La Sécurité du Système d’Information (SSI)

La Sécurité du Système d'Information

Les bonnes pratiques à mettre en œuvre

Votre compte informatique et votre ordinateur sont des outils de travail : il est de votre responsabilité de les utiliser correctement

Signalez les incidents et activités suspectes au support : https://support.univ-lyon1.fr

Vos identifiants sont personnels et doivent le rester, ne pas les partager !

N'utilisez pas votre mot de passe Lyon 1 pour d'autres services extérieurs.

Le support ne vous demandera jamais votre mot de passe.

Verrouillez votre poste de travail quand vous vous absentez

Windows : Touches Windows (⊞) + L (pour LOCK)

Mac OS : Touches Control (^) + Command (⌘) + Q

La Sécurité du Système d'Information

Les bonnes pratiques à mettre en œuvre

Chiffrez votre ordinateur portable

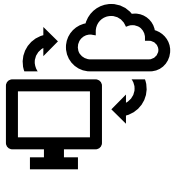
Vérifiez régulièrement que votre antivirus fonctionne

Ne pas installer de programmes en provenance de sites web louches

Ne pas ouvrir les pièces jointes ou cliquer sur les liens dans les emails d'expéditeurs inconnus

Vérifiez l'expéditeur réel du message

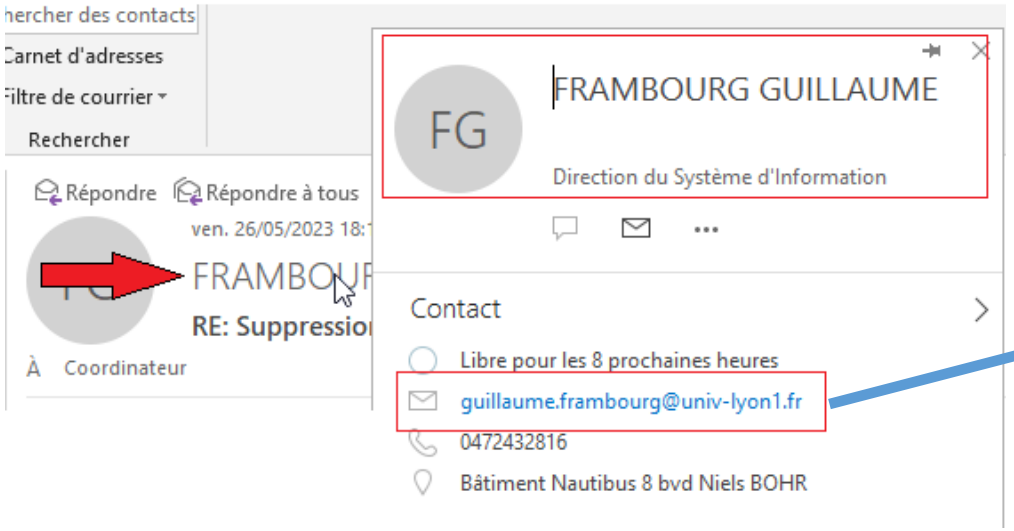
Vérifiez que vous êtes bien sur un site web de l'Université avant de saisir vos identifiants de connexion Lyon 1



