Cybersécurité au quotidien

Guide d’astuces par CALTHA TECH

1/ J’ouvre tous les e-mails même si je ne connais pas l’expéditeur

NON

Bien évidement, il est hors de question d’ouvrir n’importe quel e-mail, même si vous en êtes le destinataire.

ASTUCE :

Vérifiez toujours l’e-mail de l’expéditeur et surtout l’adresse du site après @.

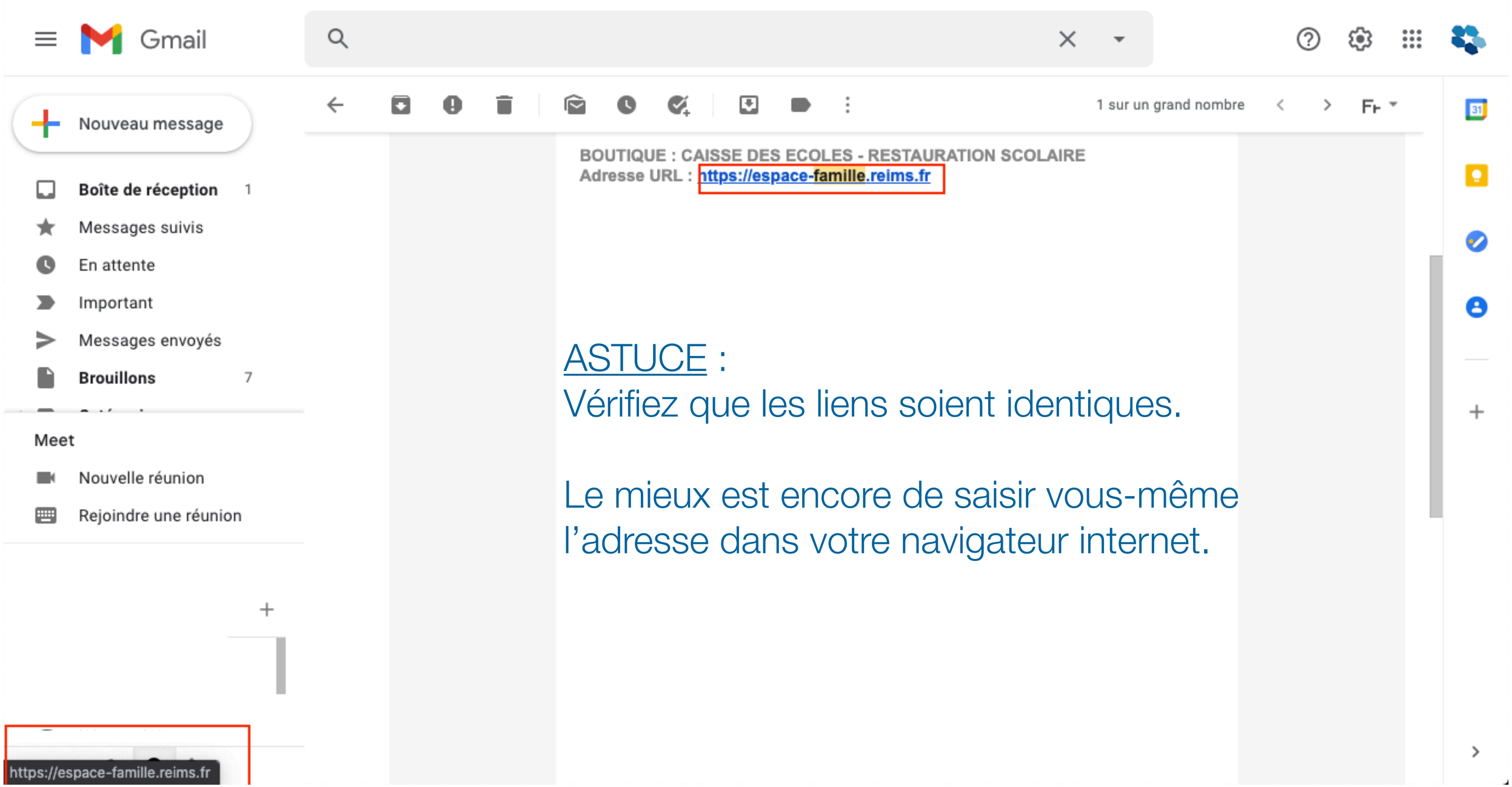
2/ Lorsque je reçois un e-mail qui a l’en-tête des impôts, je clique sur le lien qu’il contient en toute confiance

NON

> Même si l’e-mail contient toutes les références qui font penser aux impôts, il est important de vérifier le lien sur lequel vous allez cliquer.

ASTUCE :

Lorsqu’il y a un lien dans un e-mail, passer la souris dessus et regardez en bas de votre navigateur l’adresse qui est indiquée.



ASTUCE :
Vérifiez que les liens soient identiques.

Le mieux est encore de saisir vous-même l'adresse dans votre navigateur internet.

3/ Lorsque je suis sur un site qui semble être celui du gouvernement, je laisse mes coordonnées en toute confiance

NON

S’il s’agit bien d’un site du gouvernement, vous pouvez laisser vos coordonnées. Mais vérifiez bien que ça ne soit pas un site frauduleux.

ASTUCE :

Pour tous les sites type impôts et santé, vos données sont déjà enregistrées, donc il ne vous les demanderont jamais par e-mail.

4/ Généralement j’ouvre toutes les pièces jointes

NON

Si vous êtes certains de l’expéditeur, en **théorie** la pièce jointe est sûre. Sachez que certains systèmes permettent d’envoyer des e-mails en se faisant passer pour un expéditeur que vous connaissez.

