

# SAYNA

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 – Un peu plus de sécurité, on n'en a jamais assez

1. Introduction à la sécurité sur Internet
2. Créer des mots de passe forts
3. Fonctionnalité de sécurité de votre navigateur
4. Eviter le spam et le phishing
5. Comment éviter les logiciels malveillants
6. Achats en ligne sécurisés
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 à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

1/

Réponse 1

Voici les articles que nous avons retenu avec les mots-clés « sécurité sur internet » et « comment être en sécurité sur internet » :

- Article 1 = ANSSI- Dix règles de base
- Article 2 = Economie.govv-Comment assurer votre sécurité numérique
- Article 3 = Site W-Naviguez en toute sécurité sur Internet
- Article bonus = wikiHow-Comment surfez en sécurité sur internet

Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

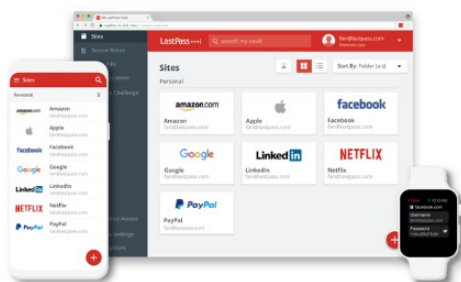
2/ Créer des mots de passe forts

1/ Utilisation de LastPass :

LastPass...<sup>®</sup>

**Un mot de passe.  
Zéro souci.**

| LastPass s'occupe du reste.



Créer un compte

ou [Connexion](#)

Adresse e-mail

Mot de passe maître



Force

Confirmer votre mot de passe Maître



Indice (facultatif)

Inscrivez-vous - c'est gratuit

Réduire

Tous les éléments

Centre de partage

Mots de passe

Notes

Adresses

Cartes de paiement

Tableau de bord de sécurité

Accès d'urgence

Paramètres du compte

Options avancées

Aide

30 jours d'essai restants.

Mettre à niveau

LastPass

rechercher dans mon coffre-fort

rakotondratafikarija...  
Utilisateur d'essai Premium

## Bienvenue dans LastPass, rakotondratafikarijanomena

Tout pour votre vie en ligne – mots de passe, cartes de paiement, comptes bancaires, identifiants et bien plus encore – au même endroit.

Commençons à organiser votre coffre-fort.

Importer beaucoup de mots de passe à la fois vers LastPass

Ajouter des éléments un par un

### Kit de démarrage

(1) novice

(5) expérimente

(10) pro

1/10

Ces 10 réussites vous feront gagner 10 % sur le prix de l'abonnement !

Ajoutez votre premier mot de passe

Laissez LastPass le mémoriser pour vous

Essayez le remplissage automatique

Épargnez-vous la peine de saisir des mots de passe et autres données

Visitez votre coffre-fort LastPass

Afficher toutes les réussites

## Extensions

### Accès total

Ces extensions peuvent voir et modifier des informations sur ce site.

- |  |                               |  |  |
|--|-------------------------------|--|--|
|  | Adblock Plus - bloqueur d...  |  |  |
|  | AdBlock — le meilleur blo...  |  |  |
|  | Adobe Acrobat : outils de...  |  |  |
|  | Bloqueur de publicité grat... |  |  |
|  | Enregistrer dans Google Dr... |  |  |
|  | IDM Integration Module        |  |  |
|  | LastPass: Free Password M...  |  |  |
|  | Visi LastPass                 |  |  |

TOUS LES ÉLÉMENTS

Ajouter un mot de passe

URL:

https://www.linkedin.com/mynetwork/

Nom:

Dossier:

Nom d'utilisateur:

rakotondratafikarijanomena@gmail.com

Mot de passe du site:

Notes:

Paramètres avancés:

Annuler

Enregistrer

LastPass

rechercher dans mon coffre-fort

rakotondratafikarija...  
Utilisateur d'essai Premium

Tous les éléments

Trier par: Dossier (a-z)

Amazon

Coordonnées de contact

facebook

Facebook

Retour

Ajoutez au moins 3 sites web  
Plus vous en ajouterez, moins vous devrez en mémoriser

2/3 sites web déjà ajoutés  
Pensez à ajouter des sites web souvent utilisés.  
Gagnez du temps, chaque jour.

