

CYBERSÉCURITÉ : UN FILM DONT VOUS ÊTES L'ACTEUR/L'ACTRICE



ACTION !

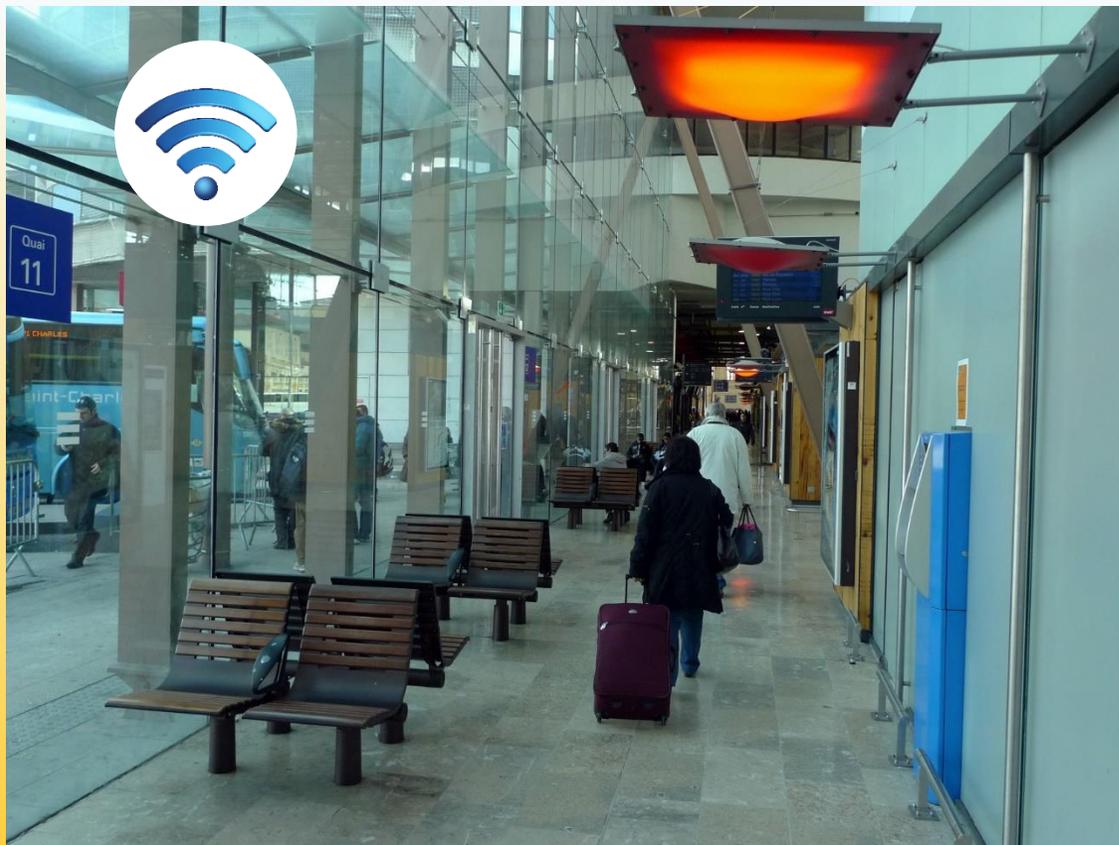


Objectifs :

- Vérifier ses bases en cybersécurité
- Montrer l'intérêt du Wiki
- Développer le collaboratif
- Sensibiliser au partage des ressources



