

Voici les résultats de votre *auto-évaluation des risques numériques.*

Sur la base de vos réponses, votre niveau de risque numérique personnel actuel est le suivant :

Modéré



Ce que cela signifie

Vos réponses suggèrent que certaines habitudes de protection sont en place, mais certaines zones d'exposition peuvent augmenter vos risques de compromission de compte, d'usurpation d'identité ou d'attaques ciblées.

À ce niveau, le risque est gérable, mais des lacunes dans les pratiques relatives aux mots de passe, à l'authentification, aux paramètres des réseaux sociaux ou à la coordination des ménages peuvent créer des vulnérabilités au fil du temps.



Où votre exposition peut être plus élevée

D'après vos réponses, une exposition peut exister dans des domaines tels que :

- Pratiques relatives aux mots de passe réutilisés ou incohérentes
- Utilisation limitée de l'authentification multifactorielle
- Activités sur les réseaux sociaux destinées au public
- Membres de la famille gérant les appareils ou les comptes de manière indépendante
- Visibilité exécutive ou importance professionnelle
- Voyages fréquents ou utilisation d'appareils dans des environnements à haut risque



Qu'est-ce qui réduit généralement le risque à ce niveau

Les personnes se situant dans cette fourchette réduisent souvent leur exposition en :

- ✓ Utilisation de mots de passe uniques pour tous les comptes
- ✓ Activation de l'authentification multifacteur partout où elle est disponible
- ✓ Réviser la confidentialité des réseaux sociaux et réduire les informations accessibles au public
- ✓ Établir des normes de sécurité cohérentes pour les ménages
- ✓ Surveillance de l'exposition des informations d'identification et des signaux d'usurpation d'identité

Pourquoi ces habitudes sont importantes

Les recherches montrent que l'utilisation de l'authentification multifactorielle associée à des mots de passe forts et uniques peut réduire le risque de compromission des comptes jusqu'à 99 %. Apprendre à reconnaître les tentatives de phishing et à vérifier les liens avant de cliquer peut réduire les risques liés à la sécurité de 70 %. Limiter ce que vous partagez publiquement sur les réseaux sociaux réduit encore davantage les informations disponibles pour le ciblage ou l'usurpation d'identité.



Richter Guardian fournit les outils, la surveillance et les conseils professionnels nécessaires pour vous aider à combler les lacunes et à renforcer la protection de l'ensemble des comptes et des ménages, y compris une surveillance continue des risques liés à l'identité, aux informations d'identification et aux appareils.

Désirez-vous un examen plus approfondi ?

Ce résumé reflète vos réponses à une brève auto-évaluation et met en évidence les domaines d'exposition courants. Un examen plus détaillé peut aider à identifier les risques spécifiques à votre situation et à préciser sur quoi vous concentrer en premier lieu.

Pour explorer votre situation plus en détail, vous pouvez demander une consultation confidentielle ou nous poser des questions afin de mieux comprendre vos résultats et les prochaines étapes.

[Demandez une consultation privée](#)

richterguardian.com