ATELIER

« LA SECURITE SUR INTERNET »

La sécurité sur Internet

Au programme

- Panorama des cybermenaces les plus courantes
- Comment s'en protéger :
  - Avoir un antivirus
  - Effectuer les mises à jour
  - Privilégier les réseaux Wifi privés
  - Effectuer des sauvegardes
  - Savoir identifier un site fiable
  - Utiliser des mots de passe forts
  - Utiliser la double-authentification si c'est possible
- Focus sur les données personnelles
- Les cookies : définition et comment les supprimer
- Comment effacer les données de navigation sur son navigateur
- Focus sur le phishing (hameçonnage)

La sécurité sur Internet

Panorama des cybermenaces les plus courantes : moyens et objectifs du cybercriminel.

Virus ou logiciel malveillant	Sites non sécurisés	Réseaux wifi non sécurisés	Mails frauduleux ou jouant sur les émotions	Propositions trop belles pour être vraies
				
Détériore l'ordinateur ou capte des données personnelles.	Les exploitent pour obtenir des informations personnelles.	Obtient les informations laissées par les internautes.	Le mail renvoie à l'aide de liens vers des faux sites ou appelant à votre compassion pour vous extorquer de l'argent.	Tromper l'internaute (faux site qui recueille des données personnelles).

La sécurité sur Internet

Comment s'en protéger : avoir un antivirus.

Vous **protège contre les logiciels malveillants**. Équivalent à la ceinture de sécurité en voiture.

Aujourd'hui, la **plupart** des équipements sont vendus avec **un système de sécurité**. Par exemple, « Windows Defender » sur les équipements Windows.

Il existe également des **antivirus payants** qui proposent des outils de sécurités supplémentaires moyennant un abonnement mensuel ou annuel.

En revanche, faîtes attention aux antivirus gratuits qui peuvent être source de désagrément (publicités, notifications anxiogènes).

Dans tous les cas, un antivirus ne vous dispense pas de faire preuve de vigilance.

Comment s'en protéger : effectuer les mises à jour.

- **Permet de corriger les failles de sécurité de votre ordinateur.**

Accepter les mises à jour quand on vous les propose !

Celles-ci permettent souvent de **corriger les failles de sécurité éventuelles** que peut avoir votre ordinateur. Cela concerne également votre **smartphone et tablette**. Parfois, un **redémarrage** de votre appareil est nécessaire pour installer correctement ces mises à jour.

La sécurité sur Internet

Comment s'en protéger : privilégier vos réseaux Wifi privés que publics.

Votre **réseau Wifi personnel est protégé** par une **clé de sécurité**. Si elle est longue, ce n'est pas pour rien. **Ne la donnez pas à n'importe qui !**

Lorsque vous n'êtes pas chez vous, **évitez les Wifi publics** qui ne sont pas tous sécurisés. Utilisez en priorité **vos données mobile sur votre smartphone** pour aller sur Internet. Sur ordinateur, vous pouvez effectuer un partage de connexion depuis votre smartphone et vous connecter en Wifi depuis celui-ci sur votre ordinateur.

Attention à votre forfait de données mobile pour votre smartphone ! Selon votre offre avec votre opérateur, vous aurez plus ou moins de données mobiles que vous pouvez dépenser pour aller sur Internet. Vérifiez bien la quantité de données que vous permet votre contrat chez votre opérateur.

Comment s'en protéger : Effectuer des sauvegardes régulières de vos données.

Pour éviter que vos données disparaissent pendant un piratage ou une panne informatique, il est conseillé d'effectuer des **sauvegardes régulières de ses données, de préférence sur plusieurs supports.** Pour ce faire, vous pouvez utiliser des disques durs externes ou bien sauvegarder vos données dans le Cloud.

La sécurité sur Internet

Comment s'en protéger : identifier un site fiable.

Le **protocole https** sécurise la transmission des données.

