PRESENTATION

CYBER

SECURITÉ

LA SÉCURITÉ DES RÉSEAUX SOCIAUX - MESSAGERIE ...

Sommaire du jour

01

Introduction à la Cyber Sécurité

Présentation génerale relative à tout ce qui entoure la Cyber Sécurité.

02

Les Réseaux Sociaux : pour qui, pour quoi

Présentation des différents réseaux sociaux, qu'ils soient professionnels ou personnels.

03

Les principaux réseaux sociaux

Tour d'horizon des principaux réseaux sociaux, pour comprendre leur fonctionnement, comment les paramétrer pour activer leur sécurité au quotidien.

04

Les bonnes habitudes à adopter

Quelles sont les actions à toujours garder en tête pour éviter les actes de malveillance.

05

La messagerie et la Sécurité autour des emails

Présentation de l'outil le plus utilisé sur la planète et comment être paré pour éviter les spams, usurpation d'identité ...

Introduction à la CYBER SECURITÉ

Qui connait ce terme ?

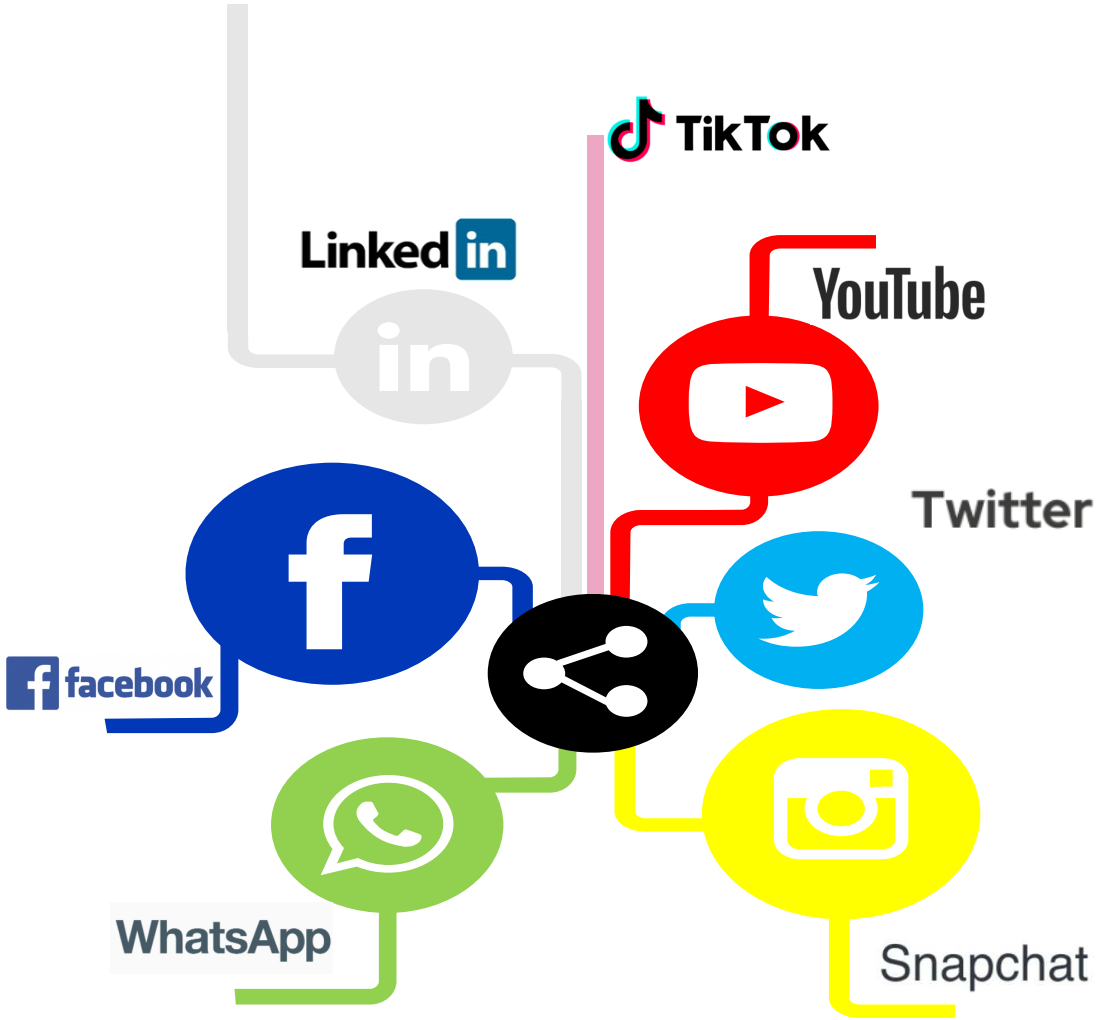
Tout le monde a déja entendu parler de ce terme, nénamoins, peu de gens savent expliquer en détail ce que signifie la Cyber Sécurité.