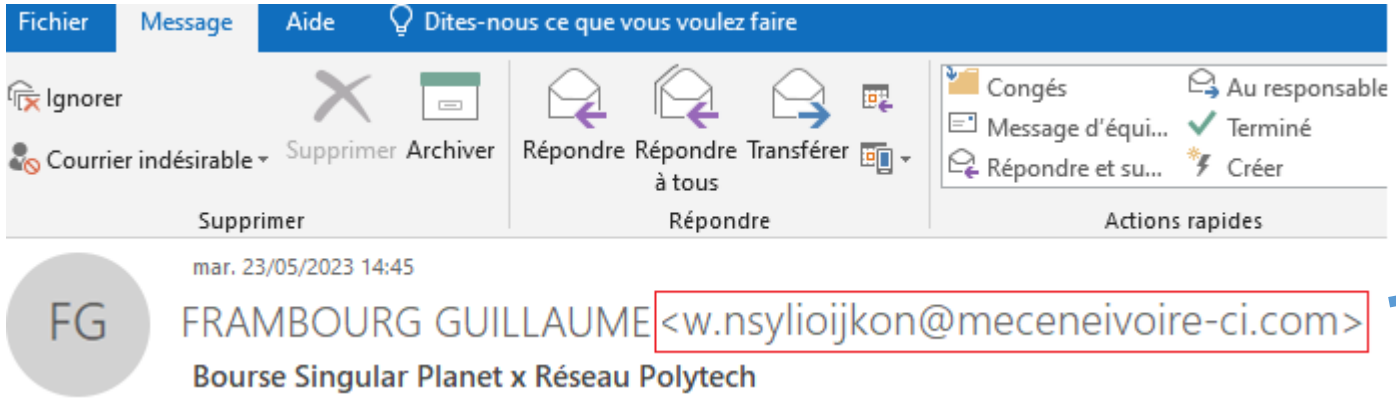
Sauvegardez vos données

Université Claude Bernard Lyon 1

Comment vérifier l'expéditeur réel d'un email



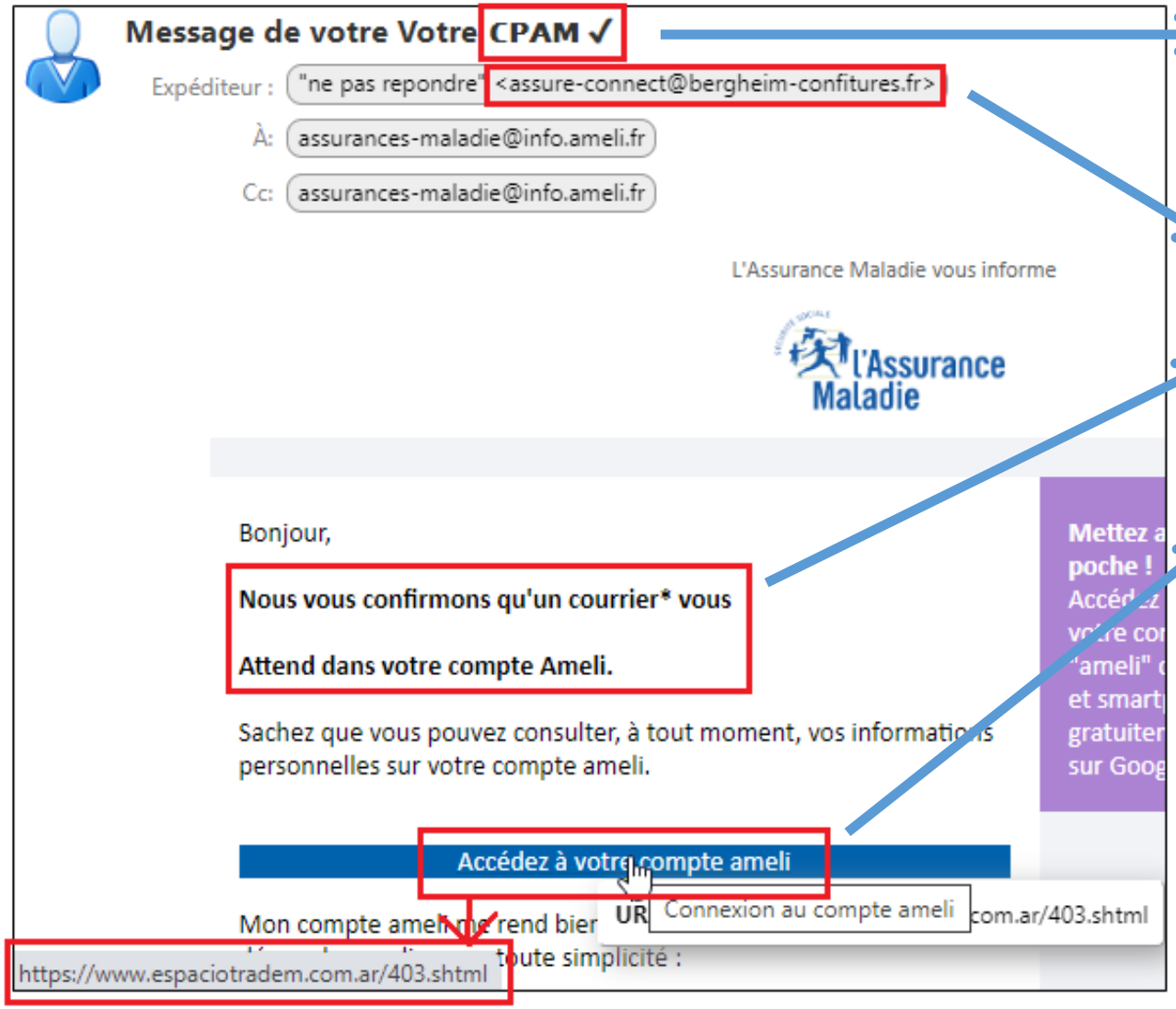
Le NOM PRENOM s'affiche, l'email source est bien @univ-lyon1.fr : cet email a été envoyé depuis un compte interne à notre organisation



