1. Introduction à la sécurité internet

La sécurité Internet est une expression qui décrit la sécurité des activités et des transactions exécutées sur Internet. Elle constitue une partie spécifique du cyber sécurité et de la sécurité informatique et implique des thèmes comme la sécurité du navigateur, le comportement en ligne et la sécurité du réseau. Nous passons une grande partie de notre temps en ligne et nous exposons à certaine menaces liées à la sécurité Internet, parmi lesquelles :

- Le piratage, au cours duquel des utilisateurs non autorisés accèdent aux systèmes informatiques, aux comptes de messagerie ou aux sites Web.
- Les virus ou logiciels malveillants (programmes malveillants), qui peuvent endommager les données ou rendre des systèmes à d'autres menaces.
- L'usurpation d'identité, au cours de laquelle les cybercriminels peuvent déborder les informations personnelles et financières.

La **sécurité Internet** est une branche de la sécurité informatique spécifiquement liés à l'internet, impliquant la sécurité du navigateur web, mais aussi la sécurité du réseau à un niveau plus général, car il s'applique à d'autres applications et au système d'exploitation dans son ensemble.
Son objectif est d'établir des règles et des mesures visant à contrer les attaques sur internet.
L'internet représente un canal non sécurisé pour l'échange d'informations conduisant à un risque élevé d'intrusion ou de fraude, tes que l'hameçonnage. Différentes méthodes sont utilisées pour protéger la transmission de données, par exemple le chiffrement ou la mise en de pare-feu ou de tunnels réseau.

Consultation des trois articles qui parlent de sécurité internet. On pense à la vérification des informations et on essaye de consulter des articles récentes pour que les informations soit à jours

Voici les 3 articles que je viens de trouver pour cette exercice (avec les mots-clés ''sécurité internet'' et ''comment être en sécurité sur internet'') sont :

- ✓ Article 1 = berger-levrault.com – **10 conseils en cyber sécurité pour assurer votre sécurité numérique**
- ✓ Article 2 = desgeeksetdeslettres.com – **Guide 2023 sur la sécurité numérique personnelle et la sécurité internet**
- ✓ Article 3 = www.axido.com – **comment se protéger du piratage informatique ?**
- ✓ Article bonus = www.expertitech.com – **comment se protéger sur Internet : Astuces et conseils**

2. Crée des mots de passes forts

Un mot de passe fort est un mot de passe facile à retenir pour vous mais surtout difficile à deviner pour les autres.
Pour créer des mots de passe forts est essentiel pour protéger vos comptes en ligne et vos informations personnelles. Voici quelques conseils pour créer des mots de passe forts :

1. Utilisez une combinaison de lettres, de chiffres et de caractères spéciaux : Utiliser une combinaison de différents types de caractères rendra votre mot de passe plus difficile à deviner ou à craquer.

2. Évitez les mots de passe évidents : Évitez d'utiliser des mots courants, des dates de naissance, des noms de famille ou des informations personnelles que les gens pourraient facilement deviner.
3. Utilisez des phrases complexes : Utilisez des phrases complexes qui sont faciles à mémoriser mais difficiles à deviner. Par exemple, vous pouvez utiliser une phrase comme "J'aime les chats noirs" et transformer cela en un mot de passe fort en utilisant les premières lettres de chaque mot et en ajoutant des chiffres et des caractères spéciaux. Ce qui pourrait donner : "J@!m3LcN".
4. Utilisez un générateur de mots de passe : Utilisez un générateur de mots de passe pour créer des mots de passe aléatoires et complexes. Assurez-vous de choisir un générateur de mots de passe fiable.
5. Utilisez des mots de passe différents pour chaque compte : Évitez d'utiliser le même mot de passe pour tous vos comptes. Si un mot de passe est compromis, cela pourrait affecter tous vos comptes. Utilisez des mots de passe différents et uniques pour chaque compte.

En résumé, pour créer un mot de passe fort, utilisez une combinaison de lettres, de chiffres et de caractères spéciaux, évitez les mots de passe évidents, utilisez des phrases complexes, utilisez un générateur de mots de passe et utilisez des mots de passe différents pour chaque compte.

Le meilleur gestionnaire de mots de passe en mars 2023

Nordpass (le jeune prometteur) : est un très bon gestionnaire de mots passe sans fioritures. Il assure le service qu'on lui demande : gérer ses mots de passe et quelque donnée sensible. Ce service est simple, efficace et il bénéficie d'une politique de cyber sécurité plus que correcte. Ce pendent, il manque peut-être d'ambition en ne proposant pas de fonctionnalité innovante pour ce démarquer de la concurrence. Par exemple, LastPass permet de gérer les codes d'accès et mots de passe de vos applications installé sur Windows tandis que la version Premium de Dashlane intègre un VPN.

Dashlane (le plus ergonomique) : est gestionnaire de mots de passe réputé par ses performances et l'ergonomie de sa solution. Compatible avec les différents systèmes d'exploitation d'ordinateur et de Smartphone, il propose une extension pour la majorité des navigateurs. La confidentialité de votre compte est renforcée par différentes solution d'authentification à multiple facteurs. Très complète, son offre premium intègre aussi un VPN afin de limiter les risques de piratage lorsque vous vous connectez a vos sites depuis une borne WI-FI. On apprécie particulièrement qu'il soit désormais possible d'enregistrer un nombre illimité de mots de passe dans la version gratuite.

1Password (la solution pour une famille) : propose des applications faciles à utiliser et perfectionnées qui fonctionnent sur ordinateur (Windows, MacOs et Chromebooks) et Smartphone (IOS et Androïde). Sa fonction Watchtower vous aidez à identifier et à modifier les mots de passe faibles, réutilisés ou compromis. Sons « mode itinérant » reste original et pratique si vous allez dans des pays un peut trop curieux avec vos données personnelles. En cas de difficultés, vous pouvez contacter le support technique (par email, twiter ou chat) qui est assez réactif et précis. 1Password est un gestionnaire pour une famille ou un groupe d'utilisateurs professionnel. Pour un usage personnel et grand public, d'autres gestionnaires sont gratuits et plus adapté.

