

SAYNA-SECURITE-PROJET1

1- Introduction à la sécurité sur Internet:

Objectif: à la découverte de la sécurité sur internet

En navigant sur le web, voici 3 articles qui parlent de sécurité sur internet.

-Article 1: [ANSSI-Dix règles de base](#)

-Article 2: [Economie.gouve-comment assurer votre sécurité numérique](#)

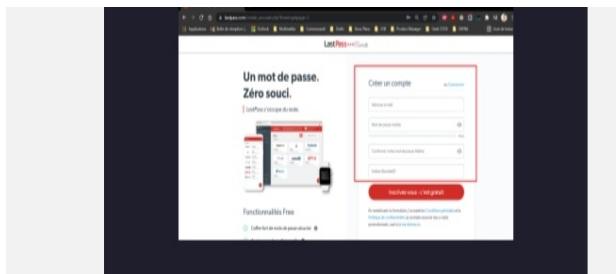
-Article 3: [SiteW-Naviguez en toute sécurité sur Internet](#)

2- Crédit d'un mot de passe fort:

Objectif: utilise un gestionnaire de mot de passe LastPass

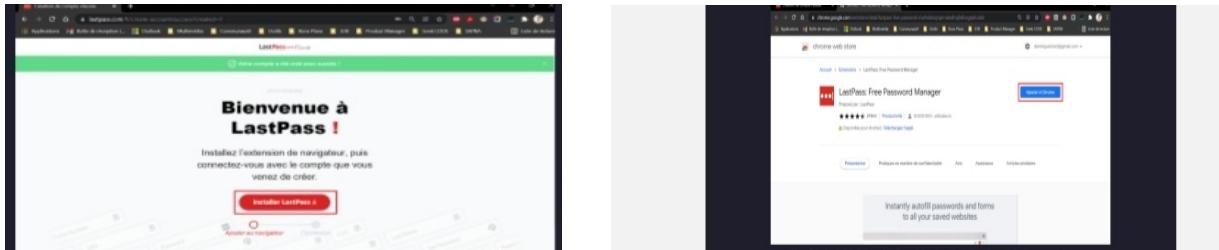
Nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. C'est une gestionnaire sous forme d'une application web qui est accessible sur tous supports (PC, Mac, Mobile) . Il est simple à prendre en main et propose un niveau de sécurité optimal. En suivant ces étapes suivantes:

-Accède au site de LastPass

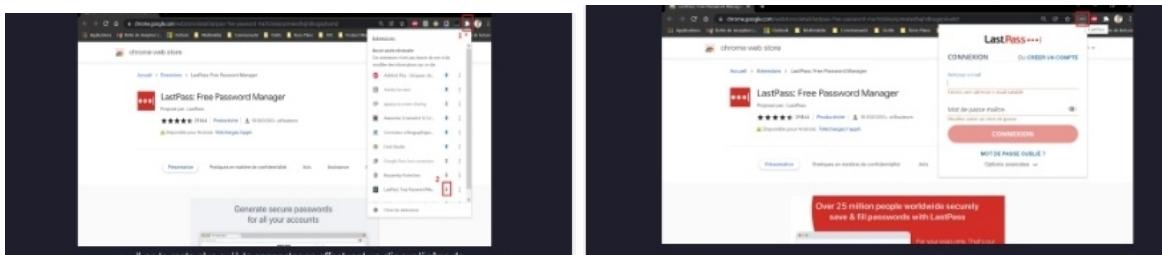


-Crée un compte en remplissant le formulaire et on doit choisir un mot de passe maître c'est-à-dire un mot de passe unique qui nous permet d'accéder à tous nos comptes.

