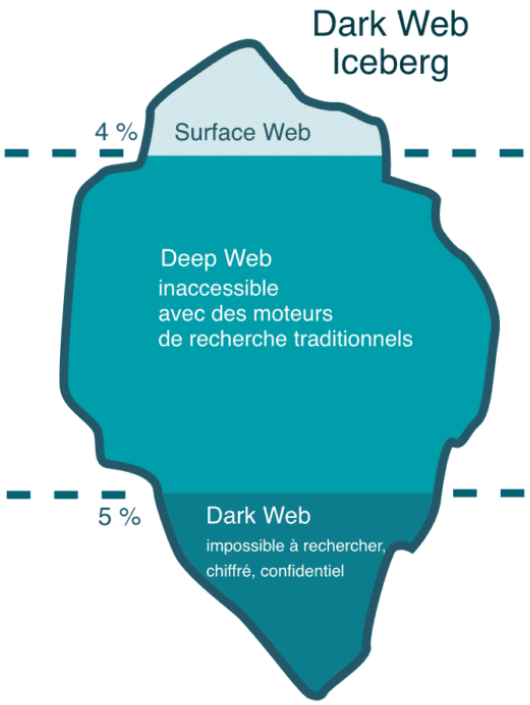
L'iceberg du dark Web expliqué en des termes simples

NDMC: J'utilise depuis quelques années et recommande le gestionnaire de mots de passe Dashlane.

Dashlane :

Internet ne se limite pas à ce que l'on peut voir en surface.
À première vue, on pourrait croire qu'il s'agit d'une bibliothèque infinie avec des droits de navigation illimités.
Mais en réalité, Internet est plus semblable à un iceberg et nous ne pouvons voir que ce qui se trouve au-dessus de l'eau.
Regardons de plus près l'iceberg d'Internet pour en découvrir la face cachée.



Qu’est-ce que le surface Web ?

Le surface Web est la partie d’Internet visible pour le public, celle que nous connaissons tous.
C’est le segment du Web auquel nous accédons en utilisant les moteurs de recherche pour explorer et indexer les pages.
La plupart des gens ne réalisent pas que le surface Web n’est que l’une des nombreuses couches d’Internet et ne représente que 4 % de l’ensemble du Web : c’est juste le sommet de l’iceberg d’Internet.

Vous voulez en savoir plus sur l’utilisation d’un gestionnaire de mots de passe ?

Découvrez nos forfaits individuels ou commencez par un essai gratuit.

Qu’est-ce que le deep Web ?

Juste en dessous du surface Web se trouve ce que l’on appelle le deep Web.
Les contenus stockés dans le deep Web ne sont pas accessibles via les moteurs de recherche traditionnels.
À la différence du surface Web, certaines pages du deep Web n’utilisent pas d’extensions de domaine courantes telles que .com, .edu ou .gov.
Étant donné que les pages ne sont pas reliées les unes aux autres par des hyperliens, elles ne sont pas non plus détectées par les robots d’indexation.
En fait, certaines pages du deep Web peuvent être paramétrées pour bloquer complètement les moteurs de recherche.
Pour accéder à une page Web bloquée ou non à partir du deep Web, vous devez posséder les bonnes autorisations et les bons identifiants.

Cette grande couche d’Internet en expansion rapide comprend des informations qui sont mises à jour fréquemment et présentées en fonction des autorisations des utilisateurs.

Tous les contenus du deep Web ne sont pas dangereux

Ce n’est pas toujours parce que les pages web sont dangereuses qu’elles se retrouvent sur le deep Web.
En effet, il existe de nos jours tellement de contenus stockés sur Internet que les rendre accessibles à tous n’est pas réalisable (ou nécessaire), et la grande majorité de ces contenus échappe au trafic Web.
Les contenus du deep Web incluent de nombreux éléments inoffensifs tels que des actualités archivées et des bases de données, des forums sur invitation et des articles de blog non publiés.

