RICHTER GUARDIAN

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 :

Haut

Faible Modéré Élevé Haut

Ce que cela signifie

Vos réponses indiquent une exposition importante qui augmente le risque de compromission du compte, d'usurpation d'identité, de fraude financière ou d'attaques ciblées.

À ce niveau, les lacunes en matière de gestion des mots de passe, d'authentification, de contrôle des réseaux sociaux, de coordination domestique ou de visibilité des dirigeants créent des conditions propices à la survenue d'incidents et à leur escalade rapide. Si vous occupez un poste de direction ou si vous maintenez une présence publique, l'exposition peut s'étendre au-delà de vous, aux membres de votre famille ou à des contacts étroits.

Où votre exposition peut être plus élevée

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

- **Mots de passe réutilisés ou non sécurisés sur plusieurs comptes**
- **Utilisation limitée ou nulle de l'authentification multifactorielle**
- **Comptes de réseaux sociaux publics qui révèlent des informations personnelles, familiales ou de voyage**
- **Gestion indépendante et non coordonnée des appareils ou des comptes au sein du ménage**
- **Visibilité auprès des dirigeants ou du public qui augmente le risque de ciblage**
- **Déplacements fréquents sans dispositifs de protection cohérents**

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

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

- **Mise en place d'un gestionnaire de mots de passe et de mots de passe uniques pour tous les comptes**
- **Activer l'authentification multifactorielle de manière cohérente**
- **Réviser et limiter les informations publiques sur les réseaux sociaux et en ligne**
- **Coordination des normes de sécurité entre les membres de la famille**
- **Mise en place d'une surveillance continue et d'une capacité de réponse guidée**

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, une surveillance continue et des conseils d'experts pour aider à réduire l'exposition active et à réagir rapidement aux risques émergents sur l'ensemble des comptes, des appareils et des ménages.

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