LastPass (la solution ergonomique) : est très facile à maîtriser. Tout est intuitif et bien organisé, que ce soit avec la version à installer sur ordinateur ou les applications mobiles. Comme d'autre

gestionnaires en ligne, la version desktop offre plus de possibilités de règles. Disponible gratuitement ou en version Premium (et Famille), LastPass répondra à tout vos besoins. Cependant, avec une année 2022 marquée par les problèmes de sécurité rencontrés par l'entreprise, la réputation de LastPass est désormais ternie, et i sera nécessaire pour le gestionnaire de redoubler d'efforts pour regagner la confiance des utilisateurs.

Bitwarden (la sécurité au juste prix) : est facile à utiliser, compatible avec Androïde et iOS et ses tarifs sons vraiment abordables. C'est aussi l'un des gestionnaires de mots de passe le plus sûrs, car sons code sources est accessible à tout le monde. Sa version gratuite offre les fonctionnalités de base dont vous avez besoin, y compris la possibilité de synchroniser autant de mots de passe que vous le souhaitez entre tous vos appareils, la prise den charge de l'authentification multiple (via une application ou une clé physique de type « Universal 2 Factor », YubiKey, Duo) et le partage. Dommage que sa version Premium n'intègre pas l'option « personne de confiance ».
KeePass (la solution en « local ») : l'interface et l'utilisation de KeePass en feront peut-être fuir plus d'un. Mais ce logiciel gratuit répond parfaitement à ce qu'on lui demande en priorité : sauvegarder nos mots de passe. Autres atouts : une pléthore de plug-ins pour personnaliser son usage (interface, synchronisation Cloud…). Il existe également des dizaines de déclinaisons pour tout appareil et système d'exploitation.

RoboForm (la solution économique, mais parfois confuse) : peut être une option intéressante pour les personnes que souhaiteraient des options avancées à petit prix. Cependant, cela vient avec une ergonomie discutable et des fonctionnalités divisées entre les différentes versions (app, web, app Windows et extension de navigateur).

EnPass (la solution ''en local'' moderne) : pour une utilisation sur PC, EnPass est un excellent choix : gratuit, stockage local, fonctionnalité abondantes, création de coffres… Cependant, pur pouvoir l'utiliser sur plusieurs appareils, l'abonnement devient obligatoire. Il est fort heureusement à prix assez abordable. On regrette tout de même des menus un peut trop touffus qui rendent la prise en main compliquée.

Dropbox Passwords (une solution simple, parfois un peut trop) : est un bon gestionnaire de mots de passe pour les personnes qui utilisent déjà le service de stockage en ligne et qui ne veulent pas être noyées sous les options. Pour les autres, la proposition ne sera pas forcément intéressante financièrement et un peut trop limitée selon ses besoins.

3. Fonctionnalité de sécurité de navigateur web

Les navigateurs modernes sont équipés de plusieurs fonctionnalités de sécurité pour protéger les utilisateurs contre les menaces en ligne. Voici quelques-unes des fonctionnalités de sécurité que l'on peut trouver dans la plupart des navigateurs web :

1. Bloqueur de pop-ups : Cette fonctionnalité permet de bloquer les fenêtres pop-up, qui peuvent être utilisées pour diffuser des publicités malveillantes ou pour rediriger l'utilisateur vers des sites Web suspects.
2. Protection contre les logiciels malveillants : Les navigateurs modernes disposent d'une protection intégrée contre les logiciels malveillants. Lorsque vous visitez un site Web malveillant, le navigateur peut vous alerter et vous empêcher d'accéder au site.

3. Filtre anti-phishing : Cette fonctionnalité permet de bloquer les sites Web de phishing qui tentent de voler vos informations personnelles ou financières. Le navigateur peut vous avertir si vous visitez un site Web suspect et vous empêcher d'y accéder.
4. Connexion sécurisée : Les navigateurs modernes utilisent le protocole HTTPS pour garantir la sécurité des communications entre votre ordinateur et le site Web que vous visitez. Vous pouvez vérifier si une connexion est sécurisée en vérifiant la présence du symbole de cadenas dans la barre d'adresse du navigateur.
5. Gestionnaire de mots de passe : Certains navigateurs modernes proposent un gestionnaire de mots de passe intégré. Cette fonctionnalité permet de stocker vos mots de passe de manière sécurisée et de remplir automatiquement les champs de connexion lorsque vous visitez un site Web.

Les sites malveillants utilisent souvent des adresses Web trompeuses qui rapprochent de site internet connu afin de tromper les utilisateurs.

Les sites web qui semblent être malveillants sont :

- www.morvel.com : un dérivé de www.marvel.com , le site officiel de monde Marvel
- www.fessebook.com : un dérivé de www.facebook.com , le plus grand réseau social du monde.
- www.istagam.com : un dérivé de www.istagram.com , un autre réseau social très utilisé.

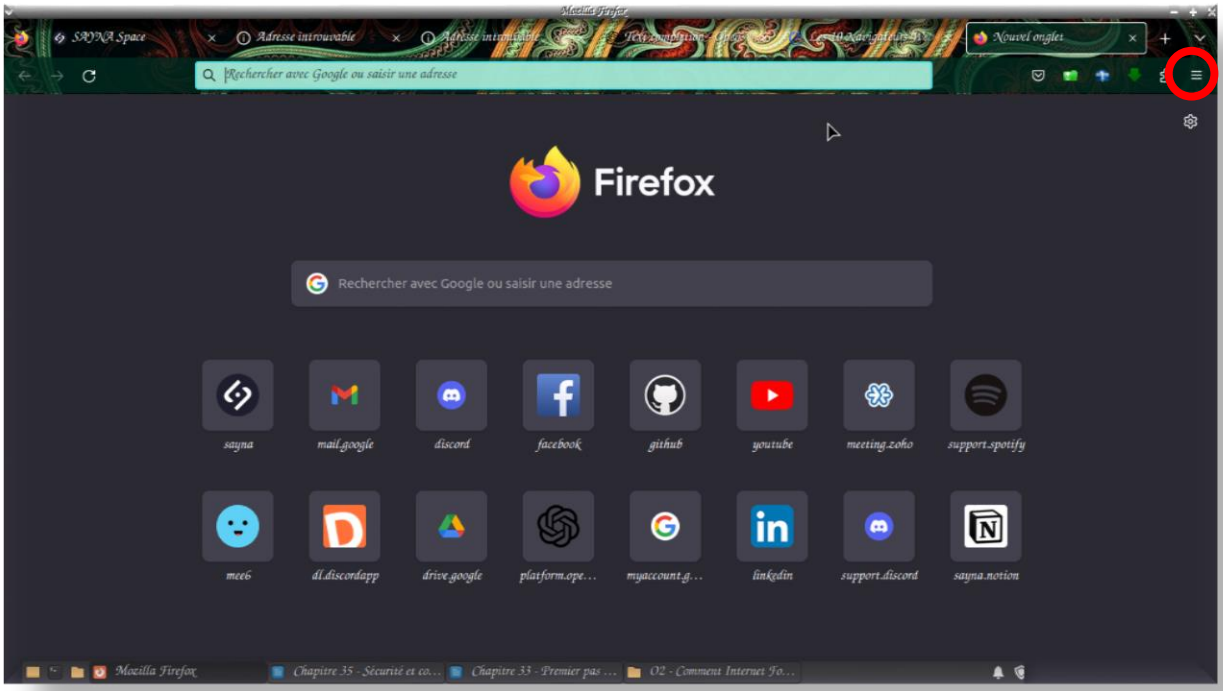
La double vérification du nom de domaine est un bon moyen de s'assurer que vous accédez au vrai site de confiance, et non à un faux site avec une adresse Web similaire. Certains navigateurs Web essaieront même de rendre le nom de domaine plus facile à lire.
Les seuls sites qui semblaient être cohérents sont donc :