ASTUCE :
Regardez les noms des pièces jointes. Si un nom vous semble bizarre, ne répondez pas au mail et n’ouvrez pas la pièce jointe. Contactez directement votre correspondant et posez lui la question (histoire vécue).

5/ Lorsque mon navigateur internet me demande de sauvegarder mon mot de passe ou une autre donnée, je l’enregistre

OUI

NON

Le problème n’est pas le stockage des données, mais l’accès. Si vous laissez votre poste ouvert, n’importe qui pourra utiliser vos données sur un site que vous fréquentez.

ASTUCE :

Si vous avez fait le choix d’enregistrer vos données dans votre navigateur, pensez toujours à fermer votre session lorsque vous quittez votre poste et à protéger l’accès à votre matériel par un mot de passe. Mais le mieux reste de ne rien enregistrer.

6/ Je peux mettre n’importe quoi comme information sur une clé USB

CA DEPEND DE LA CLE ET DES DONNEES

Vous pouvez stocker des données **non importantes** sur une **clé USB classique**. En revanche, des données sensibles voir confidentielles, NON.

ASTUCE :
Si vous devez stocker des données de votre entreprise sur une clé USB, ou des données sensibles, il existe des clés USB avec des systèmes de cryptage.

7/ Quand je suis à l’hotel, je peux utiliser le Wifi pour

Regarder NETFLIX, trier mes photos

Toute activité qui ne concerne pas votre entreprise et pour lesquelles vous n’avez pas besoin de saisir de données importantes (banque, identité) peuvent être faite sur un wifi « commun ».

ASTUCE :
Si vous devez travailler, utilisez le partage de connexion de votre smartphone directement en USB ou Wifi avec un mot de passe assez complexe.

8/ Si on me demande mes coordonnées bancaires pour vérification, je les donne

NON

> Ne communiquez jamais vos coordonnées bancaire par téléphone ou email, sauf réservation de service spécifique type hôtel par exemple.

ASTUCE :
Si vous recevez un e-mail d'un service qui vous demande de transmettre vos coordonnées bancaires soit par retour de mail, soit en contactant le numéro indiqué soit en cliquant sur lien, **ne le faite pas**. Cherchez le service en question sur internet et contactez-les directement pour savoir s'ils vous ont envoyé un e-mail.

9/ Un ransomware c’est

Une application qui bloque votre appareil et vous demande de payer une certaine somme pour être débloqué

L’ANSI dénombre 192 signalements en 2020 sur les entreprises françaises. Ces logiciels proviennent souvent d’une pièce jointe, un fichier d’une clé USB, ou un fichier installé via un site internet

ASTUCE :

Méfiez-vous des pièces jointes, n’installez pas de fichier téléchargé via des sites peu fréquentables (porno, streaming illégal, darkweb, …)

10/ Le phishing c’est

Une technique pour récupérer vos données personnelles

Vous recevez un e-mail d’un service que vous utilisez. Il vous invite à vous connecter en cliquant sur un lien et à saisir vos données.
Ne cliquez jamais sur le lien et ne complétez jamais de formulaire.

ASTUCE :
Rendez-vous toujours sur le site de votre service comme vous avez l’habitude de le faire. Si vous avez un doute, n’hésitez pas à les contacter et surtout à signaler le phishing.

10/ Exemple phishing Netflix

Voici un exemple avec Netflix

Des e-mails au nom de Netflix sont envoyés en masse.
Cet e-mail vous invite clairement à vous connecter en cliquant sur « réactivez simplement » pour saisir vos coordonnées bancaires. Mais vous êtes envoyés sur un site qui n’est pas Netflix

11/ Un malware c’est

Un logiciel malveillant

Le malware est un logiciel qui s'infiltre dans votre appareil à votre insu.
Vous le téléchargez ou l’installes sans le vouloir puis il infecte l’appareil.
Ils sont tous différents et ont des buts différents.

ASTUCE :
Faites attention aux fichiers que vous téléchargez surtout si vous l’avez téléchargé sur un site fréquentable (porno, streaming illégal, darkweb, …)

12/ Mon smartphone ne risque rien en matière de cybersécurité !

FAUX

> Les smartphones sont des ordinateurs en « miniature », ils sont donc tout aussi vulnérables que votre ordinateur.

ASTUCE :
Faites attention aux pièces jointes dans les applications de messagerie. Téléchargez toujours vos applications dans les store légaux.

13/ Je télécharge des applications via le Store de mon téléphone, je fais confiance

PRESQUE

En théorie on peut faire confiance, mais malheureusement le PlayStore d'Android est une cible et contient beaucoup d'applications malveillantes.

ASTUCE :
Controllez le développeur de l'application. Par exemple WhatsApp à pour développeur WhatsApp LLC et non Whatsapp

14/ Je sais à quoi sert la navigation privée

La navigation privée est un mode de navigation à utiliser dans votre navigateur internet. Il vous permet de ne pas enregistrer de cookies, pas d'historiques … lorsque vous consultez un site.

ASTUCE :

Utilisez toujours ce mode pour consulter votre compte bancaire ou si vous souhaitez faire un cadeau ;-)

15/ Je sais à quoi sert un VPN

Le VPN est un système permettant de créer un tunnel direct entre des ordinateurs distants. Personne d'autre ne peut y accéder. Représentez-vous le tunnel sous la Manche, l'eau autour ne rentre pas dans le tunnel.

ASTUCE :
En télétravail, il est important de l'utiliser pour vous connecter au réseau de votre entreprise.

Pour aller plus loin

N’ayez plus peur de l’informatique

- Travaillez en toute sécurité de chez vous ou au bureau
- Comprenez les virus, malwares, spywares, ransomwares
- Apprenez à détecter des e-mails frauduleux
- Détectez les fichiers frauduleux
- Allez encore plus loin

Sécurisez vos activités : contactez-nous

MERCI