Vous trouverez également des informations bancaires, des ressources stockées derrière des paywalls, et des contenus de réseaux sociaux stockés.

C’est quoi, le dark Web ?

Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

Qu'est-ce que le dark Web ? | Présentation produit - YouTube

À l’intérieur du deep Web, il existe une autre couche d’Internet plus mystérieuse, appelée le dark Web.

Le dark Web est un sous-ensemble chiffré du deep Web qui est moins accessible au grand public.

- **Le deep Web c. le dark Web.**
  À la différence du deep Web en général, le dark Web est plus communément fidèle à sa sinistre réputation qui consiste à dissimuler des activités illégales.
  La nature privée et impossible à rechercher du dark Web offre aux utilisateurs un anonymat complet.
  Bien qu’il existe une finalité légale et légitime pour le dark Web, comme la protection des sources d’information confidentielles et la communication en privé, la plupart des opérations de stockage et d’archivage des données légitimes se déroulent dans des régions plus sûres du deep Web.
- **Les cybercriminels utilisent le dark Web.**
  Les données du dark Web sont délibérément cachées et il faut des outils logiciels spécialisés pour y accéder.
  Les cybercriminels fréquentent le dark Web à des fins illicites, telles que l’achat et la vente de produits de contrebande, de logiciels malveillants et d’identifiants volés. Dans un cas alarmant, une entreprise de cybersécurité a détecté un demi-million de comptes Zoom privés à vendre sur le dark Web, accompagnés d’adresses e-mail, de mots de passe et de clés d’hôte de réunion.

Pour protéger les données de votre entreprise, vous devez savoir si elles ont déjà été compromises par une faille de données.
Utilisez cet outil gratuit et puissant sponsorisé par Dashlane pour savoir si vos données ont été exposées sur le dark Web : La sécurité de votre entreprise est-elle compromise ?

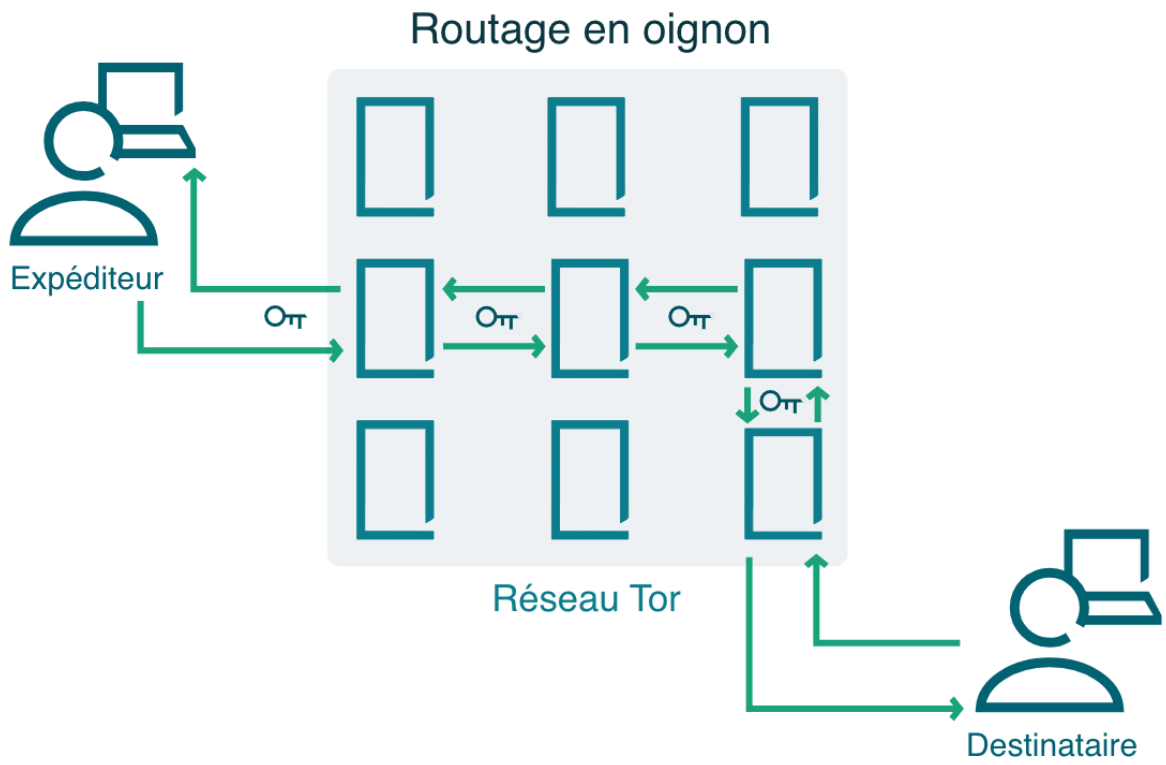
Il est possible d’aller au fond de l’iceberg d’Internet avec les bons outils et les bonnes informations en main.
En fait, des millions de personnes et d’entreprises accèdent au deep Web tous les jours pour mettre à jour des contenus de médias sociaux, des comptes de paiement et des informations uniquement sur abonnement qui ne peuvent pas être recherchés.