- www.dccomics.com , le site officiel de l'univers DC Comics
- www.ironman.com , le site officie d'une compétition internationale de triathlon (et le nom de super-héro issu de l'univers Marvel)

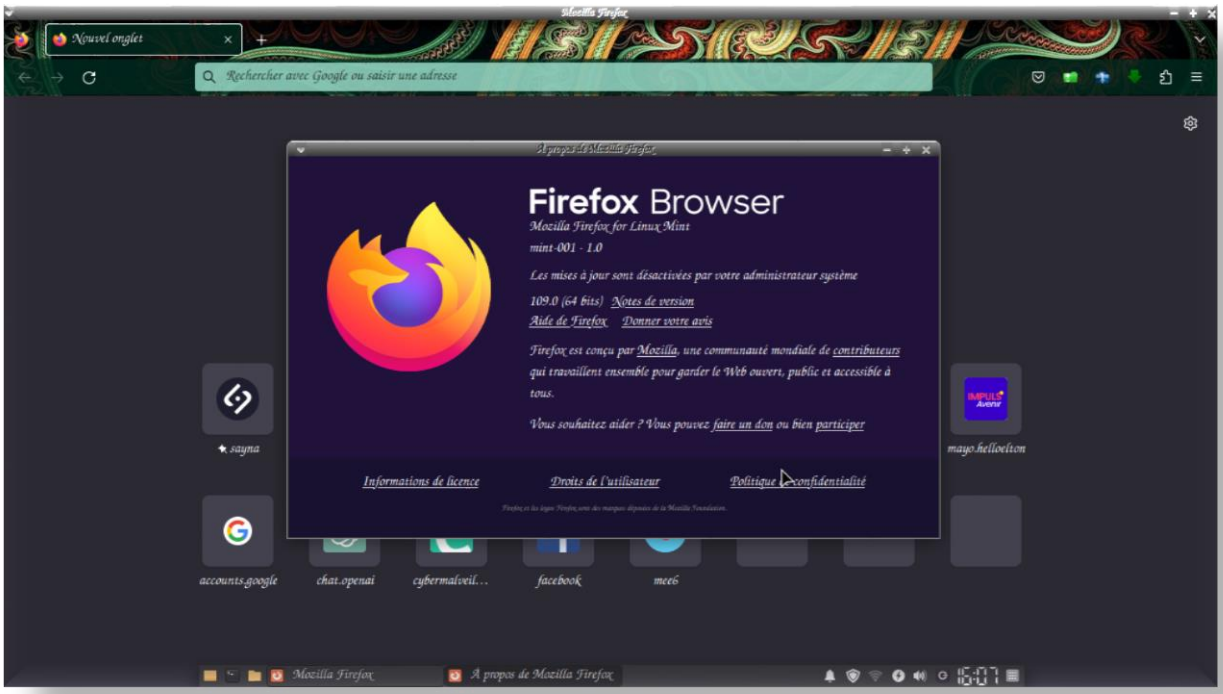
De nouveaux virus et logiciels malveillants sont crées tout le temps, il est donc important de mettre à jour notre navigateur régulièrement.
Les navigateurs avertir généralement lorsqu'une mise à jour est disponible, mais vous avez toujours la possibilité de réaliser les opérations manuellement.
Les paramètres par défaut des navigateurs sont réglés pour réaliser les mises à jours automatique.
Comme d'habitude, Firefox affiche une personnalisation des paramètres un peut plus poussée.

En résumé, les navigateurs modernes offrent plusieurs fonctionnalités de sécurité pour protéger les utilisateurs contre les menaces en ligne. Les fonctionnalités courantes incluent un bloqueur de pop-ups, une protection contre les logiciels malveillants, un filtre anti-phishing, une connexion sécurisée et un gestionnaire de mots de passe.

Vérification si mon navigateur FireFox est à jours.
Pour vérifier la version de FireFox que vous utiliser, vous pouvez ouvrir le menu en cliquant sur le bouton **Menu :**



1. Puis cliquer sur l'entrée ''Aide''
2. Puis sur l'entrée ''A propos de FireFox''
3. La version de Firefox s'affiche dans la fenêtre que s'affiche :



4. Eviter le spam et le phising

Le spam et le phishing sont des problèmes courants en ligne.
Voici quelques conseils pour éviter le spam et le phishing :

1. Utilisez une adresse email jetable : Si vous devez fournir votre adresse email pour accéder à un service en ligne, utilisez une adresse email jetable qui ne contient pas vos informations personnelles. De cette façon, si vous recevez du spam ou des emails de phishing, cela ne compromettra pas votre adresse email principale.
2. Évitez de cliquer sur des liens suspects : Si vous recevez un email qui contient des liens suspects, ne cliquez pas dessus. Les liens peuvent être utilisés pour vous rediriger vers des sites Web malveillants ou pour installer des logiciels malveillants sur votre ordinateur.
3. Ne partagez pas d'informations personnelles : Évitez de partager des informations personnelles comme votre numéro de sécurité sociale, votre numéro de carte de crédit ou votre mot de passe par email ou sur des sites Web non sécurisés. Les pirates peuvent utiliser ces informations pour voler votre identité ou pour accéder à vos comptes en ligne.
4. Vérifiez l'adresse email de l'expéditeur : Vérifiez toujours l'adresse email de l'expéditeur avant de cliquer sur un lien ou de répondre à un email. Les pirates peuvent utiliser des adresses email frauduleuses pour vous tromper et vous amener à divulguer des informations personnelles.
5. Utilisez un filtre anti-spam : Utilisez un filtre anti-spam pour bloquer les emails indésirables avant qu'ils n'arrivent dans votre boîte de réception. Les filtres anti-spam peuvent identifier les emails suspects et les bloquer automatiquement.

