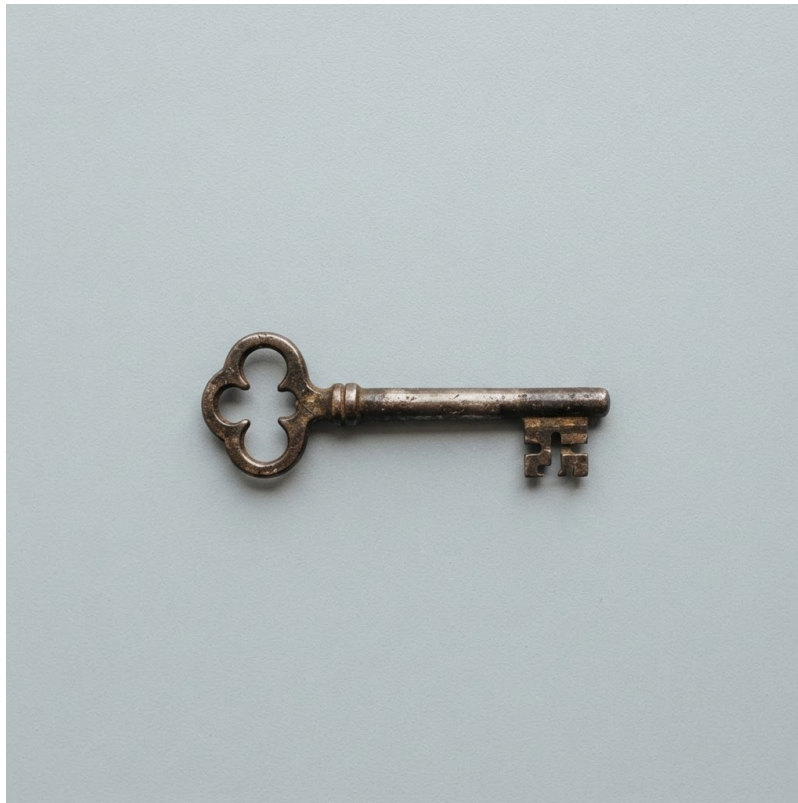


Protecting What You Have Built

Financial security erosion: the risk that does not appear in most plans, and is growing fast



Financial losses from fraud and manipulation are now large enough to be a material retirement risk.

The people who lose the most are often educated, successful, and confident in their own judgement. That confidence is part of the vulnerability.

Digital and fraud protection belongs inside a financial plan, reviewed alongside insurance, estate planning, and other protective measures.

A risk that does not appear in most financial plans

Financial planning has always been about protection as much as growth. Insurance protects against the unexpected. Diversification protects against market concentration. Estate planning protects against what happens when you are no longer able to make decisions yourself. These protections are well understood, regularly reviewed, and built into the structure of a good financial plan.

There is a fourth category of protection that most plans do not include, and it is the one growing fastest. Fraud, manipulation, and digital vulnerability are now responsible for losses large enough to change retirement outcomes. In New Zealand, losses reported to agencies such as Netsafe and the Banking Ombudsman have grown consistently year on year, and the reported figures represent only a fraction of what actually occurs. Most people who are defrauded do not report it, because they are embarrassed, because they did not realise until it was too late, or because they believed, even after the money was gone, that the relationship or opportunity was real.

This paper is not about scams in the way that word is usually understood. The word 'scam' carries associations that make people feel the risk belongs to someone else: the naive, the careless, the elderly. It does not describe what is actually happening. The right term is **financial security erosion**: a category of risk that sits alongside market risk and behavioural risk, is growing faster than either, and is almost entirely absent from conventional financial planning conversations.

Moneyworks has worked with people on digital protection and fraud prevention for many years. We raise it in annual reviews, we write about it in our newsletter, and we have, on more than one occasion, intervened directly when we believed someone was at risk. This paper formalises that work, gives it intellectual context, and makes the case that it belongs inside the planning conversation as a permanent fixture, not an occasional warning.

Three categories of financial risk

Market risk: the value of your investments falls. Visible, measured, and much discussed.

Behavioural risk: you make poor decisions under pressure. Increasingly understood and managed.

Financial security erosion: your assets are extracted through fraud or manipulation. Growing fast, almost entirely absent from most financial plans.

Most financial planning frameworks recognise two categories of risk: market risk and behavioural risk. Market risk is visible, measured, and extensively discussed. It is the risk that the value of your investments falls. It is managed through diversification, asset allocation, and time horizon planning. Behavioural risk is less formally modelled but increasingly understood: it is the risk that you make poor decisions under pressure, sell at the wrong time, or allow emotion to override a sound long-term plan. Good advisers work to reduce both.

