Parcours : DISCOVERY
Module : NAVIGUER EN TOUTE SECURITE
Projet 1 - **UN PEU PLUS DE SECURITE, ON N'EN A JAMAIS ASSEZ !**

1. Introduction à la sécurité sur internet
2. Créer des mots de passes forts
3. Fonctionnalité de sécurité de votre navigateur
4. Eviter le spam et le phishing
5. Comment éviter les logiciels malveillants ?
6. Achat en ligne sécurisées
7. Comprendre le suivi du navigateur
8. Principes de base de la confidentialité des médias sociaux
9. Que faire si votre ordinateur est infecté par un virus ?

1. INTRODUCTION A LA SECURITE SUR INTERNET

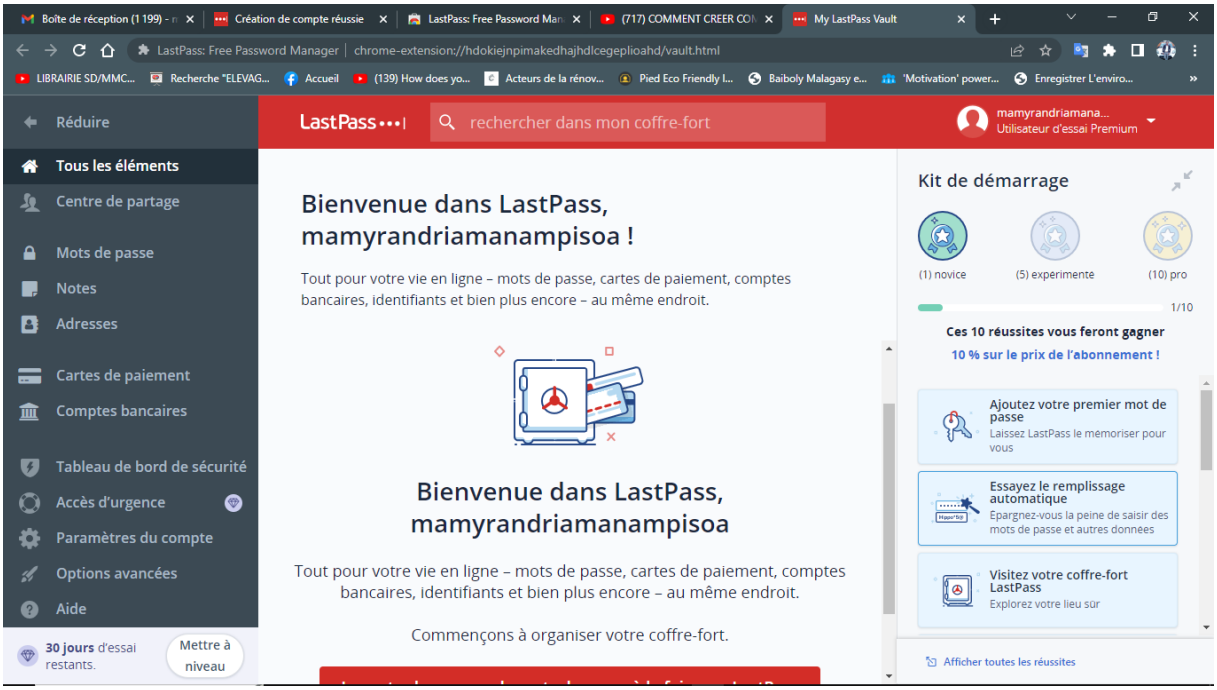
Dans le domaine du numérique, plusieurs entre les utilisateurs ne savent pas sur la question de la sécurité pendant leurs navigations en ligne. Dans ce document, on va découvrir ce thème pour être au courant et pouvoir protéger les données personnelles des utilisateurs.