Même si aujourd'hui la majorité des sites utilise par défaut le protocole sécurisé https, lorsque vous **saisissez des données sensibles** (mot de passe, numéro de Sécurité Sociale, numéro de carte bancaire…), **vérifiez bien** que vous êtes bien sur une **page utilisant ce protocole.**

http:// → http://exemple.com
Mot de passe : abcd123
→ **Sans** cryptage des données
Le hacker voit « abcd123 »

https:// → https://exemple.com
Mot de passe : abcd123
→ **Avec** cryptage des données
Le hacker voit « xJip0dFPmkKa6v0 »

Comment s'en protéger : identifier un site fiable.

L'adresse URL est un bon moyen de savoir si un site Web est **fiable ou pas**.

Des **« faux sites »** existent en se faisant passer pour **des sites connus** afin de capter les données personnelles des internautes.

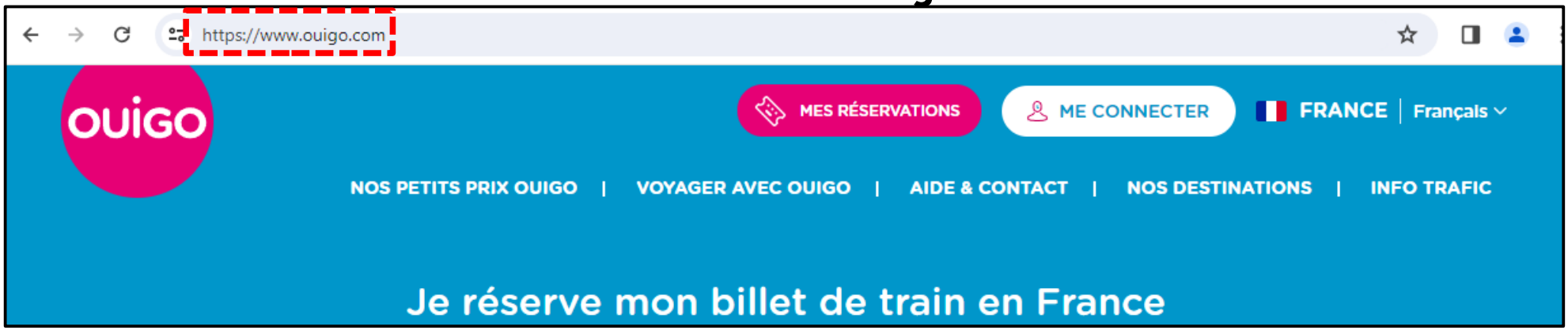
Chaque **URL est unique** ! Ainsi, le « faux site » s'inspirera grandement de celle du site qu'il veut copier mais sera obligé d'avoir une adresse URL avec quelques **caractères différents ou en plus**.

L'icône du cadenas qui apparaît à gauche de l'adresse URL est également un bon moyen de savoir si le site est sécurisé.

