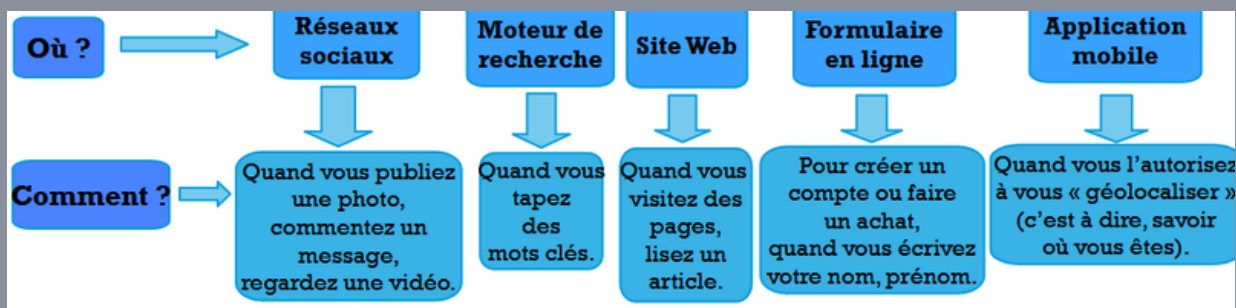


FICHE RÉSUMÉE

LA SÉCURITÉ DES DONNÉES

I 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.



- ▶ 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 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.

Qu'est-ce qu'un cookies

Le cookie est un petit fichier texte que les sites web ont l'autorisation de déposer sur votre ordinateur via votre navigateur. Historiquement, il a été créé dans les années 1990

L'idée était de laisser un fichier sur l'ordinateur de l'internaute qui était renvoyé et lu par le site marchand à la reconnexion afin que celui-ci se souvienne du visiteur. Il peut par exemple servir à ce qu'un site se souvienne de vous et vous propose de nouveau les derniers articles lus par exemple.

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 ».

Continuer sans accepter Fermer et accepter

RUE DU COMMERCE FAITES UN CHOIX POUR VOS DONNÉES

Sur notre site, nous recueillons à chacune de vos visites des données vous concernant. Ces données nous permettent de vous proposer les offres et services les plus pertinents pour vous, de vous adresser, en direct ou via des partenaires, des communications et publicités personnalisées et de mesurer leur efficacité. Elles nous permettent également d'adapter le contenu de nos sites à vos préférences, de vous faciliter le partage de contenu sur les réseaux sociaux et de réaliser des statistiques.

Vous pouvez paramétrer vos choix pour accepter les cookies ou vous y opposer si vous le souhaitez.

Nous conservons votre choix pendant **6 mois**. Vous pouvez changer d'avis à tout moment en cliquant sur le lien **contrôler mes cookies** en bas de chaque page de notre site.

Pour en savoir plus, consultez notre [politique de cookies](#).

Réglages Tout accepter

Recherche sur Internet

En faisant une recherche simple de votre nom sur google, vous pouvez ainsi voir les données vous concernant sur Internet.

II Comment les données sont récupérées par les escrocs

Ils utilisent pour la plupart le navigateur Tor qui permet à un Internaute de naviguer sur le Web de manière anonyme, Les pirates détournent ce système pour accéder à Internet de manière incognito. En réalité, en utilisant Tor ils accèdent au DarkNet (sites Web qui ne sont pas accessibles par votre navigateur classique.)

Le hacking est la pratique qui permet aux pirates de voler et échanger nos données personnelles de manière illégale en utilisant tous les moyens possibles pour subtiliser mots de passe, identité bancaire etc...

III Différentes menaces :

1. Le virus

C'est un programme informatique causant des problèmes dans l'ordinateur. Souvent cachés dans des pièces jointes frauduleuses ou dans des logiciels.

2. Le phishing

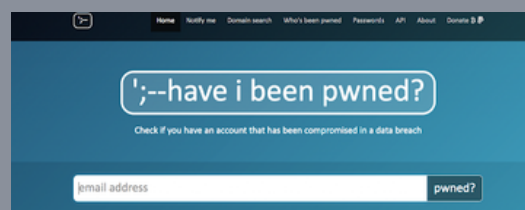
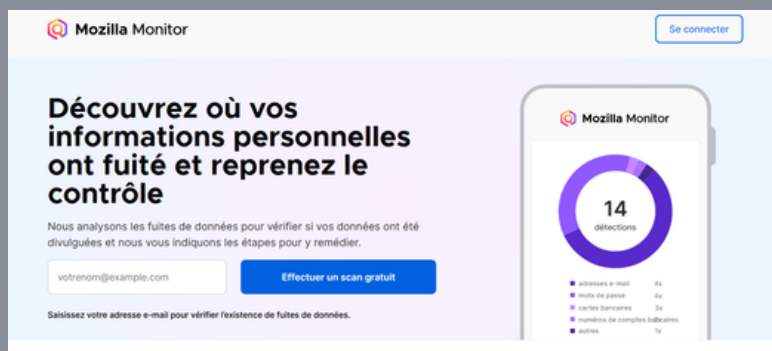
Un mail de votre banque vous invitant à vous connecter sur leur site pour récupérer vos données de cartes bancaires par exemple. Il s'agit en réalité d'un faux site construit à l'identique pour créer l'illusion.

