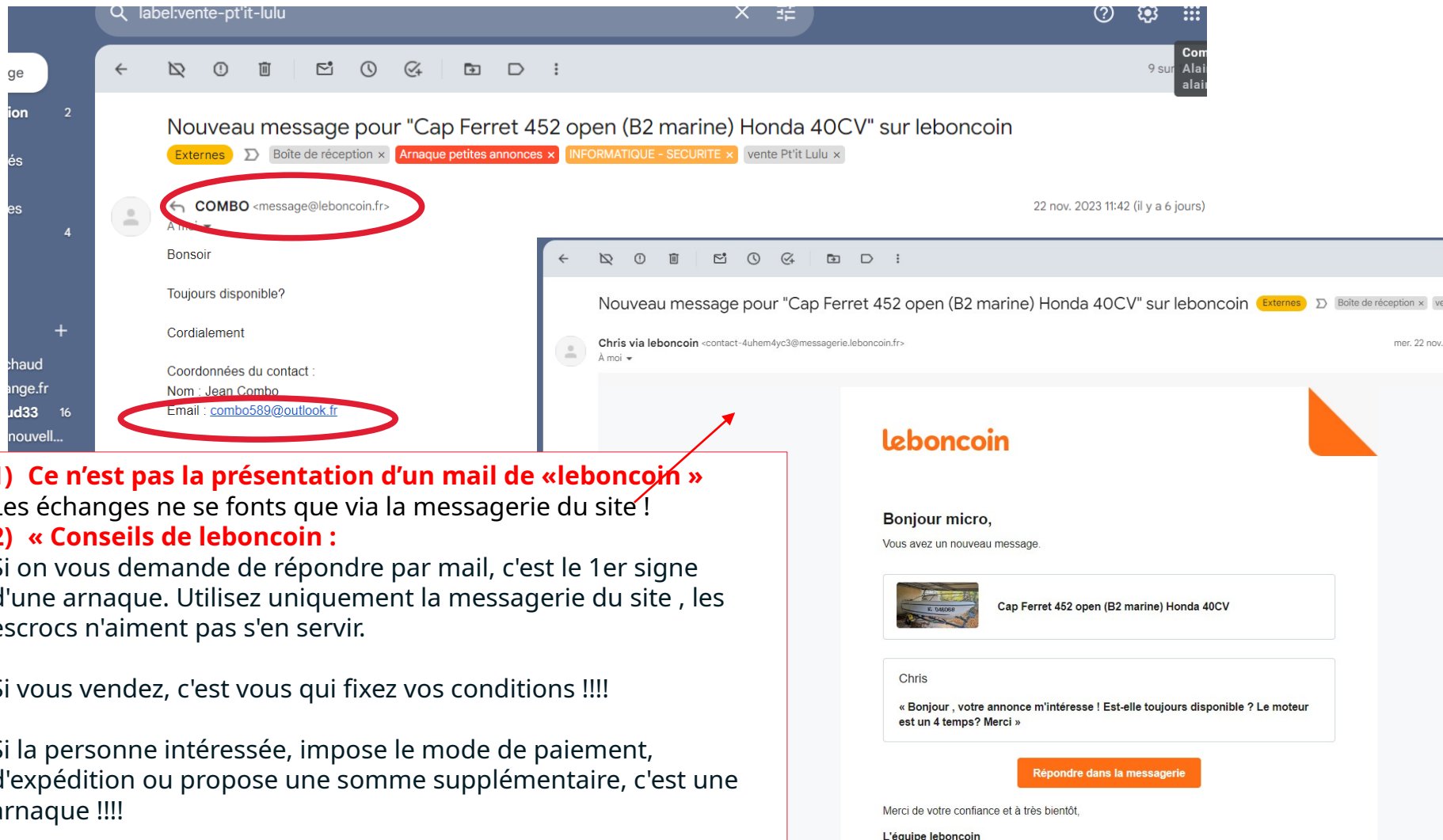
Nous avons détecté un problème avec votre moyen de paiement, ce qui a malheureusement entraîné l'annulation de votre abonnement Disney+.

Pour réactiver votre abonnement, il vous suffit de mettre à jour vos informations de paiement en cliquant sur le bouton ci-dessous. C'est facile et rapide !

Nous espérons vous retrouver bientôt parmi les abonnés Disney+. Si vous avez des questions ou des préoccupations, n'hésitez pas à contacter notre équipe d'assistance.

[ACCÉDER À MON COMPTE](#)

Merci de ne pas répondre à cette communication car nous ne pouvons malheureusement pas vous répondre individuellement. Cet e-mail de service contient des informations essentielles relatives à votre compte ou à un achat ou un abonnement à l'un de nos services. Nous respectons et œuvrons à protéger la vie privée de nos utilisateurs. Pour toute question relative au traitement et à...



Nouveau message pour "Cap Ferret 452 open (B2 marine) Honda 40CV" sur leboncoin

Externes Boîte de réception x Arnaque petites annonces x INFORMATIQUE - SECURITE x vente Pt'it Lulu x

COMBO <message@leboncoin.fr> 22 nov. 2023 11:42 (il y a 6 jours)

Bonsoir

Toujours disponible?

Cordialement

Coordonnées du contact :

Nom : Jean Combo

Email : combo589@outlook.fr


Nouveau message pour "Cap Ferret 452 open (B2 marine) Honda 40CV" sur leboncoin

Chris via leboncoin <contact-4uhem4yc3@messagerie.leboncoin.fr> mer. 22 nov.

leboncoin

Bonjour micro,

Vous avez un nouveau message.

 Cap Ferret 452 open (B2 marine) Honda 40CV

Chris

« Bonjour , votre annonce m'intéresse ! Est-elle toujours disponible ? Le moteur est un 4 temps? Merci »

Répondre dans la messagerie

Merci de votre confiance et à très bientôt,

L'équipe leboncoin

1) Ce n'est pas la présentation d'un mail de «leboncoin»

Les échanges ne se font que via la messagerie du site !