Continuer

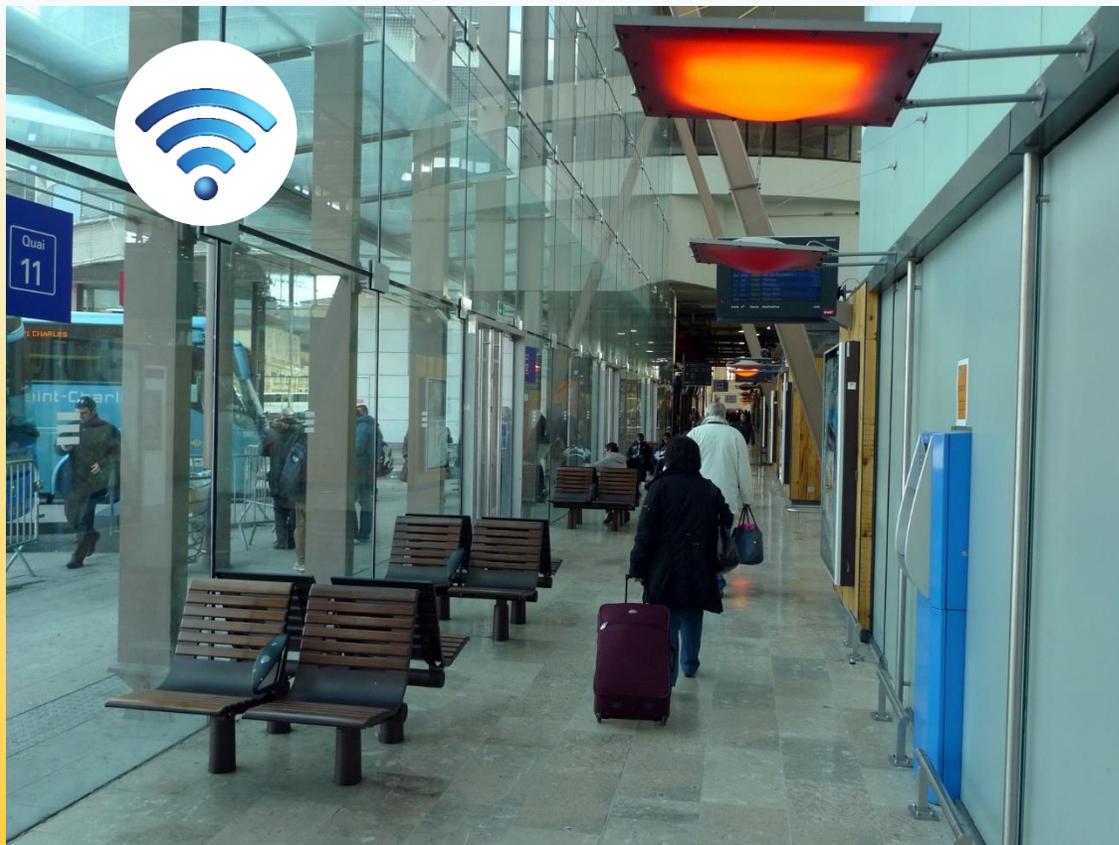


Je suis en train d'attendre mon bus. J'ai épuisé le crédit internet de mon forfait téléphonique et, pour passer le temps, je souhaite aller sur mon réseau social favori.

Il y a un point d'accès Wi-Fi gratuit à la gare SNCF, à 5 minutes de là. Chic ! Je décide de m'y rendre.



Continuer



Je me connecte au réseau, puis **je lance un navigateur en mode privé et je m'apprête à m'authentifier avec mon mot de passe pour accéder à mon profil.**

Est-ce sans risque ?

OUI

NON



Il y a pourtant un risque. De quoi est-ce que je prends l'option d'être la cible ?

Une attaque de l'Homme du milieu (MITM)

Une attaque par hameçonnage

Une attaque par déni de service distribué (DDOS)

[Pour en savoir plus](#)



+1

C'est exact ! Et de quoi est-ce que je prends particulièrement le risque d'être la cible ?

Une attaque de l'Homme du milieu (MITM)

Une attaque par hameçonnage

Une attaque par déni de service distribué (DDOS)

[Pour en savoir plus](#)

En fait, voici ce à quoi je suis confronté.e



Attaque de l'homme
du milieu

attaque qui a pour but **d'intercepter les communications et transmissions de données** entre deux parties, sans que ni l'une ni l'autre ne puisse s'en douter



[Pour en savoir plus](#)



+1

Bien vu !



Attaque de l'homme
du milieu

attaque qui a pour but **d'intercepter les communications et transmissions de données** entre deux parties, sans que ni l'une ni l'autre ne puisse s'en douter



[Pour en savoir plus](#)





Y a-t-il une façon de protéger mes données tout en naviguant sur ce genre de réseau ?

Non, il vaut mieux éviter de naviguer sur les réseaux publics en général.

Oui, je peux utiliser un VPN.

Oui, en protégeant mes comptes par un mot de passe très robuste.

[Pour en savoir plus](#)

Il y a toujours un moyen sûr : via un réseau privé.