Comment repérer un mail de phishing ?

1. Une notification de la messagerie ou de l'antivirus

Votre messagerie ou votre antivirus peut vous signaler la réception d'un mail frauduleux. N'ignorez pas leur avertissement et **assurez-vous régulièrement que votre antivirus est activé et à jour**.

2. Un email d'un service ou d'une société dont vous n'êtes pas client

Les cybercriminels n'ont généralement pas accès aux bases de données d'utilisateurs des entreprises dont ils usurpent l'identité et envoient parfois leur mail de phishing au hasard. **Si vous recevez un email d'un service ou d'une société dont vous n'êtes pas client, méfiez-vous. Attention cependant, un cybercriminel peut également s'en prendre aux vrais clients** d'un service ou d'une société, soit parce que le hasard voudra que dans leur envoi de masse leur message de phishing soit adressé à des clients du service usurpé, soit parce qu'ils ont réussi à récupérer une base d'adresses des clients du service concerné.

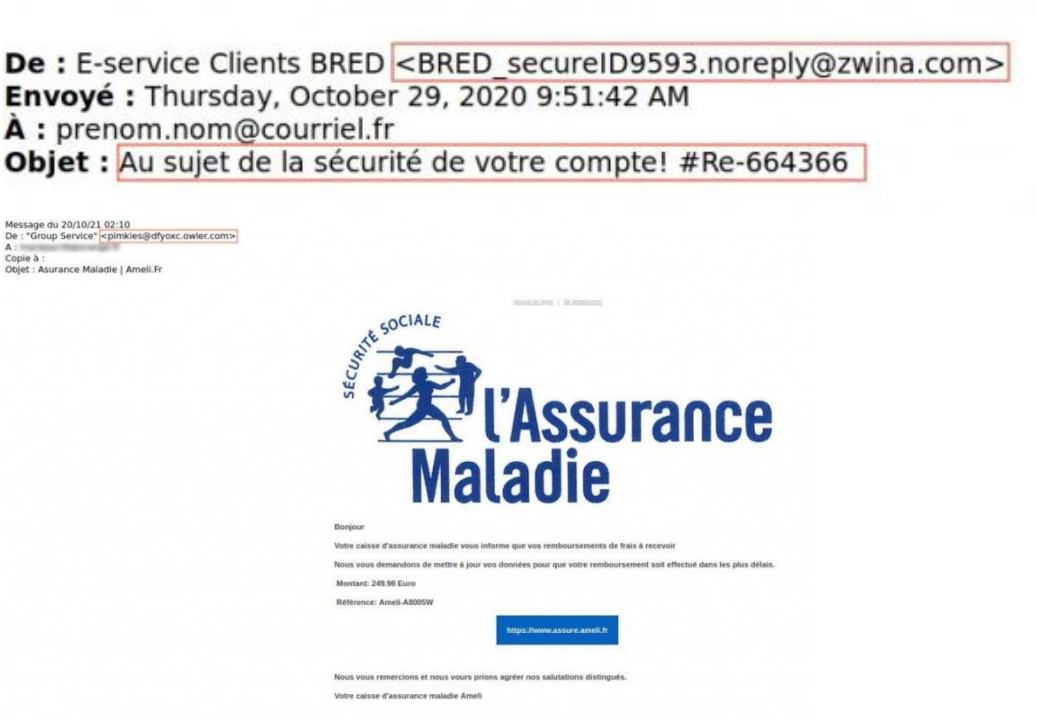
3. Mail phishing: un nom d'expéditeur inhabituel

La réception d'un message inattendu d'une adresse email inhabituelle, que vous ne connaissez pas ou qui ne fait pas partie de vos contacts, doit éveiller votre attention, même si celle-ci est d'apparence légitime. Si l'adresse email de l'expéditeur vous paraît suspecte, posez-vous les questions suivantes : connaissez-vous l'expéditeur ? Est-il possible que ce dernier vous adresse un message ? Est-ce que le contenu du message vous est réellement destiné ? Est-ce que le sujet abordé vous parle ? S'il s'agit d'un mail de phishing envoyé à échelle industrielle, il sera en effet très peu personnalisé.

4. Une adresse d'expédition fantaisiste

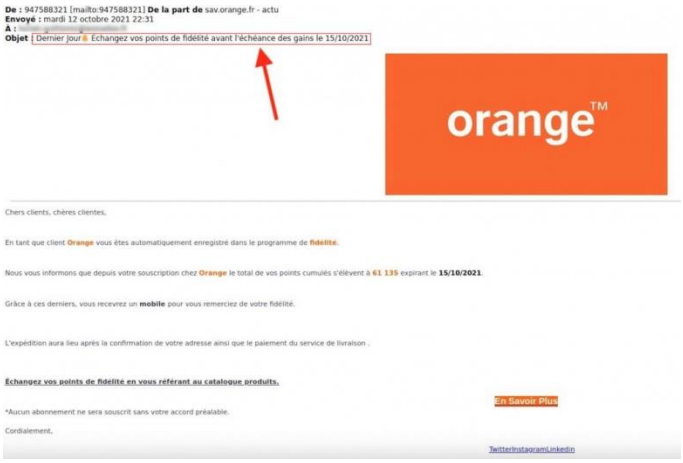
La plupart des phishing par email utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles. **Pour vérifier qu'il s'agit bien d'un message officiel, pensez à vérifier l'adresse email de l'expéditeur.** Si cette dernière ne comporte pas le nom de l'entité, qu'elle

présente des fautes d'orthographe ou que le nom vous paraît suspect, n'ouvrez pas le message. Il s'agit sûrement d'un mail frauduleux.



5. Un objet d'email trop alléchant ou alarmiste

L'objet d'un mail de phishing est généralement sommaire et cherche à inciter la victime à ouvrir le message. **Un intitulé aguicheur ou inquiétant** – comme « remboursement » ou « alerte de sécurité » – qui transmet un sentiment d'urgence inhabituel.