2) « Conseils de leboncoin :

Si on vous demande de répondre par mail, c'est le 1er signe d'une arnaque. Utilisez uniquement la messagerie du site , les escrocs n'aiment pas s'en servir.

Si vous vendez, c'est vous qui fixez vos conditions !!!!

Si la personne intéressée, impose le mode de paiement, d'expédition ou propose une somme supplémentaire, c'est une arnaque !!!!

Si on vous demande de payer par mandat, coupons (PCS , transcash, toneo, neosurf...) mandat..... c'est une arnaque !!!! Ces moyens de paiements sont utilisés par les escrocs car ils sont intraquables.

← [Icons] 7 sur 15 < > Fr ▾

RE Externes ▶ Boîte de réception x Arnaque petites annonces x vente Pt'it Lulu x

Jean Luc <combo589@outlook.fr> à moi ▾ mer. 22 nov. 15:18 (il y a 6 jours) ☆ ↶ ⋮

Bonjour
 Merci pour votre réponse rapide, je suis d'accord pour vous acheter ,je vous informe que je réside à Mandelieu La Napoule mais actuellement en déplacement professionnel Hors de la croix rouge) , Par conséquent, je souhaiterai donc procéder à la vente par une réservation. Postal qui est un paiement instantané que vous auriez la facilité de récupérer l'argent à la poste rmations suivantes afin que je puisse vous envoyer les fonds : -Nom-Prénoms-Adresse-Contacts lundi matin pour finaliser la réservation et me le réserver jusqu'à mon retour. J'espère pouvoir récupérer le bien NB: Concernant la récupération je m'encharge personnellement

Cordialement
 Monsieur Combo Jean-Luc
 ...

[Message tronqué] [Afficher](#)

Et en cas de doute, le bon réflexe !!!! Copier/coller dans un moteur de recherche ou directement dans un site spécialisé.

signal-arnaques.com/scam/view/178658

Accueil Signaler une arnaque Infos Arnaques Forum Analyse fiabilité site Web [Créer un compte](#) [Connexion](#)

signal arnaques
 Ensemble contre les Arnaques
[Signaler une Arnaque](#)
 S'inscrire à la newsletter

ARNIQUE SUSPECTÉE !!!

Arnaque site annonce
[monieur.combo@outlook.fr](#) Jean-Luc Combo [Suivre ce signalement](#)

Date	17/09/2019
Email	monieur.combo@outlook.fr
Pseudonyme utilisé	Jean-Luc Combo

Bonjour, Je suis d'accord pour vous l'acheter mais je tiens à vous informez que je suis en déplacement pour des raisons professionnelles. Ceci étant, je vous verserais l'argent par un paiement via le service postal que vous allez recevoir en espèce c'est à dire en liquide pour la réservation et après encaissement du

- Antivirus et outils de nettoyage
- Sauvegarde des données personnelles

- **Antivirus et outils de nettoyage**

- ☞ Il est recommandé d'installer un antivirus payant (Bitdefender, Norton...)(1) ou gratuit (Avast...) et de réaliser périodiquement un scan de ses disques durs
- ☞ Il est recommandé d'installer un outil de nettoyage (fichiers, registres, applications) : CCLEANER, Wise Disk Cleaner et Wise Registry Cleaner par exemple
- ☞ Il est impératif de réaliser les mises à jour système et des applications pour prendre en compte les corrections des bugs de sécurité

- **Sauvegarde des données personnelles**

- ☞ Il est impératif de réaliser des sauvegardes de ses équipements (ordinateur, tablette, téléphone) sur :
 - Un support externe : disque dur amovible mais **pas** clé USB
 - Un espace de stockage réseau (cloud) (2)

- 1) et de l'installer sur tous les ordi, tablettes, mobiles avec lesquels vos données sont partagées. En général, les antivirus payants proposent l'installation sur 4 à 5 supports. Les mises à jour des bases de données sont quotidiennes, parfois plus !!!
- 2) Souvent fourni avec les abonnements payants type Microsoft 365 ou autres

- Vos équipements électroniques (ordinateur, tablette, smartphone) peuvent tomber en panne
 - Une attaque virale peut infecter vos équipements
 - Vos données peuvent subir un chiffrement assorti d'une demande de rançon (ransomware ou rançongiciel)
- Nécessité de conserver un double de vos données
- ☞ Sur un support externe
 - ☞ Dans le cloud

- Sauvegarde sur support externe
 - ☞ Utiliser un disque dur externe mais pas une clé USB
 - ☞ Copier périodiquement ou après enregistrement de documents importants le ou les répertoires contenant les données
 - ☞ Utiliser l'outil de sauvegarde de Windows 10 pour synchroniser ces répertoires avec le disque externe
- Sauvegarde dans le cloud
 - ☞ Activer la synchronisation de votre équipement avec le cloud utilisé : One drive de Windows, Google drive, iCloud d'Apple...