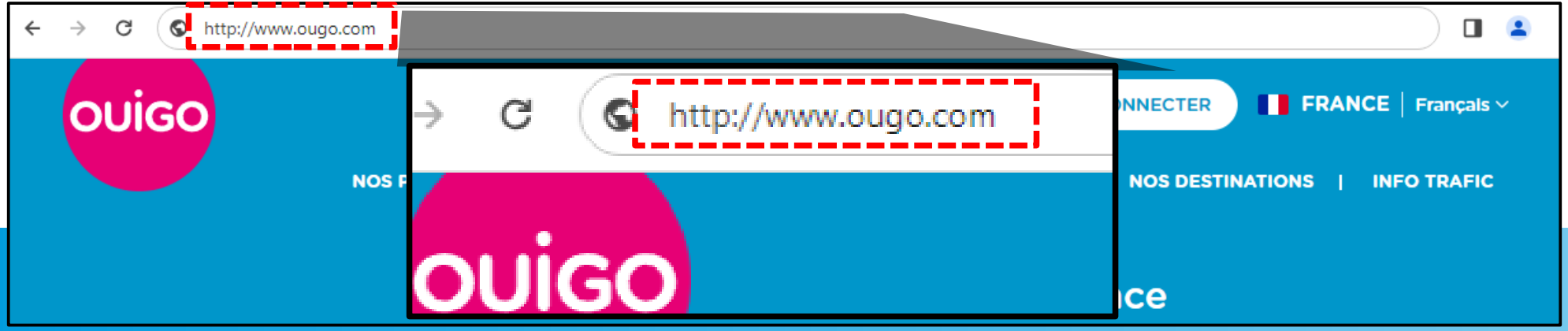
La sécurité sur Internet

Comment s'en protéger : identifier un site fiable (exemple)

Vrai site de Ouigo



Faux site s'inspirant du vrai mais avec l'adresse URL différente



Comment s'en protéger : Utiliser des mots de passe forts.

Il est important d'avoir des **mots de passe « forts »**, surtout lorsqu'ils protègent l'accès à des sites Internet **sensibles** : messageries, ameli, impôts, sites utilisant vos données bancaires ou personnelles, etc.

Votre mot de passe doit être **unique pour chaque site** (sécurité si fuite de données)

Dans l'idéal, il vaut mieux le changer tous les 6 mois environ.

Comment s'en protéger : Utiliser des mots de passe forts.

Plusieurs **méthodes** existent pour créer un mot de passe sécurisé mais votre mot de passe **doit contenir** :

- Majuscules
- Minuscules
- Chiffres
- Au moins 8 caractères (12 recommandé)
- Signes de ponctuation (. , ; : ! ? …)
- Symboles (€ $ % # @ …)

Surtout, il ne doit pas contenir de données à caractères personnelles (nom, date de naissance…)

Comment s'en protéger : Utiliser des mots de passe forts.

Voici quelques exemples de méthodes de création de mot de passe « forts » :

- La méthode des premières lettres :

« **J**e **c**rée **u**n **m**ot **d**e **p**asse **s**uper **s**écurisé **!** **P**lus **d**e **12** **c**aractères **e**t **6** **t**ypes **d**ifférents **!** »

Jcumdpss!Pd12ce6td!

Comment s'en protéger : Utiliser des mots de passe forts.

Voici quelques exemples de méthodes de création de mot de passe « forts » :

- La méthode phonétique :

« J'ai acheté huit CD pour cent euros cet après-midi »

Ght8CD%E7am

Comment s'en protéger : Utiliser des mots de passe forts.

- Il existe des logiciels appelés « **gestionnaire de mots de passe** » permettant de sauvegarder vos mots de passe de façon sécurisé à l'aide d'un **mot de passe « maître »** unique et hyper-sûr (ex : Keepass).

- Vous pouvez sinon noter vos mots de passe dans un **carnet**.

  - Dans ce cas, choisissez un **mot secret** à vos mots de passe mais ne le notez pas sur le carnet. Ce mot sera **ajouté au début** de tous vos mots de passe.
    Pour vous en souvenir toujours, il faut qu'il soit très simple et facile à retenir.
    Veillez néanmoins qu'il ne doit **rien rappeler de votre famille ou de ce qui vous passionne**.

Comment s'en protéger : Utiliser la double authentification.

Certains sites vous proposent d'activer la **« double-authentification »***.

Activez-la et lors de chaque **connexion** à ce site, on vous demandera un **code unique temporaire** que vous recevrez par **SMS** ou par votre **boîte de messagerie électronique.**

* également appelée « authentification forte », « vérification à deux étapes », « vérification en deux temps »… selon les services.

La sécurité sur Internet

Focus sur les données personnelles.

Chaque fois que vous **cherchez une information** sur internet ou que vous **visitez** un site, vous laissez des **informations sur vous**. On les appelle des **« données personnelles »** : elles permettent de **vous identifier**.