Le nom d'affichage « FRAMBOURG GUILLAUME » est valide et existe dans notre système d'information, mais il est usurpé !

On voit l'adresse réelle d'envoi entre les <crochets> qui n'est pas @univ-lyon1.fr

Des indicateurs d'un email douteux



Police de caractère différente entre le début du sujet et la fin (subtil) + caractère étrange à la fin qui est une fantaisie rarement utilisée par des organismes officiels

Email d'origine rigolo mais clairement pas lié à Ameli

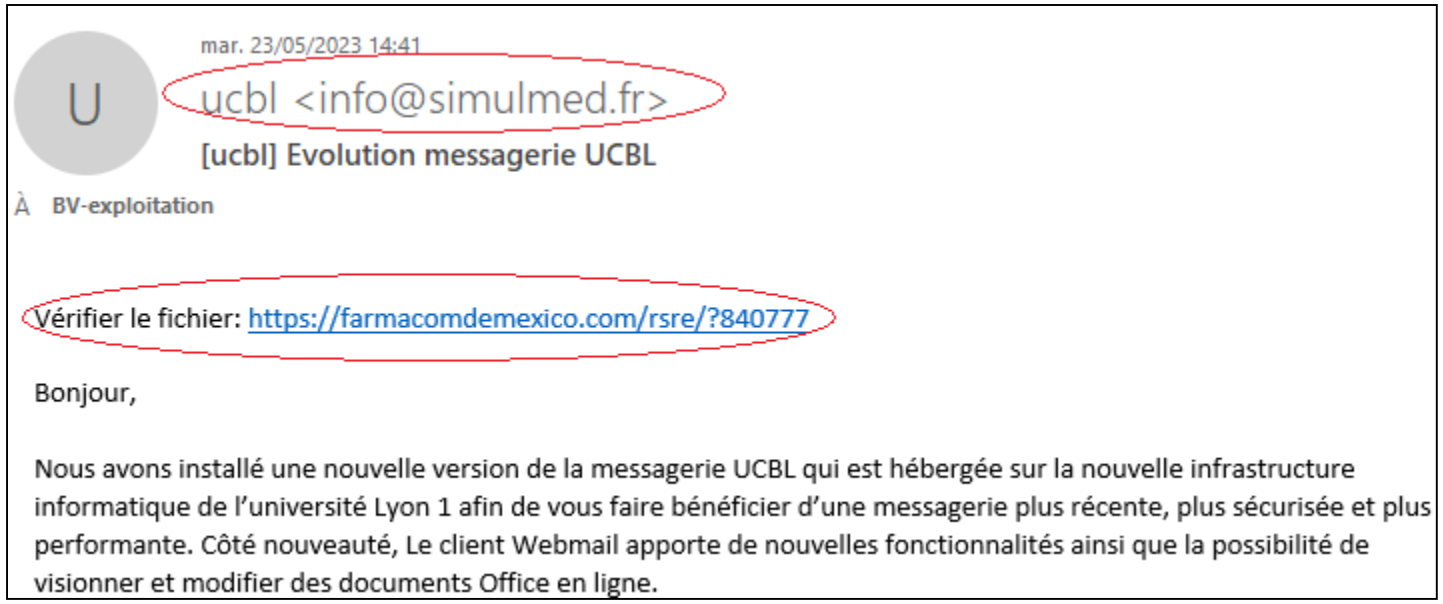
Fautes de frappes et d'orthographe dans un email supposé automatisé. Parfois en français approximatif.