3. Le pharming

Les hackers vont profiter des failles de certains sites pour récupérer les données personnelles des utilisateurs. Pas de panique, cela arrive rarement !

IV Comment s'en prémunir :

Exemples d'outils permettant de faire face à ces attaques
C'est là que le site « Have i been pwned » (« Est-ce que je me suis fait avoir ? ») ou l'outil Firefox monitor sont utiles. Ils rendent publics l'ensemble des sites qui ont été hackés et dont les données ont fuité.



Création d'un mot de passe fort

La définition d'un bon mot de passe



Un mot de passe sécurisé est :

- Long : au moins 8 caractères
- Composé de chiffres, lettres, caractères spéc
- Difficile à deviner : sans lien avec votre vie pe

Comment créer un mot de passe

Voici une autre astuce pour retenir mon mot de passe :

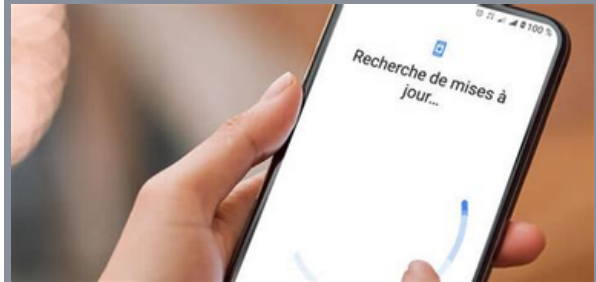
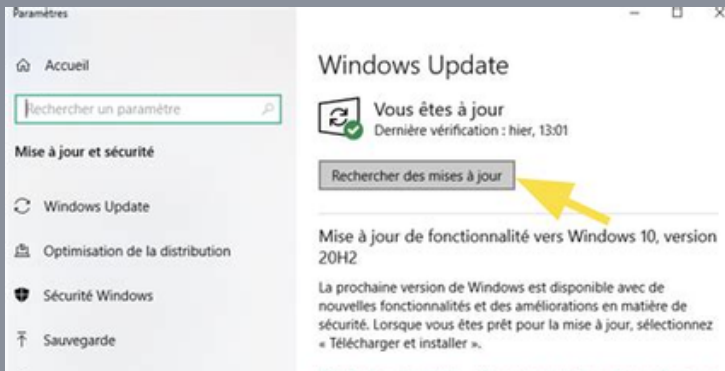
J'écris une phrase facile à me souvenir et je fais mon mot de passe avec la première lettre de chaque mot

Par exemple : **M**aman **h**abite **a**u **43** rue **P**asteur !

Mon mot de passe sera donc : Mha43rP!



Être bien protéger en ayant les équipements à jour




V Paramétrer son navigateur

CHANGER SON MOTEUR DE RECHERCHE

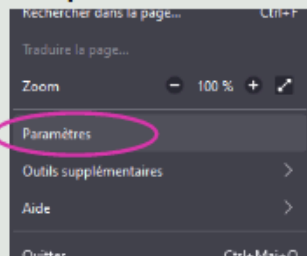
I. Ouvrir son navigateur



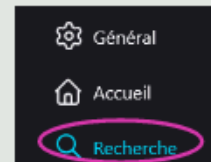
II. Cliquer sur 

En haut à droite de votre navigateur

III. Cliquer sur paramètres



IV. Cliquer sur l'onglet recherche



V. Sur cette même page, cliquer sur la flèche du moteur de recherche

Moteur de recherche par défaut

Ceci est votre moteur de recherche par défaut pouvez le changer à tout moment.



UTILISER LE MODE NAVIGATION PRIVÉE

I. Ouvrir son navigateur

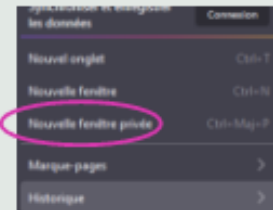


II. Cliquer sur



En haut à droite de votre navigateur

III. Cliquer sur nouvelle fenêtre privée



La navigation privée est une fonction de la plupart des navigateurs Web permettant de naviguer sur le Web sans que les données de navigation comme l'historique ou les cookies soient conservées.