D'après les trois sites internet proposée qui parlent la sécurité sur internet :

A- **Cybermalveillance** : comment se protéger sur l'internet, comment assurer votre connexion internet
B- **Cybersécurité** : Ces objectifs s'appliquent dans différents domaines ou champs d'applications, chacun faisant appel à des techniques différentes pour atteindre le ou les mêmes objectifs
C- **Kaspersky** : décrit la sécurité des activités et des transactions exécutées sur Internet et les 5 conseil sur la sécurité internet

2. Créer des mots de passes forts

Dans cette section, on commence à devenir en sécurité par la création des mots passes forts. Cette séance nous guide de créer un compte LastPass et mettre là-dedans tous nôtres mots de passes des différents comptes. Ce compte est attaché à tous les comptes, donc il suffit de mémoriser seule son mot de passe. Mais son mot de passe est véridiquement fort car il nous enseigne qu'un mot de passe fort comporte des différents caractères et des chiffres



Pas seulement qu'avec LastPass qu'on peut gérer notre mot de passe mais il y a plusieurs gestionnaires, voici les meilleurs gestionnaires des mots de passes, le comparatif 2023 : (par ordre décroissante du plus utilisées)
-Nordpass
-Dashlane
- 1Password
-LastPass

3. Fonctionnalité de sécurité de vitre navigateur

Identification des sites malveillants :

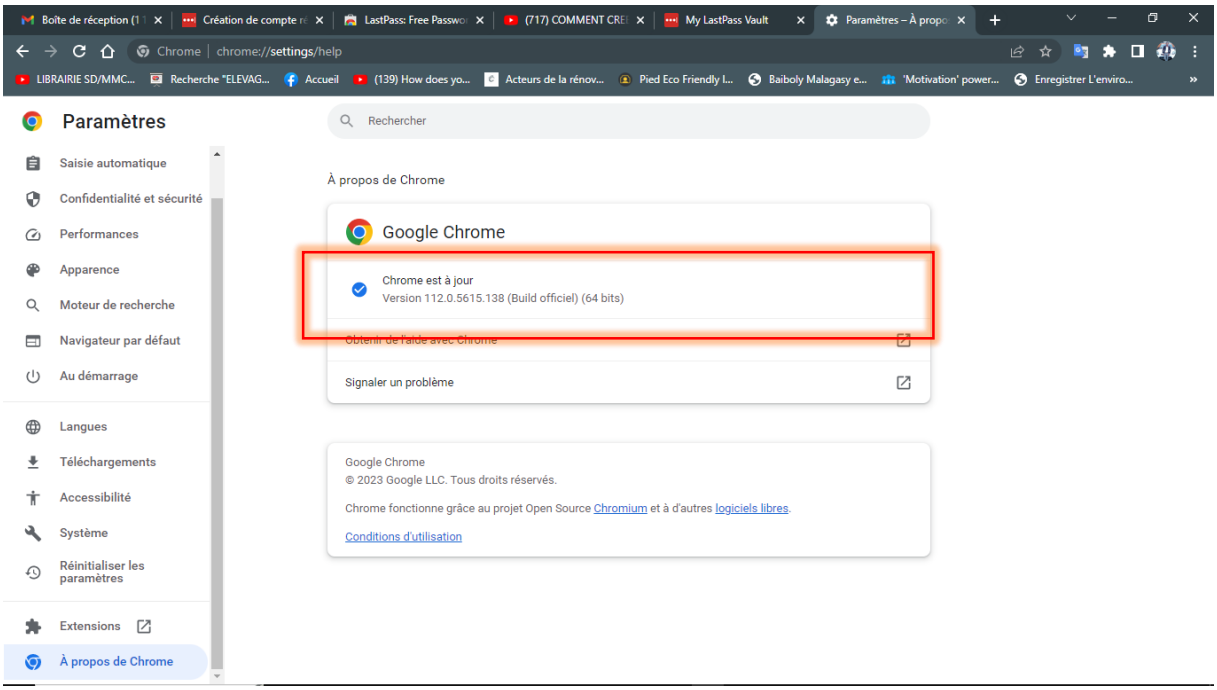
Il y a des sites qui sont malveillantes et être la dérivée des différents sites originales comme les exemples suivants :

-www.morvel.com : dérivée de www.marve.com, un site officiel de l'univers Marvel.
-www.fessebook.com : dérivée de www.facebook.com, le plus grand réseau social du monde.
-www.intagam.com : dérivée de www.instagram.com, un autre site très utilisé.

