

SECURITY ADVISORY

Even sophisticated families have *ordinary* security gaps

Where families tend to be exposed, how the risk is changing, and what meaningful protection involves.

INTRODUCTION

For high-net-worth families, digital risk has never been confined to the business. What has changed is the focus of threat actors, who increasingly target the individual and the wider family, exploiting personal email, mobile devices, social media, financial accounts, household members, and trusted advisors.

AT A GLANCE

Key takeaways

14%

USE A UNIQUE PASSWORD FOR EVERY ACCOUNT

At onboarding, only 14% of new Richter Guardian users report using a unique password for every account, and just 39% report multi-factor authentication on every account where it is available. These are self-reported practices.

~138%

RISE IN IMPERSONATION ALERT VOLUME

Among Richter Guardian users, impersonation alert volume rose by approximately 138% and account-discovery alert volume rose by approximately 100% from January to October 2026, based on technology-partner data. These are alert volumes, not counts of unique attacks.

72→86%

AVERAGE SECURITY SCORE AFTER REVIEW

After onboarding, as gaps are identified and closed, families protected by Richter Guardian who were reviewed improved their average Richter Guardian Security Score by nearly 14 percentage points, from approximately 72% to 86%. This is a proprietary measure and an internal review, not an industry benchmark.

Ongoing

REDUCE, THEN MONITOR

Strong protection starts with reducing everyday vulnerabilities and continues with ongoing monitoring.

If you want to see where your own exposure sits, the Richter Guardian What's My Risk self-assessment is a simple place to start.

Recent reporting on a breach affecting Cresset clients, along with research from Presage Global and Nines and coverage in Insurance Business America, points to an environment where attackers pursue identities, relationships, and family members, not only company systems. This article looks at where families tend to be exposed, how the risk is changing, and what meaningful protection involves.

01

Why digital risk now follows the family, not just the business

Personal accounts, devices, and the people around a principal can each become a route to sensitive information or assets. For affluent families, compromised personal information can enable identity theft, account takeover, impersonation, and social engineering, even when money is not immediately stolen.

Waiting to respond after something goes wrong is an approach, but it is not a strategy. In many cases, people are not even aware of how exposed they are. Finding and fixing those gaps, or simply learning they exist, before anything happens matters far more than reacting afterward. That is the work Richter Guardian focuses on: finding the gaps, closing them, and keeping watch as risks change.

Waiting to respond after something goes wrong is an approach, but it is *not a strategy.*

FINDING THE GAPS · CLOSING THEM · KEEPING WATCH

02

Together this creates a baseline and a clear set of actions to work through with the family or on their behalf.

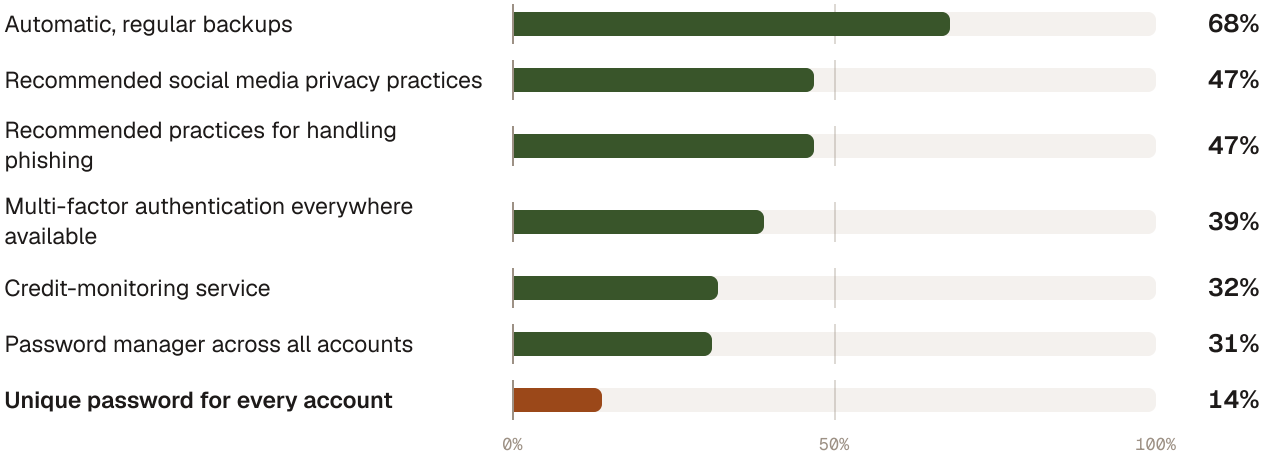
What cybersecurity gaps do high-net-worth families have?