- Gestion des mots de passe
- Configuration du navigateur
- Quelques règles de navigation prudente sur Internet
- Piratage via microsoft sur le web et appel téléphonique
- Utilisation d'un VPN

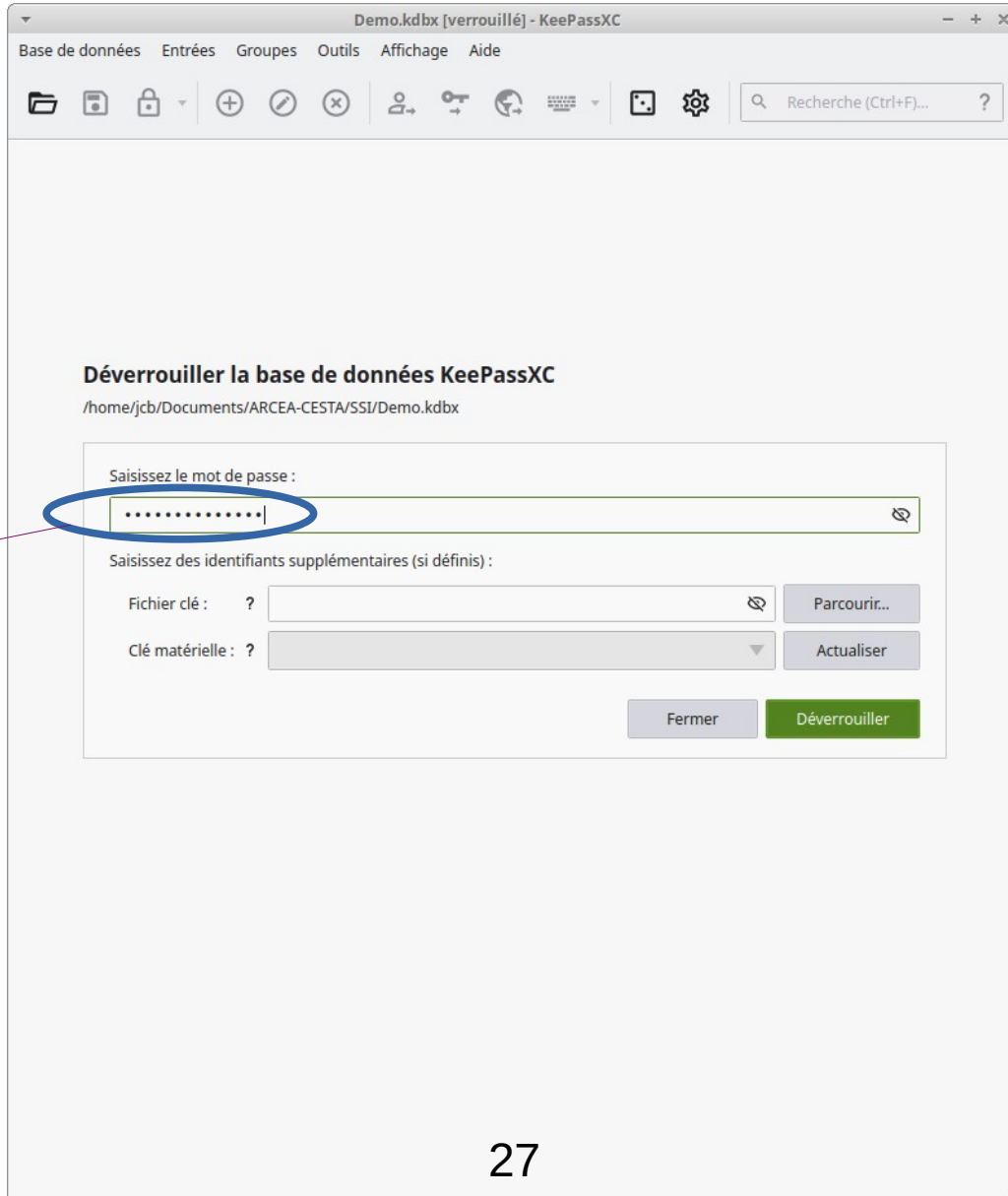
- Je définis un mot de passe différent pour chaque service
- Chaque mot de passe contient au moins 12 caractères contenant au moins 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial
→ ,?. ;!-
- Chaque mot de passe ne contient pas un mot du dictionnaire
- Comment définir et retenir autant de mots de passe ?
 - ☞ Utiliser un « coffre-fort » à mots de passe
 - ☞ Utiliser un générateur de mot de passe