On ne clique pas sur le lien ! Positionnez le pointeur dessus et regardez en bas à gauche de votre navigateur la vraie adresse vers laquelle ce lien vous envoie

(Note : Les liens dans les emails externes sont remplacés par https://mailinblack.univ-lyon1.fr/securelink/... pour analyse par MailInBlack)

Des indicateurs d'un email douteux

Une technique de phishing utilisée consiste à reprendre un vrai email déjà envoyé et à le renvoyer.
On retrouve le même expéditeur (sauf l'adresse entre crochets), destinataires (parfois masqués), sujet, contenu mais est ajouté un lien vers un site de phishing ou une pièce jointe malveillante :


mar. 23/05/2023 14:41

U

ucbl <info@simulmed.fr>

[ucbl] Evolution messagerie UCBL

À BV-exploitation

Vérifier le fichier: https://farmacomdemexico.com/rsre/?840777

Bonjour,

Nous avons installé une nouvelle version de la messagerie UCBL qui est hébergée sur la nouvelle infrastructure informatique de l'université Lyon 1 afin de vous faire bénéficier d'une messagerie plus récente, plus sécurisée et plus performante. Côté nouveauté, Le client Webmail apporte de nouvelles fonctionnalités ainsi que la possibilité de visionner et modifier des documents Office en ligne.

Les pirates siphonnent le contenu des comptes qu'ils réussissent à pirater et s'en servent comme « base » pour tenter de pirater d'autres comptes.

Des indicateurs d’un email douteux

Quand un compte Lyon 1 se fait pirater, il peut être utilisé pour envoyer des pièces jointes avec une charge virale afin de pirater d’autres comptes en interne.

Un email bel et bien en provenance d’un compte @univ-lyon1.fr n’est donc pas toujours sûr.

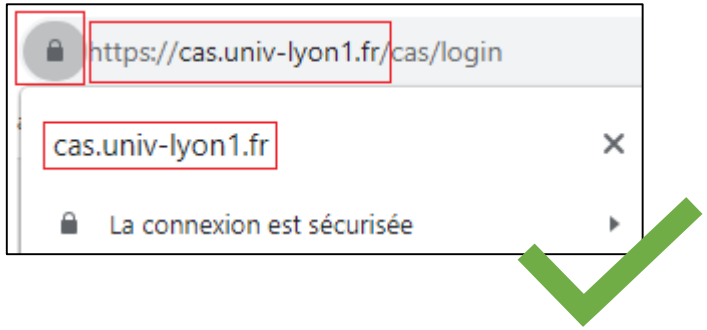
- Cette personne m’envoie-t-elle des pièces jointes habituellement ?
- Est-ce logique qu’une pièce jointe soit dans cet email spécifique ?
- Cette personne m’envoie un lien vers un site externe qui me demande de m’authentifier: je vérifie l’adresse du site (voir pages suivantes)
- J’ai un doute : je contacte l’émetteur du message par téléphone ou je contacte le support : https://support.univ-lyon1.fr

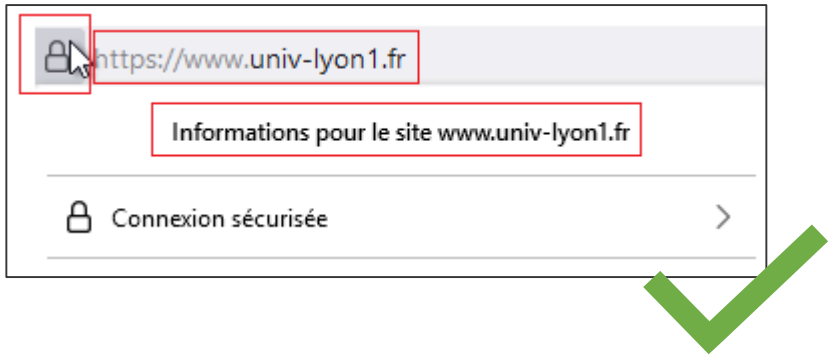
Comment vérifier que vous êtes sur un site valide

1) La connexion doit être sécurisée (présence du petit cadenas dans la barre d'adresse)