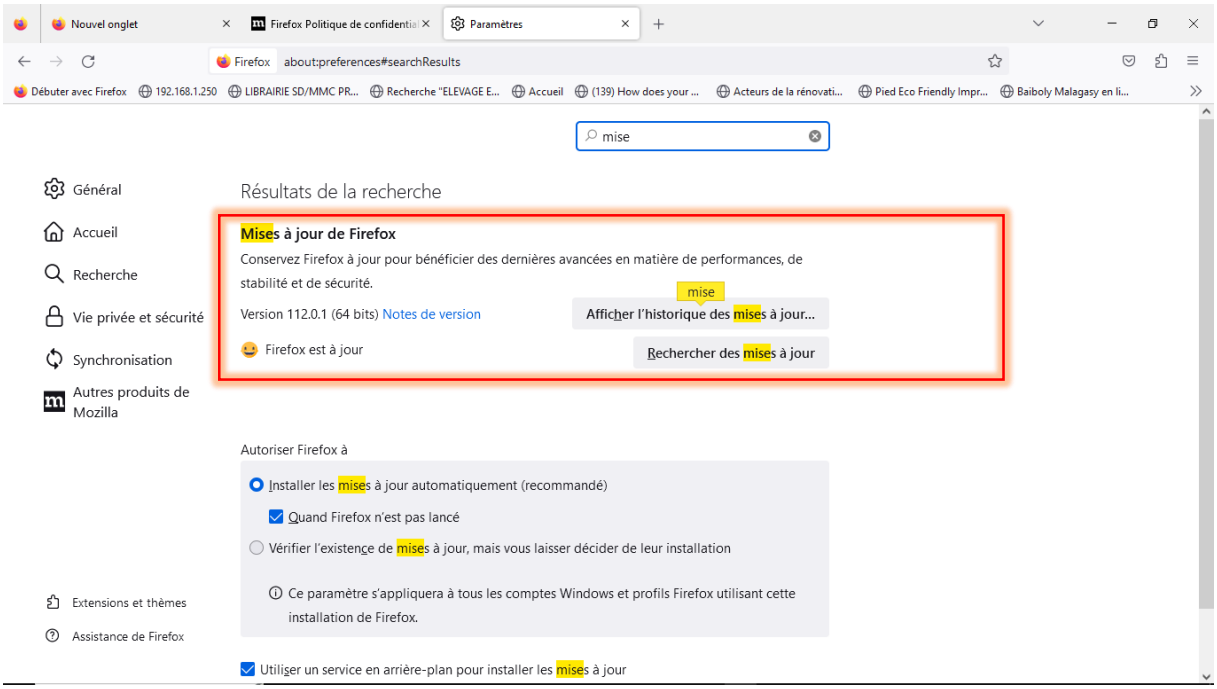
On fait aussi les vérifications si les navigateur « Chrome » et « Firefox » est à jour :

En regardant dans le paramètre de chaque navigateur, on peut voir si ce navigateur est à jour ou non .