Financial security erosion is the third category, and it is the one most likely to be ignored entirely. It is the risk that your financial assets are extracted by someone else through deception, manipulation, or technical means. Unlike market risk, it does not appear in your

portfolio reporting. Unlike behavioural risk, it is not something your adviser can observe by watching how you respond to market volatility. It can happen quickly or slowly, visibly or invisibly, and it is often not identified until the damage is done.

The scale of the problem in New Zealand is not fully captured in any single dataset because under-reporting is endemic. The Netsafe and Global Anti-Scam Alliance State of Scams 2025 report, based on a nationally representative survey of 1,000 New Zealand adults, found that total scam-related losses reached approximately \$3 billion in the year to March 2025, equal to nearly 0.75% of GDP. Nearly a quarter of New Zealand adults reported losing money to scams in the previous twelve months, with an average loss of \$3,352 per person. Seventy-two percent reported experiencing a scam in the past year. Those figures cover only what is known. The real losses are understood to be substantially higher, because most people who are defrauded do not report it.¹

Total scam-related losses in New Zealand reached approximately \$3 billion in the year to March 2025.

Nearly a quarter of New Zealand adults reported losing money to scams in the previous twelve months.

87% of New Zealanders believe they can spot a scam. Victim numbers have not dropped.

How the threat has changed

The mental model most people carry of fraud is outdated. It centres on the unsophisticated: the email from a foreign prince, the obviously fake website, the implausible prize notification. These exist, and some people still fall for them, but they are not the primary risk for people that Moneyworks works with.

The threats that have caused the most significant financial harm to people we work with in recent years fall into five main categories. Each is worth understanding on its own terms, because the protective response to each is different.

Investment fraud

Investment fraud has become sophisticated enough to pass initial scrutiny from educated, analytically minded people. The typical pattern involves an approach through social media, an online ad, or a personal referral. The investment looks credible, often featuring a professional-looking website, a trading portal where the investor can watch their money appearing to grow, and responsive 'support' staff. The fraud is not revealed until the investor tries to withdraw funds, at which point the terms of the contract are suddenly enforced, more money is demanded to release the principal, or the operation simply goes silent.

One of our clients invested over \$100,000 with a company calling itself FX Revenues. The client had chosen not to discuss it with us beforehand, acknowledging later that they had expected we would say no. The investment portal showed consistent growth. When the client asked to withdraw, FX Revenues cited contract terms requiring a minimum number of monthly trades, then demanded additional funds to 'release' the original investment. They then suggested the client take a mortgage on their home to meet the demands. They threatened legal action for breach of contract when the client refused. When the client's

bank confirmed it was a scam, FX Revenues simply stopped responding. The money was gone.

Because FX Revenues was not registered as a financial services provider in New Zealand, the client had no legal mechanism to recover the funds and no regulator to complain to. The investment screens showing profit were entirely fabricated. The relationship that had felt credible and responsive for months was a script.

In New Zealand it is illegal to sell a financial product through a cold call or an unsolicited email. If a company offering an investment opportunity is not registered on the Financial Services Providers Register, you have no redress and no protection. That is not a technicality; it is the central mechanism by which these frauds operate with impunity.

In New Zealand it is illegal to sell a financial product through a cold call or an unsolicited email.

If the company is not registered on the Financial Services Providers Register, you have no legal recourse and no regulator to complain to.

Check any investment opportunity at companiesoffice.govt.nz/fsp before you engage further.

Impersonation

Impersonation fraud involves someone contacting you while posing as a person or organisation you trust: your bank, a government agency, your investment adviser, or the IRD. The caller or message presents a problem that requires urgent action, and the urgency is part of the technique. The more pressure you feel, the less likely you are to pause and verify.

I received one of these calls myself. An 'unknown number' with a scratchy line. The caller sounded like a New Zealander and identified themselves as calling from Kiwibank about a suspicious transaction on my account. I kept asking which account. They had to ask me three times before they deviated from their script. When they said it was my cheque account, I told them I did not have a cheque account with Kiwibank and ended the call. It would have been more difficult if I had.

The lesson is not that I was clever. The lesson is that the call was plausible enough that I engaged with it at all, and that the protection came from asking a specific question they could not answer, not from identifying anything obviously suspicious in the approach. Most people would not have asked that question three times.