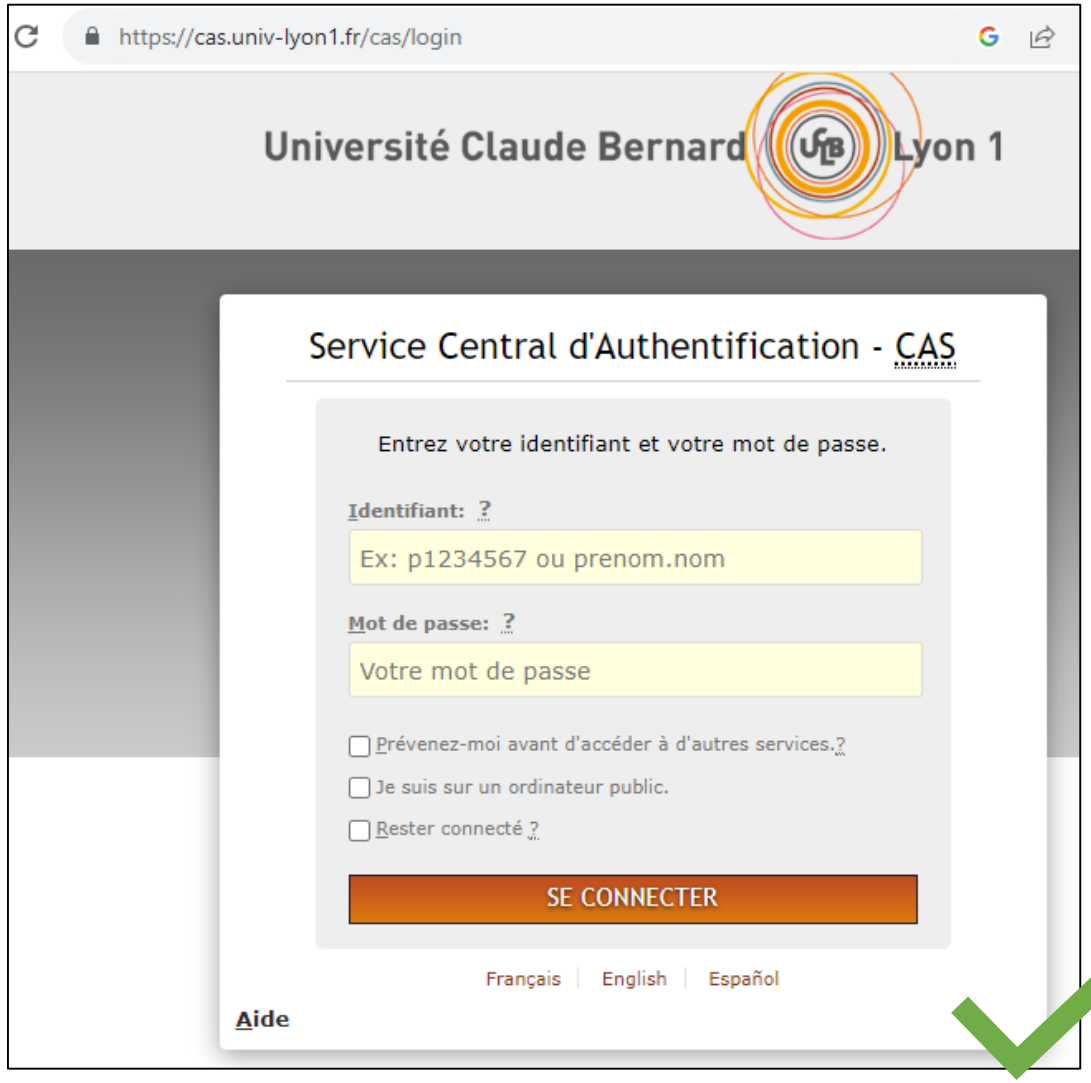
2) La barre d'adresse et le nom du site doivent correspondre à ce que vous souhaitez consulter