Se méfier des Wi-fi publics en accès libre qui peuvent être de faux points internet créés par des pirates



Ne pas transmettre d'informations personnelles ou sensibles via des réseaux non sécurisés



Privilégier les **réseaux sécurisés avec un mot de passe** ou utiliser un **réseau privé virtuel (VPN)**

[Pour en savoir plus](#)



+1

Exact !



Se méfier des Wi-fi publics en accès libre qui peuvent être de faux points internet créés par des pirates



Ne pas transmettre d'informations personnelles ou sensibles via des réseaux non sécurisés



Privilégier les **réseaux sécurisés avec un mot de passe** ou utiliser un **réseau privé virtuel (VPN)**

[Pour en savoir plus](#)



Finalement, je n'ai décidé de consulter que des sites de résultats sportifs, d'actualité, de mode et de mes prochains plans du week-end, sans me connecter à un compte personnel.

Une fois rentré.e chez moi, je vois que n'ai plus de batterie sur mon téléphone et mon chargeur est introuvable.

Je me connecte alors à mon réseau social préféré depuis l'ordinateur commun, car je ne vis pas seul.e (avec ma famille, un.e conjoint.e ou un.e colocataire).

Sauf qu'aucun des contacts à qui je souhaitais parler n'est en ligne en ce moment. Pas grave, j'ai d'autres possibilités en attendant.



**Afficher les
possibilités**

Y a-t-il quelque chose que je n'ai pas encore fait ?

Vérifier mes mails

Voir les offres pour un
nouveau téléphone
(le mien est défectueux)

Regarder un film en
streaming

J'ai fini !

Me voilà sur ma messagerie. J'ai reçu un mail m'informant de mises à jour à faire sur mon compte Instagram. Ce mail contient le logo **Instagram** et comporte une pièce jointe.



Ouvrir le mail



Instagram <serviceusager@mail-instagram.com>

À : [REDACTED]

Madame, Monsieur,

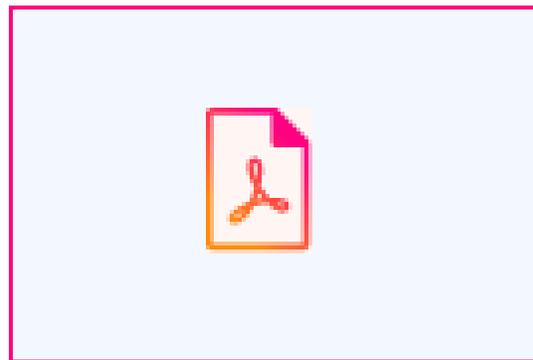
Pour des raisons de sécurité, suite à la modification de la politique des données d'Instagram, il vous est demandé de mettre à jour vos coordonnées personnelles et votre mot de passe.

Veuillez pour cela utiliser [le lien suivant](#) ou le formulaire en pièce jointe.

En cas de refus de votre part, nous serons contraint de procéder à la fermeture de votre compte.

Respectueusement.

Le service d'assistance d'Instagram.



Formulaire.exe

71.5kB



Fermer le mail



Quelle est la meilleure réaction que je puisse avoir dans cette situation ?

J'ouvre la pièce jointe pour en savoir plus

Je me contente simplement de télécharger la pièce jointe sans l'ouvrir ni cliquer sur le lien. On verra plus tard.

Je ne fais rien et je me connecte directement sur mon compte

Je clique sur le lien pour en savoir plus

Il vaut mieux éviter !
Comment appelle-t-on ce genre de fraude ?

Une injection SQL

Une tentative de
rançonnage

Une tentative de phishing
(hameçonnage)

[Pour en savoir plus](#)



+1

Exact ! Et comment appelle-t-on ce genre de fraude ?

Une injection SQL

Une tentative de rançonnage

Une tentative de phishing (hameçonnage)

[Pour en savoir plus](#)

Et non ! Voici la bonne réponse :



Phishing
(hameçonnage)

= récupération de données personnelles par mail via une usurpation d'identité



[Pour en savoir plus](#)



+1

Exact ! Et comment appelle-t-on ce genre de fraude ?



Phishing
(hameçonnage)

=

récupération de données personnelles par mail via une usurpation d'identité



[Pour en savoir plus](#)





Instagram <serviceusager@mail-instagram.com>

À : [Redacted]

Adresse incorrecte et mail non nominatif

Fautes grammaticales et orthographiques

Madame, Monsieur,

Pour des raisons de sécurité, suite à la modification de la politique des données d'Instagram, il vous est demandé de mettre à jour vos coordonnées personnelles et votre mot de passe.