Signification de Cyber Sécurité

Désigne l'ensemble des outils et des processus de sécurité utilisés pour la protection de l'environnement numérique.

Qu'est –ce que le numérique ?

Représente l'ensemble des ordinateurs, telephones portables, fournisseurs Internet, Logiciels, normes (Wi-Fi, 5g) ...



Les Réseaux Sociaux

Pour qui ? – Pour quoi ?

Le réseau social pro

Les 2 plus connus sont LinkedIn et Viadeo. Ils permettent aux professionnels d'échanger sur leur carrière et d'étoffer leur propre réseau.

Le réseau social perso

Tout le monde en connait un, que ce soit Facebook, Instagram, Twitter, Snapchat...

WhatsApp est plus un outil de communication

Pour qui ?

Pour toute personne connectée a Internet et qui aime l'interaction virtuelle.

Pour quoi ?

Pour partager avec ses amis ou à la planète entière son quotidien de vie, et aussi pour voir, suivre la vie des autres (amis ou non, stars ...)

Les Principaux Réseaux Sociaux

Comment bien les sécuriser - Partie 1

Facebook Instagram Twitter WhatsApp

Pour ces 3 réseaux sociaux, il est important de sécuriser et d'avoir le contrôle sur :
- L' accès à votre compte.
- Qui peut consulter votre profil : vos publications et celles où vos ami(e-s) vous ont identifiée (statuts, photos, vidéos, partages, localisation…).
- Qui peut vous contacter et vous identifier (ajout comme ami(e), messages privés, invitation à des évènements ou à aimer des pages…).
- Les autorisations des applications tierces (ex : jeux en ligne, applications de musique) … peuvent présenter des failles de sécurité importantes et irréversibles.

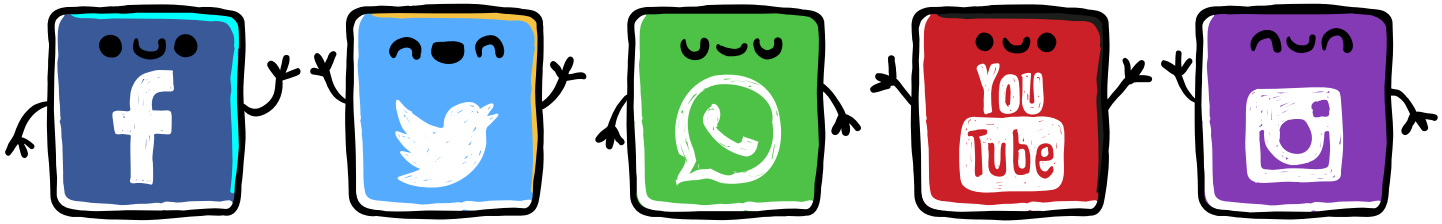
Une personne malintentionnée pourrait essayer :
- D'accéder à votre compte : en connaissant votre mot de passe, en ayant accès à votre boîte mail, via des techniques de *spam* …
- D'usurper votre identité ou d'un ami en créant un faux compte pour demander des informations voire des accès aux personnes que vous connaissez.
- D'utiliser les réseaux sociaux comme moyen de menaces, de diffusions de vos informations personnelles, voire intimes …