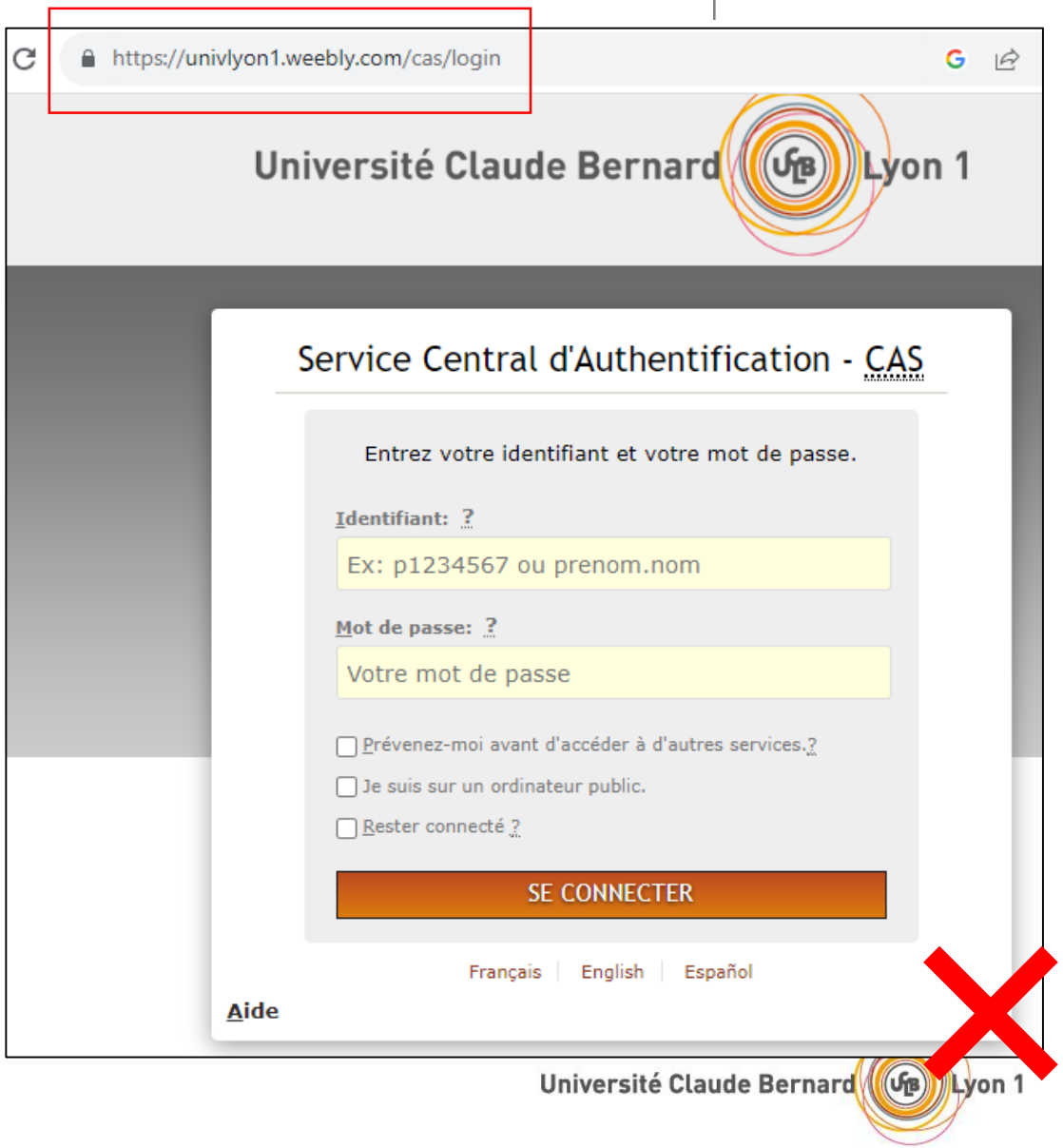
3) S'il s'agit d'une page de connexion avec vos identifiants Lyon 1, vérifier que le début de l'adresse contient bien univ-lyon1.fr et qu'il s'agit d'une adresse dont vous avez l'habitude, par exemple cas.univ-lyon1.fr





Attention aux faux sites





La Sécurité du Système d'Information

Protection de vos données : le cas des I.A.

Il faut voir les IA comme des clouds externes : les requêtes que vous y faites contiennent souvent des données sensibles / à caractère personnel, parfois des mots de passe !

Ces requêtes sont stockées et peuvent ressortir chez d'autres utilisateurs.

Certains clouds proposent des espaces « privés » (exemple : version pro Copilot de Microsoft) mais vos données sont quand mêmes parties dans un cloud externe…

Donc attention à ce que vous donnez « à manger » aux I.A.