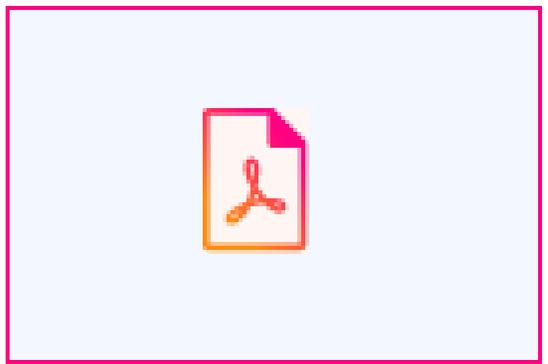
Veuillez pour cela utiliser [le lien suivant](#) ou le formulaire en pièce jointe.

En cas de refus de votre part, nous serons contraint de procéder à la fermeture de votre compte.

Ton pressant

Pièce jointe suspecte ('.exe' est un format logiciel et non de texte)

Respectueusement.



Formulaire.exe

71.5kB

stagram.

Voici les indices qui doivent m'inciter à la prudence !

., 1601 Willow Road, Menlo Park, CA 94025
[Redacted] et était destiné à
voie des mises à jour comme celle-ci
nouveauités. Vous pouvez vous en
votre e-mail s'il ne s'agit pas de votre
[cliquez-vous](#) ou [supprimez votre e-mail](#) de
votre compte.

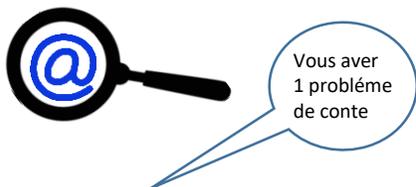




Faire **attention** lorsqu'un mail me demande des **données personnelles ou sensibles**



Si un **mail suspect** provient d'un de mes **contacts**, l'**appeler** ou lui **envoyer un message** (autre que par la boîte mail)



Vérifier l'adresse de l'expéditeur, le **style de rédaction**, les **fautes** grammaticales, le **motif du message**



Dans le doute, ne pas cliquer sur les liens et faire attention aux **pièces jointes** (ex: un fichier intitulé « formulaire » ...qui se termine par .exe)

[Pour en savoir plus](#)



Je reçois un mail m'informant que des photos Facebook où je suis tagué.e sont disponibles. Le mail contient un lien sur lequel je clique. J'arrive sur la page de Facebook où on me demande de saisir mon identifiant et mon mot de passe. Le site web possède un cadenas et l'inscription **https** à côté de la barre d'adresse.



Cliquez pour
afficher la page

facebook

Avec Facebook, partagez et restez en contact avec votre entourage.

Continuer

Adresse e-mail ou numéro de tél.

Mot de passe

Se connecter

[Mot de passe oublié ?](#)

Créer nouveau compte

Créer une Page pour une célébrité, une marque ou une entreprise.

Est-ce que j'accepte de saisir mon identifiant et mon mot de passe sur le site web ?

Non, ce n'est peut-être pas une bonne idée.

Oui, car c'est selon toute vraisemblance la page officielle du site.

Oui, car c'est sécurisé: il y a le symbole du cadenas et l'adresse commence par https.

En fait, ce n'est pas prudent !
Quel indice, si je fais une recherche rapide, peut me
laisser penser que cette page est frauduleuse?

Les couleurs de la page

Les fautes d'orthographe

Le nom de domaine dans la
barre d'adresse



Revoir la page

+1

Bien vu ! Quel indice, si je fais une recherche rapide, peut me laisser penser que cette page est frauduleuse?

Les couleurs de la page

Les fautes d'orthographe

Le nom de domaine dans la
barre d'adresse



Revoir la page

Voici en réalité ce qui doit attirer mon attention :

Voici l'adresse de la page qui s'affiche :

  <https://fr.fr.facebook.com>



LA
DIFFÉRENCE
EST SUBTILE,
PAS VRAI ?

Voici l'adresse de la page officielle du site :

  <https://fr-fr.facebook.com>



+1

Tu es très observateur (observatrice) !

Voici l'adresse de la page qui s'affiche :

  <https://fr.fr.facebook.com>



Voici l'adresse de la page officielle du site :

  <https://fr-fr.facebook.com>



LA DIFFÉRENCE EST SUBTILE, PAS VRAI ?