WhatsApp est plus une application de messagerie qu'un réseau social. Elle est globalement sécurisée car elle utilise le cryptage des données ce qui veut dire qu'il est très difficile pour une personne malveillante d'intercepter la transmission de vos communications. De plus, elle fonctionne seulement en présence du téléphone lié et ne requiert pas d'identifiant de connexion (qui pourraient être connus par autrui).
Cependant, gardez en tête qu'une personne malintentionnée pourrait avoir accès à vos messages, historiques d'appels, photos, etc., sur WhatsApp si elle parvient à s'introduire sur votre téléphone :
- Soit physiquement (en connaissant le code d'accès de votre téléphone, ou en accédant à un ordinateur synchronisé avec votre compte WhatsApp).
- Soit avec un logiciel espion , qui peut passer outre le cryptage des communications.
- Ou en utilisant la méthode du spam : une personne malveillante peut vous rediriger vers un faux lien afin d'accéder à votre compte (ex : avec un faux QR Code.

Autres points à garder en tête :
- Quelques informations pourraient être publiques : heure de connexion, photo, heure d'ouverture d'un message (« Vu à »)…
- Les conversations WhatsApp en elles-mêmes sont sécurisées, mais pas leur sauvegarde, donc attention à qui accède à votre téléphone.

Les Principaux Réseaux Sociaux

Comment bien les sécuriser - Partie 2



Facebook

Protégez l'accès à votre compte Facebook :
- Renforcez votre mot de passe
- Activez la double authentification même si cela peut être contraignant.
- Activez les alertes en cas de connexion non reconnue.
- Il est conseillé de se déconnecter de son compte après chaque utilisation (plutôt que de fermer la fenêtre) et de décocher l'option « Se connecter automatiquement
- En accédant au compte email associé à votre compte Facebook, quelqu'un peut changer le mot de passe et prendre le contrôle de ce dernier : assurez-vous donc bien que votre compte email est également sécurisé.

Configurez vos paramètres de confidentialité :
- Paramétrez qui peut consulter votre profil, qui peut vous contacter et qui peut vous trouver avec une recherche.
- Contrôlez les publications sur lesquelles on vous identifie
- Pour que l'on ne puisse pas trouver votre profil Facebook en entrant votre nom sur un moteur de recherche, désactivez son référencement.
- Dans les paramètres de votre téléphone, désactivez les services de localisation pour

Instagram

Protégez l'accès à votre compte Instagram :

- Activez la double authentification.
- Il est conseillé de se déconnecter de son compte après chaque utilisation surtout si vous utilisez un appareil partagé ou qui n'est pas le vôtre.
- Configurez vos paramètres de confidentialité : Paramétrez vos publications (photos, vidéos, story) en mode privé pour qu'elles ne soient vues que par vos abonnés.
- Attention, si votre profil était public et que vous le basculez en mode privé, vos potentiels abonnés inconnus auront toujours accès à votre profil.
- Vous pouvez également bloquer un utilisateur afin de l'empêcher de vous contacter, de voir vos publications et de vous suivre.

Twitter

Protégez l'accès à votre compte Twitter :

- Activez la double authentification.

Il est conseillé de se déconnecter de son compte après chaque utilisation

- Protégez vos tweets en passant votre profil en mode privé. Tous vos nouveaux et anciens tweets passeront en mode privé et ne seront vus que par vos abonnés.
- Contrôlez les publications sur lesquelles on vous identifie.
- Désactivez la localisation de vos tweets et de l'application.
- Désactivez la détectabilité de votre compte : cela permet d'empêcher que l'on vous retrouve à partir de votre adresse mail ou de votre numéro de téléphone.

WhatsApp

Protégez l'accès à votre compte WhatsApp :

- Activez la double authentification.
- Si vous utilisez WhatsApp web, n'oubliez pas de vous déconnecter après chaque utilisation.
- Autorisez uniquement vos contacts à voir votre photo de profil, votre actu, votre statut.
- Vous pouvez bloquer toute personne en qui vous n'auriez pas confiance – elle n'en sera pas notifiée mais pourra s'en rendre compte par elle-même.
- Désactivez la sauvegarde des conversations, des photos et des vidéos WhatsApp sur le Cloud
- Si vous avez perdu votre téléphone ou qu'il a été volé, se connecter à partir d'un autre téléphone permettra de se déconnecter de celui qui a été perdu/volé, car WhatsApp n'autorise

Les Bonnes Habitudes à Adopter

VOUS êtes le premier niveau sur l'échelle des vulnérabilités

Double Authentification

Privilégiez les systèmes d'authentification forte (en deux étapes). Les simples mots de passe offrent un faible niveau de sécurité.

