THE LITTLE BLACK BOOK of scams

FRAUD

CFFC

Building wealthy lives

"The CFFC is often asked to help New Zealanders who are victims of scams that started out as an offer of friendship, romance or a business opportunity.

Scammers' methods are increasingly sophisticated and they are persistent in their efforts. The impact on victims can be soul destroying.

I hope this book arms you with the knowledge to be cautious - in the world of cold-calling and online contact, not everyone is worthy of our trust."

Jane Wrightson
Retirement Commissioner

CONTENTS

FRAUD FIGHTING 101

Become a real-life superhero by arming yourself with the information you need to fight fraud and keep yourself, your family and your money safe.

You work hard for your money. You want to spend it on things that matter to you - whether it's your children's education, an exciting trip or a new phone.

Fraudsters are real. They are out there every day looking for victims. They will target you online, over the phone, by mail or in person.

You're a target. Thousands of New Zealanders lose millions of dollars to fraudsters every year. The impact of fraud on families and businesses can be devastating.

Learn to fight fraud. This booklet includes 11 of the most common scams currently targeting New Zealanders. It is filled with tips and tricks on how to protect yourself and what to do if you get scammed.

Report it! Anyone can be targeted, from teenagers, to grandparents, to senior corporate officers. The best thing you can do is to report the fraud, whatever the amount, to the appropriate authorities. Don't be embarrassed as it will help others from falling for it.

KNOWLEDGE IS POWER

Protect yourself by seeking out more information.

In addition to this booklet, you can also consult numerous trusted websites for more information.

www.scamwatch.govt.nz

INVESTMENT scams

Are you a target?

Investment scams are becoming more sophisticated. Fraudsters are smart, friendly, charming and persuasive. Websites look professional and you may even be given an online account showing details of 'trades' you've made. It can be hard to tell a scam apart from a genuine investment, which is why it's even more important you know what to look out for.

Anyone can lose money through a scam. It's no longer only vulnerable members of the community, such as the elderly, who are being targeted. In fact if you're an experienced investor, you're more likely to be a target.

In New Zealand it's illegal to sell financial products off the back of a cold call. If you receive an unexpected call about an investment opportunity, hang up straight away. Don't engage the caller as they'll use their skill to persuade you to part with your money.

Contact the Financial Markets Authority (FMA), *for more information refer to page 17.*

TIPS TO PROTECT YOURSELF

- ✔ Find out the **legal name** of the business you're dealing with.
- ✔ Check that the business/individual is **regulated by FMA**.
- ✔ If the business is not based in New Zealand, **find out who regulates them.**
- ✔ **Check** the regulators' warning lists.
- ✔ If you have lost money through a scam, you are highly likely to be targeted again – **stay alert.**

IDENTITY *theft*

Help ensure your identity remains yours alone!

Scammers are always on the lookout to collect or reproduce your personal information to commit fraud. Thieves can make purchases using your accounts, obtain passports, receive government benefits, apply for loans, and more. This could turn your life upside down.

Fraudsters use techniques that range from unsophisticated to elaborate. **Offline,** they can go through trash bins or steal mail.

Online, they can use spyware and viruses, as well as hacking and phishing.

They look for credit card information, bank account details, full name and signature, date of birth, full address, mother's maiden name, online usernames and passwords, driver's licence number, and passport number.

Identity theft is a serious crime! *For more information refer to page 18.*

TIPS TO PROTECT YOURSELF

- ✔ Never provide your personal information **over the phone, via text message, email or the internet.**
- ✔ **Avoid public computers or Wi-Fi hotspots**, such as in coffee shops, to access or provide personal information; they put you at risk.
- ✔ Create **strong and unique passwords** for each of your online accounts. Password-protect your devices and home Wi-Fi network.
- ✔ Use **2 Factor Authentication.**
- ✔ **Update** your computer operating system.
- ✔ Use a secure and reputable payment service when buying online—look for a URL starting with **"https"** and a **closed padlock symbol.**
- ✔ Avoid giving out personal information **on social media**. It can be used along with your pictures to commit fraud.
- ✔ Always s**hield your PIN** when using your card. If you hand it over to a cashier, never lose sight of it.
- ✔ **Shred and destroy** documents with personal information.
- ✔ **Protect** your mobile phones.