Les méthodes d'accès aux pages du deep Web dépendent du site que vous recherchez et des protections en place.
Certains sites nécessitent des identifiants et une autorisation, tandis que d'autres nécessitent des outils spéciaux.
Par exemple, une page Web qui se retrouve sur le deep Web parce qu'elle n'a pas d'hyperliens consultables peut être accessible simplement en saisissant l'URL complète. D'autres sites trouvés dans le sous-ensemble du deep Web, communément appelé dark Web, peuvent nécessiter un logiciel spécialisé pour y accéder.

Qu'est-ce qu'un navigateur Tor ?

Tor est un moteur de recherche du deep Web.
Il a été développé par le gouvernement américain pour protéger les lanceurs d'alerte et empêcher la censure du surface Web.
En 2006, la marine américaine a transféré la propriété du réseau Tor à une organisation à but non lucratif appelée Tor Project.

The Onion Router (TOR) est un navigateur anonymisant populaire qui utilise plusieurs couches pour bloquer l'identité d'un utilisateur.
Une série de serveurs proxy rend l'adresse IP introuvable et les messages sont chiffrés à chaque point d'accès, ce qui fait que la trace de communication est presque impossible à suivre.
Le routage en oignon fait référence au processus de suppression systématique des couches de chiffrement des communications sur Internet, comme lorsqu'on épluche un oignon.
De manière appropriée, le suffixe .onion remplace .com ou .org pour les sites Web qui sont hébergés sur le réseau Tor.