Google

Facebook

LinkedIn

PayPal

Dropbox

### 3 - Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

#### 1/ Réponse 1

Les sites web qui semblent être malveillant sont :

- [www.morvel.com](http://www.morvel.com) un dérivé de [www.marvel.com](http://www.marvel.com) ,le site web officiel de l'univers marvel
- [www.fessebook.com](http://www.fessebook.com), un dérivé de [www.facebook.com](http://www.facebook.com) , le plus grand réseau social au monde
- [www.instagram.com](http://www.instagram.com) , un dérivé de [www.instagram.com](http://www.instagram.com) , un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

- [www.dcomics.com](http://www.dcomics.com) , le site officiel de l'univers DC Comics
- [www.ironman.com](http://www.ironman.com) , le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2/

Vérification de mise à jour

#### 1- Pour Chrome

À propos de Chrome



Google Chrome

© 2024 Google LLC. Tous droits réservés.

Chrome fonctionne grâce au projet Open Source [Chromium](https://chromium.org/) et à d'autres [logiciels libres](#).

[Conditions d'utilisation](#)

## 2- Pour Firefox

Conservez Firefox à jour pour bénéficier des dernières améliorations de stabilité et de sécurité.

Version 122.0.1 (32 bits) [Notes de version](#)

😊 Firefox est à jour

Autoriser Firefox à

☒ Installer les mises à jour automatiquement (recommandé)

☒ Quand Firefox n'est pas lancé

#### 4 – Eviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux



Bon travail, rija  
nomena !  
Vous avez obtenu un  
score de 6/8.

Plus vous vous entraînez, mieux vous saurez identifier les  
pièges et vous protéger des tentatives d'hameçonnage.

Quelques mesures très simples à mettre en place peuvent  
également améliorer la protection de vos comptes en ligne.  
Pour plus d'informations, consultez la page [g.co/2SV](https://g.co/2SV).

**Partager le questionnaire :**



5- Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites.

Réponse 1

3- <https://www.amazon.fr/>

1. Indicateur de sécurité

https

amazon.fr



La connexion est sécurisée

2. Analyse google

Google Transparence des informations

Présentation

État d'un site

## État du site selon la navigation sécurisée

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysées chaque jour afin de détecter les sites Web suspect. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous s'ensuivent ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site particulier présente un danger.

Vérifier l'état du site

<https://www.amazon.fr/>

4- <https://www.leboncoin.fr/>

1. Indicateur de sécurité

https

leboncoin.fr



La connexion est sécurisée

## 2. Analyse google

### Vérifier l'état du site

<https://www.leboncoin.fr/>

État actuel

✓ Aucun contenu suspect détecté

5- <https://www.playstation.com/fr-fr/>

1. Indicateur de sécurité

https

playstation.com



La connexion est sécurisée



Voir les détails de la connexion



Cookies et données des sites



Paramètres des sites



À propos de cette page



En savoir plus sur sa source et son thème

## 2. Analyse google

### Vérifier l'état du site

<https://www.playstation.com/fr-fr/>

État actuel

✓ Aucun contenu suspect détecté

## 6/ Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

Voici mes libellés

### Nouveau libellé



Entrez le nom du nouveau libellé :