ROMANCE scams

Who is really behind the keyboard?

Keep your guard up and look out for potential scammers who will try to lower your defences by appealing to your romantic and compassionate side. They can prey on you through email, social media, dating websites, other websites and apps.

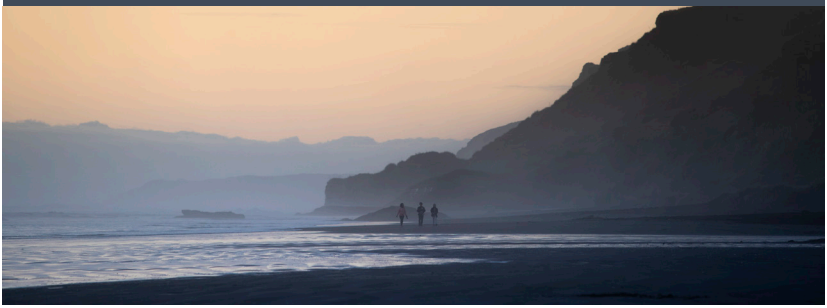
A scammer might send you a few messages and a good-looking photo of themselves, or of someone they claim to be. Once you are charmed, they will start asking you to send money. They may claim to have a very sick family member or a desperate situation with which they need your help.

They will move quickly, confessing their love or strong feelings within a short time of meeting. They may ask for money to help with airfares to come and see you, but never arrive due to an emergency.

Refer to page 18 to report the scam.

TIPS TO PROTECT YOURSELF

- ✔ **Never send money** or give financial details on a dating site.
- ✔ **Be cautious** about who you communicate with online.
- ✔ **Don't respond** to requests or hints for money.
- ✔ **Never send money** to anyone you don't know or haven't meet in person.
- ✔ Avoid giving our personal details that **could be used to impersonate you.**
- ✔ If you think you are being scammed, **stop all contact and avoid sending further payments.** Protect your mobile phones.



BUSINESS EMAIL COMPROMISE *scams*

Your CEO is asking for money urgently; make sure the email is legitimate!

Do you work in accounting or finance? Do you have the authority to move money at work? Do you report to a chief executive officer (CEO)? If yes, **be on the lookout;** this scam specifically targets you!

In a typical **"CEO scam,"** fraudsters will impersonate a senior company executive, either by gaining access to their email address or by imitating one. They will send realistic-looking emails that try to trick you into sending money to a third party.

The emails will make the request sound urgent and confidential. **For example,** they may say the money is needed to secure an important contract, complete a confidential transaction, or update a supplier's payment information.

Fraudsters are usually strategic about the timing of these emails.

They send them when executives are away or hard to reach. This lucrative scam can cost businesses tens of thousands to millions of dollars.

BEC scams are a growing global threat that targets small local businesses and large corporations alike.

TIPS TO PROTECT YOURSELF

- ✔ Keep your computer systems secure with an **up-to-date, reputable antivirus software** and **strong passwords**.
- ✔ **Validate all transfer requests** either on the phone or in person. Never use the contact information provided in emails.
- ✔ **Verify the sender's email address** — scammers will often create addresses that are very similar to legitimate ones, with just one or two different letters.
- ✔ Encourage your company to create a standard process for money transfers that **requires multiple levels of approvals**.
- ✔ **Limit the details you share publicly.** Fraudsters use information that's available online and on social media to find potential victims and to time their fraud.

PHISHING AND SMISHING *scams*

Be on the lookout. Messages are easily fabricated!

As we spend more time online, fraudsters are getting more creative with scams in the digital space.