When families first come to Richter Guardian, they complete a short onboarding review of their current practices. At the same time, Richter Guardian runs initial dark-web scans for exposed email addresses, identities, and compromised credentials, and reviews device security and social media accounts. Together this creates a baseline and a clear set of actions to work through with the family or on their behalf.

The self-reported results are revealing. Only 14% use a unique password for every account. Just 31% use a password manager across all their accounts, and 39% have multi-factor authentication turned on everywhere it is available. Fewer than half follow Richter Guardian's recommended social media privacy practices, at 47%, or Richter Guardian's recommended practices for recognizing and handling phishing attempts, also at 47%. Only 32% use a credit-monitoring service, though 68% do have automatic, regular backups in place.

AT ONBOARDING

Share of new Richter Guardian users who report each practice



Self-reported habits rather than independently verified behaviour.

These are self-reported habits rather than independently verified behaviour, but the pattern is clear. Even families with significant resources can carry surprisingly ordinary security gaps, often simply because they are busy and have a great deal to manage. These are people leading complex lives, made more complex by wealth, reputation, and public profile, who would rather have someone advise and guide them than manage technical security themselves.

03

Are impersonation and account takeover attempts increasing?

Across Richter Guardian users, technology-partner data shows the risk environment shifting. From January to October 2026, impersonation alert volume rose by approximately 138%, and account-discovery alert volume rose by approximately 100%. These figures reflect alert volumes among the people Richter Guardian protects, and they count alerts rather than unique attacks or affected families. The direction, however, is unmistakable.

JAN → OCT 2026

~138%

rise in impersonation alert volume

JAN → OCT 2026

~100%

rise in account-discovery alert volume

Among Richter Guardian users, based on technology-partner data. These figures count alerts rather than unique attacks or affected families.

These shifts sit within a wider rise in AI-enabled scams. Reporting from Wealth Professional and Canadian Family Offices points to growing concern about AI-powered fraud aimed at individuals and families. This is background on the environment, not the cause of the increases above.

For a closer look at who is most exposed and how to protect them, see Protecting the People Behind the Family Office, in the Age of AI.

The direction, however, is *unmistakable.*

04

Families are not handed a list of recommendations to manage alone.

How personal cybersecurity protection closes these gaps

Identifying a weakness is only the starting point. Richter Guardian works directly with families to put practical protections in place. That can include setting up a password manager and training family members to use it, enabling multi-factor authentication on important accounts, guiding safer social media habits, and providing tools and support designed to stop phishing attempts from succeeding rather than only helping people recognize them. Families are not handed a list of recommendations to manage alone. They receive hands-on help and ongoing support as their needs and risks change.

The results show up after onboarding. As Richter Guardian identifies and closes each family's gaps, their security posture improves. Among families protected by Richter Guardian who were reviewed, the average Richter Guardian Security Score rose by nearly 14 percentage points, from approximately 72% to 86%, and in some cases more.

RICHTER GUARDIAN SECURITY SCORE

nearly +14 percentage points in the average score among families who were reviewed



The Richter Guardian Security Score is a proprietary measure of a family's security posture, not an external industry benchmark, and this reflects an internal review rather than a guaranteed result for every family.

Richter Guardian helps families put these protections in place and keeps watch as new risks appear. Learn more about Personal Digital Protection.

05

Why personal cybersecurity has to be ongoing

Improving passwords and multi-factor authentication is only part of the picture. New exposures keep appearing, as a $4.5-million account raid and exposed Canadian identity-verification data both show. Richter Guardian helps families reduce preventable vulnerabilities while maintaining ongoing visibility into a changing risk environment.

06

Final thoughts

Cybersecurity for high-net-worth families is not simply about responding when something goes wrong. It starts with reducing everyday vulnerabilities and continues with monitoring for new risks and exposures.

The data shows that families can arrive with real gaps in basic practices, that impersonation and account-discovery activity is rising, and that after Richter Guardian works through those gaps, families who were reviewed improved their security posture meaningfully.

NEXT STEP

A sensible next step is simply understanding where your own exposure sits. The What's My Risk self-assessment takes only a few minutes. For a closer look, you can request a private consultation.