AI is now making impersonation significantly more difficult to detect. Voice cloning technology can reproduce a familiar voice from a short audio sample. A call that sounds like your financial adviser, your adult child, or your bank manager can now be generated with tools that are widely available. The question 'does this sound right?' is no longer reliable protection.

Romance and relationship manipulation

Romance scams are among the most financially devastating and least discussed forms of fraud, not because they are rare but because the combination of financial loss and emotional harm makes victims reluctant to come forward. The FBI describes them as

occurring when a criminal adopts a fake identity to gain a victim's affection and trust, then uses the illusion of a relationship to manipulate and extract money.²

The pattern typically begins on a social media platform, a dating site, or in an online community where the target is active. The fraudster identifies a point of contact, initiates conversation, and gradually escalates the relationship. They are patient. The manipulation can develop over months before any financial request is made, which is part of why it works: by the time money is involved, the victim has invested time, emotion, and trust.

Margaret, a widow living alone in a major city, began a conversation online after commenting on a quiz result. Someone responded, flattered her, and the relationship moved to Google Chat. Over the following months Margaret and the person she knew as 'David' communicated daily. He was attentive, interested in her life, and made her feel less alone. There were video calls. She saw photographs of his home. Then in August things began to go wrong for David, and he needed help with money. Then more money. Then there was a story about an oil rig, a storm, an insurance delay. He could not travel to see her because something always came up.

Margaret used her bank accounts, drew her credit cards and overdraft to their maximum. She contacted us to release investment funds to cover what she said was a debt, without explaining the full picture. We paid out the first time. The second time, the alarm bells rang. We said we would only release further funds if she could confirm this was not a scam. She confirmed it was not. We were not convinced. After a sleepless night we phoned her and went through the details. We asked what she would do if it turned out to be a scam. She said she had enough money for another five years, she did not think she would live that long, and she had been happier these past months than she had been in years.

We paid the smaller amount requested and told her it was the last we would release. A few weeks later came a breathless call requesting another \$4,500 urgently. We said no. Because the funds were held in a trust structure, we were in a position to refuse without her unilateral consent. Had the money been in her name alone, we would have been legally obliged to pay it out. Twenty or more emails later, after we sent her links to the Economist's 'Scam Inc' podcast series, Margaret accepted that David was not real. By then she had made 42 separate cash withdrawals, drove across her city to deposit them into cryptocurrency ATMs using a QR code he had provided. She had given away half her wealth and would need to live on a strict budget for the rest of her life. Even at the end of the meeting where this was all acknowledged, as we were walking out, she said she did not know what she would do if she found out David had harmed himself because she could not send the final amount. She still believed, weeks later, that the relationship had been real.

This case illustrates something that no checklist fully captures: the protection that financial structures provide when someone is being manipulated. The trust deed gave us the legal standing to intervene. Without it, we would have been witnesses to a loss we could see happening and been powerless to stop it.

Since then, we have taken a number of steps to help protect the people we work with. We now ask every person we work with what they would like us to do if we ever believe they are being scammed and they are not willing to listen to us. Most have nominated someone for us to contact: a family member or trusted friend who can, in their words, 'talk sense into me.' That conversation is now a standard part of how we plan.

Digital account takeover

Digital account takeover occurs when someone gains access to your online accounts, typically your email, your bank, or your investment platform. Once inside an email account, a fraudster can reset passwords on linked financial accounts, intercept communications, and operate with access to your financial life for an extended period before you notice. The entry point is often a data breach at an unrelated site where you have used the same password, a phishing link clicked in a moment of distraction, or physical theft of an unlocked device.

Smartphones present a particular and underappreciated risk. A phone that is unlocked, or whose PIN has been observed, provides access not just to the device but to every account linked to it. There are now organised theft rings that watch people enter PINs in public, then steal the phone and use the PIN to access and transfer funds before the owner realises what has happened. The time between theft and account access can be minutes. The damage done before a phone is blocked can be significant.

Imposter websites and fake investment platforms

The Financial Markets Authority issues regular warnings about websites that impersonate legitimate financial institutions or create the appearance of regulated investment platforms. These sites are sophisticated: professional in appearance, complete with terms and conditions, telephone support, and in some cases live chat. They may appear in search results above the sites they are imitating. The FMA publishes a list of known fraudulent entities and sends alert emails to subscribers, which is a service worth using.