Pour le chrome

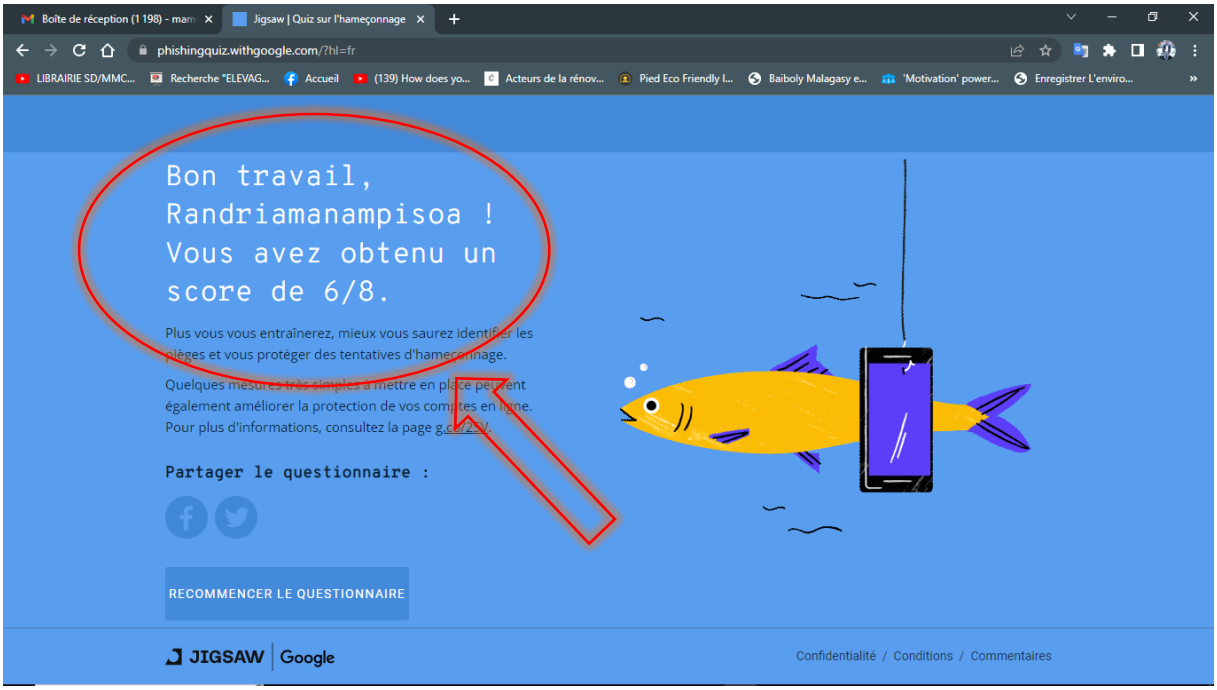


Pour le Firefox



4. Eviter le spam et le phishing

Dans cette section, on à faire un quizz qui nous teste si nous connaissons des sites légaux ou pas : il y a huit questions et voilà la note que j'ai obtenue :



Vous pouvez le faire comme vous voulez. Mais en plus on a visité aussi le site « Cybermalveillance.gouv.fr qui explique à propos des spam et phishing en détails.

5. Comment éviter les logiciels malveillants ?

Pour connaitre les sites malveillants, il est indispensable de comprendre les significations des différents indicateurs de sécurités. Comme ceux-ci :

1e site :

Indicateur de sécurité :

HTTPS

Analyse Google :

Aucun contenu suspect

2e site :

Indicateur de sécurité :

Not sécure

Analyse Google :

Aucun contenu suspect

3e site :

Indicateur de sécurité :

Not sécure

Analyse Google :

Vérifier un URL en particulier [analyse trop générale]

6. Achat en ligne sécurisées

Pour être au courant de tous ceux que vous avez acheté en ligne, on peut créer un libelle sur le compte Google. Cette libellée peut gérer toutes les factures qu'on a pendant tous les achats en ligne. Et on peut faire des vérifications pour eux.