6. Une apparence suspecte

De nouveaux phishing sont créés chaque jour et les cybercriminels redoublent de créativité pour mettre au point des stratagèmes innovants. Si les méthodes employées sont donc de plus en plus sophistiquées, **certains phishing par email revêtent néanmoins une apparence douteuse**. Images et logos de mauvaise qualité, flous, déformés, pixélisés ou pris de loin, peuvent être le signe qu'il s'agit de captures d'écran ou d'éléments volés sur des sites officiels. Idem si le message vous semble légitime mais que son apparence ne semble plus d'actualité (logo désuet). **De manière générale, si vous observez des différences entre l'apparence de l'email reçu et celle**

des mails habituels, méfiez-vous. Il peut arriver que des bugs surviennent mais ces anomalies doivent vous mettre en alerte : il s'agit peut-être d'un mail de phishing.

envoyé : 18 octobre 2021 à 18:16
de : Sylviane <ferencziimre@t-online.hu>
à : f.d.j@capital.fr
objet : Informations

7. Une absence de personnalisation

Généralement, les emails officiels qui vous sont adressés mentionnent votre nom, or **l'hameçonnage « bon marché » consiste à envoyer à échelle industrielle le même mail de phishing de manière dépersonnalisée** à une large base de données d'adresses mail. Si le message ne mentionne pas votre nom ou encore qu'il utilise une formule un peu vague de type « Cher client privilégié », méfiez-vous.

8. Une demande inhabituelle

Connaître l'adresse email de l'expéditeur n'est pas un critère de confiance absolu : le cybercriminel peut avoir usurpé l'adresse de messagerie d'un proche ou d'un service connu. Remarquez-vous une incohérence, sur la forme ou le fond, entre l'email reçu et ceux que l'expéditeur vous envoie d'habitude ? Soyez vigilant aux éléments suspects, notamment si le message contient un lien cliquable, une pièce jointe, ou vous demande des informations.

9. Une demande d'informations confidentielles

En règle générale, les demandes d'informations personnelles – identifiants de connexion, informations bancaires… – ne se font jamais par email. Aucune entité légitime, gouvernementale, professionnelle ou autre n'est en droit de vous demander votre code de carte bancaire ou vos codes d'accès personnels par message. **Ne communiquez rien de confidentiel par écrit**, même s'il s'agit d'un expéditeur qui prétend faire partie de votre entourage.


Envoyé: vendredi 15 Octobre 2021 11:07
De : "Relation Clientèle Floa-Bank"
A :
Objet : Authentification-Mobile

FLOA

Bonjour,

En accord de la Directive européenne,

La double authentification devient une obligation.

Confirmer votre mobile ici

Nous vous remercions de votre confiance.

Cordialement,
Votre Conseiller FLOATBANK.

1) Sous réserve d'un fonctionnement normal de votre compte et du solde disponible lorsdu traitement de votre demande.FLOABANK
, Société Anonyme au capital de 41 228 000 euros - Bâtiment G7, 71 Rue Lucien Faure, 33300 Bordeaux, RCS Bordeaux 434 130 423, ORIAS n°07 028 160, Entreprise soumise au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) 4 Place de Budapest, CS 92469, 75430 Paris Cedex 09.
Ce message et toutes les pièces jointes sont confidentiels et établis à l'intention exclusive de son ou ses destinataires. Si vous avez reçu ce message par erreur, merci d'en avertir immédiatement l'émetteur et de détruire le message. Toute modification, édition, utilisation ou diffusion non autorisée est interdite. L'émetteur décline toute responsabilité au titre de ce message s'il a été modifié, déformé, falsifié, infecté par un virus ou encore édité ou diffusé sans autorisation.

10. Un message aguicheur ou inquiétant

Un mail de phishing fait souvent part d'une offre, d'un remboursement ou d'un gain inespéré. Vous venez de remporter un lot important alors que vous n'avez pas joué et que vous n'êtes pas client de l'entreprise qui vous a soi-disant envoyé le message ? Il s'agit probablement d'une tentative de phishing. **Un mail frauduleux peut également faire état d'un besoin urgent ou d'une menace imminente qui requiert une action immédiate**, comme la fermeture de votre compte si vous n'agissez pas tout de suite. En pressant leurs victimes, les cybercriminels tentent de les déstabiliser et de les pousser à prendre des décisions erronées.


DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

Votre remboursement de 228,35 € est disponible Référence de l'avis : 1875094580391

Bonjour,

Nous vous informons que votre remboursement de **228,35 €** est disponible.

Vous pouvez vous abonner à nos services en ligne et obtenir un nouveau certificat.

Il vous suffit de vous connecter sur le portail fiscal , Espace Particuliers

Nous vous remercions de l'intérêt que vous portez aux services en ligne du Ministère du Budget, des Comptes Publics et de la Fonction Publique et vous prions d'agréer l'expression de notre considération.

La Direction Générale des Finances Publiques

Ce courriel vise à vous informer sur notre offre de services en ligne.

Si vous ne souhaitez plus recevoir ce type de courriel, merci de vous désabonner à la rubrique "Gérer mon profil" de votre espace particulier sur impots.

Des questions sur le prélèvement à la source ? Allez sur le site prelevementalasource

Ce courriel vise à vous informer sur notre offre de services en ligne. Si vous ne souhaitez plus recevoir ce type de courriel, merci de vous désabonner à la rubrique "Gérer mon profil" de votre espace particulier sur impots.

IMPOTS EST UN SITE DE LA DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES

11. Mail phishing : des fautes de français surprenantes

Soyez vigilant à la qualité du texte de l'email. L'hameçonnage par mail comporte souvent des fautes de frappe, d'orthographe ou de grammaire. Des erreurs de formulation, de mauvaise traduction ou une syntaxe inhabituelle dans des communications officielles doivent également vous alerter. Certains textes de phishing proviennent de l'étranger et sont traduits par des logiciels, ce qui peut expliquer des tournures de phrases inhabituelles et des caractères accentués mal retranscrits. Toutefois, on constate au fil du temps que le niveau de français des tentatives d'hameçonnage s'améliore de plus en plus. Faites donc preuve de vigilance.