Evitez trop de partages intimes

Les parts de vie privée que chacun révèle sur les réseaux sociaux sont autant de matière pouvant être retourné contre soi.

Sauvegarder vos données

En cas de soucis informatique, quel qu'il soit, mieux vaut sauvegarder régulièrement ses fichiers importants, soit sur un disque dur externe, soit dans un cloud.

Ne cliquez pas au hasard

Prenez le temps de lire, de vérifier qui vous contacte, et surtout en cas de doute, attendez ou demandez conseil avant de cliquer sur un lien.

La Messagerie et les Emails

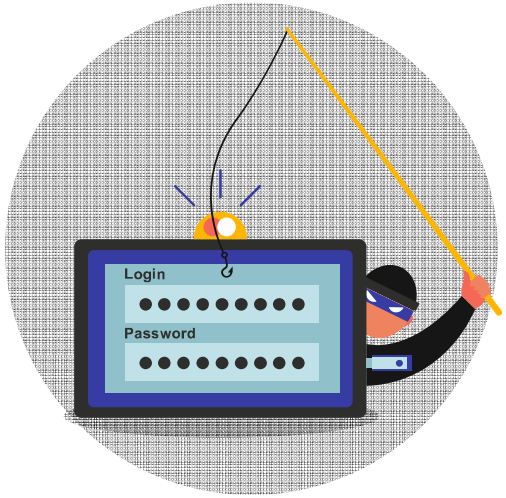
Explications

81%

des fichiers malveillants ont été distribués par e-mail

Securité

Contrairement aux idées reçues, la sécurisation de nos courriers électroniques ne s'arrête pas à l'authentification du compte de notre boîte mail via un mot de passe. D'autres éléments comme le contenu du message ou l'identité de l'expéditeur peuvent également être validés et sécurisés.



Menaces

On parle souvent d'hameçonnage (ou phishing en anglais). Cette technique vise à leurrer l'internaute en se faisant passer pour un tiers de confiance afin de l'inciter à communiquer ses données personnelles ou bancaires. Les spams, les virus et malwares sont des menaces tout aussi redoutées par les utilisateurs de messagerie électronique.

Précautions

Optez pour un mot de passe robuste afin de mieux sécuriser l'accès à votre compte de messagerie.

Soyez toujours vigilant à la réception de nouveaux mails.

Ne répondez jamais à une demande d'informations confidentielles

Dans vos emails, ne cliquez pas sur des liens qui ne vous inspirent pas confiance.

Méfiez-vous des pièces jointes à vos messages, ne répondez jamais aux emails de type pyramide financière ou encore chaîne porte-bonheur. Il s'agit souvent de tentatives d'escroquerie.

Les Bonnes Habitudes avec les Emails

Le piratage de messagerie est la deuxième menace de cyber malveillance la plus courante

- Évitez les mots de passe trop simples et communs à plusieurs comptes
- Utilisez un mot de passe complexe et différent pour chaque compte
- activez la double authentification
- Effectuez les mises à jour de votre client de messagerie régulièrement
- N'ouvrez pas les messages inhabituels, ne cliquez pas a la hâte sur des liens dont vous ne connaissez pas la destination
- Évitez aussi de vous connecter à un ordinateur ou à un réseau Wifi publics, sauf si vous disposez d'un VPN

N'oubliez pas ...

C'est vous qui décidez

Quand vous êtes avec votre ordinateur ou smartphone, vous seuls pouvez juger de ce que vous allez accepter ou pas.

Ne laissez quiconque accéder à vos appareils en dehors de votre présence.