KeePass, un gestionnaire de mots de passe sécurisé et gratuit

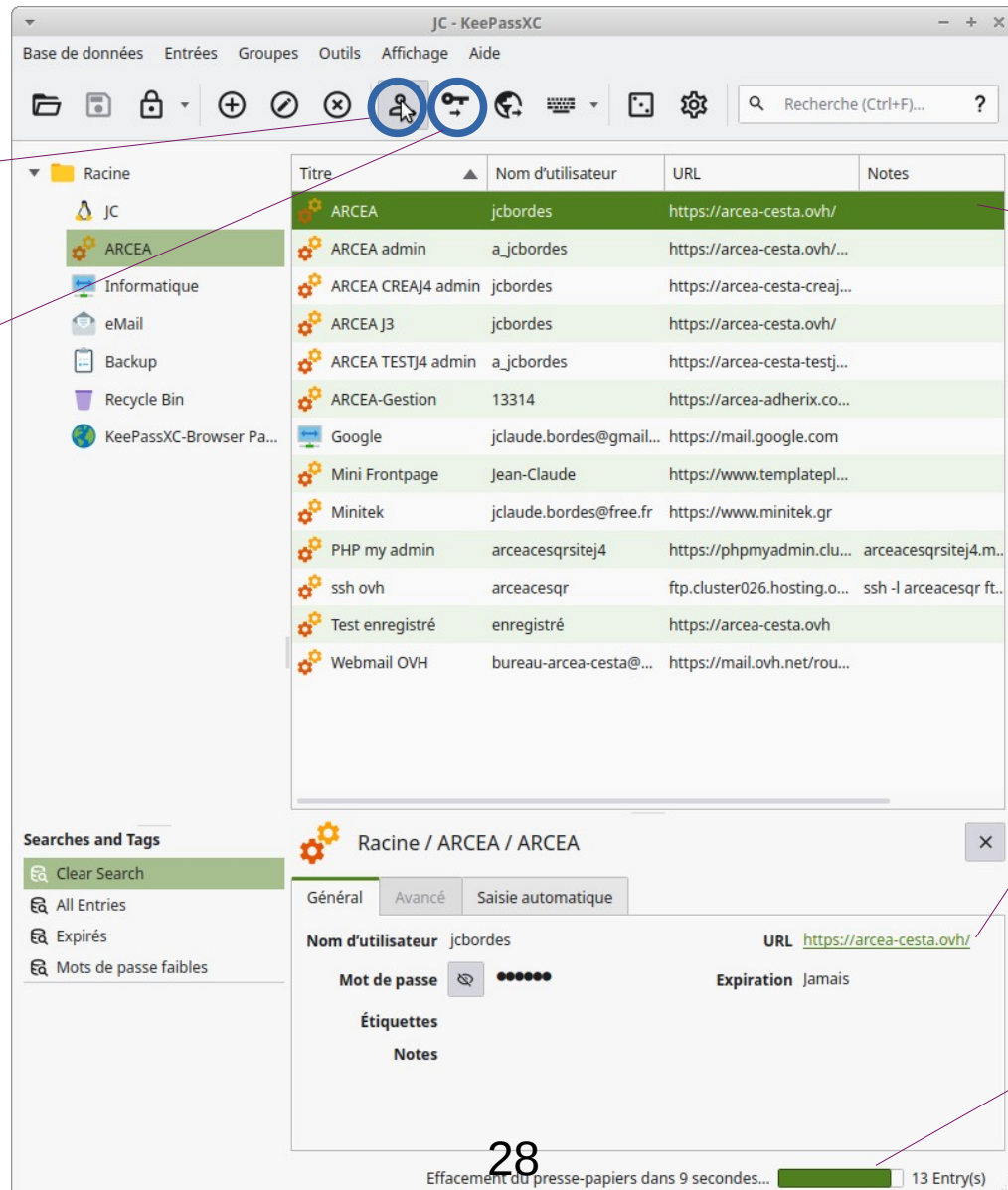
Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. [KeePass](#) dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

<https://www.cybermalveillance.gouv.fr>

- Logiciel open source, certifié niveau 1 par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) , gratuit et multi-plateformes (Windows, Linux, Android, IOS).
- Base de données stockée dans un répertoire de l'utilisateur (disque dur, clé USB, cloud...)
- Base de données protégée et chiffrée par un mot de passe qui doit être très sécurisé : c'est le seul mot de passe à retenir !
- Le mot de passe ne peut pas être récupéré ni modifié si on l'a oublié.
- Fonctions de copie en 1 clic de l'identifiant, du mot de passe et de l'URL.
- Intégration possible aux principaux navigateurs (firefox, edge, chrome...)



Mot de
passe
principal



Copie
1 clic
identifiant

Copie
1 clic
mot de
passe

Entrée
active

Accès
direct
À l'URL

Présence
dans
presse-
papiers

Connexion ou création d'un compte

création de compte refusée si non adhérent

jcbordes

Remplir les identifiants à partir de KeePass

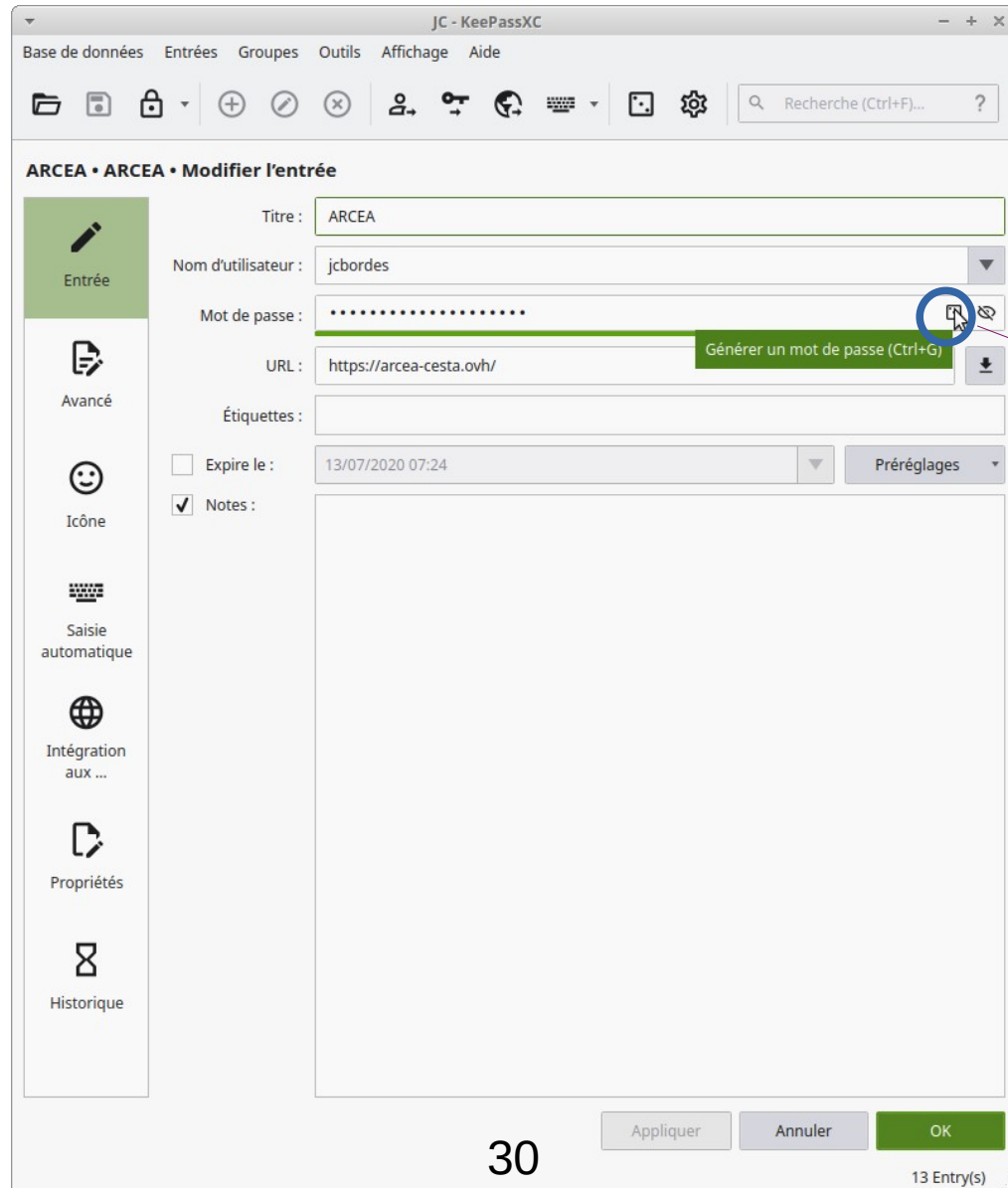
.....