Où ?	Réseaux sociaux	Moteur de recherche	Site Web	Formulaire en ligne	Application mobile
Comment ?	Quand vous publiez une photo, commentez un message, regardez une vidéo.	Quand vous tapez des mots clés.	Quand vous visitez des pages, lisez un article.	Pour créer un compte ou faire un achat, quand vous écrivez votre nom, prénom.	Quand vous l'autorisez à vous « géolocaliser » (c'est à dire, savoir où vous êtes).

Focus sur les données personnelles.

- **Informations précieuses** car permettent à des **entreprises** (réseaux sociaux, moteurs de recherche, sites, applications…) de **savoir qui vous êtes et ce qui vous intéresse** pour vous faire acheter.
- Certaines entreprises, comme Google et Facebook (Meta), à qui vous avez donné des centaines d'informations sur vous, vous **montrent des publicités qui correspondent à vos goûts** sur les sites que vous visitez et sur Facebook. **D'autres entreprises les paient** pour montrer leurs publicités aux personnes intéressées. On appelle ça des **publicités « ciblées »**.
- D'autres entreprises s'en servent **pour vous montrer et vous faire acheter** des objets qui **ressemblent à ce que vous aimez** chaque fois que vous retournez sur leurs sites.

Focus sur les données personnelles.

- Les services publics en ligne, comme France Travail et la Caf, enregistrent aussi des informations sur vous mais ils ne les utilisent pas pour gagner de l'argent. Ces informations sont nécessaires pour que l'administration traite votre dossier.

Focus sur les données personnelles (exercice).

À votre avis, quelles entreprises enregistrent les informations qu'Alex laisse sur Internet ?

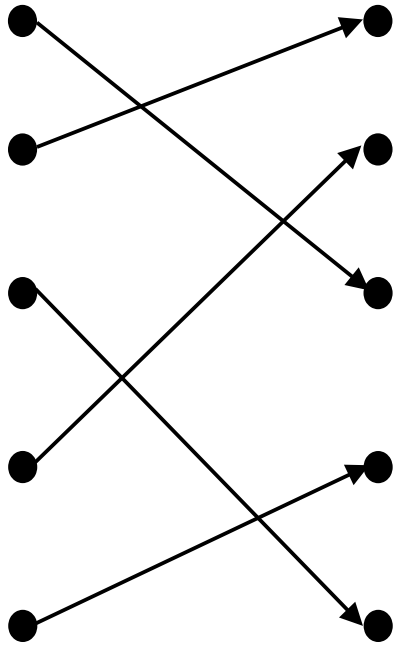
Alex écrit son adresse sur son profil

Alex écrit sur son moteur de recherche : crèche Paris.

Alex écrit son numéro de téléphone dans un formulaire pour créer une boîte mail.

Alex clique sur J'aime sous une photo de chat.

Alex cherche des chaussures noires pour homme taille 43.



Le moteur de recherche Google enregistre qu'il est intéressé par une crèche à Paris

Facebook enregistre qu'il aime les chat.

Whatsapp enregistre son adresse.

Le Bon Coin enregistre qu'il aime les chaussures noires pour homme taille 43.

Outlook enregistre son numéro de téléphone.

Refuser les cookies.

- **Fichier** que les sites internet que vous visitez **enregistrent** sur votre ordinateur.
- Contient des **informations sur vous** pour vous permettre de naviguer plus facilement sur ces sites.
- **Certains** cookies sont **nécessaires** pour que le site fonctionne bien.
- Mais d'autres **enregistrent tout ce que vous faîtes** pour vous montrer des **publicités ciblées.** Mieux vaux les refuser surtout si vous naviguer sur un **ordinateur public** !

La sécurité sur Internet

Refuser les cookies.

Les sites ont l'obligation de vous demander votre accord et à vous dire à quoi servent ces cookies.

Vous **refusez** les cookies à chaque fois que vous visitez un site Web en cliquant, selon les sites, sur « **refuser** » ou « **paramétrer les cookies** » ou « **continuer sans accepter** ».