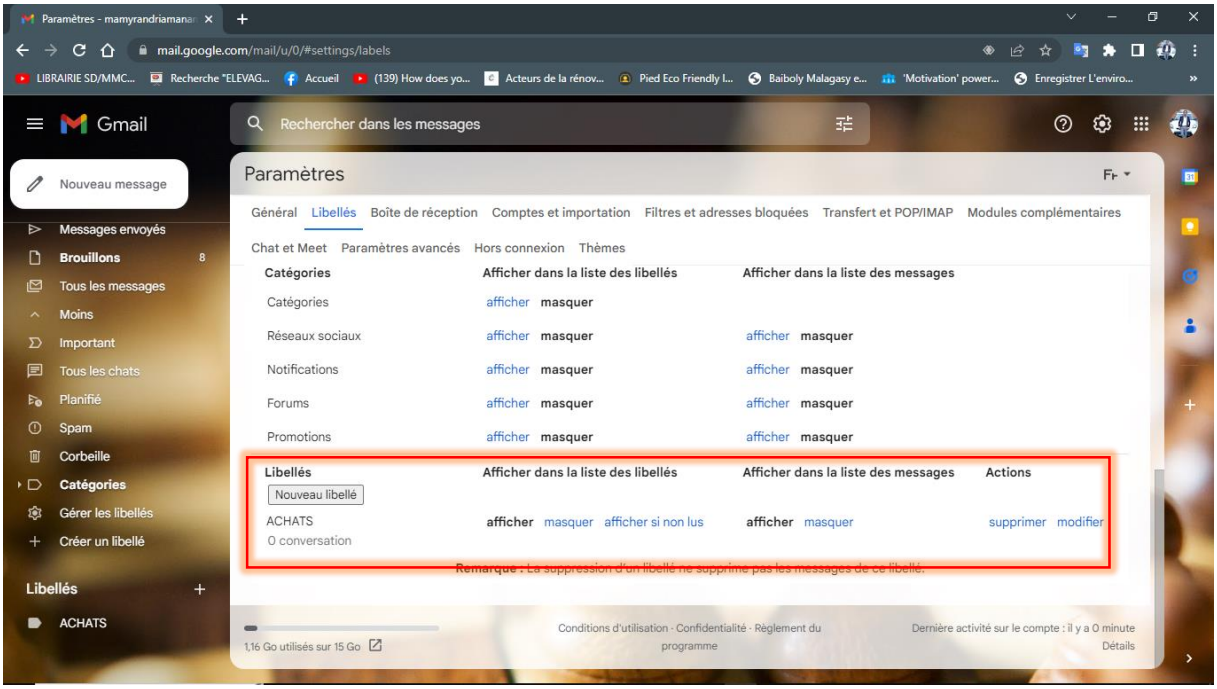
Pas seulement les factures mais aussi les différentes tâches qu'on peut stocker comme :

-Administratif : tous les documents administratifs

-Banque : tous les documents et les conversations liées à la banque personnelle

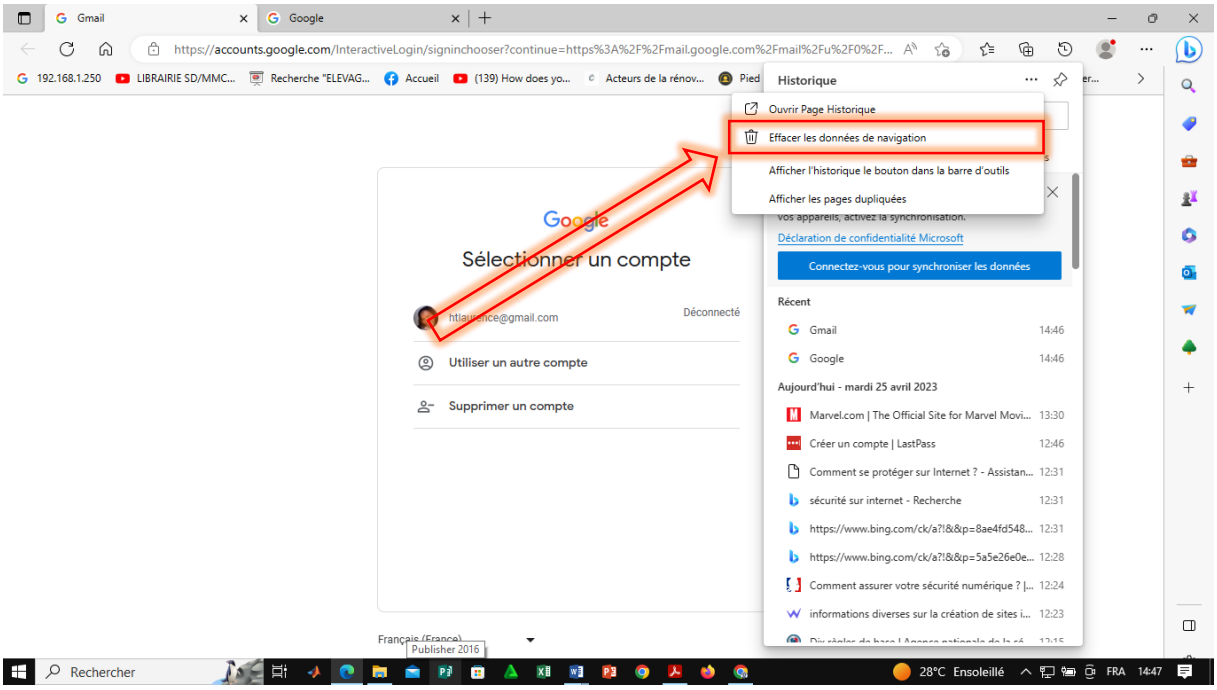
-Création du compte : tout le message lié à la création d'un compte.

