**Procédure de base pour vérifier la sécurité de votre PC**

Pour garantir la sécurité optimale de votre PC et protéger vos données personnelles, il est essentiel de suivre une procédure méthodique de vérification et de renforcement des mesures de sécurité

**Mise à jour du système d'exploitation et des logiciels** :

Assurez-vous que votre système d'exploitation (Windows, MacOs, Linux, etc.) ainsi que tous vos logiciels sont à jour avec les derniers correctifs de sécurité. Vous pouvez vérifier cela dans les paramètres de votre système d'exploitation ou à l'aide d'un outil de mise à jour automatique.

**Analyse antivirus et antimalware** :

Exécutez une analyse complète de votre système à l'aide d'un logiciel antivirus et antimalware réputé. Assurez-vous que votre logiciel de sécurité est également mis à jour avec les dernières définitions de virus.

**Gestion des mots de passe** :

Assurez-vous que vous utilisez des mots de passe forts et uniques pour chaque compte en ligne. Si vous ne l'avez pas déjà fait, envisagez d'utiliser un gestionnaire de mots de passe pour stocker et générer des mots de passe sécurisés.

**Pare-feu :**

Vérifiez que votre pare-feu est activé pour protéger votre PC contre les connexions non autorisées. Vous pouvez vérifier et ajuster les paramètres du pare-feu dans les paramètres de sécurité de votre système d'exploitation.

**Authentification à deux facteurs (2FA) :**

Activez l'authentification à deux facteurs pour les comptes en ligne qui le prennent en charge. Cela ajoute une couche de sécurité supplémentaire en plus du mot de passe.

**Navigation sécurisée :**

Utilisez un navigateur web sécurisé et assurez-vous qu'il est configuré pour bloquer les pop-ups, les téléchargements automatiques et les sites web malveillants. Vous pouvez également envisager d'installer des extensions de sécurité telles que bloqueurs de publicités et bloqueurs de scripts.

**Réseaux Wi-Fi :**

Assurez-vous que votre réseau Wi-Fi domestique est sécurisé avec un mot de passe fort et utilisez le cryptage WPA2 ou WPA3 si possible. Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés lorsque vous effectuez des opérations sensibles.

**Sensibilisation à la sécurité :**

Éduquez-vous sur les pratiques de sécurité informatique et restez informé des menaces actuelles. Soyez conscient des techniques de phishing et des escroqueries en ligne, et ne partagez jamais d'informations sensibles avec des sources non fiables.