Ouvrir une fenêtre de navigation privée.

En utilisant une **fenêtre de navigation privée** pour aller sur Internet, les **cookies** enregistrés sur votre ordinateur seront **automatiquement effacés** à la fermeture de votre navigateur.

Attention : Naviguer dans une fenêtre de navigation privée ne vous rend pas anonyme pour autant !

La sécurité sur Internet

Effacer les données de navigation.

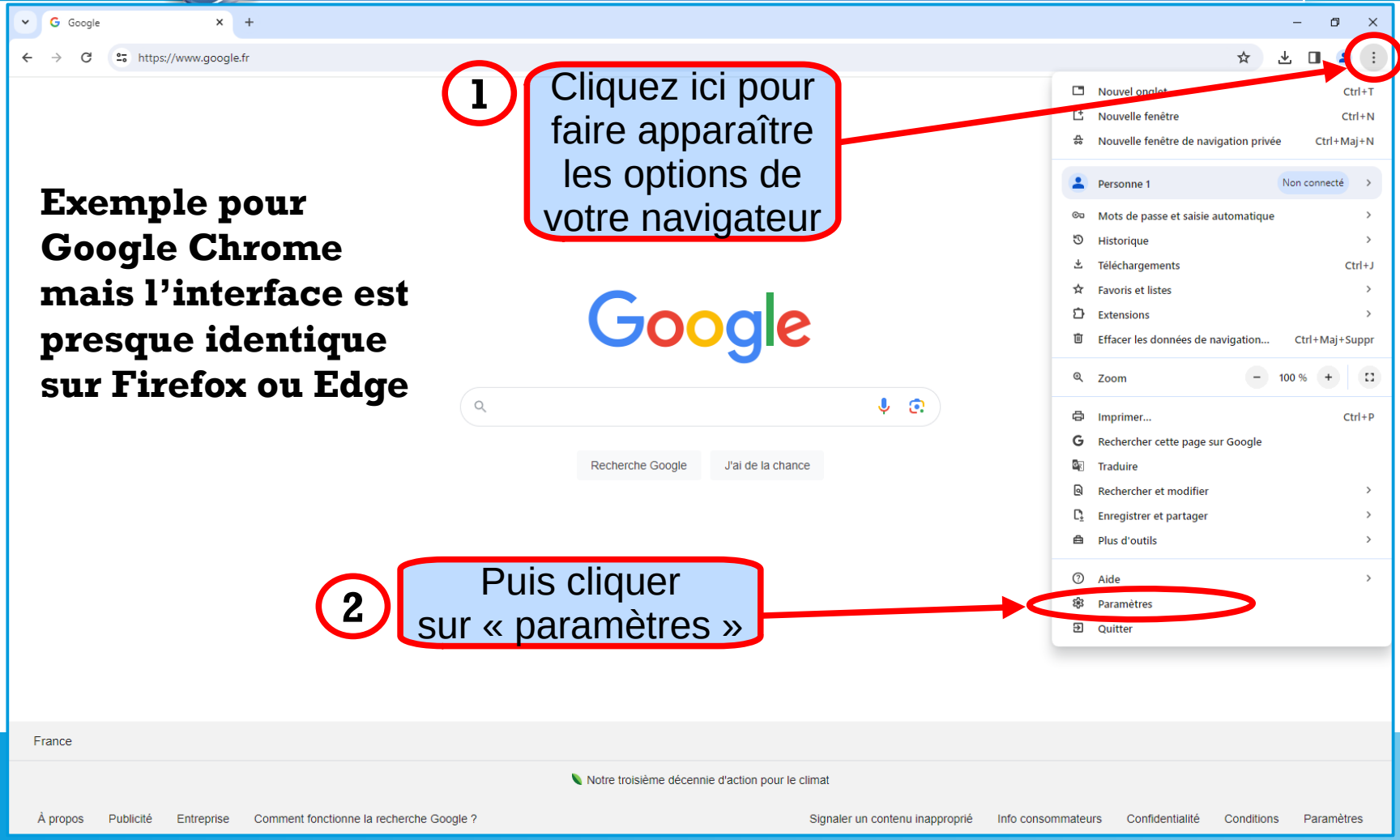
Les données de navigation sont **propres à chaque navigateur** !
Ainsi, vous devrez **effectuer les démarches suivantes pour chaque navigateur** que vous utilisez (si vous en utilisez plusieurs).