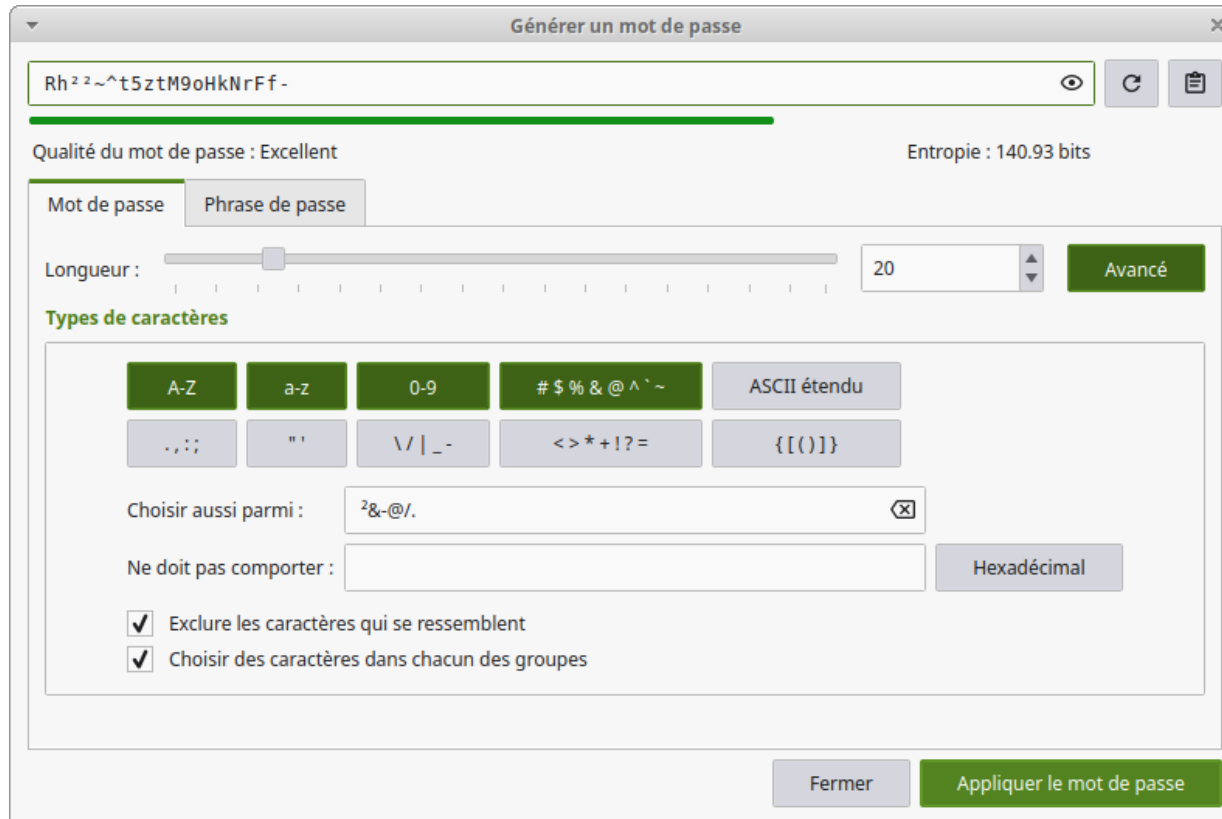
Se souvenir de moi

Connexion

Mot de passe perdu ?
Identifiant perdu ?
Créer un compte +

Intégration
KeePass
Dans
navigateur



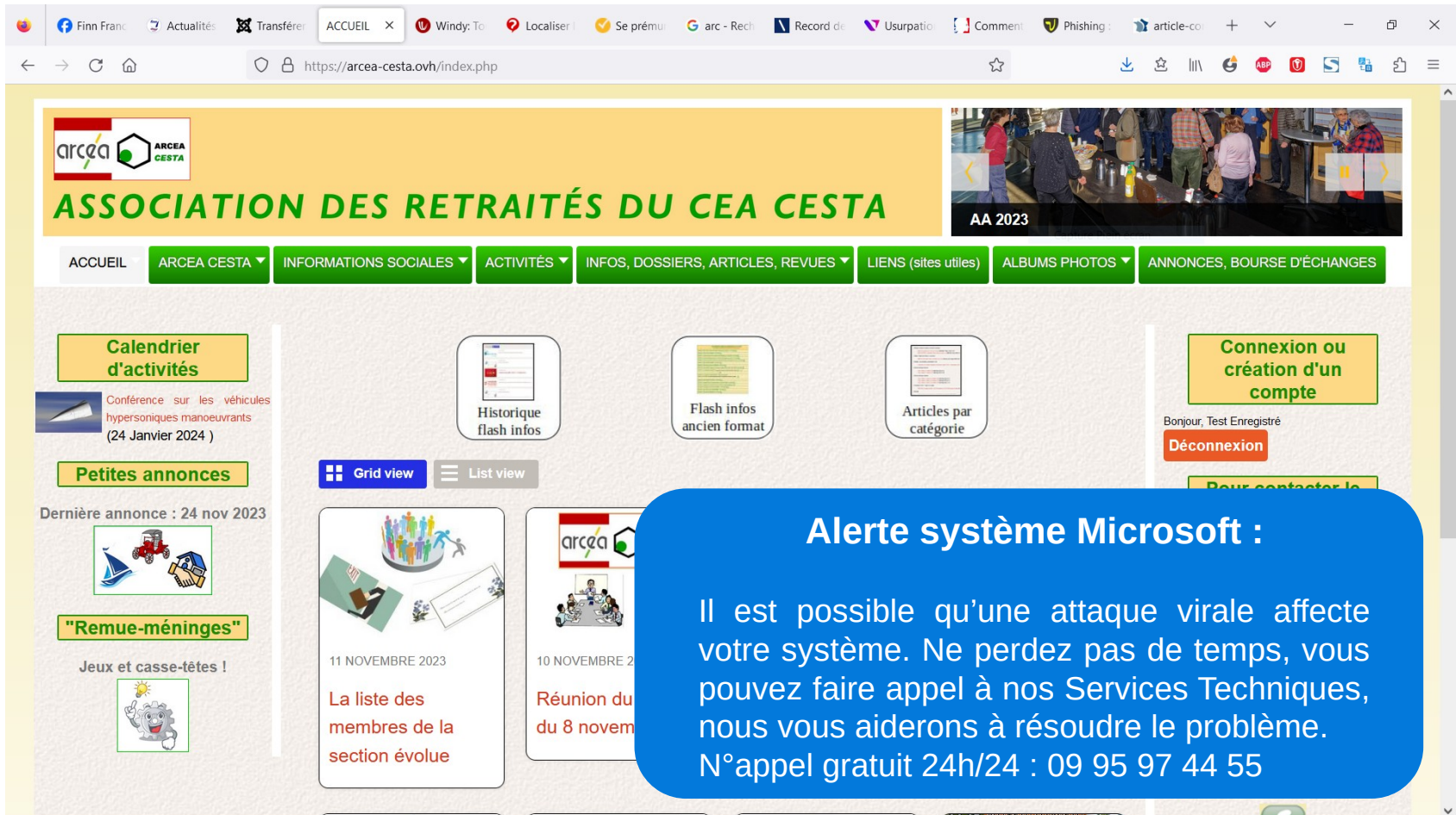


- Outil de recherche : pourquoi pas DuckDuckGo, Qwant ou Ecosia à la place de Google ?
- Vie privée et sécurité
 - ☞ Effacer les cookies et l'historique de navigation à la fermeture
 - ☞ Ne pas accepter d'enregistrer les identifiants et les mots de passe
 - ☞ Utiliser le mode de navigation privée s'il est disponible
 - ☞ Bloquer les fenêtres pop-up

- Vérifier que l'adresse du site consulté commence par https://
- Achats sur internet
 - ☞ Ne réaliser des achats que sur des sites marchands « connus » : grandes enseignes, réputation reconnue, achats déjà réalisés...
 - ☞ Éviter les sites marchands situés dans des pays où la législation commerciale n'est pas connue ou semble douteuse
 - ☞ Vérifier que l'adresse du site commence par https:// et qu'un cadenas figure dans la barre d'adresse
 - ☞ Pour les paiements par carte bancaire, préférer les sites qui s'appuient sur les outils de confirmation d'achat sur smartphone (Visa ou Mastercard selon le cas)

La méthode « d'accrochage » :

à l'ouverture de votre navigateur ou d'une page web, un popup apparaît :



The screenshot shows a web browser displaying the homepage of ARCEA CESTA. The browser's address bar shows the URL <https://arcea-cesta.ovh/index.php>. The website header includes the ARCEA CESTA logo and the title "ASSOCIATION DES RETRAITÉS DU CEA CESTA". A navigation menu contains links for ACCUEIL, ARCEA CESTA, INFORMATIONS