12. Une incitation à cliquer sur un lien ou une pièce-jointe

Un mail de phishing cherche généralement à pousser la victime à cliquer sur un lien. Même si le lien semble rediriger vers la page officielle d'un site, il l'amènera sur une page frauduleuse ressemblant beaucoup au site officiel. Avant de cliquer, pensez à vérifier l'adresse des sites web mentionnés. Pour cela, positionnez le curseur de votre souris sur le lien proposé sans cliquer afin d'afficher le lien complet et l'adresse où il mène réellement. S'agit-il bien de l'adresse officielle

du site annoncé dans le message ? Si l'adresse n'est pas ressemblante, qu'elle est mal orthographiée, qu'elle ne vous dit rien et que le lien vous paraît douteux, il s'agit peut-être d'une tentative d'hameçonnage. Lisez attentivement les liens avant de cliquer. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Pour vérifier que l'adresse correspond exactement à la page de connexion officielle, rendez-vous directement sur le site de l'organisme en question en saisissant manuellement son adresse dans votre navigateur.

5. Comment éviter les logiciels malveillants

Les logiciels malveillants sont l'un des dangers les plus courants pour votre ordinateur lorsque vous êtres en ligne, mais il est facile de les éviter
Pour éviter les logiciels malveillants, utilisez un logiciel antivirus, évitez les sites Web suspects, mettez à jour votre système d'exploitation et vos logiciels, utilisez un pare-feu et soyez vigilant en ligne.
Ici nous allons testez ensemble quelque le site web par une outilles de Google : Google Transparence des Informations. Afin d'améliorer notre lecture de s

Site N°1 https://www.fifa.com/fr Aucun contenu suspect détecté

Site N°2 http://xinhuanet.com/ Aucun contenu suspect détecté

Site N°3 http://www.baidu.com Vérifier une URL particulier

Site N°4 nnindonesia.com Aucun contenu suspecté détecté

6. Achat en ligne sécurisés

Les achats en ligne sont un moyen pratique d'acheter presque n'importe quoi tout en à la maison.
Bie que les achats en ligne comportent certains risques, il existe également de nombreuses façons de protéger cos informations bancaires.
Voici quelques conseils pour effectuer des achats en ligne de manière sécurisée :

1. Utilisez des sites Web de confiance : Effectuez des achats en ligne uniquement sur des sites Web de confiance. Vérifiez les avis et les commentaires des clients avant de faire un achat.
2. Assurez-vous que le site Web est sécurisé : Assurez-vous que le site Web sur lequel vous effectuez un achat est sécurisé. Recherchez un cadenas dans la barre d'adresse ou un "https" dans l'URL pour indiquer que la connexion est sécurisée.
3. Utilisez des mots de passe forts : Utilisez des mots de passe forts et uniques pour chaque site Web sur lequel vous effectuez un achat. Utilisez un gestionnaire de mots de passe pour vous aider à générer et à stocker des mots de passe forts.
4. Évitez les réseaux Wi-Fi publics : Évitez d'effectuer des achats en ligne sur des réseaux Wi-Fi publics non sécurisés. Les pirates peuvent intercepter les données sur ces réseaux et accéder à vos informations personnelles.
5. Utilisez une carte de crédit protégée : Utilisez une carte de crédit protégée pour effectuer des achats en ligne. Les cartes de crédit offrent souvent une protection contre les fraudes et les achats non autorisés.
6. Vérifiez les relevés de carte de crédit : Vérifiez régulièrement les relevés de carte de crédit pour détecter les activités suspectes ou non autorisées. Signalez immédiatement toute activité suspecte à votre banque ou à l'émetteur de la carte.

En résumé, pour effectuer des achats en ligne de manière sécurisée, utilisez des sites Web de confiance, assurez-vous que le site Web est sécurisé, utilisez des mots de passe forts, évitez les

réseaux Wi-Fi publics, utilisez une carte de crédit protégée et vérifiez régulièrement les relevés de carte de crédit.

7. Comprendre le suivi du navigateur

Le suivi du navigateur, également appelé "suivi des cookies", est une technique utilisée par les sites Web pour recueillir des informations sur les utilisateurs et leur comportement en ligne. Les cookies sont de petits fichiers texte stockés sur l'ordinateur d'un utilisateur par un site Web qu'il visite. Les cookies peuvent être utilisés pour stocker des informations telles que les préférences de l'utilisateur, les données de connexion et les données de navigation.

Suivi de données dur vos comptes, même si vous n'autorisez jamais les sites web à stocker des cookies, il existe d'autre moyens de suivre cos habitudes de navigation.
Par exemple, lorsque vous créez un compte sur un site comme Facebook ou Google, vous leur donnez également la permission de suivre et d'enregistrer des informations sur votre activité. Au lieu d'enregistrer ces informations dans un cookie, elles sont stockées par la société et associées à votre compte.
Dans de nombreux cas, ces informations de comptes sont ensuite fournies ou vendues à des annonceurs tiers, qui peuvent utiliser ces informations pour diffuser des publicités personnalisées sur Internet. Et bien que vous puissiez généralement désactiver ces paramètres des suivis, ils seront activés par défaut.

Le suivi des navigateurs peut être utilisé à des fins diverses, telles que la personnalisation de la publicité, l'analyse de l'utilisation du site Web et l'amélioration de l'expérience utilisateur. Cependant, le suivi des navigateurs peut également être utilisé à des fins moins souhaitables, telles que la collecte d'informations personnelles et la surveillance des activités en ligne.
Pour protéger votre vie privée en ligne, voici quelques conseils :

1. Utilisez un navigateur avec des paramètres de confidentialité améliorés : Les navigateurs modernes offrent des options pour bloquer les cookies et les trackers tiers.
2. Utilisez un bloqueur de publicité : Les bloqueurs de publicité peuvent aider à bloquer les publicités indésirables et les trackers.
3. Effacez régulièrement les cookies : Effacez régulièrement les cookies de votre navigateur pour supprimer les informations stockées sur votre ordinateur.
4. Utilisez un VPN : Un VPN (Virtual Private Network) peut aider à masquer votre adresse IP et à protéger vos informations de suivi en ligne.
5. Soyez vigilant en ligne : Soyez prudent lorsque vous partagez des informations personnelles en ligne et évitez les sites Web et les publicités suspectes.
6. Vous pouvez utiliser un mode de navigation privée chaque fois que vous connectez. Cela empêchera l'enregistrement de cookies dans votre navigateur. Le mode de navigation privée ne protège pas contre tous les types de suivi du navigateur, mais limite la collecte de certaines données.