Who is actually targeted

The persistent belief that fraud victims are naive, careless, or simply elderly is not supported by the evidence, and it is one of the reasons fraud is so effective. The assumption that 'I would know better' is itself a risk factor. People who are confident in their own judgement are precisely the demographic that sophisticated fraudsters target, because their confidence makes them more likely to engage, more resistant to outside intervention once engaged, and more reluctant to seek help when something goes wrong.

Investment fraud disproportionately affects people who have accumulated wealth, because they are the ones with something worth targeting. Romance fraud disproportionately affects people who are lonely or recently bereaved, because emotional vulnerability creates the opening that financial manipulation requires. Digital account takeover affects people who have not kept pace with security practice, which describes a large proportion of the population regardless of education or professional background. In New Zealand, people aged 18 to 40 were involved in nearly half of reported online fraud losses, demonstrating that this is not generationally bounded.³

Analytically minded professionals with accumulated assets and a high degree of confidence in their own judgement are not a protected demographic. They are a target demographic, sought out precisely because they have something worth taking and the self-assurance to engage with what looks like a credible opportunity.

What AI is changing

Artificial intelligence is accelerating the problem in ways that require a recalibration of the instincts most people rely on to protect themselves. Voice cloning can reproduce a familiar voice from a short audio sample. Deepfake video can simulate a trusted face in a video call. AI-generated text is now indistinguishable from human-written text, which means that the quality of written communication is no longer a reliable signal of legitimacy. AI is also being used to generate volume at scale: thousands of personalised phishing messages, fake advertisements, and fraudulent investment opportunities can be created and distributed at a cost and speed that was not possible a few years ago.

The practical implication is that the old test, which ran roughly as 'does this look and sound like something real?', no longer provides the protection it once did. Something can look real, sound real, and be generated by a machine running a fraud operation from another country. The protections that work are procedural ones: verification steps that a fraudster cannot easily replicate regardless of how convincing the approach appears.

What goes into a financial plan on this topic

Fraud and digital protection have traditionally been excluded from the financial planning conversation. They are treated as a technology problem, or a personal security matter, or something to mention briefly in a newsletter. They belong in the plan itself, reviewed annually alongside insurance, estate planning, and investment strategy. These are the elements that have a place in every plan.

A trusted contact person

A trusted contact is someone your financial adviser can reach if they have concerns about unusual activity in your account or believe you may be at risk. This is distinct from a power of attorney, which grants decision-making authority. A trusted contact simply gives the adviser permission to reach out to a nominated person and share their concern. It provides a circuit-breaker at a moment when you may not be in a position to act in your own interests. Most people, when we have raised this in annual reviews, have nominated someone immediately. Adding a trusted contact to your plan takes minutes and can prove to be one of the more consequential things in it.

A family safe word

A safe word is a word or phrase, known only to close family members, that can be used to verify identity in an emergency. If you receive a call from someone claiming to be your child in difficulty and needing money urgently, the safe word test is simple: ask for it. A fraudster cannot provide it. A genuine family member can. This requires a brief conversation with the people in your life, which is itself useful.

Password hygiene and two-factor authentication

Using a unique password for every account sounds impractical but is achievable with a reputable password manager. The alternative, reusing passwords across multiple accounts, means that a data breach at any one service can expose all of them. Two-factor authentication adds a second layer of verification that is significantly harder to bypass than a password alone. At a minimum, it should be enabled on any account connected to financial information: your bank, your investment platform, your KiwiSaver provider, and

your primary email address. Your email account is the master key; if a fraudster gains access to it, they can reset passwords on everything linked to it.

Device security

Your smartphone is a concentration of financial access. Bank accounts, investment platforms, authenticator apps, and email accounts are all typically accessible from a single device. Using a PIN or biometric lock that is not observable in public places is the baseline. Apple's Stolen Device Protection feature and equivalent Android settings provide additional protection by requiring biometric confirmation before allowing changes to security settings. If you use your device for financial transactions in public spaces, be conscious of who can see your screen and your hands.

Verification before any financial transfer

The single most effective protection against impersonation fraud is a verification step that runs independently of the channel used to make a request. If you receive a call, email, or message asking you to transfer money or provide financial information, verify by calling back on a number you have sourced independently, not one provided in the message. This applies even when the request appears to come from your bank, your adviser, or a family member. The inconvenience of one extra step is small relative to the risk of acting on a fraudulent instruction.

Staying informed

The FMA publishes regular investor warnings and maintains a list of known fraudulent entities. Subscribing to their alerts takes a few minutes and provides early notice when new fraudulent websites or entities are identified. Netsafe is the other primary New Zealand resource for reporting and advice. Both are worth knowing and worth checking if you encounter something that does not feel right.