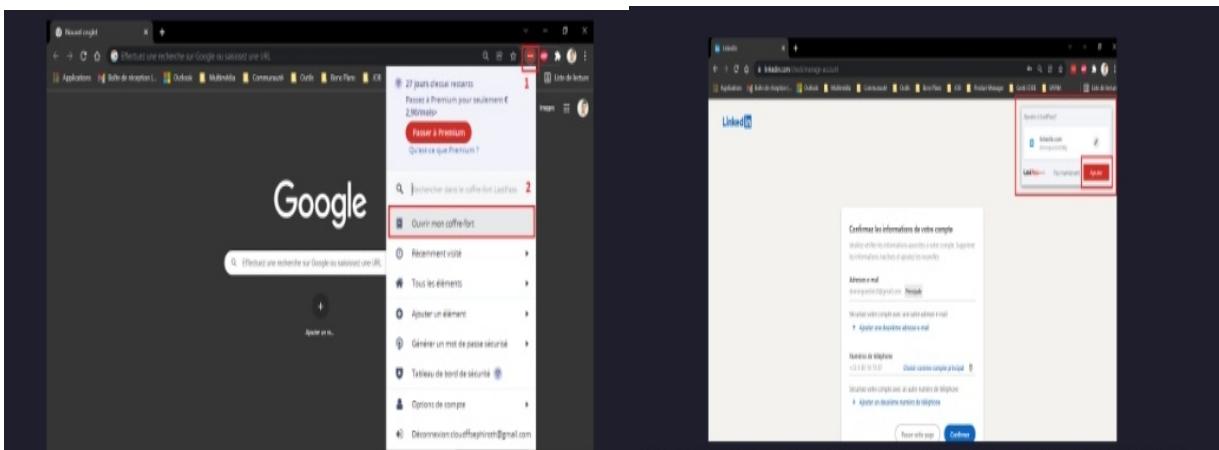
-Une fois la création du compte effectuée, on arrive sur une page de validation qui propose le téléchargement de l'extension sur le bouton prévu à cet effet.



- Il faut cliqué sur le logo extension et epingle l'extension de LastPass l'icone.



Desormais, lorqu'on connecte à nos comptes , on peut enregistrer le mot de passe grâce à LastPass.Et on peut aussi ajouter des comptes manuellement en accédent au coffre-fort, espace de stockage de tous les mots de passe. Pour y accéder, cliqué sur l'icone de l'extension puis sur "ouvrir mon coffre-fort".On arrive alors sur une page de gestion de compte LastPass.



Maintenant on peut dire qu'on connaît les grande lignes de l'utilisation du gestionnaire de

mot de passe LastPass.

3- Fonctionnalité de sécurité de votre navigateur:

Objectif: identifie les élément à observer pour naviguer sur le web en tout sécurité.

1/ Identification des adresses internets qui semblent provenir de site web:

-www.morvel.com: qui vient de www.marvel.com (site web)

-www.fassebook.com: qui vient de www.facebook.com (réseau social)

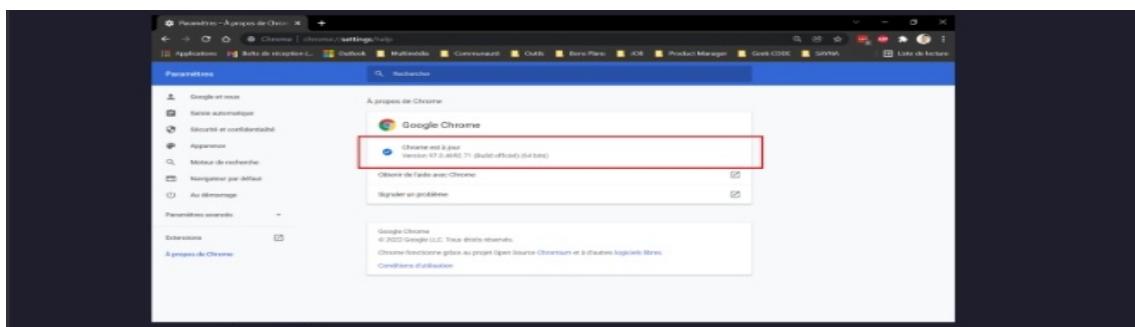
-www.instagam.com: qui vient de www.instagram.com (réseau social)

2/ Nous allons vérifier si les navigateurs utilisés : chrome et firefox sont à jour. Donc, pour le faire, on doit suivre ces étapes suivant.

Pour chrome: -ouvre le menu du navigateur et accède aux "Paramètres".

-clic sur la rubrique " A propose de chrome ".