Comment appelle-t-on ce genre de fraude ?

De l'IP tracking

Une tentative
d'URL spoofing

Une tentative d'espionnage

[Pour en savoir plus](#)

En fait, le nom exact est :



Spoofing
(usurpation)

=

récupération de données personnelles via un faux site qui imite un service connu (l'adresse peut être très proche du site original)



[Pour en savoir plus](#)



+1

Bravo !



Spoofing
(usurpation)

=

récupération de données personnelles via un faux site qui imite un service connu (l'adresse peut être très proche du site original)



[Pour en savoir plus](#)



 <https://fr-fr.facebook.com> <https://www.gouvernement.fr/>

- **Faire attention en tapant l'url** d'un site car une faute de frappe peut nous renvoyer vers une page malveillante avec une adresse qui en imite l'officielle.
Un seul caractère manquant ou différent peut tout changer.
- Vérifier la **présence** du **https** et du **cadenas** en début d'adresse.
- Vérifier notamment **la fin (.fr, .com, .org)** (*par exemple, l'url d'un site gouvernemental finissant par .org et non .fr*)

[Pour en savoir plus](#)



Comme mon téléphone fonctionne de plus en plus mal, je décide d'en acheter un d'occasion sur Le Bon Coin. Je me crée un compte et, pour gagner du temps, j'envisage d'utiliser le mot de passe de mon compte Facebook pour le sécuriser.

Un même mot de passe peut-il être utilisé pour **plusieurs services** (boîtes mail, réseaux sociaux, banque, site de e-commerce, administrations...) ?

Oui, quand les services n'ont rien à voir les uns avec les autres

Oui, mais uniquement si le mot de passe est assez long (15 caractères)

Oui, mais uniquement si le mot de passe contient des caractères spéciaux

Non, chaque service doit avoir un mot de passe différent

En réalité, si j'utilise toujours le même mot de passe je risque...

Au pire, de provoquer une fuite de données (les miennes en l'occurrence).

Au pire, de perdre l'accès à un ou plusieurs de mes comptes personnels.

Les deux.

[Pour en savoir plus](#)



+1

Bien vu ! Mais au fait, qu'est-ce que je risque en utilisant toujours le même mot de passe ?

Au pire, de provoquer une fuite de données (les miennes en l'occurrence).

Au pire, de perdre l'accès à un ou plusieurs de mes comptes personnels.

Les deux.

[Pour en savoir plus](#)

Oui, mais pas que...



UN MÊME MOT DE PASSE RÉUTILISÉ PARTOUT, C'EST COMME UN TROUSSEAU DE CLÉS : SI QUELQU'UN DE MALVEILLANT LE RÉCUPÈRE, IL POURRA OUVRIR TOUS LES ACCÈS À CE QUE JE POSSÈDE (COMPTES, DONNÉES PERSO)

Il faut donc penser à en choisir un différent pour chaque site ou application.

[Pour en savoir plus](#)



+1

C'est tout à fait juste !



UN MÊME MOT DE PASSE RÉUTILISÉ PARTOUT, C'EST COMME UN TROUSSEAU DE CLÉS : SI QUELQU'UN DE MALVEILLANT LE RÉCUPÈRE, IL POURRA OUVRIR TOUS LES ACCÈS À CE QUE JE POSSÈDE (COMPTES, DONNÉES PERSO)

Il faut donc penser à en choisir un différent pour chaque site ou application.

[Pour en savoir plus](#)



En allant sur un site de streaming gratuit, j'ai ouvert involontairement un onglet et un message bloquant mon ordinateur est apparu, signalant un problème technique grave, un risque de perdre mes données et la présence de virus.

Que faire dans ce genre de situation ?



Cliquez pour
afficher le message

** Windows Warning Alert **

** VOTRE ORDINATEUR A ÉTÉ BLOQUÉ **

Téléphone: 04-65-43-00-13

Erreur # DW6VB36

Nous vous prions de nous appeler immédiatement au: 04-65-43-00-13
Ne pas ignorer cette alerte critique.
Si vous fermez cette page, votre accès à l'ordinateur sera désactivé pour
éviter d'autres dommages à notre réseau.

Notre ordinateur nous a alerté qu'il A été infecté par un virus et un
spyware. Les informations suivantes sont volées...