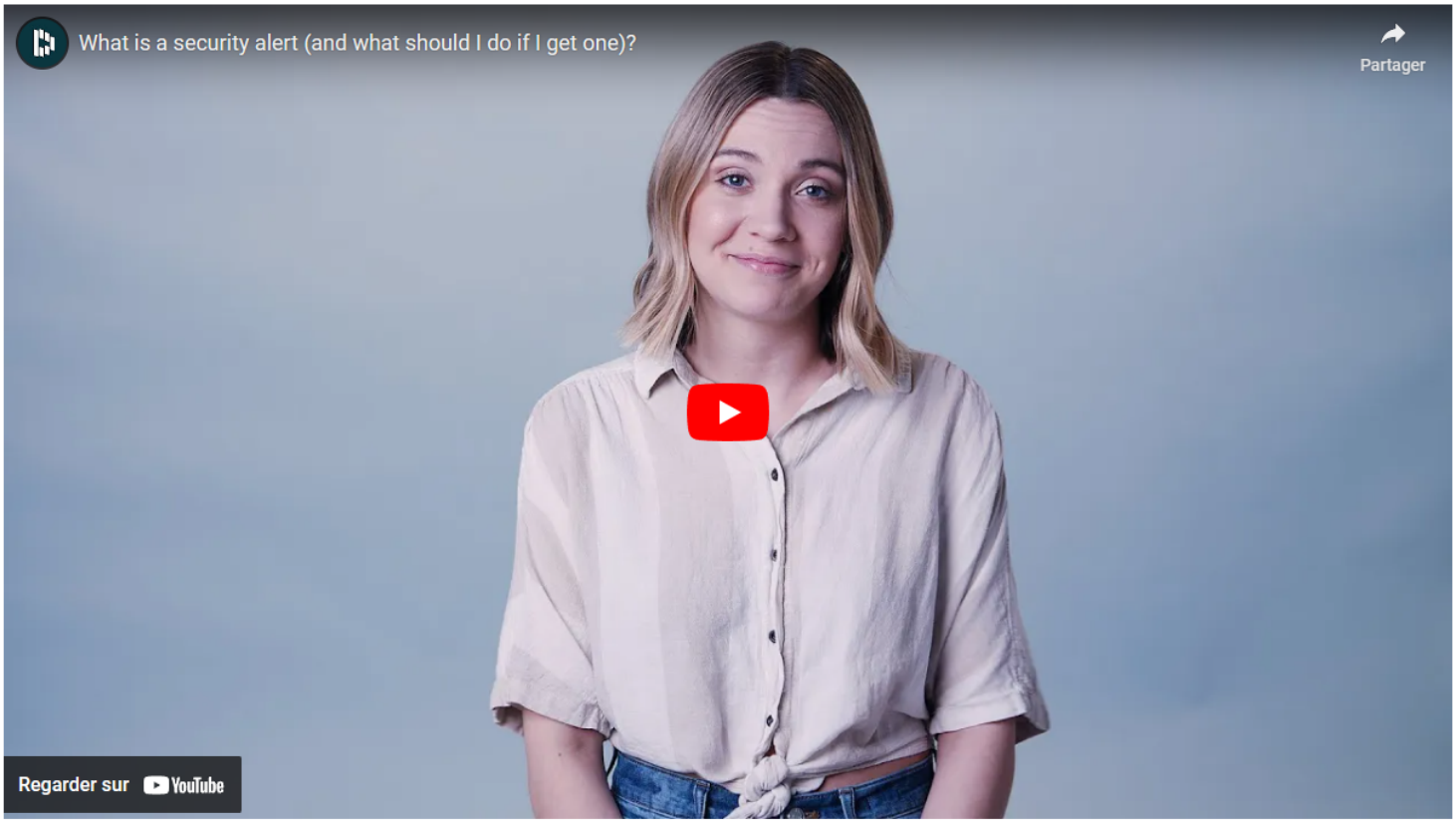
Devrais-je accéder au dark Web ?

Bien qu'il existe des outils logiciels disponibles qui vous permettent d'accéder au deep Web, ou même au dark Web, cela n'est pas recommandé et encore moins nécessaire. Les fichiers que vous téléchargez à partir du dark Web peuvent comporter des logiciels malveillants dangereux.
Les professionnels de la cybersécurité tels que les chasseurs de menaces sont formés pour suivre des protocoles de sécurité lorsqu'ils recueillent des informations dans les couches plus profondes de l'iceberg d'Internet, mais nous devrions être prudents.

Astuces pour protéger vos informations du dark Web

Il est préférable de limiter votre navigation à la partie supérieure de l'iceberg du dark web. Mais comment savoir si vos informations sont échangées sur le dark Web et vous protéger des failles de données ?

Heureusement, il existe de nombreux outils de cybersécurité avancés disponibles pour protéger vos informations à distance.