Attention : supprimer les données de navigation vous **déconnectera** de la plupart des sites auxquels vous êtes connecté ! Pensez à **noter vos identifiants et mots de passe** pour chaque site avant.

Pour **effacer les données de navigations** de votre navigateur (historique, cookies, vider le cache…), vous devez :

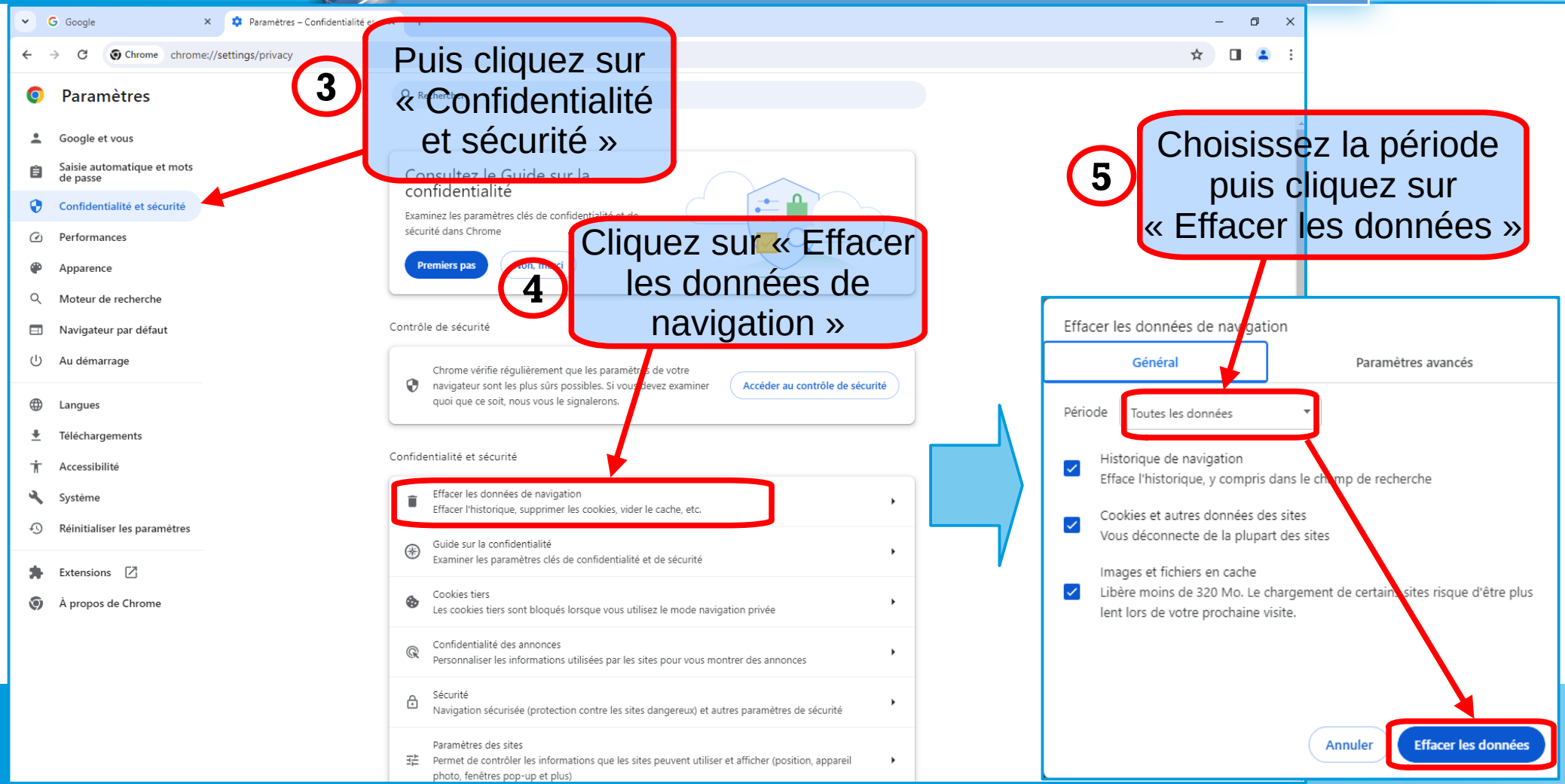
La sécurité sur Internet

Exemple pour Google Chrome mais l'interface est presque identique sur Firefox ou Edge



Bassens - Damien Courty - 2024

La sécurité sur Internet



Focus sur le « phishing » (hameçonnage).

Vous avez peut-être déjà reçu dans votre boîte de courrier électronique un mail assez étrange soit disant venant du ministère de l'Intérieur vous sommant de régler une amende en ligne via un lien cliquable.