ACHAT

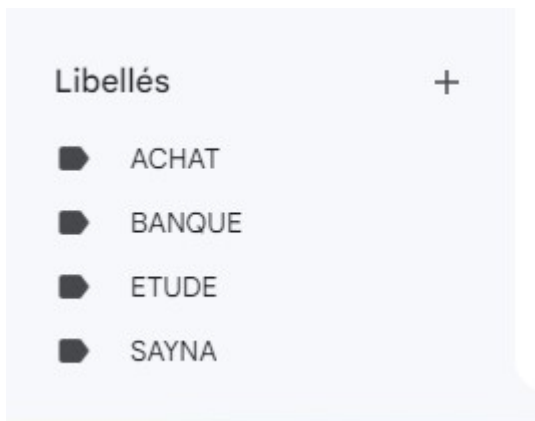
☐ Imbriquer le libellé sous :

Annuler

Créer

Libellés	Afficher dans la liste des libellés	Afficher dans la liste des messages	Actions
<a href="#">Nouveau libellé</a>			
ACHAT 0 conversation	<a href="#">afficher</a> <a href="#">masquer</a> <a href="#">afficher si non lus</a>	<a href="#">afficher</a> <a href="#">masquer</a>	<a href="#">supprimer</a> <a href="#">modifier</a>
BANQUE 0 conversation	<a href="#">afficher</a> <a href="#">masquer</a> <a href="#">afficher si non lus</a>	<a href="#">afficher</a> <a href="#">masquer</a>	<a href="#">supprimer</a> <a href="#">modifier</a>
ETUDE 0 conversation	<a href="#">afficher</a> <a href="#">masquer</a> <a href="#">afficher si non lus</a>	<a href="#">afficher</a> <a href="#">masquer</a>	<a href="#">supprimer</a> <a href="#">modifier</a>
SAYNA 0 conversation	<a href="#">afficher</a> <a href="#">masquer</a> <a href="#">afficher si non lus</a>	<a href="#">afficher</a> <a href="#">masquer</a>	<a href="#">supprimer</a> <a href="#">modifier</a>

**Remarque :** La suppression d'un libellé ne supprime pas les messages de ce libellé.



## 7- Comprendre le suivi du navigateur

Objectif :exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

## 8 – Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

### 1/ Réponse 1

Voici mon paramétrage de compte Facebook

## Assistance confidentialité

Nous vous aiderons à prendre les bonnes décisions pour les paramètres de votre compte.  
Par quelle rubrique voulez-vous commencer ?



Qui peut voir ce que vous partagez



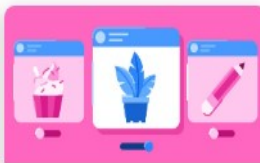
Comment il est possible de vous trouver sur Facebook



Comment protéger votre compte




Les paramètres de vos données sur Facebook



Vos préférences publicitaires sur Facebook

## Stories

Choisissez qui peut voir vos stories. Ces dernières sont visibles pendant 24 heures sur Facebook et Messenger.

 Ami(e)s

## Limiter l'audience des anciennes publications

Changez la confidentialité des publications passées de Public ou Ami(e)s et leurs ami(e)s à Ami(e)s uniquement. Toute personne identifiée dans ces publications et ses amis les verront peut-être encore.

Limiter

Retour

Suivant

## Followers et contenu public

### Qui peut me suivre


Vos followers voient vos publications, reels et stories dans le Fil. Vos amis suivent vos publications, reels et stories par défaut, mais vous pouvez aussi autoriser quiconque ne faisant pas partie de vos amis à suivre vos publications, reels et stories publics. Utilisez ce paramètre pour choisir qui peut vous suivre.

Chaque fois que vous créez ou publiez un reel ou une story, vous choisissez l'audience avec laquelle vous voulez les partager.

Ce paramètre ne s'applique pas aux personnes qui vous suivent sur Marketplace et dans les groupes d'achat et de vente. Vous pouvez gérer ces paramètres sur Marketplace.


 Ami(e)s

### Qui peut voir vos followers sur votre journal ?

 Public


### Qui peut voir les personnes, Pages et listes que vous suivez ?

N'oubliez pas que les personnes que vous suivez le savent.