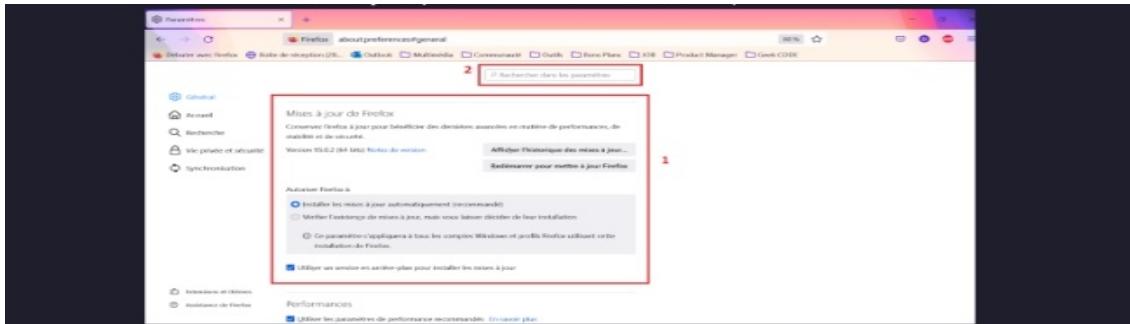
-si on constate le message "chrome est à jour" c'est-à-dire ok.



Pour Firefox: -ouvre le menu du navigateur et accède aux "Paramètre".

-dans la rubrique "Général", fais défiler jusqu'à voir la section "Mise à jour de Firefox".

-vérifie que les paramètre sélectionnés sont identiques que sur la photo.



On a pu le constater que les paramètres par défaut de ces deux navigateur sont réglés pour réaliser les mises à jour automatiquement. Et comme d'habitude, firefox affiche une personnalisation des paramètres un peu plus poussée.

4- Eviter le spam et le phishing

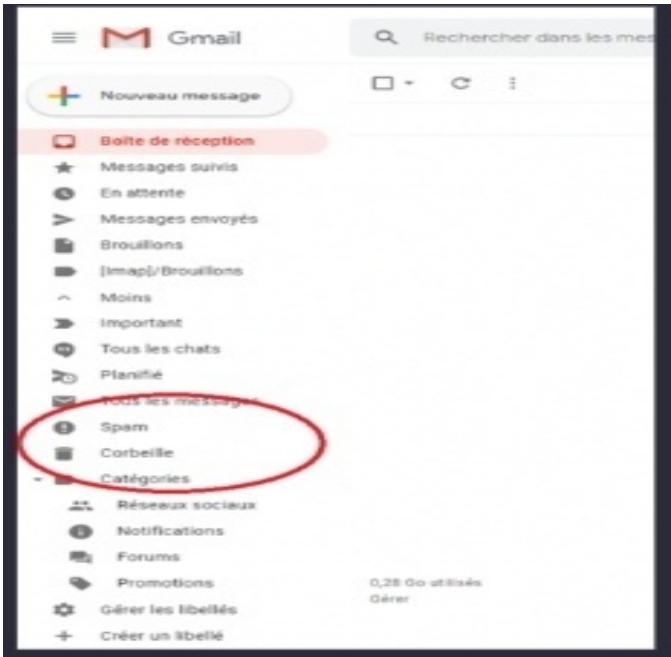
Objectif: reconnaître plus facilement les messages frauduleux.

Le spam et phishing ce sont des courrier indésirable.

-Le message de spam peut encombrer notre boite de réception et le rendre plus difficile la recherche des e-mails. Le pire est le spam comprend souvent des escroqueries par phishing et des logiciels malveillants qui peuvent présenter des risques pour l'ordinateur ou l'appareil utilisé. Mais aujourd'hui, la plupart des services de messageries incluent plusieurs fonctionnalités pour nous aider à protéger notre boîte de réception du spam.

Pour éviter le spam, chaque fois que nous receve un e-mail, les fournisseurs de messagerie vérifient s'il s'agit d'un vrai message ou d'un spam. Tous les messages de spam probablement seront placés dans le dossier spam pour que nous ne les ouvre pas par accident. Il y a également le système de blocage des spams qui ne sont pas parfait car il peut arriver que des vrais e-mails se trouvent dans votre dossier spam.

Donc, pour ne pas manquer aucun e-mail important, il faut le vérifier.



Pour marquer les e-mails comme spam : sélectionnez le message et cliquez sur le bouton “marquer comme spam”.

- Le phishing est un sorte d'escroqueries par messages qui tentent de nous inciter des informations sensibles. Le plus souvent provient d'une adresse qui se fait passer pour des stucture qu'on a l'habitude de rencontrer qui incite à saisir un mot de passe, de vérifier une date de naissance,etc. Cepedant, ce que nous devons savoir que les établissements officiels et sécurisés ne demandent jamais nos informatios sensibles par mail. Alors pour l'éviter il suffit juste de ne pas répondre à ce mail.