Ceci est un **mail frauduleux**. Le but est de **récupérer les données bancaires** d'une personne qui clique sur le lien renvoyant vers un faux site.
Le cybercriminel joue alors sur les émotions de la personne qui croit être en situation d'urgence.

Étudier chaque mail soupçonneux avant de répondre, de télécharger une pièce jointe ou de cliquer sur un lien.

Respecter la règle du **R.L.V. : Recul, Lecture, Vigilance**

Focus sur le « phishing » (hameçonnage).

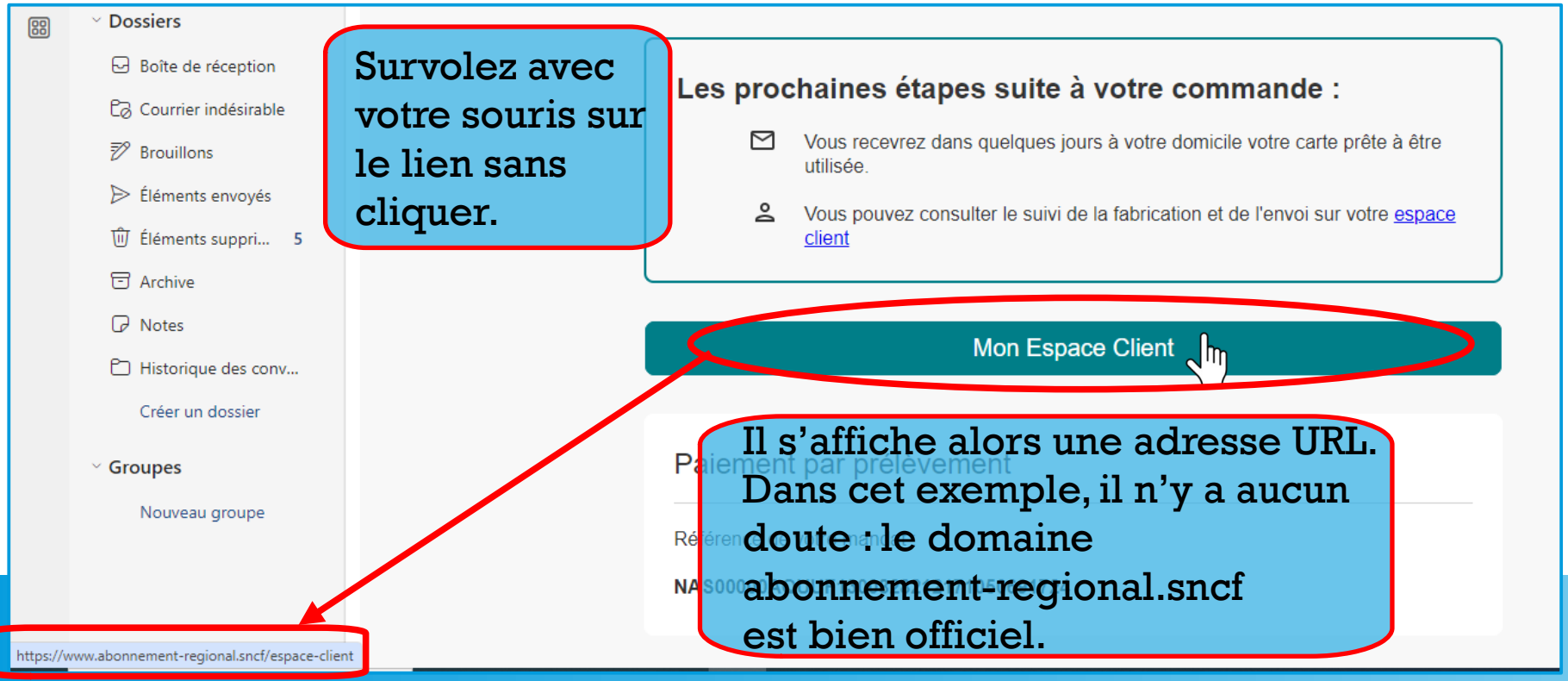
Si vous recevez un mail d'un organisme public ou privé sur lequel vous avez **déjà créé un compte, ne cliquez pas sur les liens proposés.**
Connectez vous directement sur votre compte pour vérifier l'information.
Gardez à l'esprit qu'un organisme quel qu'il soit ne vous **demandera jamais** votre mot de passe ou vos coordonnées bancaires. Même votre conseiller bancaire ne connaît pas votre code d'accès à votre compte.