Par exemples on peut le créer sur le compte mail et voilà ce pu s'est passée



7. Comprendre le suivi du navigateur

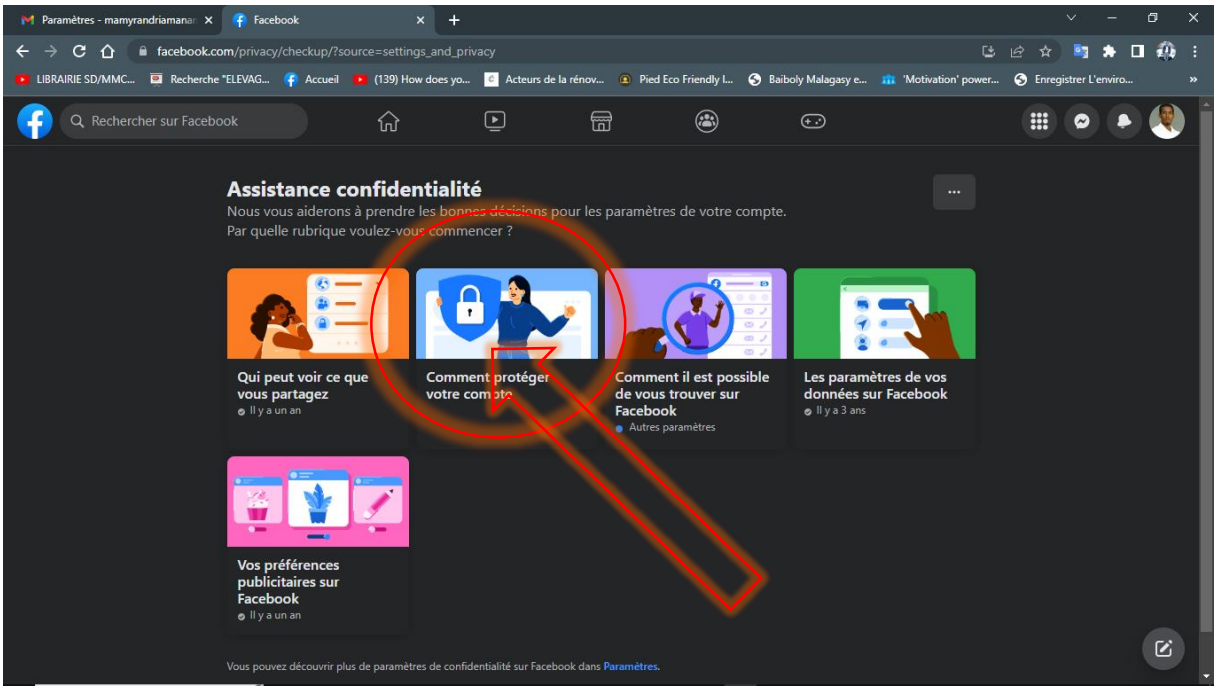
Dans cette section, on étudie sur le paramètre spécifique. Par exemple : contrôler les pages web qui peuvent enregistrer vos cookies, ou accéder à votre emplacement. Pour le faire, on va dans le paramètre de contenu.