Ne donnez pas votre confiance facilement

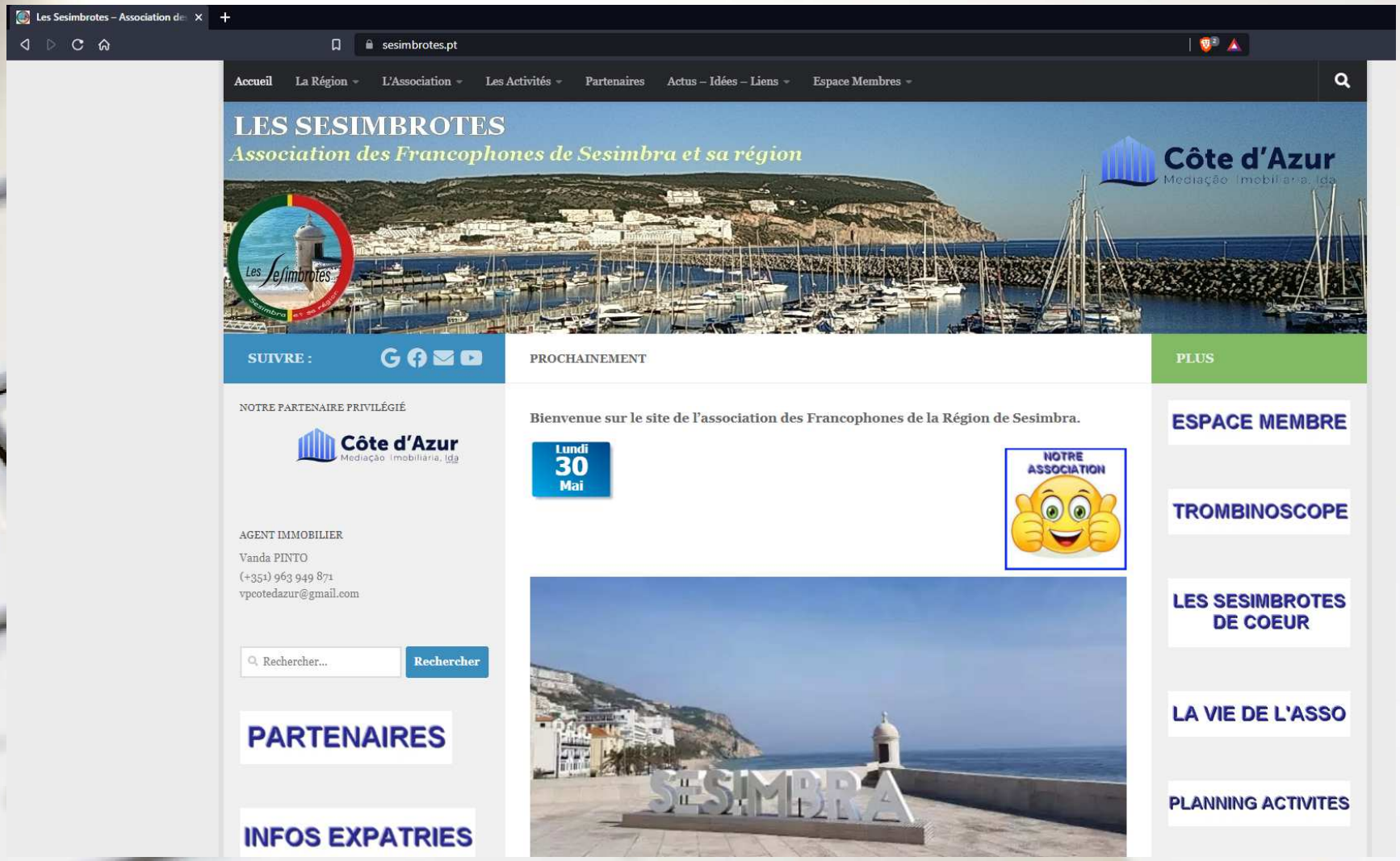
Soyez vigilants sur tout type d'information que l'on peut vous envoyer, rien n'est gratuit, les personnes malveillantes essaieront de vous prendre par les sentiments (guerre, famine ...) ou l'attrait du gain.