 Moi uniquement

### Qui peut commenter vos publications publiques ?

Choisissez qui est autorisé à commenter vos publications publiques. Il se peut que les personnes identifiées dedans et leurs amis puissent toujours les commenter. **En savoir plus**

 Public

Vous pouvez mettre à jour cette option sur chaque publication sans affecter les

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

1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé

2/ Proposer un exercice pour installer et utiliser un antivirus+ antimalware en fonction de l'appareil utilisé.

Réponse 1

Si votre matériel est infecté par un virus

- 1- Déconnecter votre ordinateur ou votre appareil du réseau internet
- 2- Analyser avec un logiciel antivirus : scanner et détecter les programmes malveillants .
- 3- Supprimer les programmes suspects , et ou les fichiers suspects sur votre matériel .
- 4- Mettez à jour votre système d'exploitation et vos logiciels : mettez à jours avec les derniers correctifs de sécurité .
- 5- Effectuer des sauvegardes de données si vous n'avez pas encore sauvegardé vos données importantes ,dans des stockages externe ou utiliser des services de sauvegard en ligne comme par exemple (google drive)
- 6- Restaurez les fichiers corrompus à partir de sauvegardes si c'est possible
- 7- Utiliser un pare-feu ou des outils de détection des logiciels malveillant

## Réponse 2

Si vous utilisez un système Windows **authentique** rassurez-vous Windows Defender est un antivirus et un antimalware intégré dans le système d'exploitation Windows. Il offre une protection de base contre les virus, les logiciels malveillants, les logiciels espions et autres menaces potentielles pour les utilisateurs de Windows.

Voici quelques fonctionnalités clés de Windows Defender :

- Protection en temps réel : Windows Defender surveille continuellement votre système pour détecter et bloquer les menaces dès qu'elles sont détectées.
- Analyse complète du système : Vous pouvez effectuer des analyses manuelles sur demande pour rechercher les logiciels malveillants dans l'ensemble de votre système.
- Protection basée sur le cloud : Windows Defender utilise également des analyses basées sur le cloud pour détecter les nouvelles menaces et les signatures de logiciels malveillants.
- Protection contre les programmes potentiellement indésirables (PUP) : Windows Defender peut également détecter et bloquer les programmes potentiellement indésirables qui pourraient compromettre la sécurité de votre système.

Si vous voulez faire une analyse complète vous pouvez suivre ces étapes

Ouvrir Windows Security :

- Cliquez sur le bouton Démarrer de Windows (l'icône Windows dans le coin inférieur gauche de l'écran) et tapez "Sécurité Windows" dans la barre de recherche.
- Sélectionnez l'application "Sécurité Windows" dans les résultats de la recherche pour ouvrir Windows Security.
- Accéder aux options de scan :
- Dans l'interface de Windows Security, cliquez sur "Protection contre les virus et menaces" ou une option similaire, selon la version de Windows que vous utilisez.
- Lancer une analyse complète :
- Dans la section "Protection contre les virus et menaces", recherchez l'option "Analyse des menaces" ou "Analyse des options avancées" et cliquez dessus.
- Ensuite, cliquez sur "Analyse complète" ou "Analyse complète maintenant" pour démarrer une analyse approfondie de votre système.
- Attendez la fin de l'analyse :

Windows Defender commencera à analyser tous les fichiers et dossiers de votre ordinateur pour détecter les menaces potentielles.

L'analyse peut prendre un certain temps en fonction de la taille de votre disque dur et du nombre de fichiers à analyser.

Consultez les résultats :

Une fois l'analyse terminée, Windows Defender vous montrera un résumé des résultats, y compris les éventuelles menaces détectées.

Si des menaces sont détectées, suivez les instructions pour les supprimer ou les mettre en quarantaine.



Voici un exemple de son fonctionnalité :



## Protection contre les virus et menaces

Protection de votre appareil contre les menaces.



### Menaces actuelles

Aucune menace actuelle.

