10 conseils pour garantir son anonymat en 2023

Internet et les réseaux sociaux peuvent être utiles pour communiquer et rester connecté avec les autres, mais ils peuvent également être source de préoccupation en ce qui concerne la vie privée et la protection de l'identité en ligne. Heureusement, il existe plusieurs moyens de garantir son anonymat sur Internet et les réseaux sociaux. Voici cinq de ces moyens :

1. **Utilisez un VPN :** Les réseaux privés virtuels (VPN) masquent votre adresse IP réelle en la remplaçant par une adresse IP différente. Cela peut vous aider à protéger votre identité en ligne et votre activité en ligne des regards indiscrets. Pas besoin de dépenser de l'argent, un très bon VPN que vous pouvez utiliser est ProtonVPN, il existe en version premium mais vous pouvez également l'utiliser en version gratuite et illimitée.
2. **Soyez vigilant quant aux informations que vous partagez :** Évitez de partager des informations sensibles ou personnelles sur les réseaux sociaux ou les sites Web. Vous le savez déjà, partager des informations telles que votre adresse, votre numéro de téléphone et votre adresse électronique est fort néfaste: mais évitez également de partager certaines photos autour de chez vous ou d'être trop précis concernant un sujet personnel. Avec très peu de ces informations, une personne malveillante peut aisément vous retrouver. Et n'oubliez pas, tout ce que vous partagez sur internet reste à tout jamais sur internet.
3. **Utilisez des navigateurs web qui privilégient la vie privée :** Certains navigateurs web, tels que Tor, Brave Firefox, Opera ou Vivaldi, sont conçus pour garantir la vie privée en ligne. Ils sont une excellente alternative aux navigateurs plus classiques comme Chrome ou Edge, et certains comme Opera vous fournissent un VPN gratuit. Ils peuvent aider à masquer votre identité en ligne et à protéger vos données personnelles.

4. **Configurez les paramètres de confidentialité sur les réseaux sociaux :** La plupart des réseaux sociaux vous permettent de contrôler les informations que vous partagez avec les autres. Configurez vos paramètres de confidentialité pour limiter les informations qui peuvent être vues par les autres utilisateurs. Ces informations peuvent inclure la présence en ligne, l'endroit où vous vous trouvez (par exemple la fonctionnalité de localisation sur Snapchat), le fait que votre compte soit privé ou public, et beaucoup d'autres.
5. **Utilisez des messageries chiffrées :** Le chiffrement de données peut aider à protéger les informations sensibles que vous partagez en ligne. Il existe plusieurs messageries de chiffrement de données disponibles qui peuvent vous aider à garantir la confidentialité de vos données. La plus fiable semble être Signal, l'organisation elle même ne peut pas lire vos messages étant donné que ceux-ci sont chiffrés sur leurs serveurs. D'autres messageries plus connues telles que WhatsApp chiffrent également vos conversations, mais le propriétaire des serveurs (Facebook) y a accès, donc cela n'est d'absolument aucune utilité.
6. **Utilisez un service de courrier électronique sécurisé :** Les services de messagerie traditionnels, tels que Gmail et Yahoo, sont souvent vulnérables aux attaques en ligne, et de plus sont assez floues concernant le partage de vos personelles. Utilisez plutôt un service de courrier électronique sécurisé, comme Disroot, ProtonMail ou Tutanota, pour vous aider à protéger vos données.
7. **Évitez les réseaux Wi-Fi publics non sécurisés :** Les réseaux Wi-Fi publics non sécurisés peuvent être des cibles faciles pour les pirates informatiques. Évitez d'utiliser des réseaux Wi-Fi publics non sécurisés ou utilisez un VPN pour vous protéger lorsque vous les utilisez.
8. **Évitez les sites web non sécurisés :** Les sites web qui ne sont pas sécurisés peuvent être des cibles faciles pour les attaques en ligne. Assurez-vous de vérifier si un site web est sécurisé en vérifiant s'il

utilise le protocole HTTPS au lieu de HTTP. Attention, un site web utilisant le protocole HTTPS peut être malveillant. Beaucoup d'internautes tombent parfois dans le piège.

9. **Utilisez un système d'exploitation qui respecte votre anonymat :** Si vous utilisez un ordinateur, celui-ci est probablement équipé avec Windows ou MacOS. Ces systèmes d'exploitation sont une véritable catastrophe concernant la collecte des données personelles. L'alternative principale qui existe est Linux, composé de plusieurs distributions (version) différentes. La distribution reconnue pour être la plus facile à utiliser pour les débutants est Linux Mint. Changer de systèmes d'exploitation est cependant une action qui exige de bonnes connaissances en la matière, donc réfléchissez bien et renseignez vous bien avant de faire quoi que ce soit. Soyez vigilant, copiez toujours l'intégralité de vos fichiers vers un support externe. Si vous utilisez un téléphone portable, certaines alternatives existent également, comme DotOS ou /e/. Encore une fois, copiez toujours vos fichiers ailleurs et renseignez-vous bien avant de tenter quelque chose. Ce point est particulièrement compliqué à appliquer, c'est pourquoi vous ne devez pas hésiter à rester sur votre système d'exploitation principal si vous n'avez pas d'intérêt à le changer.
10. **Utilisez un gestionnaire de mots de passe sécurisé :** Les mots de passe sont souvent la porte d'entrée pour les attaques en ligne. Utilisez un gestionnaire de mots de passe sécurisé, comme LastPass ou 1Password, pour générer et stocker des mots de passe sécurisés. Au besoin, notez vos mots de passes sur un support physique (un bloc note par exemple, ne les notez SURTOUT PAS sur votre ordinateur ou votre téléphone), cela est même plus sécurisé que les gestionnaires de mots de passes à partir du moment où vous seul avez accès à ce support est qu'il se trouve dans un endroit totalement sécurisé.

En utilisant ces moyens, vous pouvez aider à garantir votre anonymat sur Internet et les réseaux sociaux. Il est important de rester vigilant quant aux

informations que vous partagez en ligne et de prendre les mesures nécessaires pour protéger votre vie privée. Les intelligence artificielle et autres technologies qui s’entraînent sur les réseaux sociaux et sur internet en général sont de plus en plus performantes, certaines ia sont même capables d’imiter votre voix en écoutant un court extrait de quelques secondes à peine. et cela fait très peur: mais vous avez encore moyen de garantir votre anonymat.