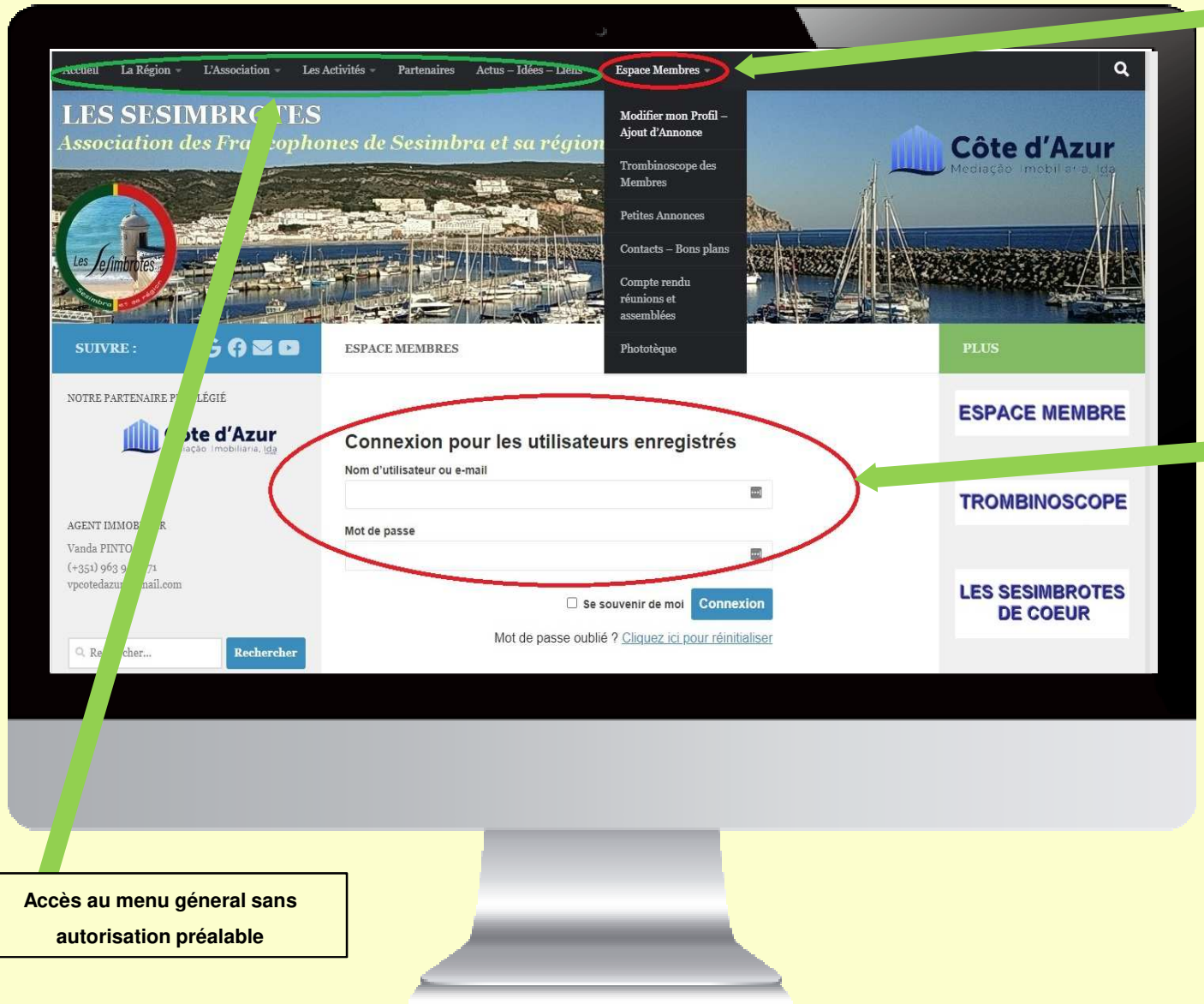
Il n'y a pas de retour possible

Tout acte de malveillance est irréversible, qu'il soit minime ou de grande ampleur. Une fois l'information envoyée et diffusée, il n'y aura pas de retour arrière possible.