SOCIALES, ACTIVITÉS, INFOS, DOSSIERS, ARTICLES, REVUES, LIENS (sites utiles), ALBUMS PHOTOS, and ANNONCES, BOURSE D'ÉCHANGES. The main content area features several sections: "Calendrier d'activités" with a notice about a conference on January 24, 2024; "Petites annonces" with a "Dernière annonce : 24 nov 2023"; "Remue-ménages" with "Jeux et casse-têtes!"; "Historique flash infos"; "Flash infos ancien format"; "Articles par catégorie"; and a "Connexion ou création d'un compte" section with a "Déconnexion" button. A blue callout box is overlaid on the right side of the page, containing the following text:

Alerte système Microsoft :
 Il est possible qu'une attaque virale affecte votre système. Ne perdez pas de temps, vous pouvez faire appel à nos Services Techniques, nous vous aiderons à résoudre le problème.
 N°appel gratuit 24h/24 : 09 95 97 44 55

La suite :

Vous êtes troublés, réticents ... mais comme l'affaire se répète, vous cédez, prenez votre tél et ...:

- une (ou un) opératrice se présente (Sté xxx « spécialiste agréé Microsoft »)
- elle vous rassure et vous assure que vous n'êtes pas seul dans ce cas (!!!!)
- elle vous précise que « rapidité et efficacité » sont de mises en pareille situation
- elle propose de procéder de suite, à distance, à la résolution du pb :
 - prise de contrôle de votre PC
 - analyse et nettoyage du système
 - éventuellement mise en place de protections supplémentaires
 - **prends vos coordonnées (adresse, email, tél, ...)**
 - vous précise (?) que la prestation est payante (virement bancaire)

Évidemment, vous acceptez ... et roule !