En résumé, le suivi des navigateurs est une technique utilisée par les sites Web pour recueillir des informations sur les utilisateurs et leur comportement en ligne. Pour protéger votre vie privée en ligne, utilisez un navigateur avec des paramètres de confidentialité améliorés, utilisez un bloqueur de publicité, effacez régulièrement les cookies, utilisez un VPN et soyez vigilant en ligne.

8. Principe des bases de confidentialité des medias sociaux

La confidentialité des médias sociaux est un sujet important pour les utilisateurs de réseaux sociaux.

Les sites des médias sociaux comme Facebook, Instagrama ou Twiter ont rendu plus facile que jamais le partage de contenu en ligne. Mais partage quelque chose sur les réseaux sociaux est un peu différent des autres types de communication en ligne.

Voici quelques principes de base pour protéger votre vie privée en ligne sur les réseaux sociaux :

1. Paramètres de confidentialité : Vérifiez les paramètres de confidentialité de votre compte pour déterminer qui peut voir vos publications et vos informations personnelles. Limitez l'accès aux informations personnelles que vous partagez sur les réseaux sociaux aux personnes que vous connaissez et en qui vous avez confiance.
2. Limitation de la collecte de données : Limitez la quantité d'informations personnelles que vous partagez sur les réseaux sociaux. Évitez de publier des informations sensibles telles que des informations de compte bancaire, des numéros de sécurité sociale ou des informations de passeport.
3. Contrôle des applications tierces : Limitez l'accès des applications tierces à votre compte de médias sociaux. Les applications tierces peuvent avoir accès à vos informations personnelles et à vos contacts.
4. Utilisation d'un pseudonyme : Utilisez un pseudonyme ou un nom d'utilisateur pour éviter de révéler votre identité réelle sur les réseaux sociaux.
5. Utilisation de mots de passe forts : Utilisez des mots de passe forts pour votre compte de médias sociaux et ne partagez pas votre mot de passe avec d'autres personnes.
6. Éviter les publicités ciblées : Évitez les publicités ciblées en désactivant la fonctionnalité de suivi des publicités sur les réseaux sociaux.
7. Éviter les réseaux Wi-Fi publics : Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés lorsque vous utilisez les réseaux sociaux.

Voici il y a 10 conseils proposer par YOURinfoGRAPHIC qu'ils ont proposent d'appliquer pour être en sécurité sur les médias sociaux :

1. **Créer son anonymat**

Créez une nouvelle adresse email. Ne pas avoir de caractéristique identifiables (elles que nom et prénom, année de naissance, ou un code postal) dans l'adresse e-mail ou les paramètres de profil. Créez des pages sur les réseaux sociaux en utilisant cette nouvelle adresse e-mail et ajouter seulement ceux en qui vous avez vraiment confiance. Evitez également l'identification des photos

2. **Utiliser des mots de passe forts**

Mettez à jours vos mots de passe pour tous les comptes que vous avez, et assurez-vous d'utiliser des mots de passe fort sur tous les nouveaux comptes que vous créez. Utilisez des lettres (au moins une Majuscule) et des chiffres, et envisagez également d'utiliser des caractères spéciaux (! @ # $ %). Ne pas utiliser en mot de passe que l'on peut deviner.

3. **Augmenter et améliorer ses paramètres de confidentialité.**

Chaque réseau social possède une option pour « les paramètre de confidentialité » pour vous permettre d'augmenter la sécurité de votre compte, de sort à ce que seuls vos amis ou des listes spécifiques de personnes peuvent voir vos message et informations privées. Ne laissez jamais les paramètres par défaut.

4. **Eviter de se faire identifier par la localisation**

Désactivez les paramètres de localisation et ne partagez jamais l'endroit où vous serez (y compris les sorties en ville et en vacances). De même, ne partagez pas l'information après coup, les gens peuvent vos habitudes et prédire quand et où vous allez être.

5. **Ajouter des amis attentivement**

Soyez sûr que vous connaissez les personnes qui vous ajoutent. Envoyez un message privé avant d'accepter une d'émende d'ami et d'émendez à la personne quelque chose qui prouve qu'elle est. Même si vous pensez avoir reconnu le nom ou la photo, on n'est jamais trop prudent (c'est une technique de piratage répandue).

6. **Ne pas partager des informations personnelles.**

Cela comprend les numéros d'assurance sociale, adresse, nom de jeune fille de votre mère, l'année de naissance, numéros de téléphone et coordonnées bancaires. Ceux-ci peuvent être utilisés par des voleurs d'identité. Si quelqu'un a légitimement besoin de ces informations, ils peuvent vous contacter d'une autre façon.

7. **Publier, republier, aimer.**

Rien sur internet n'est complètement sûr. N'importe qui peut enregistrer ou faire une capture d'écran ce que vous publiez et partagez, alors faites attention à vos publications. Supposons que tout ce que vous postez est permanent. Ne publier jamais rien sur vous, votre famille, vos amis que vous (et eux) ne voulez que cela soit public. Ne jamais poster quelque chose que vous pourriez regretter.

8. **Protéger son image et sa réputation**

Si quelqu'un publie quelque chose sur vous que vous n'aimez pas, dites que cela vous rend mal à l'aise et demandez à retirer le contenu. Vérifiez périodiquement « photos de moi » pour voir si quelqu'un à posté, et vérifier votre mur pour voir si vous êtes « tagué ». Si quelqu'un refuse de retirer quelque chose sur vous, vous pouvez bloquer la personne et/ou la signaler.

9. **Faire attention aux liens frauduleux.**

Les pirates peuvent casser votre compte ou un virus se propage si vous cliquez sur les liens dont vous n'êtes pas sûr. Si quelqu'un publie quelque chose qui ne pensez pas qu'il le ferait en temps normal, ou quelque chose que vous semble étrange, envoyez-leur un message à ce sujet et faites-leur savoir que vous pensez qu'ils sont peut-être piraté.

10. **Connaître les mesures à prendre**

Si vous êtes victime de harcèlement, veuillez sauvegarder (ou faire une capture d'écran) la communication ou la publication offensive. Signalez-les sur le site et contactez les personnes qui peuvent vous aider dans cette situation (comme un avocat, un conseiller ou un travailleur social).