Facebook Login

- > détails de carte de crédit
- > compte e-mail de connexion
- > Photos stockées sur cet ordinateur

Vous devez nous contacter immédiatement afin que nos ingénieurs
peuvent vous guider à travers le processus de suppression par
téléphone. Veuillez nous appeler dans les 5 prochaines minutes pour
éviter que votre ordinateur ne soit désactivé.

En attente de 9evrecalltodaz.tk...

Authentication requise



Le site <http://9evrecalltodaz.tk> demande un nom d'utilisateur et un mot de passe. Le site indique : « Security Update Error 0xB1983959 Help Desk: 04-65-43-00-13 (TOLL-FREE) »

Utilisateur :

Mot de passe :

Annuler

OK

**Fermer le
message**

Que faire dans ce genre de situation ?

Ne rien faire

Tenter de redémarrer mon ordinateur et, si le problème persiste, demander de l'aide à un ami

Contactez le support technique au numéro indiqué sur le message d'erreur

Il y a une meilleure option ! Au fait, que m'arrive-t-il exactement ?

On tente de m'escroquer.

Je suis victime d'un logiciel de rançonnage (ransomware).

On tente de prendre le contrôle de mon ordinateur.

[Pour en savoir plus](#)



+1

C'est une bonne décision !
Mais que m'arrive-t-il exactement ?

On tente de
m'escroquer.

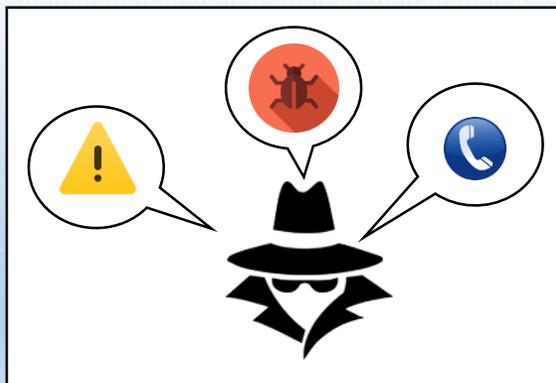
Je suis victime d'un
logiciel de rançonnage
(ransomware).

On tente de prendre le
contrôle de mon ordinateur.

Pour en savoir plus



En fait, il s'agit d'une fraude :



**Arnaque au
faux support
technique**

= attaque **faisant croire** à un utilisateur **que sa machine rencontre un problème** (infection, défaillance technique) afin de lui **faire payer un faux service**

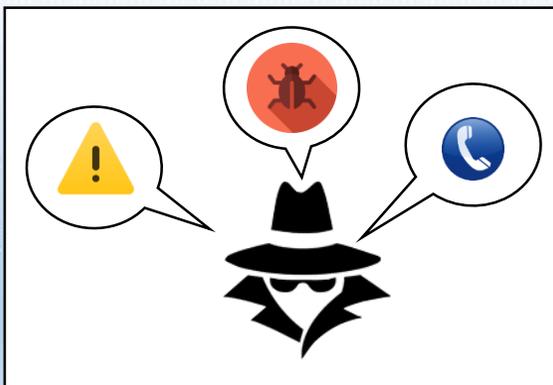


[Pour en savoir plus](#)



+1

Gagné !



**Arnaque au
faux support
technique**

=

attaque **faisant croire** à un utilisateur **que sa machine rencontre un problème** (infection, défaillance technique) afin de lui **faire payer un faux service**



Pour en savoir plus





Dans ce genre de situation, il ne faut en aucun cas appeler de numéro, ni, à plus forte raison, verser de paiement.



En général, redémarrer sa machine ou son navigateur web (en fermant l'onglet bloquant avant qu'il ne s'affiche de nouveau) suffit à régler le problème.



Si le problème persiste, ne pas hésiter à demander de l'aide autour de soi.

Pour en savoir plus





J'ai terminé ce que j'avais à faire. Je m'apprête à laisser la place sur l'ordinateur commun, où précisons-le, il n'y a qu'une session unique, accessible à tous.

Je peux encore faire preuve de plus de prudence.

J'ai une connexion sécurisée, j'ai utilisé des mots de passe solides et variés, je ne suis pas tombé dans le piège des arnaques. J'assume contre tout.

En réalité, même quand je ne suis pas en ligne, il y a toujours un risque.





+1

Mais oui ! C'est exact !