Le processus (toujours en liaison téléphonique):

- elle vous guide pas à pas pour vous faire installer TeamViewer ou autre
- la prise de contrôle de votre PC est faite ... et à partir de là : **vous ne maîtrisez plus rien ... et n'osez plus rien, vous êtes quasiment « sous hypnose » !**
- 1 heure parfois plus se passent, ...vous voyez plein de choses se passer sur votre écran !
- ... ça y est, c'est fini, la technicienne vous dit que tout est réglé ! (* au bémol près...)
- elle vous donne quelques conseils (!) et on passe au paiement, 350 euros !!!
- ... paiement sécurisé, et volontaire puisque en fait, c'est vous qui y procédez depuis votre écran, et avec la double identification sur votre mobile en plus !
- ça y est, votre compte a été soulagé de 350 euros ... et vous recevez instantanément par mail une facture acquittée !!!!

En fait, à par le mode d'accroche pour le moins litigieux, **tout a été fait avec votre consentement**. Quant à la société émettrice de la facture, elle existe bel et bien et c'est effectivement une société avec un département « maintenance informatique » !!!!! ... à méditer ! Histoire vraie, vécue par André et Claudine Sarps cette année.

Dans quel monde vivons-nous !!!!!

Microsoft ne vous contactera jamais de manière proactive pour vous fournir un support technique non sollicité.

Si vous recevez un appel téléphonique de Microsoft ou qu'une fenêtre contextuelle s'affiche sur votre PC avec un faux message d'avertissement et un numéro de téléphone à appeler afin de résoudre votre « problème », il est préférable de ne pas cliquer sur les liens et de ne fournir aucune information personnelle.

Ne jamais appeler le numéro fourni dans le message d'erreur. Les véritables messages d'erreur Microsoft n'incluent jamais un numéro de téléphone à appeler.

Si vous estimez que vous êtes la cible d'une escroquerie de support technique, vous pouvez aider Microsoft à arrêter les cybercriminels en la signalant.

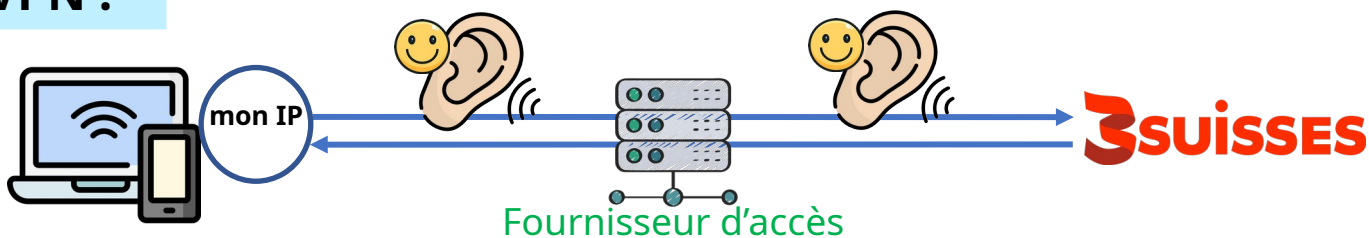


Un VPN c'est quoi, à quoi ça sert et pourquoi l'utiliser ?

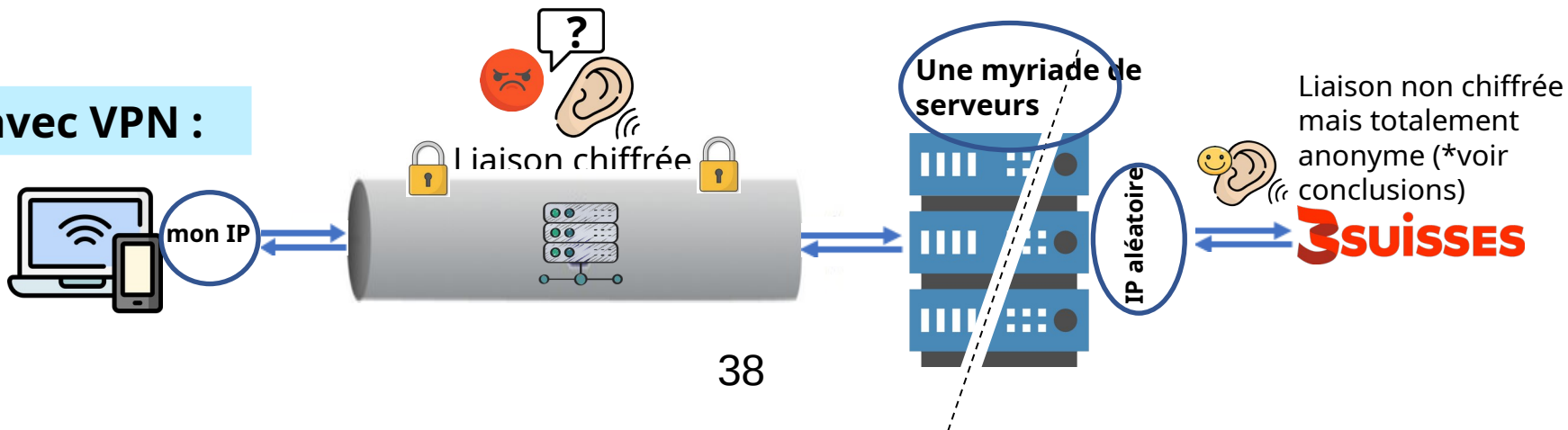
"Virtual Private Network" : "Réseau privé virtuel"

Le principe :

sans VPN :