Supprimer l'historique du navigateur sous Firefox

SUPPRIMER L'HISTORIQUE DE VOTRE NAVIGATEUR

I. Ouvrir son navigateur

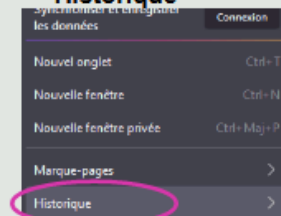


II. Cliquer sur

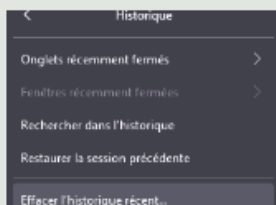


En haut à droite de votre navigateur

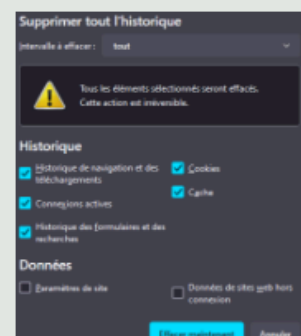
III. Cliquer sur Historique



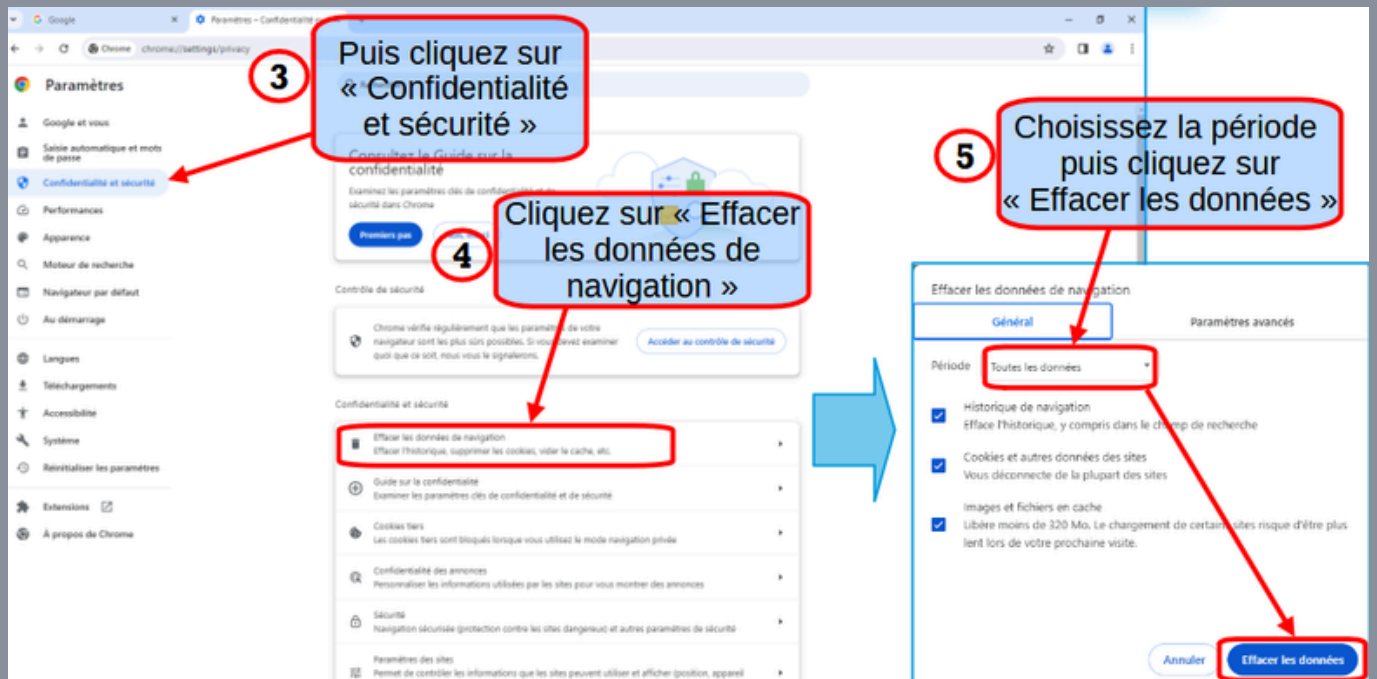
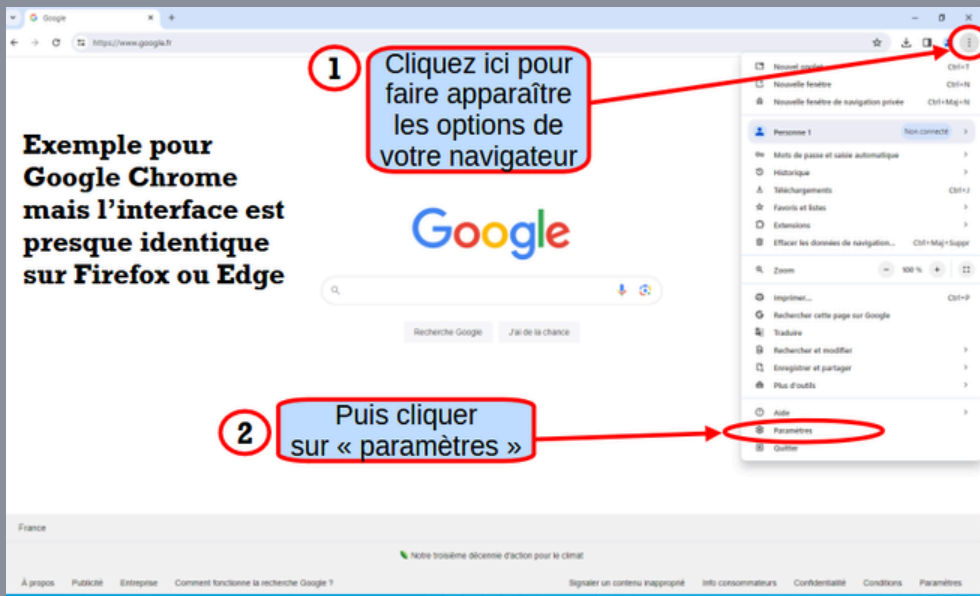
IV. Cliquer sur effacer l'historique récent



