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 :

Faible

Faible Modéré Élevé Haut

Ce que cela signifie

Vos réponses indiquent de fortes habitudes numériques et des zones limitées à forte exposition.

Vous utilisez des mesures de protection qui réduisent les risques de compromission de votre compte, d'usurpation d'identité ou d'exposition évitable. À ce niveau, le risque est présent mais généralement bien géré.

Où votre exposition peut être plus élevée

Même à un niveau de risque plus faible, l'exposition peut toujours exister dans des domaines tels que :

- **Informations personnelles ou professionnelles accessibles au public**
- **Comptes de réseaux sociaux qui révèlent des habitudes, des relations ou des voyages**
- **Membres de la famille gérant les appareils ou les comptes de manière indépendante**
- **Visibilité accrue liée aux rôles de direction ou de conseil**

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

Les individus de cette aire de répartition maintiennent souvent leur protection en :

- **Maintien de pratiques cohérentes en matière de mots de passe et d'authentification multifacteur**
- **Révision périodique de la confidentialité et des informations publiques sur les réseaux sociaux**
- **Surveillance de l'usurpation d'identité et de l'exposition à des informations d'identification**
- **Coordination des normes numériques de base entre les membres du ménage**

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 mettre en œuvre et à maintenir ces habitudes de protection, y compris une surveillance continue des risques liés à l'identité, aux informations d'identification et aux appareils.

Désirez-vous un 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