Phishing is when you get an unsolicited email that claims to be from a legitimate organisation, such as financial institutions, businesses or government agencies. Scammers ask you to provide or verify, either via email or by clicking on a web link, personal or financial information, like your credit card number, passwords, driver's license or passport details.

Smishing is the same thing, except it occurs via text messages.

These messages often copy the tone and logo of organisations you trust, and usually include a call to action. ***They take many shapes and forms but the bottom line is that they seek your personal details.***

For more information refer to page 18.

TIPS TO PROTECT YOURSELF

- ✔ Know that **reputable organisations will never ask** for your personal information through email or text.
- ✔ **Ignore communications** from unknown contacts.
- ✔ **Delete suspicious messages** as they can carry viruses.
- ✔ **Don't reply to spam messages**, even to unsubscribe, and don't open any attachments or follow any links.
- ✔ To verify a hyperlink without clicking, hover your mouse over it. **Carefully check if it is accurate.**
- ✔ Update your antivirus software **on all devices**.
- ✔ Never use the phone number or email address provided in the suspicious message — **use contact information listed on verified websites.**

TAX SCAMS

Got a call or email from Inland Revenue? Make sure it's real!

You get a text message or an email from Inland Revenue (IR) claiming you're entitled to an extra refund and all you need to do is provide your banking details. Watch out – this wonderful-if-true situation is exactly what a tax scam looks like.

Another variation is that they call you to say that you owe IR money and that you need to pay right away, or else they will report you to the police.

In any case if you do receive a call, letter, email or text saying you owe money to IR, contact IR in the first instance.

www.ird.govt.nz/identity-security/phishing/

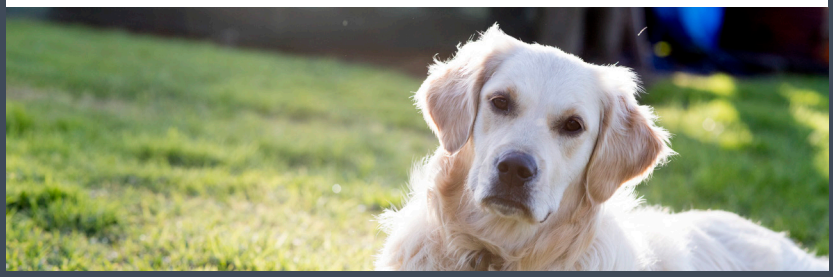
TIPS TO PROTECT YOURSELF

Phone calls and emails from Inland Revenue will never:

- ✔ Call you using aggressive or threatening language
- ✔ Threaten you with arrest or to send the police to your home
- ✔ Ask for payments via prepaid credit cards or gift cards, such as iTunes, Steam, etc
- ✔ Ask you to provide your myIR login or password
- ✔ Ask you to enter personal information into a third party website

Inland Revenue suggests:

- ✔ Keep your personal details up to date:
- ✔ The best way to keep your personal details up to date – such as address, mobile number, bank account number, etc – is in your secure online myIR account



DOOR-TO-DOOR *scams*

Knock, knock! Who's there? A scammer!

Despite living in the digital age, there are still some old fashioned scams that come right to your door, posing a threat to you and to businesses. With this trick, door-to-door salespeople use high-pressure tactics to convince you to buy a product or sign up for a service you don't want or need.

These aggressive pitches are often for charitable donations, investment opportunities or home services and maintenance of various appliances, like water heaters and air conditioners.

In many cases, you'll never receive the product or service promised. In others, the products or services are of poor quality or not as represented.

TIPS TO PROTECT YOURSELF

- ✔ **Don't feel pressured** to make a quick decision — take time to do some research on the seller and the products first.
- ✔ **Ask for photo ID,** get the name of the person and of the company or charity they represent.
- ✔ Ask for the charity's breakdown of where funds are allocated. **Be sure to get this in writing.**
- ✔ **Never share any personal information** or copies of any bills or financial statements.
- ✔ Only allow access to your property to **people you trust.**
- ✔ Research before you invest. Don't sign anything and **always read the fine print.**
- ✔ **Know your rights.** Contact Consumer Protection for more information on the Consumer Guarantees Act. www.consumerprotection.govt.nz
- ✔ **Use a Do Not Knock sticker** www.consumer.org.nz/articles/do-not-knock

EMERGENCY SCAMS

Caring grandparents, don't act too quickly!