Pour vérifier l'**émetteur** du message, **vérifiez son adresse mail.**

La sécurité sur Internet

Focus sur le « phishing » : vérification mail.

Pour vérifier si le lien cliquable renvoie effectivement vers le vrai site auquel le mail fait référence :



Focus sur le « phishing » : vérification mail.

L'objet du mail frauduleux évoque souvent un **sujet peu ordinaire** :

Quelques exemples :

- Un prétendu pirate aurait trouvé des vulnérabilités sur un site Internet et demande une rançon pour ne pas utiliser vos données personnelles.
- Un ami aurait grand besoin d'aide, mais refuse d'être appelé par téléphone.
- Un organisme important (votre banque, EDF, etc.) aurait perdu votre identifiant et votre mot de passe à la suite d'un incident technique.
- Une entreprise vous annonce qu'elle vous accorde un trop perçu pour une facture.
- Des félicitations pour avoir gagné un lot important lors d'un tirage au sort dont vous n'avez jamais entendu parler.

Si vous avez un doute sur un mail, contactez si possible directement l'organisme concerné pour confirmer ou non le message que vous avez reçu.

Focus sur le « phishing » : cas particulier du « Smishing ».

Depuis quelques années se répand de plus de plus une forme dérivée de **hameçonnage ciblée sur les SMS**.

Vous recevez dans votre messagerie SMS un message d'un expéditeur souvent inconnu visant généralement **à vous tromper et à vous soutirer de l'argent** par le biais d'une **communication payante** (appel vers un numéro spécial payant ou envoi d'un SMS vers un numéro court à 5 chiffres surtaxé) ou d'un **lien URL** redirigeant vers un **site captant les données** que vous enregistrez.

N'y répondez surtout pas, ne cliquez pas sur les liens !

Vous pouvez signaler ce SMS sur la **plateforme de lutte contre les SMS et appels indésirables** au 33700 en remplissant un formulaire ou en envoyant une capture d'écran.