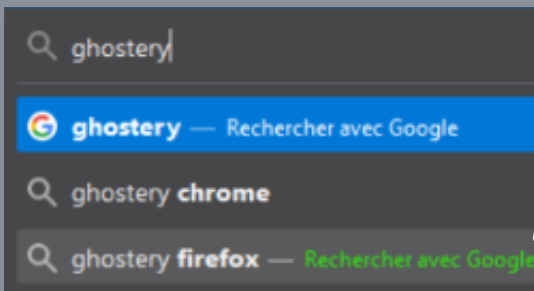
V. Choisir l'intervalle à effacer et son contenu



Sous google chrome

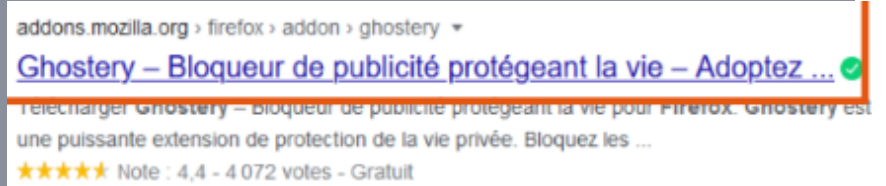


Installer des bloqueurs de publicités (exemple ici avec Ghostery)



1) Ouvrez votre navigateur et tapez nom_de_l'extension nom_du_navigateur

2) Vérifiez bien les adresses avant de cliquer elles doivent contenir "addons.mozilla.org"

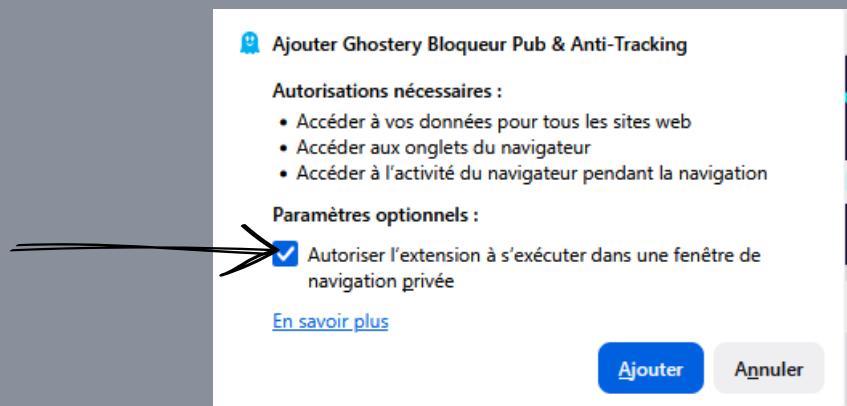


3) Une fois sur la page du web store cliquez sur "Ajouter"

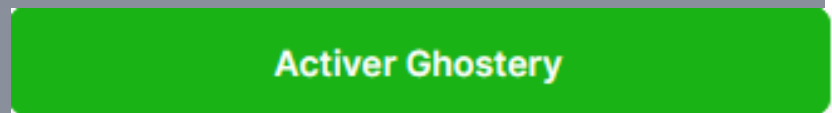


4) Une fenêtre va vous demander de confirmer votre choix

Case à cocher pour autoriser l'extension en navigation privée



5) Une nouvelle fenêtre vous demandera d'activer ghostery



Sur le smartphone

Il est possible d'installer des bloqueurs sur un smartphone en utilisant Firefox, navigateur à télécharger depuis l'Appstore et le Playstore.