How to raise this with the people in your life

One of the more difficult aspects of financial security erosion is that the people most at risk are often the least likely to discuss it. Older relatives may be embarrassed to raise concerns about a relationship they have formed online. Adult children may struggle to raise the subject with a parent without it feeling like an accusation of vulnerability. The conversation is worth having before a problem arises, not during one.

The Economist's podcast series 'Scam Inc' is one of the better resources for raising awareness without making the conversation feel personal or accusatory. Listening together, or sharing an episode, often opens the discussion more effectively than a direct conversation. Netsafe also publishes guides specifically for raising fraud awareness with older family members.

If you have any concern about whether an investment, a relationship, or an approach you have encountered is legitimate, bring it to your financial adviser. They will not be judgmental. They can usually form a view within minutes, and if there is any doubt they know who to contact. What they cannot do is help if they do not know the situation exists.

The underlying point

You have spent decades making financial decisions carefully. The assets you have built represent that care. Protecting them from financial security erosion deserves the same attention as growing them, and it belongs in the same conversation. It is not about being fearful or treating every approach with suspicion. It is about having structures in place before you need them, knowing what to look for, and understanding that the sophistication of fraud has advanced to a point where instinct and experience alone are not reliable protection.

This is part of what good financial planning looks like now. We raise it because we have seen what happens when it is not raised, and because the people who have been most harmed were not people who lacked the intelligence to protect themselves. They were people who had not been given the right framework to recognise the risk.

Your financial security checklist

Work through this list and tick off each item. If any are incomplete, we can help you address them at your next review.

Account and device security

☐	I use a unique password for every financial account and email address, stored in a reputable password manager such as Bitwarden, 1Password, LastPass or similar.
☐	I have two-factor authentication enabled on my bank accounts, investment platform, KiwiSaver account, and primary email.
☐	My smartphone is protected with a PIN or biometric that I do not enter in public where it can be observed.
☐	I have enabled Stolen Device Protection (Apple) or equivalent lock settings (Android) on my phone.
☐	I know how to remotely lock or erase my phone if it is stolen.

Financial planning protections

☐	I have nominated a trusted contact person that my financial adviser can reach if they have concerns about my account.
☐	My family has agreed on a safe word we can use to verify identity in an emergency.
☐	My will and enduring power of attorney are current and reflect my current wishes.
☐	I subscribe to the FMA's investor warning alerts.
☐	I know the direct phone numbers for my bank and financial adviser and use those to verify any unexpected contact, not numbers provided in the message.

Awareness and verification habits

☐	Any investment opportunity I encounter that I did not seek out goes to my financial adviser before I take any action.
☐	I verify unexpected contact from my bank or government agencies by calling back on a number I sourced independently.
☐	I do not transfer money or provide financial information in response to an unsolicited call, text, or email, regardless of how credible the approach appears.
☐	I am aware that AI can convincingly replicate familiar voices and that a call sounding like someone I know is not proof of who is calling.
☐	I have had a conversation with close family members about fraud risks and we know what to do if something looks wrong.

Notes and sources

1. Netsafe and Global Anti-Scam Alliance, State of Scams in New Zealand 2025 Report. Fieldwork conducted 26 February to 14 March 2025 with a nationally representative sample of 1,000 New Zealand adults. Total loss figure of approximately NZ\$3 billion extrapolated from survey data. Reported figures represent only a fraction of actual losses due to endemic under-reporting.

2. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). Romance scam definition and methodology as cited in Netsafe guidance materials.

-
- 3.** Netsafe and Global Anti-Scam Alliance, State of Scams in New Zealand 2025 Report. Millennials (76%), those in urban areas (79%), and those with higher education (81%) are among the demographics most likely to report having been scammed.
 - 4.** Financial Markets Authority (FMA). Investor warnings and register of known fraudulent entities. Subscribe at fma.govt.nz/subscribe-to-fma-news-and-alerts. Select 'alert and warning updates'.
 - 5.** Apple Stolen Device Protection: support.apple.com/en-nz/120340. Android Theft Protection Lock: support.google.com/android/answer/15146908.
 - 6.** The Economist, 'Scam Inc' podcast series. Available on major podcast platforms. Recommended as an accessible resource for raising fraud awareness with family members.

Moneyworks NZ Limited | FSP 15281 | 7c Hall Street, Cambridge 3434 | 0800 225 621 | www.moneyworks.co.nz