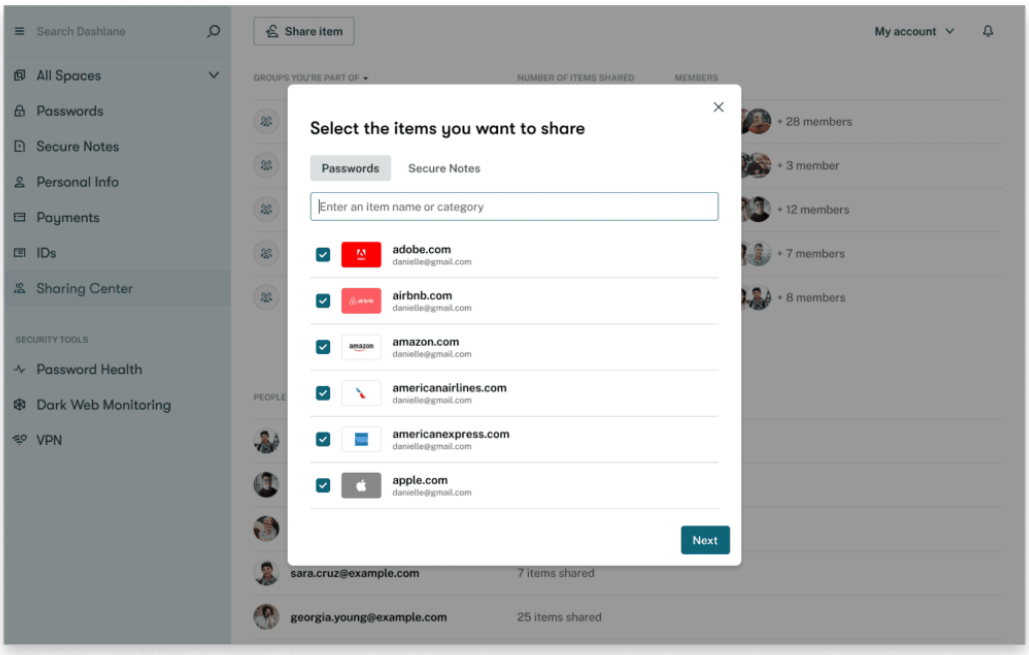
Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

Qu'est-ce qu'une alerte de sécurité (et que faire si j'en reçois une) ? | Présentation produit - YouTube

1. **Effectuez une analyse du dark Web :** des politiques de mots de passe fortes et des logiciels anti-malware peuvent limiter les risques de faille de données, mais aucun outil de cybersécurité n'est infaillible à 100 %.
   Effectuer une analyse du dark Web vous aide à déterminer si vos mots de passe, vos adresses courriel ou d'autres informations privées ont été compromis et doivent être mis à jour.
2. **Utilisez Dark Web Insights de Dashlane :** avec Dark Web Insights, les entreprises peuvent protéger leurs employés des failles de sécurité et d'autres vulnérabilités en utilisant un outil intégré pour analyser en permanence plus de 20 milliards d'enregistrements du dark Web.
   Les employés et les administrateurs informatiques sont immédiatement alertés si des informations privées sont détectées.
   Les analyses prennent en compte tous les travailleurs, même ceux qui n'utilisent pas encore Dashlane, car elles sont basées sur le domaine de l'entreprise.
   Cette approche holistique et proactive aide les équipes informatiques à atténuer les menaces avant qu'elles ne s'aggravent.
3. **Activez la double authentification (2FA) :** la double authentification (2FA) utilise un deuxième identifiant, tel qu'un code envoyé via une application ou un SMS, pour confirmer votre identité.
   Cela rallonge votre processus de connexion, mais il est presque impossible pour un intrus d'accéder à vos comptes et de voler vos informations sans avoir votre appareil en sa possession.
   L'authentification multi-facteur (MFA) utilise deux ou plusieurs facteurs, tels que des identifiants biométriques, la reconnaissance faciale ou les empreintes digitales.
4. **Utilisez un VPN sur les réseaux Wi-Fi publics :** les réseaux sans fil dans les aéroports, les cafés, les hôtels et d'autres lieux publics peuvent être sujets à des attaques de type « homme du milieu » et à d'autres tactiques de piratage destinées à intercepter des informations.
   Un VPN minimise le risque que vos informations se retrouvent du mauvais côté de l'iceberg d'Internet en chiffrant toutes les données qui entrent ou sortent de votre appareil et en les acheminant via un portail sécurisé.
   Un VPN masque également votre adresse IP afin que vous puissiez naviguer sur Internet de manière plus privée.
5. **Évitez de réutiliser vos mots de passe :** il est facile de prendre pour habitude de réutiliser vos mots de passe, car cela minimise la mémorisation et la création de nouveaux mots de passe.