Emergency frauds usually target loving grandparents, taking advantage of their emotions to rob them of their money.

The typical scam starts with a grandparent receiving a phone call from someone **claiming to be their grandchild**. The "grandchild" goes on to say they're in trouble - common misfortunes include having been in a car accident, getting locked up in jail, or trouble returning home from a foreign country — and they need money immediately.

The caller will ask you questions, getting you to reveal personal information. **They'll also swear you to secrecy,** saying they are embarrassed and don't want other family members to find out what's happened.

One variation of this ploy features two people on the phone, one pretending to be a grandchild and the other a police officer or lawyer. In other cases, the scammer will pretend to be an old neighbour or a family friend in trouble.

TIPS TO PROTECT YOURSELF

- ✔ **Take time to verify the story.** Scammers are counting on you wanting to quickly help your loved one in an emergency.
- ✔ **Call the child's parents or friends** to find out about their whereabouts.
- ✔ Ask the person on the phone questions that only your loved one would be able to answer and **verify their identity** before taking steps to help.
- ✔ Never send money to anyone you **don't know and trust**.
- ✔ **Never give out** any personal information to the caller.

SUBSCRIPTION *traps*

Good deals can bait you into falling for expensive traps!

A subscription trap can trick you by offering **"free"** or **"low-cost"** trials of products and services. Products commonly offered are weight loss pills, health foods, pharmaceuticals and anti-ageing products.

Once you provide your credit card information to cover shipping costs, you are **unknowingly locked into a monthly subscription**. Delivery and billing can then be difficult, if not almost impossible, to stop.

Scammers use websites, emails, social media platforms and phones to reel people in. ***Remember, high-pressure sales tactics like a "limited time offer" are often used to rush you into making a decision.***

TIPS TO PROTECT YOURSELF

- ✔ **Trust your instincts.** If it's too good to be true, don't sign up.
- ✔ Before you sign up for a free trial, **research the company** and read reviews, especially the negative ones. Consumer Protection is a great source of information.
- ✔ **Don't sign up** if you can't find or understand the terms and conditions. Pay special attention to pre-checked boxes, cancellation clauses, return policies, and any vague charges.
- ✔ If you go ahead with a free trial, **keep all documents, receipts, emails, and text messages.**
- ✔ Regularly **check your credit card statements** for frequent or unknown charges.
- ✔ If you have trouble cancelling your subscription, **contact your credit card provider** or your local consumer protection organisation.

HEALTH AND MEDICAL *scams*

Watch out for magical cures that offer quick and easy fixes.

There are fraudsters out there who hope to take advantage of people's suffering. **The three most common** types of health scams are miracle cures, weight loss programmes and fake online pharmacies. In all cases, they often appear as sponsored posts on social media or website pop-ups.

Scammers offer products and services that seem to be legitimate alternative medicines and treatments that quickly and easily treat serious conditions.

Some of these may seem to be **endorsed by celebrities** or promoted by testimonials of people claiming to have been cured.

Weight loss scams promise dramatic results with little to no effort. The scammers might promote unusual diets, revolutionary exercises, fat-busting devices, or breakthrough products, such as pills, patches or creams.

Fake online pharmacies offer drugs and medications at very cheap prices or without a doctor's prescription. They advertise on the internet and send spam emails. ***If you do receive the promised products, there is no guarantee they are the real thing or safe to take.***

TIPS TO PROTECT YOURSELF

- ✔ Remember that **there are no magic pills** or miracle cures for achieving quick weight loss or treating medical conditions.
- ✔ Don't trust claims about medicines, supplements or other treatments. **Get the facts straight from your healthcare professional.**
- ✔ **Never commit to anything under pressure**, especially if a large advance payment or long-term contract is required.
- ✔ Know that if an online pharmacy is legitimate, it will require **valid prescriptions.**
- ✔ **Be sceptical** of celebrity endorsements or testimonials.
- ✔ **Check** with your doctor in the first instance.