Dernière analyse : Non disponible

Analyse rapide

[Options d'analyse](#)

[Menaces autorisées](#)

[Historique de protection](#)



### Paramètres de protection contre les virus et menaces

Aucune action requise.

[Gérer les paramètres](#)



## Protection contre les virus et menaces

Protection de votre appareil contre les menaces.



### Menaces actuelles

Analyse rapide en cours

Temps restant estimé : 00:03:56

1604 fichiers analysés

Annuler

Vous pouvez continuer à travailler pendant que nous analysons votre appareil.

[Historique de protection](#)



### Paramètres de protection contre les virus et menaces

Aucune action requise.

[Cliquez ici pour modifier les paramètres](#)



## Protection contre les virus et menaces

Protection de votre appareil contre les menaces.



### Menaces actuelles

Aucune menace actuelle.

Dernière analyse : 19/02/2024 16:12 (analyse rapide)

0 menaces trouvées.

L'analyse a duré 4 minutes 15 secondes

49356 fichiers analysés.

Analyse rapide

[Options d'analyse](#)

[Menaces autorisées](#)

[Historique de protection](#)

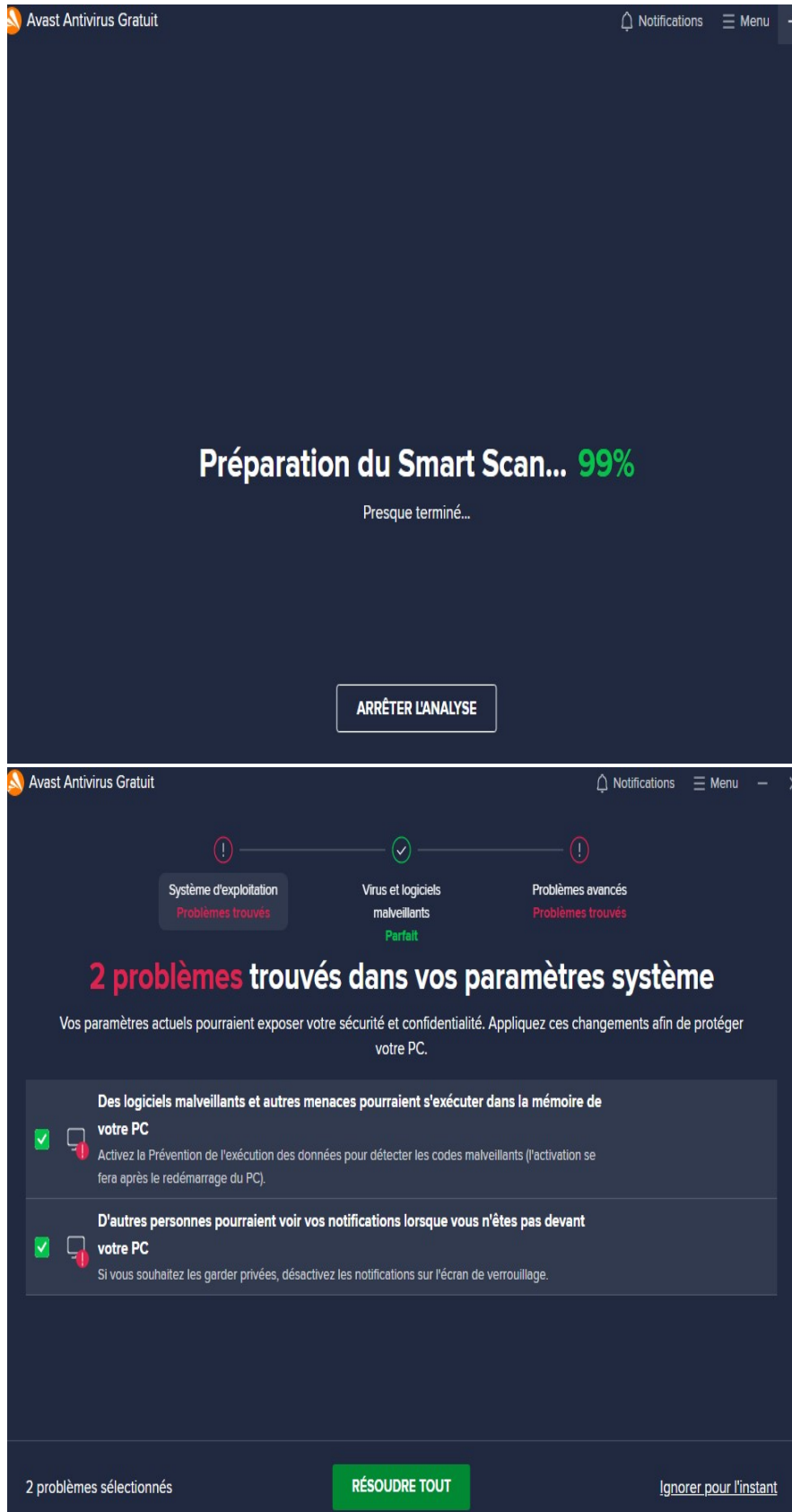
[Paramètres de protection contre les virus et menaces](#)