5- Comment éviter les logiciels malveillants:

Objectif: sécuriser votre ordinateur et identifier les suspects.

Lors de la navigation sur web, il arrive d'avoir des doutes sur la sécurité de certaines sites. Comme on a pu le voir précédemment le premier de niveau de vigilance à voir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet. Lorsque le doute persiste on peut s'appuyer sur un outil proposé par Google:[Google Transparency](#)

Report (en anglais) ou Google transparence des information (en français) . Pour chaque site on devra préciser l'indicateur de sécurité et de rapport d'analyse de l'outil Google. Il se suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google.

Site n°1: - Indicateur de sécurité : HTTPS

- Analyse Google: Aucun contenu suspect

Site n°2: - Indicateur de sécurité: Not secure

- Analyse Google: Aucun contenu suspect

Site n°3: - Indicateur de sécurité: Not secure

- Analyse Google: Vérifier un URL en particulier

6- Achats en ligne sécurisés

Objectif: créer un registre des achats effectués sur internet.

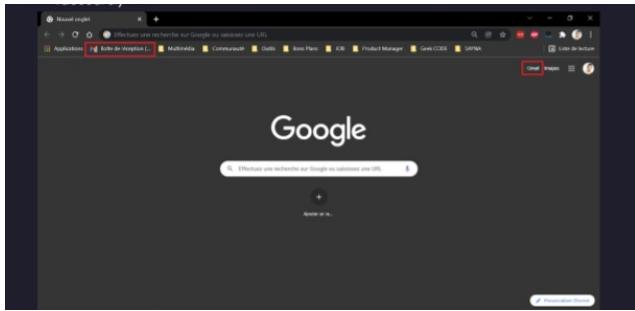
Les achats en ligne sont un moyen d'acheter presque n'importe quoi tout en restant à la maison. Même s'ils comportent certains risques, il existe également des façons de protéger nos informations bancaires.

On va créer un registre des achats en ligne qui a pour but de conserver les informations relatives aux achats en lignes. Il y a 2 possibilités qui s'offrent à nous pour organiser ce registre :- créer un dossier sur la messagerie électronique

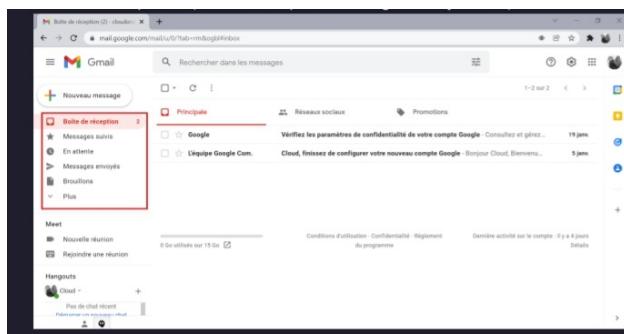
- créer un sur l'espace de stockage personnel (en local ou sur le cloud)

Donc, pour commencer, accède à la messagerie électronique, on peut y accéder en ouvrant un nouvel onglet.

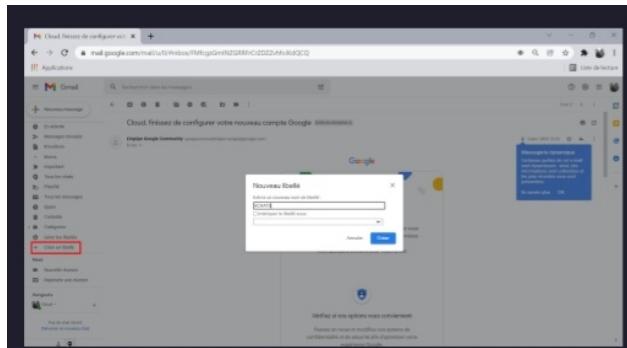




On trouvera sur la gauche des libellés initialement prévus dans la page d'accueil de la messagerie.