https://sesimbrotes.pt

Le Site Internet
des Sesimbrotes

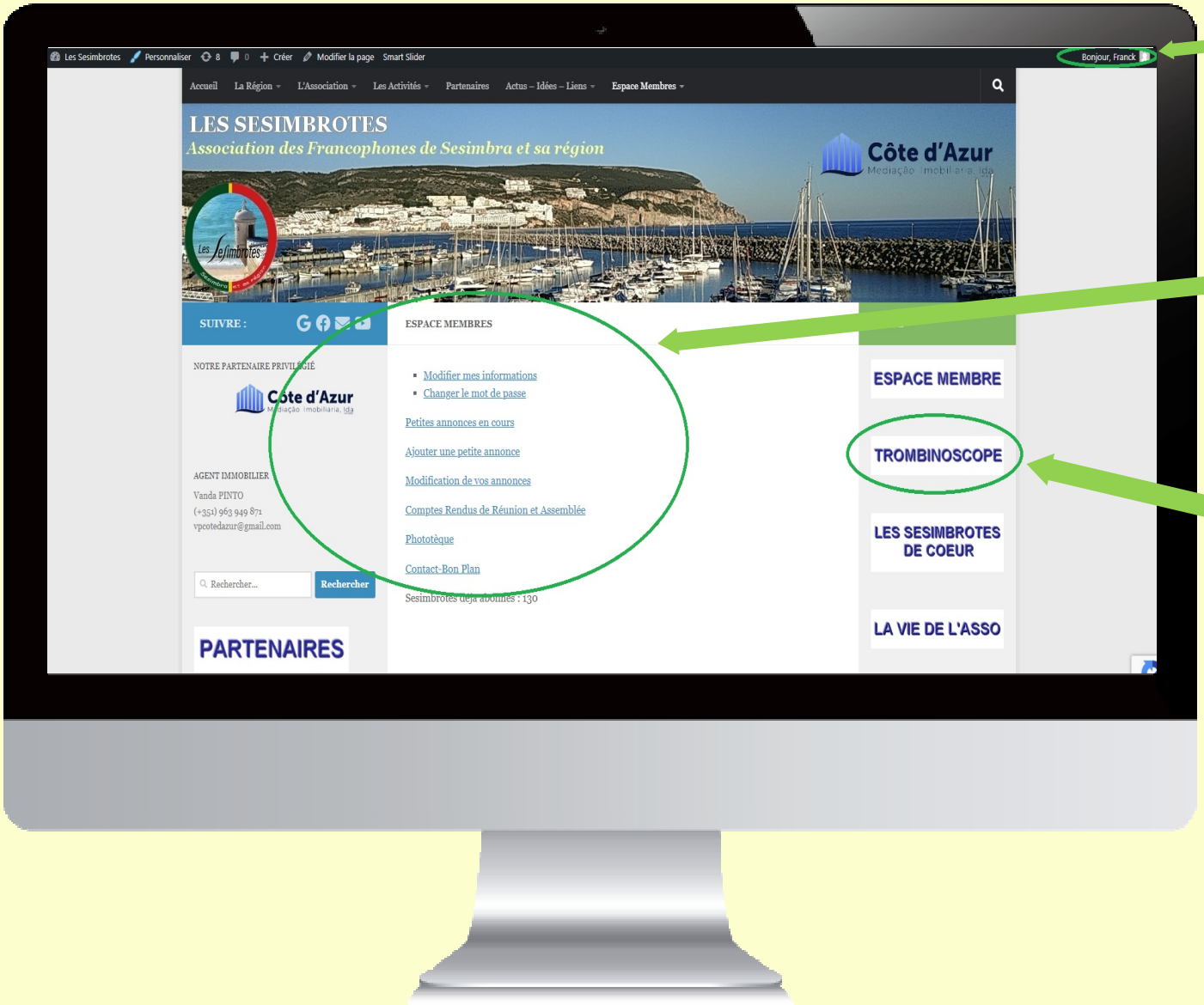




Cliquez sur Espace Membre

Renseignez vos identifiants pour accéder à l'Espace Membre, au Trombinoscope et autres possibilités

Accès au menu géneral sans autorisation préalable



Membre identifié

Accès aux menus membre :

- **Petites annonces**
- **Comptes rendu d'assemblée**
- **Photothèque**
- **…**

Accès au trombinoscope des membres enregistrés

QUESTIONS RÉPONSES