Effacer l'historique récent

Intervalle à effacer : la dernière heure ▾

Historique

Historique de navigation et des téléchargements Cookies

Connexions actives Cache

Historique des formulaires et des recherches

Données

Paramètres de site Données de sites web hors connexion

QUAND JE NAVIGUE DEPUIS UN ORDINATEUR UTILISÉ PAR PLUSIEURS PERSONNES, J'ESSAYE AUSSI DE NE PAS LAISSER MES DONNÉES PERSOS À PORTÉE DES AUTRES.

Je pense à me déconnecter de mes profils et à vider mon historique de navigation (caches, cookies, mots de passe enregistrés, etc.)



C'est le moment de compter mes points !

J'ai moins de 7 points !

J'ai entre 7 et 10 points !

J'ai entre 11 et 13 points !



Visiblement je viens de trouver la meilleure raison de me sensibiliser un peu à la cybersécurité ou revoir mes bases et tant qu'à faire, partager le concept autour de moi. En tout cas, je sais que j'ai tout ce qu'il faut dans les ressources CNFS pour bien démarrer. Je ne peux que progresser, c'est ça qui est chouette !

**UN DERNIER
MOT...**



Franchement pas mal ! Mes petits réflexes m'ont certainement déjà rendu service au quotidien. Je peux même encore m'améliorer et continuer à apprendre quelques notions, de temps à autres. J'ai sûrement une belle marge de progression devant moi !

**UN DERNIER
MOT...**



Les bases de la cybersécurité et moi ça fait un ! Je peux compliquer la tâche aux cybercriminels. Je sais me documenter et utiliser intelligemment les ressources disponibles. Et pourquoi ne pas ajouter mes propres connaissances sur Mednum42 ?

**UN DERNIER
MOT...**

**LA CYBERSÉCURITÉ N'EST PAS QUELQUE CHOSE DE
RÉSERVÉ AUX EXPERTS: CE SONT AVANT TOUT DES
PETITS RÉFLEXES À ADOPTER POUR BIEN PROTÉGER MON
SYSTÈME INFORMATIQUE.**



**MERCI D'AVOIR PARTICIPÉ À CE JEU DE RÔLE !
MAIS VOUS RESTEZ ENCORE ACTEUR/ACTRICE
DANS VOTRE QUOTIDIEN.**



Un dernier mot avant de se quitter...



La licence CC-by-nc-sa 4.0 permet toute exploitation de l'oeuvre (partager, copier, reproduire, distribuer, communiquer, réutiliser, adapter) par tous moyens, sous tous formats. Toutes les exploitations de l'oeuvre ou des œuvres dérivées, sauf à des fins commerciales, sont possibles.



**Le partage de ce document est autorisé
en respectant les conditions suivantes :**

- > *citer l'auteur mentionné ci-contre*
- > *pas de modifications*
- > *pas de commercialisation*

Pierre MARGET

Conseiller Numérique en cybersécurité

Contact: 06 11 32 54 98

pierre.marget@loire.fr

Département de la Loire

Dir. Déléguée Stratégie et Modernisation de
l'Action Publique

Transition Numérique

3 rue Charles-de-Gaulle 42000 Saint-Étienne

**VOUS POUVEZ QUITTER
À PRÉSENT ! À BIENTÔT !**

Le jeu de rôle se présente de la manière suivante :

Je me retrouve dans plusieurs situations pour lesquelles je suis en train d'utiliser le numérique et internet avec un risque de sécurité.

J'ai à chaque fois le choix entre plusieurs réponses, une seule est juste :

- si je clique sur la bonne réponse, je marque 1 point
- si je choisis une mauvaise réponse, je ne marque aucun point

À la fin, je vois mon score et j'évalue mon niveau de base en cybersécurité.





C'est parti !

facebook

Avec Facebook, partagez et restez en contact avec votre entourage.

Continuer

Adresse e-mail ou numéro de tél.

Mot de passe

Se connecter

[Mot de passe oublié ?](#)

Créer nouveau compte

Créer une Page pour une célébrité, une marque ou une entreprise.

facebook

Avec Facebook, partagez et restez en contact avec votre entourage.

Continuer

Adresse e-mail ou numéro de tél.

Mot de passe

Se connecter

[Mot de passe oublié ?](#)

Créer nouveau compte

Créer une Page pour une célébrité, une marque ou une entreprise.