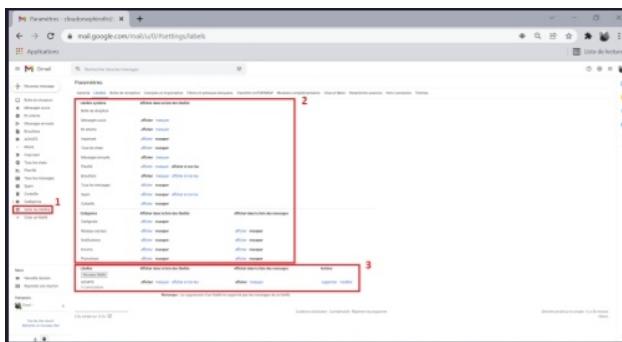
Pour créer la rubrique des achats, il faut cliqué sur "Plus" et allé en bas des libellés.



Faire un clic sur le bouton "créer" pour valider l'opération. On peut aussi gérer les libellés en effectuant un clic sur gérer les libellés, gérer l'affichage des libellés initiaux et gérer les libellés personnels.



Modifier avec WPS Office



Maintenant on a un libellé pour stocker tous ses messages électronique rélatif aux achats effectués sur internet qui confirme de l'achat.

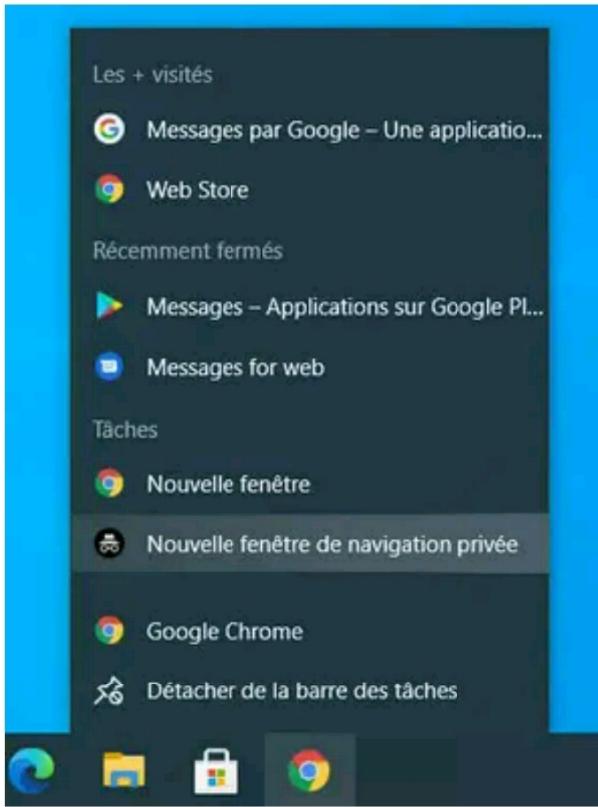
7- Comprendre le suivi du navigateur:

Objectif: exercice sur la gestion des coockies et l'utilisation de la navigation privée.

Les cookies peuvent stocker des informations spécifique sur les sites qu'on visite et les différents éléments sur lesquels on clique. C'est-à-dire que si on a pas un compte sur un site particulier, ces informations sont généralement enregistrées dans les cookies sur notre navigateur.

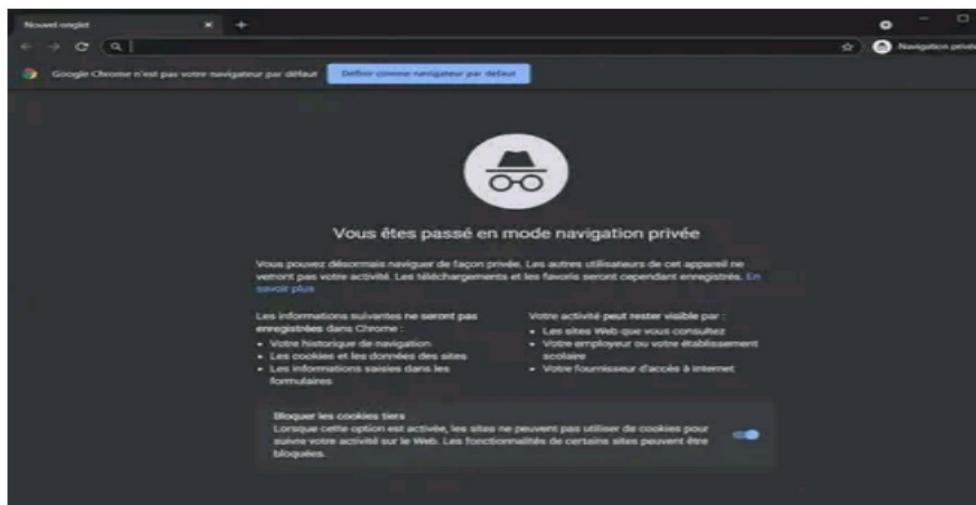
En général, les cookies ne présentent pas des risque pour notre sécurité en ligne car il y a un moyen pour le désactiver complètement si on le souhaite en activant le paramètre "Ne pas suivre" dans le navigateur. Si on veut l'éviter complètement, utilise juste le mode de navigation privée à chaque fois qu'on se connecte. Cela empêchera l'enregistrement des cookies dans notre navigateur.