Les mots de passe réutilisés affaiblissent également votre sécurité en exposant plusieurs comptes si un seul mot de passe est volé et vendu sur le dark Web.
Vous devriez remplacer vos mots de passe réutilisés par des mots de passe forts qui comportent au moins 12 caractères, un mélange aléatoire de lettres, de chiffres et de caractères spéciaux et laisser de côté des phrases d'identification telles que votre prénom ou votre adresse.

6. **Ne partagez vos mots de passe que de manière sécurisée :** le partage de mots de passe est presque inévitable pour des choses telles que les services de streaming vidéo et les comptes de vente au détail, mais vous devriez toujours essayer de partager vos mots de passe de manière aussi sécurisée que possible. Les mots de passe partagés exposent tout le monde dans le groupe si l'un d'entre eux est touché par une faille.
La façon la plus sûre de partager des mots de passe est d'utiliser le portail de partage chiffré d'un gestionnaire de mots de passe. L'outil de partage de mots de passe de Dashlane peut être utilisé pour envoyer des notes sécurisées ou des mots de passe à d'autres utilisateurs de Dashlane.



Découvrez comment Dashlane vous protège du dark Web

Le dark Web est un endroit que la plupart d'entre nous ne visiterons jamais ou que nous souhaiterions ne jamais visiter.
Heureusement, les fonctionnalités avancées de Dashlane telles que Dark Web Insights nous permettent de nous assurer que nos informations confidentielles restent privées. Des fonctionnalités standard supplémentaires telles qu'un générateur de mots de passe avancé, le chiffrement AES-256, la double authentification et un score de sécurité qui suit les mots de passe faibles, réutilisés et compromis vous aident à protéger vos informations et à les empêcher de se voir exposées sur le dark Web.

Dashlane n'a jamais été compromis, et notre architecture brevetée « zero-knowledge » signifie que personne (pas même Dashlane) ne peut voir vos mots de passe et vos données personnelles.

Découvrez ce qui fait de Dashlane gestionnaire de mots de passe ultra sécurisé**.**

Références

1. Incognito, « The Layers of the Web – Surface Web, Deep Web and Dark Web », 2023.
2. OEDb, « The Ultimate Guide to the Invisible Web », 2023.
3. Dashlane, « C'est quoi, le dark Web ? » mars 2020.
4. Dashlane, « Le chiffrement expliqué par Dashlane », mars 2019.
5. Dashlane, « 500,000 Zoom Accounts on the Dark Web », avril 2020.
6. Business Breach Report, « Has Your Business Been Breached ? » 2023.
7. Tor Project, « History ».

8. Crowdstrike, « What is the Dark Web ? » septembre 2022.
9. Dashlane, « Rapport sur les failles de données de votre entreprise ».
10. Dashlane, « Dark Web Monitoring », 2023.
11. Dashlane, « A Beginner's Guide to Two-Factor Authentication », août 2022.
12. Incognia, « What are the Key Differences between 2FA and MFA? » 2023.
13. Dashlane, « How Would I Hack You ? With White-Hat Hacker Rachel Tobac », 2023.
14. Dashlane, « How Password Reuse Leads to Cybersecurity Vulnerabilities », mai 2023.
15. Dashlane, "How Strong Is Your Password & Should You Change It?" août 2022.
16. Dashlane, "Best Way to Store Passwords at Home or Work", septembre 2022.
17. Dashlane, « Everything You Need to Know About Your Password Health Score », octobre 2020.
18. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.
19. Dashlane, « Understanding Your Dashlane Password Health Score, » octobre 2020.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230731
"C'est ensemble qu'on avance"