PURCHASE OF MERCHANDISE *scams*

Not all online vendors are reputable!

Online shopping is a favourite pastime for many consumers. But many deals you see online — from inexpensive designer purses to significantly discounted electronic goods — are too good to be true.

Fraudsters can create accounts on legitimate auction sites, such as eBay or Trademe, or on an online marketplace, like Facebook. They will advertise their products at very low prices, **enticing you to buy them.**

At the end of the day, if you do get something, it might be of poor quality or a bad imitation of what you expected.

In other instances, fraudsters will lure you into clicking on sponsored links that will direct you to a seemingly genuine website. If you decide to buy from there, you won't benefit from any protection or services that legitimate websites offer.

There is also an increase in fraudsters using .co.nz domain names and selling counterfeit goods at realistic prices.

TIPS TO PROTECT YOURSELF

- ✔ Buy from companies or individuals **you know by reputation** or from past experience.
- ✔ Never make a deal **outside the auction site**.
- ✔ **Beware** of sellers from far away or that have limited or no reviews.
- ✔ Use a credit card when shopping online and **use a card with a reduced limit**.
- ✔ **Be wary of websites** that contain spelling mistakes and grammatical errors.
- ✔ Read the **refund and return policies** carefully, including the fine print.
- ✔ **Ask the supplier questions** and confirm service delivery timelines and the total cost.
- ✔ Does the website information **match the product they are selling.**

RED FLAGS
things to watch for

Learn to recognise the signs that something is amiss.

WIRE TRANSFER

Many scams involve a request to wire money electronically using a money transfer service, like MoneyGram, Western Union, or using cryptocurrency, such as Bitcoin. Remember that sending a transfer through these services is like sending cash — ***once the amount is picked up, it's almost impossible to get your money back.***

OVERPAYMENT

When you're selling something —especially online— be wary of how you get paid. A fraudster may send you a counterfeit cashier's, personal or corporate cheque in an amount in excess of what they owe. You'll be asked to deposit the cheque and wire the excess funds immediately back to them. ***Once your bank realises the cheque is a fake, you'll be on the hook for the money withdrawn.***

SPELLING MISTAKES

Be sceptical of emails, messages or websites that contain misspelled common words; grammar errors that make it difficult to read or expressions that are used incorrectly. Email and web addresses should also be examined closely to see if there are subtle mistakes or differences.

PERSONAL INFORMATION REQUEST

Fraudsters may ask potential victims to provide more personal or financial information than is required for the transaction or discussion. ***Be suspicious if someone asks for copies of your passport, driver's licence or birth date, especially if you don't know the person.***

UNSOLICITED CALLS

You might get a call from someone claiming that you have a virus on your computer, you owe taxes or there has been fraudulent activity in your bank account. Hang up and call the organisation yourself using the number from a trustworthy source, such as the phone book, their website, or even invoices and account statements.

UNSOLICITED FRIEND REQUESTS ON SOCIAL MEDIA

Don't accept friend requests from people you don't know until you review their profile or ask your real-life friends if they know them. Does their profile look fairly empty or have posts that are very generic? Do they seem to be promising more than friendship? ***These are some red flags that point to a scam. Delete that request and block future ones.***

ASTOUNDING MAIL OFFERS

You received a scratchie card in the mail. It guarantees you will or have already won. Prizes might range from money to cars and trips. ***If you have not entered a contest, throw that card away. It's probably a scam!***

IT'S JUST TOO GOOD TO BE TRUE

Everybody loves a great deal. But shocking offers, unbelievable discounts and unreal rates may signal that the offer isn't quite what it seems. Cheap prices usually equal cheap products, or counterfeit goods. Free offers may require providing your credit card for shipping. ***Small tactics like these can lead to big profits for scammers.***

WORDS OF WISDOM FROM NZ POLICE

Prevention is the only effective way to avoid losing money through scams. Do not send money to anyone you may have met on social media but not met in person, or to any person or organisation who emails you asking for money.