Le mode de navigation privée ne protège pas contre tous les types de suivi du navigateur, mais limite la collecte de certaines données. Pour le faire, il suffit d'ouvrir un fenêtre de navigation privée.



Placez le curseur à la fin de la ligne, puis appuyez sur la barre d'espace du clavier.
Cliquer ensuite sur le bouton “Appliquer”, puis sur OK pour le valider.

Désormais, lorsque vous faites une double clique sur le raccourci de votre navigateur, il ouvrira automatiquement une fenêtre de navigation privée.



Modifier avec WPS Office

8- Principe de base de la confidentialité des médias sociaux:

Objectif: régler les paramètres de confidentialité de facebook

Les médias sociaux comme facebook ont rendu plus facile le partage du contenu en ligne. En général, les choses que nous partageons sur les réseaux sociaux sont publics, c'est-à-dire que beaucoup du monde peut voir les choses qu'on partage sur les réseaux sociaux.

Malgré cela, les médias sociaux offrent des outils de confidentialités et des options de paramétrage pour nous aider à régler la portée de nos publications.

Pour le faire: il suffit juste de défiler la page facebook jusqu'en bas et appuyez sur paramètres et confidentialité. Puis, clic sur "Audience et visibilité" et appuyez sur l'option dont vous souhaitez modifier la confidentialité.



9- Que faire si votre ordinateur est infecté par un virus:

Objectif: sécuriser un ordinateur contre les virus malveillants.

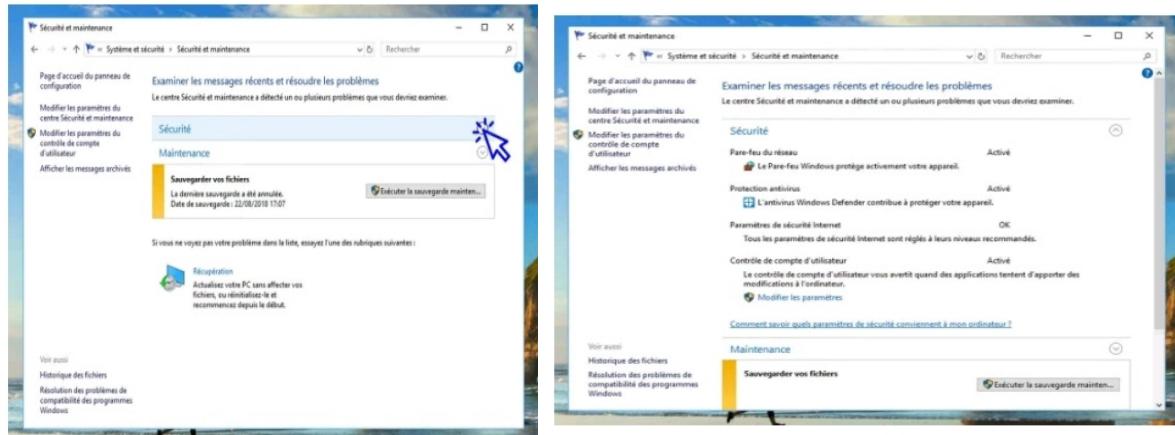
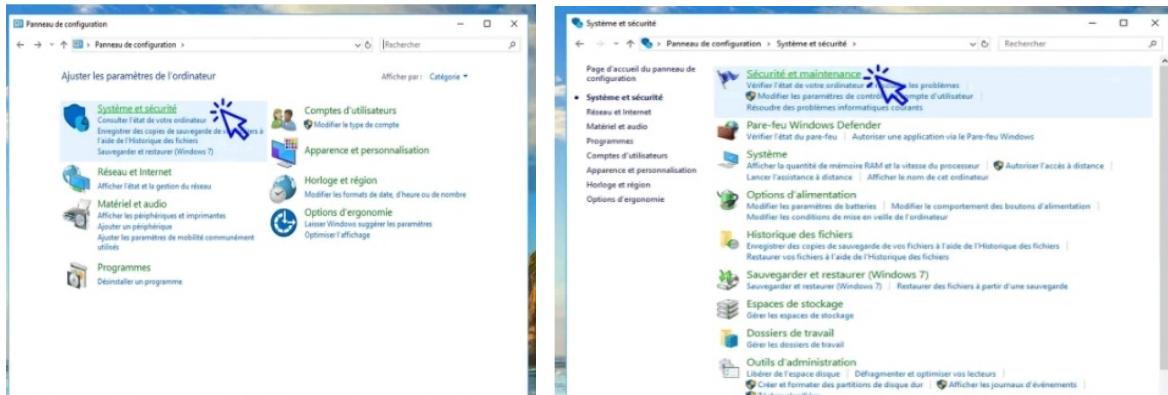
Pour protéger son ordinateur, il est impératif d'utiliser un ou plusieurs logiciels de sécurité. En général, le plus connu d'entre tous est l'antivirus mais il faut le couplé avec