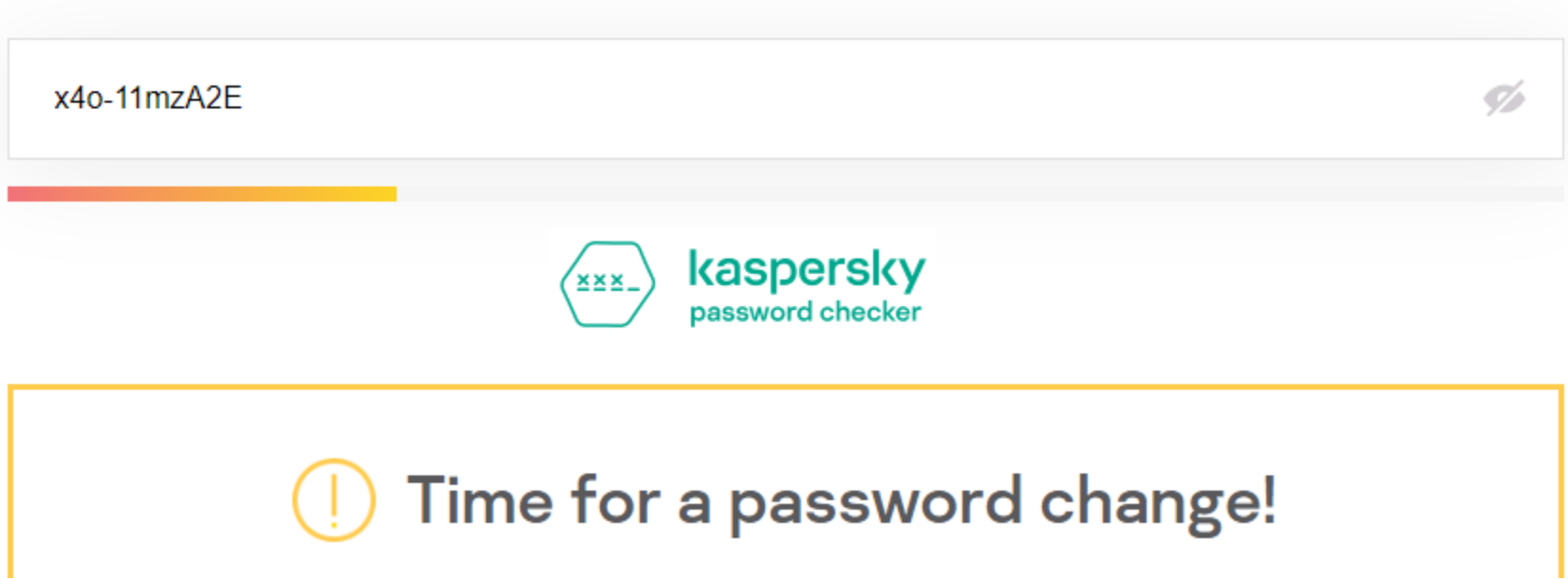
D'une façon générale, attention aux clouds : une fois vos données externalisées, vous n'avez plus de maitrise dessus : elles peuvent finir dans des pays où la législation est bien moins protectrice qu'en France.

La Sécurité du Système d'Information

Les mots de passe

Choisir un mot de passe complexe : c'est simple !

Ne pas choisir un mot de passe cryptique trop dur à retenir qui au final n'est pas particulièrement sécurisé (et finira sur un post-it) :



La Sécurité du Système d'Information

Les mots de passe

Utiliser des passphrases avec de petites variations, faciles à mémoriser et rapides à saisir pour réduire le risque des regards indiscrets :

@J'aime_Les_Frites!!!