En résumé, pour protéger votre vie privée sur les réseaux sociaux, vérifiez les paramètres de confidentialité de votre compte, limitez la quantité d'informations personnelles que vous partagez, limitez l'accès des applications tierces, utilisez un pseudonyme, utilisez des mots de passe forts, évitez les publicités ciblées et évitez les réseaux Wi-Fi publics non sécurisés.

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

Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire.

Les virus informatique peuvent être dangereux et doivent être pris au sérieux, mais il existe des moyens de les supprimer voir de les bloquer avant que ne se produisent de graves dommages.

1. **Vérification de la sécurité sur Windows 10**

Windows 10 inclut Sécurité Windows (Windows Defender) qui met à votre disposition la dernière protection antivirus. Votre appareil sera activement protégé dès le moment où vous démarrez Windows. Sécurité Windows effectue en permanence des analyses pour détecter des programmes malveillants (logiciels malveillants), les virus et les menaces liées à la sécurité. En plus de cette protection en temps réel, des mises à jour sont automatiquement téléchargées pour contribuer à sécuriser votre appareil et à le protéger contre les menaces.

Effectuer une analyse manuelle des programmes malveillants sur Windows Defender

Si vous êtes préoccupé par un fichier ou un dossier spécifique sur votre appareil local, vous pouvez cliquer avec le bouton droit sur le fichier ou le dossier dans l'Explorateur de fichiers, puis sélectionner Analyser avec Microsoft Defender.

Conseil : Sur Windows 11, vous devrez peut-être sélectionner Afficher d'autres options, après avoir cliqué avec le bouton droit, pour afficher l'option permettant d'analyser le fichier ou le dossier.

Si vous suspectez la présence d'un programme malveillant ou d'un virus sur votre appareil, vous devez immédiatement exécuter une analyse rapide.

Exécuter une analyse rapide dans Sécurité Windows

Remarque : En raison d'une sécurité simplifiée, ceci n'est pas disponible si vous exécutez Windows 10 ou 11 en mode S.

1. Sélectionnez Démarrer> Paramètres >Mise à jour et sécurité >Sécurité Windows, puis Protection contre les virus et menaces.
   Ouvrir les paramètres de Sécurité Windows
2. Sous Menaces actuelles, sélectionnez Analyse rapide (ou, dans les versions précédentes de Windows 10, sous Historique des menaces, sélectionnez Analyser maintenant).

Si l'analyse ne détecte aucun problème, mais que vous êtes toujours préoccupé, vous souhaiterez peut-être vérifier votre appareil de manière plus approfondie.

Exécuter une analyse avancée dans Sécurité Windows

1. Sélectionnez Démarrer> Paramètres >Mise à jour et sécurité >Sécurité Windows, puis Protection contre les virus et menaces.
2. Sous Menaces actuelles, sélectionnez Options d'analyse (ou, dans les versions précédentes de Windows 10, sous Historique des menaces, sélectionnez Exécuter une nouvelle analyse avancée).
3. Vous pouvez sélectionner l'une des options d'analyse suivantes :
   - Analyse complète (vérifie les fichiers et les programmes actuellement sur votre appareil)
   - Analyse personnalisée (analyse des fichiers ou des dossiers spécifiques)
   - Analyse Microsoft Defender hors ligne (redémarre votre ordinateur et exécute une analyse approfondie avant le chargement de Windows pour intercepter les programmes malveillants particulièrement sournois). Si vous souhaitez en savoir plus sur Microsoft Defender hors ligne
4. Sélectionnez Analyser maintenant.

Vous pouvez planifier votre propre analyse

Même si Sécurité Windows analyse régulièrement votre appareil pour le protéger, vous pouvez également définir l'heure et la fréquence auxquelles l'analyse se produit.

Remarque : En raison d'une sécurité simplifiée, ceci n'est pas disponible si vous exécutez Windows 10 ou 11 en mode S.

Planifier une analyse

1. Sélectionnez le bouton Démarrer, saisissez Planifier des tâches dans la case Rechercher, et, dans la liste des résultats, sélectionnez Planifier des tâches.
2. Dans le volet de gauche, sélectionnez la flèche (>) en regard de Bibliothèque du Planificateur de tâches pour la développer, faites-en de même avec Microsoft>Windows, puis faites défiler l'écran vers le bas et sélectionnez le dossier Windows Defender.
3. Dans le volet en haut au centre, sélectionnez Analyse planifiée de Windows Defender (Pointez sur les choix pour afficher les noms complets).
4. Dans le volet Actions à droite, faites défiler l'écran vers le bas et sélectionnez Propriétés.
5. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet Déclencheurs, puis Nouveau.
6. Définissez la durée et la fréquence de votre choix, puis sélectionnez OK.
7. Vérifiez la planification, puis sélectionnez OK.

2. Exercice d'installation et d'utilisation Avira + antimalware sur windows

Étape à suivre pour l'installation d'une antivirus et antimalware pour Windows
Voici quelques étapes à suivre pour installer un antivirus et un anti-malware sur un système d'exploitation Windows:

1. Tout d'abord, téléchargez un logiciel antivirus et anti-malware à partir d'un site Web réputé. Il existe de nombreux programmes disponibles, comme Avira
2. Une fois le programme téléchargé, double-cliquez sur le fichier d'installation pour lancer le processus d'installation.
3. Suivez les instructions à l'écran pour terminer l'installation du programme. Il est recommandé de lire attentivement chaque étape de l'installation pour éviter d'installer des programmes supplémentaires non désirés.
4. Après l'installation, lancez le programme antivirus et anti-malware et effectuez une analyse complète du système pour rechercher les virus, les logiciels malveillants et les autres menaces potentielles.
5. Mettez à jour régulièrement votre programme antivirus et anti-malware pour garantir une protection maximale contre les dernières menaces.
6. Évitez de télécharger des fichiers ou des programmes à partir de sites Web non fiables et n'ouvrez pas les pièces jointes d'e-mails d'expéditeurs inconnus ou suspects.
7. Enfin, effectuez régulièrement des analyses de votre système avec votre programme antivirus et anti-malware pour détecter et supprimer toute menace éventuelle.

Scanne avec Avira

Pour lancer un Scan intégral,

- Ouvrez l'interface utilisateur Avira et cliquez sur Sécurité.
- Scans antivirus
- Puis cliquez sur Analyser sous Scan intégral.
- Un scan antivirus complet prend plus de temps qu'un scan rapide ou personnalisé.

Le résumé des résultats du scan s'affichera une fois le scan terminé.