En outre, on peut supprimer aussi l'historique de navigation pour ne pas avoir des traces dans les sites qu'on a visités. Pour faire cette suppression, on va dans le menu du navigateur ; ensuite aller à l'historique ; après sélectionner les cases à supprimer et cliquer sur Supprimer les éléments sélectionnés et enfin confirmer sur supprimer.

8. Principes de base de la confidentialité des médias sociaux

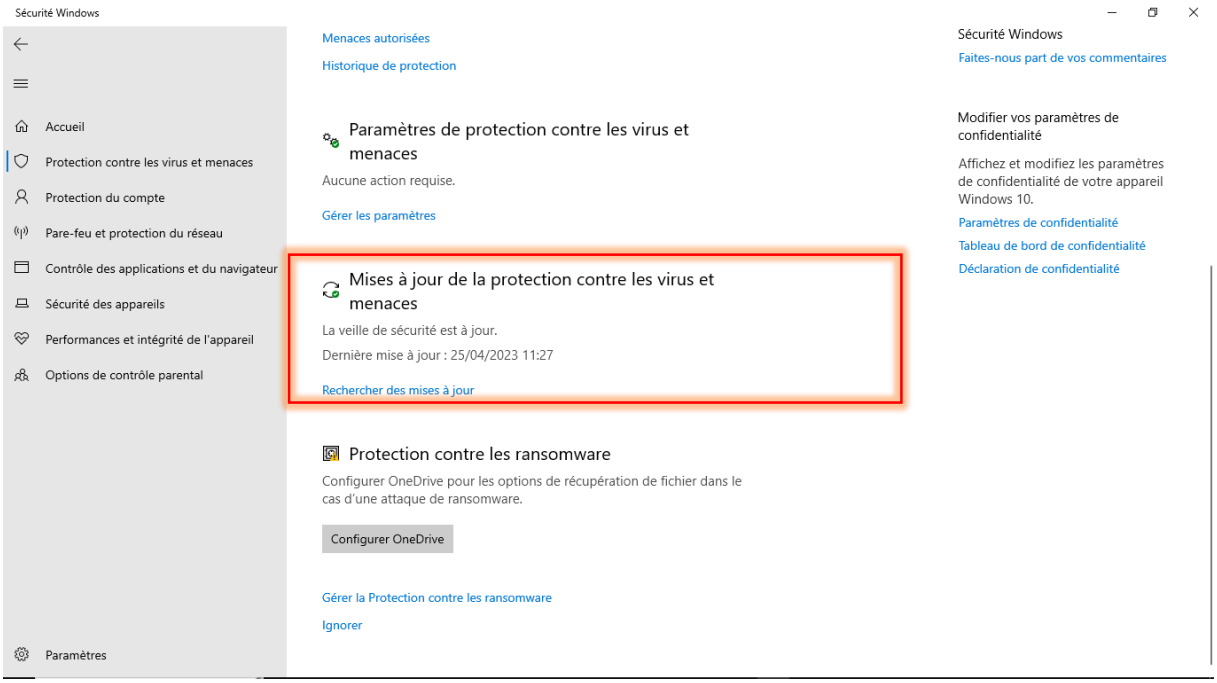
C’est une section intéressante. Toute au long de cette partie, on va régler les paramètres de confidentialités de Facebook.



On peut régler la visibilité de tes informations personnelles ; comme aussi la visibilité de ton profil pour la gestion des invitations. Pas seulement eux mais aussi gestion de la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela et enfin la gestion des informations récoltées par Facebook utiles pour annonceurs

9. Que faire si votre ordinateur est infecté par un virus ?

La meilleure action pour lutter contre les virus est de protéger votre ordinateur en installant les logiciels anti-virus ou mettre à jour le Windows defender, cette anti-virus est un accessoire de système pour le Windows.



Mais dans cet instant c'est le cas que votre ordinateur est attaqué par le virus. Comment en faire ?

Pour vérifier la sécurité en fonction de l'appareil utilisée, aller dans votre paramètre et regarder si votre état est bon ou pas.

Si vous n'avez pas des logiciels anti-virus, c'est l'heure de l'installation maintenant. Aller le télécharger sur internet et suivre les étapes pour l'installer dès votre poste.