kaspersky
password checker

Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

La Sécurité du Système d'Information

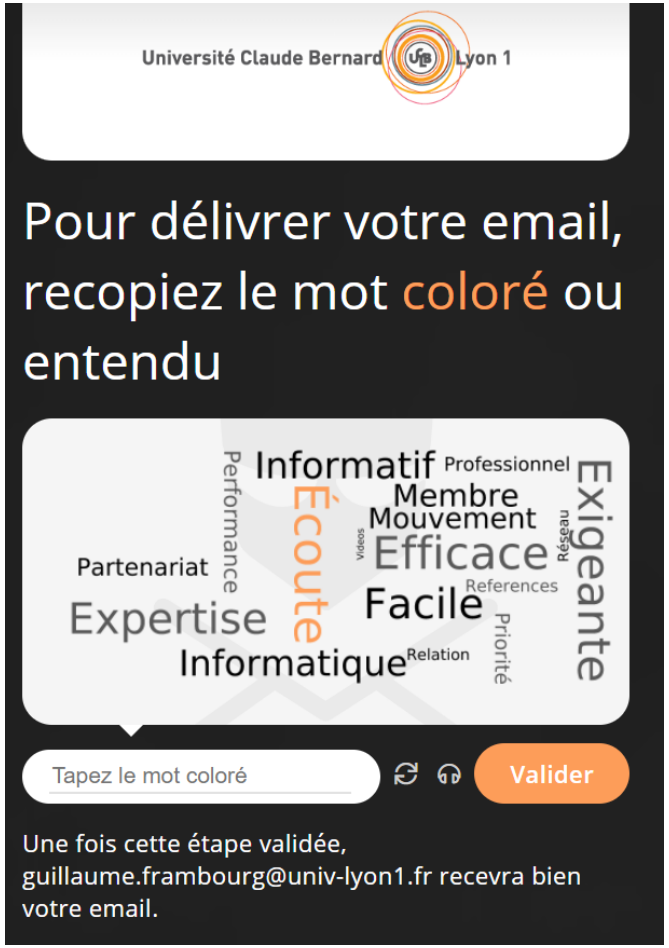
Les mots de passe

- Rappel : les actions effectuées avec votre compte sont de votre responsabilité
- Utiliser des mots de passe différents pour chaque système d'information / site web
- Les changer régulièrement (~6 mois, 1 an max)
- Ne pas les écrire ni les communiquer, même aux services informatiques
- Ne pas les partager même avec des personnes de confiance : ils ne protégeront pas aussi bien que vous vos mots de passe
- Vérifiez que personne ne vous espionne (ou filme avec un téléphone ou autre) quand vous saisissez votre mot de passe
- Lors de la saisie de vos identifiants, arrêtez vous au milieu du mot de passe, levez le nez et vérifiez que vous êtes en train de le saisir au bon endroit…
- Ne saisissez pas votre mot de passe sur des ordinateurs publics ou de personnes inconnues
- Si vous avez besoin de mémoriser beaucoup de mots de passe différents, utilisez un coffre fort électronique pour les stocker (KeePass par exemple)
- En cas de doute : changez votre mot de passe le plus rapidement possible depuis un poste de confiance

MailInBlack Protect

https://mailinblack.univ-lyon1.fr

- Solution antispam antivirus pour le personnel uniquement
- Les personnes extérieures qui vous contactent pour la première fois doivent saisir un CAPTCHA
- Vous recevez des rapports (3/j, personnalisable) pour les emails en attente
- Vous pouvez valider instantanément les emails en attente en vous connectant sur l'interface web Mailinblack
- Vous gérez votre propre liste blanche et liste noire
- Les liens dans les emails extérieurs sont automatiquement renvoyés vers https://mailinblack.univ-lyon1.fr/securelink/... (analyse de sécurité des liens)



Université Claude Bernard Lyon 1

La Sécurité du Système d'Information

Quelques astuces avant de terminer

Installez le module « ublock origin » (https://ublockorigin.com) qui va bloquer les publicités dans votre navigateur (firefox ou chrome) : les publicités sont parfois un vecteur d'attaque.

Si vous devez stocker des données dans un cloud externe, chiffrez vos données avant de les stocker (compresser dans une archive avec un mot de passe ou utiliser un logiciel de chiffrement comme par exemple https://www.veracrypt.fr/)

Désactivez le bluetooth de vos appareils quand vous en avez pas l'usage

N'utilisez pas les réseaux wifi sans mot de passe

Quand vous avez un avertissement de certificat invalide, arrêtez-vous là! Certains réseaux (hôtels, lieux publics…) positionnent un certificat menteur pour déchiffrer vos données

Ne connectez pas de périphérique USB inconnu (trouvé par terre, prêté par un inconnu, …) ni sur vos ordinateurs ni sur vos smartphones, même un câble !

N'hésitez pas à nous contacter : https://support.univ-lyon1.fr