Bien que Windows Defender offre une protection de base, certains utilisateurs choisissent d'installer des solutions antivirus tierces pour une protection plus avancée et des fonctionnalités supplémentaires comme par exemple l'Avast Free antivirus

Voici quelques caractéristiques d'Avast Free Antivirus :

- 1- Protection antivirus en temps réel : Avast surveille votre système en temps réel pour détecter et bloquer les menaces dès qu'elles sont détectées.
- 2- Analyse de fichiers et de dossiers : Vous pouvez effectuer des analyses manuelles sur demande pour rechercher les logiciels malveillants dans des fichiers spécifiques ou des dossiers particuliers.
- 3- Protection du réseau domestique : Avast propose également une fonction de protection du réseau domestique pour sécuriser votre réseau Wi-Fi contre les intrusions et les attaques potentielles.
- 4- Analyse des vulnérabilités : Il peut également scanner votre système à la recherche de vulnérabilités de sécurité, telles que les logiciels obsolètes ou les paramètres de sécurité non sécurisés.
- 5- Blocage des sites Web malveillants : Avast dispose d'une fonction de blocage des sites Web malveillants qui vous protège contre les sites Web frauduleux et les tentatives de phishing.

Voici un exemple de son fonctionnalité



Avast Antivirus Gratuit

NotificationsMenu

✓

Système d'exploitation  
Tous résolus

✓

Virus et logiciels  
malveillants  
Parfait

!

Problèmes avancés  
Problèmes trouvés

Tout va bien !

Votre configuration est super, vous n'avez rien à craindre !

✓

Des logiciels malveillants et autres menaces pourraient s'exécuter dans la mémoire de votre PC

Activez la Prévention de l'exécution des données pour détecter les codes malveillants (l'activation se fera après le redémarrage du PC).

✓

D'autres personnes pourraient voir vos notifications lorsque vous n'êtes pas devant votre PC

Si vous souhaitez les garder privées, désactivez les notifications sur l'écran de verrouillage.

SUIVANT

Corrigez vos problèmes avancés avec Avast Premium Security

✓ Protégez vos documents sensibles avec l'Agent de données sensibles

✓ Bloquez les attaques de ransomwares avec l'Agent anti-ransomwares

✓ Empêchez les pirates d'accéder à votre PC avec le Pare-feu avancé

✓ Évitez les sites Web frauduleux et sécurisez vos achats et transactions bancaires sur Internet avec Real Site

Abonnement 1 an

1,99 €/mois

Soit 23,88 €/1 an

Abonnement 2 ans

RECOMMANDÉ

1,89 €/mois

Soit 45,36 €/2 ans

Abonnement 3 ans

1,79 €/mois

Soit 64,44 €/3 ans

ACHETER

Garantie satisfait ou remboursé de 30 jours