“Firewall” pour avoir une grande efficacité.

Un antivirus est logiciel installé sur notre ordinateur qui a pour objectif de nous protéger des menaces d'internet tels que les virus et les programmes malveillants. Cet outil va vérifier tous les fichiers que nous téléchargeons ou ce que nous exécutons sur notre ordinateur.

Pour sécuriser notre appareil, la première chose à faire est d'installer un antivirus.

Donc, on doit vérifier si l'antivirus est bien installé: il faut y aller sur le panneau de configuration , puis cliquez sur le système et sécurité, ensuite cliquez sur la sécurité et maintenance, enfin déroulez l'onglet sécurité en cliquant sur la flèche située à droite.



Maintenant on peut voir que l'antivirus est bien installé dans l'ordinateur. On va cliqué sur l'icône représentée par une petite flèche sur la barre des tâches, afin d'ouvrir la zone

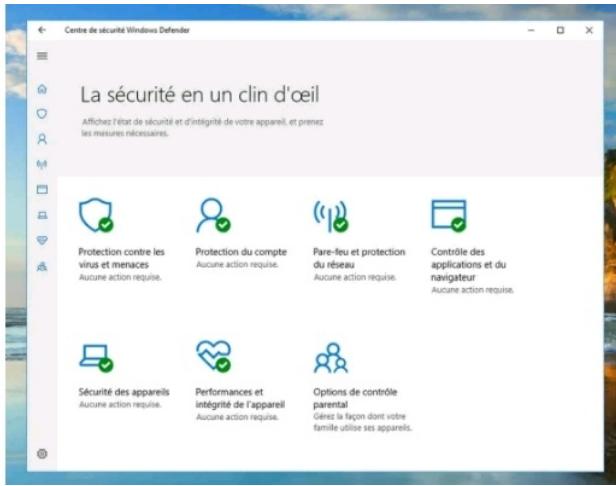
de notification.



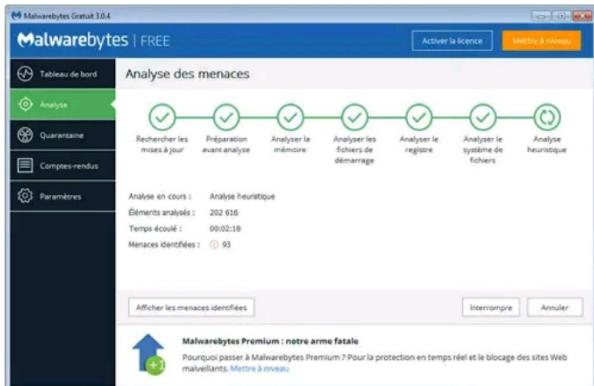
Cliquez ensuite sur l'icône "centre de sécurité"



Verifiez maintenant l'état actuel de la protection antivirus



Si l'ordinateur ne répond pas comme d'habitude, on peut installer également un anti-malware qui analyse le système à la recherche de programmes malveillants et des fichiers infectés en qu'il le peut mettre en quarantaine .



En fait, le mots “antivirus” et “anti-malware” ont presque le même sens. Leurs fonctions se réfèrent à un logiciel conçu pour détecter les logiciels malveillants, assurer la protection contre ces logiciel et les supprimer.