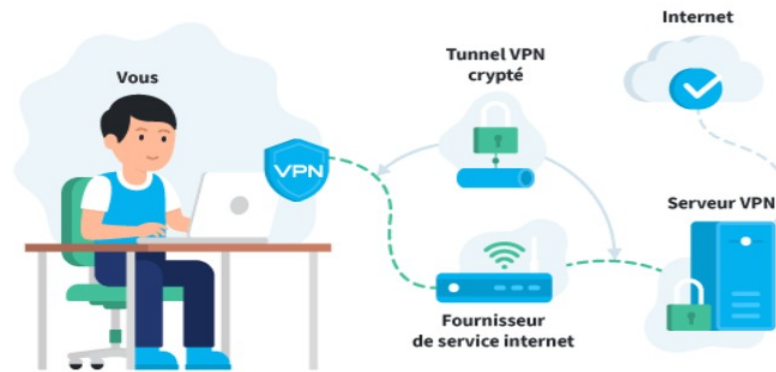
avec VPN :





Un VPN c'est quoi, à quoi ça sert et pourquoi l'utiliser ?

Le principe :



- o Cacher son IP
- o Cacher son trafic et/ou éviter une censure
- o Changer de pays ou contourner une censure (Chine, Russie, ...)
- o Sécuriser une connexion internet ou Wifi (dans les lieux publics)
- o Dans un environnement professionnel



Mais attention ! Le VPN a ses limites !

- **Ce n'est pas un antivirus**
- **Ce n'est pas un firewall**
- Il peut présenter ses propres failles
 - le VPN n'anonymise pas totalement pour le FAI
 - le VPN n'est pas une cape d'invisibilité
 - le VPN n'anonymise pas non plus la navigation à 100%
 - le VPN peut être lui-même source de fuite de données



Conclusion :

Un VPN présente un intérêt indéniable, mais gardons à l'esprit que :

- o il ne vous tient pas la main dans vos **navigations parfois imprudentes sur le NET !**
- o Il ne vous empêchera pas de fournir des **infos personnelles parfois nécessaires mais souvent inutiles**

Comme pour se protéger contre la grippe et la covid :

- o **Soyez réfléchis et prudents** dans vos navigations sur le WEB, un clic de souris peut-être lourd de conséquences !
- o **Installer un bon antivirus** ... et comme pour les vaccins, veillez à ce qu'il soit mis à jour régulièrement


- Exposition des données personnelles

- ☞ Il est impératif de limiter l'accès à ses données personnelles au strict nécessaire
- ☞ Malgré cette limitation, toutes les données déposées sur un réseau social deviennent sa propriété et il peut les utiliser comme il l'entend : revente à des annonceurs...
- ☞ Les données que vous effacez ne sont plus visibles mais rien ne garantit qu'elles sont effectivement effacées des serveurs du réseau social
- ☞ La liste des données conservées peut être très « complète »

Des outils de protection globale (comme Bitdefender par exemple) proposent une analyse en temps réel des expositions de vos données personnelles. ... vous sensibilise et vous propose de remédier à leur impact potentiel !

C'est édifiant et ça vous laisse pantois !

- A titre d'exemple, voici les données recueillies et conservées par Facebook

 Internet sans danger : Le guide du bon sens numérique de Virginie Sellier (Bayard Jeunesse)

• Demandez au site de vous créer un dossier d' « Archive étendue »

des données collectées depuis le jour de votre inscription. Cliquez sur la petite étoile en haut à droite de votre page d'accueil, puis tout en bas « Télécharger une copie de vos données sur Facebook ». Deux possibilités : « Créer mon archive », ou plus complet, « Télécharger une archive étendue » .

• Vous allez découvrir, dans votre dossier Facebook d' « Archive étendue »

- vos données renseignées (date de naissance, ville, formation, citations, emploi, opinions politiques, etc. figurant dans « À propos de moi » ;
- les photos et vidéos que vous avez publiées ;
- vos publications ;
- vos messages privés et vos conversations instantanées ;
- le nom de vos amis et leurs adresses mails ;
- la liste des groupes auxquels vous appartenez ;
- vos liens de parenté avec les autres membres ;
- l'historique du statut de votre compte (dates de réactivation, de désactivation ou de suppression) ;
- les sessions actives (connexions et déconnexions) stockées avec les infos relatives à la date, l'heure, l'appareil, l'adresse IP,

- les cookies de la machine et le navigateur ;
- l'identification des pubs sur lesquelles vous avez cliqué (à quelle date et à quelle heure),
- votre adresse mail et toutes les autres adresses y ayant figuré depuis la création de votre compte ;
- les sujets de publicité dont vous étiez la cible ;
- la liste des sujets susceptibles de vous intéresser en fonction de vos mentions « J'aime », de vos intérêts et de diverses autres données de votre journal ;
- les applications auxquelles vous êtes abonné(e) ;
- la liste des personnes que vous avez supprimées de votre liste d'amis ;
- les demandes d'amitié en attente ;
- tout ce que vous avez un jour masqué dans votre fil d'actualité ;
- vos réseaux (affiliations avec des écoles ou des lieux de travail) ;
- la liste de toutes les notifications ;
- la liste des pages que vous administrez ;
- les numéros de téléphone mobile que vous avez ajoutés à votre compte ;
- la liste des personnes que vous avez pokées ou qui vous ont poké. Cette liste est non exhaustive. Vous pouvez la consulter sur : <https://www.facebook.com/help/405183566203254>

- Configuration des comptes
 - ☞ Dans son profil ne faire apparaître que les informations strictement nécessaires
 - ☞ Parcourir toutes les rubriques « Sécurité – vie privée » pour paramétrer la visibilité que vous voulez accorder à vos données
 - ☞ Si nécessaire, protéger l'affichage de données dans votre espace personnel (mur facebook, par exemple)
 - ☞ Si besoin, interdire l'indexation de ses données personnelles par les moteurs de recherche (impossible pour un compte Google+)