Take What's My Risk

Request a private consultation

QUESTIONS FAMILIES ASK

FAQs

01

What is digital risk for a high-net-worth family?

It is the chance that personal accounts, devices, social media, or trusted relationships are used to reach sensitive information or assets. It follows the individual and family, not only the business.

02

Why do wealthy families still have security gaps?

Wealth and professional sophistication do not automatically produce strong everyday habits. These are busy people with a lot to manage, and at onboarding many Richter Guardian users self-report gaps in passwords, multi-factor authentication, and phishing awareness.

03

What is the Richter Guardian Security Score?

It is Richter Guardian's proprietary measure of a family's security posture. It is not an external or industry-standard benchmark.

04

Does stronger protection actually improve a family's security?

After onboarding, as Richter Guardian identifies and closes each family's gaps, families who were reviewed improved their average Richter Guardian Security Score by nearly 14 percentage points. This is an internal review and not a guaranteed result for every family.

REFERENCED IN THIS PIECE

1. What's My Risk self-assessment
   richterguardian.com
2. Presage Global research (InvestmentNews)
   investmentnews.com
3. Wealth Professional
   wealthprofessional.ca
4. Canadian Family Offices
   canadianfamilyoffices.com
5. Protecting the People Behind the Family Office, in the Age of AI
   richterguardian.com
6. Personal Digital Protection
   richterguardian.com
7. A $4.5-million account raid
   richterguardian.com
8. Canadian identity-verification data breach
   richterguardian.com

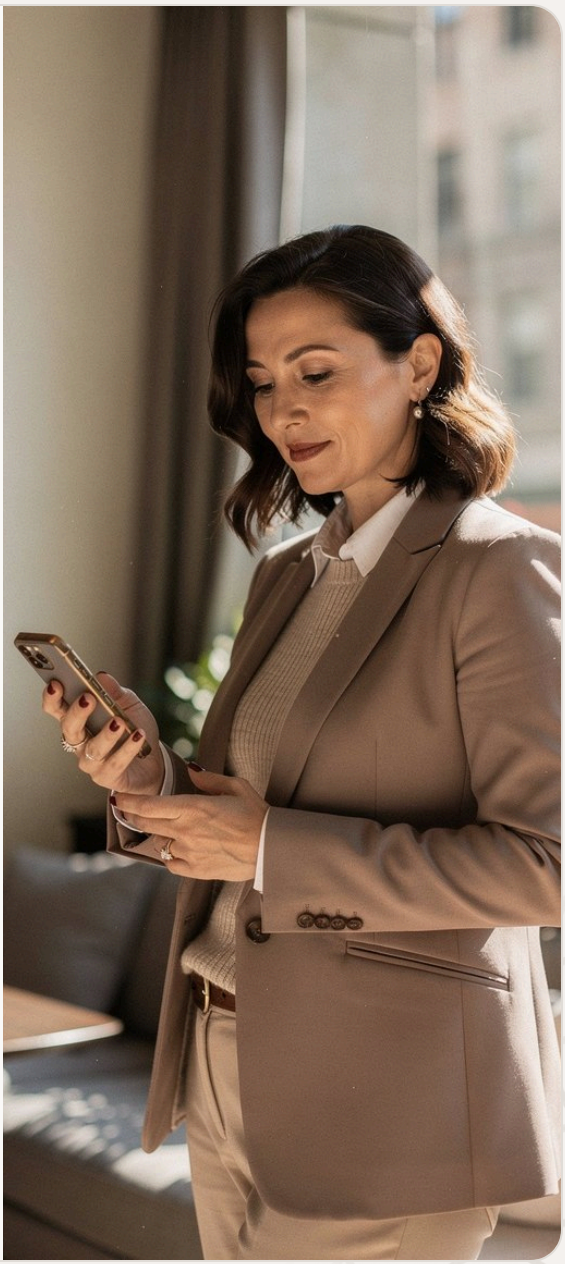
Protect your digital life by detecting risks *before they escalate*

Richter Guardian gives you enterprise-level cybersecurity tailored for individuals, families, and executives.

- 24/7 monitoring & threat intelligence
- Identity theft & impersonation detection
- Fast incident recovery & expert guidance

Request a private consultation

Take the What's My Risk self-assessment



Strong protection starts with reducing everyday vulnerabilities and continues with ongoing monitoring.

RICHTER GUARDIAN

richterguardian.com

© 2026 Richter Guardian. All rights reserved.