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 :

## *Élevé*

Faible Modéré Élevé Haut

## Ce que cela signifie

Vos réponses indiquent des zones d'exposition importantes qui augmentent le risque de compromission du compte, d'usurpation d'identité ou d'attaques ciblées.

À ce niveau, des lacunes dans les pratiques en matière de mots de passe, d'authentification, de contrôle des réseaux sociaux ou de coordination des ménages créent des conditions dans lesquelles un seul incident peut rapidement dégénérer. Le risque peut également être plus élevé si vous occupez un poste en contact avec le public ou si vous occupez un poste de direction.

### 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 gestion limitée des mots de passe**
- **Utilisation incohérente ou minimale de l'authentification multifactorielle**
- **Comptes de réseaux sociaux publics qui révèlent des informations personnelles ou familiales**
- **Gestion indépendante des appareils et des comptes pour tous les membres du foyer**
- **Visibilité exécutive ou importance professionnelle**
- **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 :

- **Implémentation de mots de passe uniques et d'un gestionnaire de mots de passe pour tous les comptes**
- **Activer l'authentification multifactorielle de manière cohérente**
- **Révision et renforcement des paramètres des réseaux sociaux et des informations publiques**
- **Établir des normes de sécurité coordonnées pour les ménages**
- **Surveillance continue de l'usurpation d'identité, de l'exposition à des informations d'identification et des menaces émergentes**

### 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 la surveillance, les outils et les conseils professionnels nécessaires pour réduire l'exposition et renforcer la protection des comptes personnels et des environnements domestiques, avec 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