FUTURA

Dark Web : Google se retire… faut-il s’inquiéter ?

Podcast écrit et lu par Adèle Ndjaki

[*Générique d’intro, une musique énergique et vitaminée.*]

Google ne surveillera plus le dark web, la situation est-elle critique ? C'est le décryptage de la semaine dans *Vitamine Tech*.

[*Fin du générique.*]

Sommes-nous plus vulnérables que jamais? Il y a quelques jours, Google a annoncé fermer, début 2026, son outil gratuit de surveillance du dark web. Ce service est pourtant censé prévenir les utilisateurs lorsque leurs informations personnelles circulent après une fuite de données. Cette décision pose alors une question : à quoi pouvons-nous nous attendre après la clôture de cet outil? Bonjour à toutes et à tous, je suis Adèle Ndjaki et aujourd'hui dans *Vitamine Tech*, on parle dark web et cybersécurité !

[*Une musique électronique calme.*]

Quand on parle de fuite de données, la notion qui revient assez naturellement, c’est celle du dark web. Une notion qui fait peur, car souvent associée aux hackers ou aux trafics illégaux. Mais qu’est-ce qui se cache réellement derrière ? Et au fond, qu’est-ce que le dark web ? En fait, le dark web, c’est juste une petite partie du Net. Concrètement on peut dire qu'Internet a plusieurs couches. Tout en haut, il y a le web classique, celui qui est connu, qui est visible, avec Google, vos sites préférés, vos réseaux sociaux… Un espace qui est accessible à tous. Ensuite, en dessous, il y a ce qu'on appelle le deep web. Ici, on trouve tout ce qui n’est pas public, donc vos e-mails, vos comptes bancaires, vos espaces privés. Rien d’illégal… Juste des données protégées par des mots de passe. Et puis tout en bas, il y a notre fameux dark web. Une partie du Net qui n’est pas accessible avec des navigateurs classiques comme Chrome ou Safari. Pour y accéder, il faut des outils spécifiques, comme Tor, un navigateur qui permet de naviguer sur Net mais de façon anonyme. Alors même si cet anonymat peut être utilisé à des fins légitimes comme protéger la vie privée, contourner la censure entre autres, cet anonymat peut aussi être utilisé à des fins illégales. Ça vous le savez. Les cybercriminels n'hésitent pas à utiliser cet espace pour échanger des informations volées sans se faire attraper. Et c’est à partir de ce moment-là qu'on peut commencer à parler de fuites ou plutôt de vol de données. Car quand un site est piraté, vos informations ne disparaissent pas. Elles sont souvent revendues, échangées, ou publiées sur des forums clandestins du dark web. Et le pire, c'est que quand ça arrive, beaucoup ne sont presque jamais prévenus et que par conséquent beaucoup continuent à utiliser leurs comptes sans mettre en place des actions pour se protéger. C’est pour ça qu’ il existe des

Dark Web Monitoring, des services de surveillance de fuites de données. Leur travail consiste à scruter des bases de données et les espaces du dark web, pour vous alerter si vos informations apparaissent. Même si ces outils ne suppriment pas les données piratées, ils permettent quand même de réagir assez vite. Et l'un des points positifs de ces services de Monitoring, eh bien c'est qu'ils peuvent autant servir aux particuliers qu'aux entreprises. Parmi les plus connus, on peut nommer Have I Been Pwned, pour savoir si votre email a été exposé, Norton 360 Dark Web Monitoring, ou encore NordProtect qui surveille forums et marketplaces clandestins. Il y a donc le choix ! Mais même si ces outils sont utiles, suffisent-ils vraiment ? Il semblerait qu'il manque encore l'essentiel…

[*Virgule sonore, une cassette que l'on accélère puis rembobine.*]
[*Une musique de hip-hop expérimental calme.*]

On pourrait se dire que le plus important, c'est d'être alerté quand ses données se retrouvent sur le dark web. Mais les dernières actualités montrent que prévenir seul ne suffit pas. Prenons l'exemple de Google. Depuis mai 2023, les abonnés à Google One pouvaient utiliser son fameux « rapport sur le Dark Web », et depuis juillet 2024, il était même gratuit pour tous. L'idée était simple : vous avertir si vos informations personnelles, donc nom, adresse, numéro de téléphone, circulaient dans les recoins du dark web, à la suite d'une fuite de données. Mais après seulement deux ans, Google a annoncé que cet outil disparaîtrait en février 2026. Alors concrètement, la surveillance des nouveaux résultats s'arrêtera dès le 15 janvier mais l'outil ainsi que toutes ses données seront supprimés le 16 février. Pourquoi une telle décision ? Selon Google, le rapport fournissait peu d'informations concrètes pour les utilisateurs. Vous étiez alertée, mais on ne vous disait pas vraiment quoi faire après. Donc il n'y avait pas de plan d'action clair, juste un signal d'alerte. Google dit ainsi vouloir se concentrer sur des outils plus pratiques et efficaces, capables de guider l'utilisateur, pour par exemple, changer un mot de passe compromis automatiquement ou activer la double authentification… Bref, des actions concrètes pour protéger ses comptes. Cette décision montre alors une chose essentielle : aucun outil, même développé par un géant comme Google, ne peut remplacer votre vigilance. Google n'est pas le seul à se heurter à cette limite. Beaucoup de services de dark web Monitoring fournissent des alertes mais pas toujours de solutions complètes. Les alertes sont utiles, mais elles ne suffisent pas si vous ne réagissez pas rapidement. Alors pour vous aider à protéger vos données personnelles voici quelques astuces données par la CNIL, la Commission Nationale de l'Informatique et des Libertés ainsi que l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information : déjà changer régulièrement vos mots de passe, surtout si vous apprenez qu'un compte a été compromis; activer la double authentification partout où c'est possible, pour ajouter une couche de sécurité; ne jamais réutiliser le même mot de passe sur plusieurs comptes, un classique; et bien sûr rester vigilant face aux messages suspects de type phishing ou mails et SMS demandant vos informations personnelles. Donc ce qu'il faut retenir de cet épisode, c'est qu'au final la protection de données est une responsabilité qui incombe à chacun. Des outils peuvent aider, mais les bonnes pratiques quotidiennes sont les meilleures de toutes les protections.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de *Vitamine Tech.* Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le dernier épisode des aventures de Zoé et Eliot, raconté par Mélissa Lepoureau, au cœur d'une mystérieuse grotte dans les gorges du Verdon ! Pour le reste, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

[*Un glitch électronique ferme l'épisode*.]