If you do send money and think you've been scammed, you must contact your bank immediately. Once this action has been taken, you can contact your local police, Netsafe or CERT to lodge your complaint.

The sooner your loss is reported to your bank, and then to law enforcement, the better.

All complaints to police are assessed in the same way and prioritised. But members of the public must be realistic - if you do not check things out carefully before sending money offshore, and then discover you've been a victim of fraud, there is little chance you will recover your money, and little chance that the offenders will be apprehended or that anyone will be held accountable. Often, all police can do is share intelligence with our partner agencies offshore.

Acceptance of this loss is key in moving on with your life, rather than trying to make someone accountable.

Remember, the best way to avoid being scammed is to stop before you start:

DO NOT send money to anyone you have not met in person, and trust.

REPORTING A SCAM

Who to contact depends on what type of scam is involved. Whether you've been scammed or targeted by a fraudster, you should always report it.

New Zealand authorities may not always be able to take action against scams, but there are ways you can help. By reporting the scam, authorities may be able to warn other people and alert the media to minimise the chances of the scam spreading further. You should also warn your friends and family of any scams you come across. ***Below is advice on where to report various types of scams:***

Anyone who believes they are a victim of any crime, in person or online, should **report the matter to their local Police.**

Financial and investment scams

Contact Financial Markets Authority

You can report financial and investment scams to the Financial Markets Authority.

www.fma.govt.nz
Ph: 0800 434 567

Cyber Security Scams

You can report any cyber security issues to CERT NZ. They can help to identify the issue and give you advice about next steps.

www.cert.govt.nz
Ph: 0800 237 869

Netsafe takes reports of all scams — whether or not they happen online.

www.netsafe.org.nz
Ph: 0508 638 723

Banking and credit card scams

Contact your bank or financial institution

In addition to reporting these scams to other authorities, you should alert your bank or financial institution about any suspicious correspondence that you receive regarding your account.

They can advise you on what to do next. When contacting your bank or financial institution, make sure to use the telephone number found in the phone book, on your account statement or on the back of your card.

Spam emails and text messages

Contact the Department of Internal Affairs

The Department of Internal Affairs is responsible for investigating complaints about unsolicited commercial electronic messages, commonly referred to as spam. If you want to report email spam there are two easy options. You can either **fill out an online form** or forward the spam email to us directly at **complaint@spam.govt.nz.**

TXT Spam – Forward the offending TXT message from your phone free of charge to our short code: **SPAM (7726)** **www.spam.govt.nz**

Age Concern New Zealand

Age Concern provides free confidential advice and support for older people and their families who have been scammed or financially abused. Contact one of the national network of 33 local groups.
www.ageconcern.org.nz

Identity theft

Contact the Police and IDCare.

Identity theft refers to the acquisition and collection of someone else's personal information for criminal purposes.

If you suspect or know that you are a victim of identity theft or fraud, or if you unwittingly provided personal or financial information, you should:

- ✔ Contact your local police and file a report.
- ✔ Contact your bank or financial institution and credit card company.
- ✔ Contact the 3 credit reporting companies and place a fraud alert on your credit reports.

Creditors of potential fraud:

Centrix
www.centrix.co.nz
Ph: 09 9669706

Dun & Bradstreet (NZ) Ltd
www.checkyourcredit.co.nz
Ph: 0800 362 222

Equifax NZ
www.mycreditfile.co.nz
Ph: 0800 692 733

IDCare
www.idcare.org

Always report identity theft and fraud.

This booklet was created with the input of a variety of stakeholders and their contributions are greatly appreciated. We would like in particular to recognize the Australian Competition and Consumer Commission (ACCC), who originally developed the The Little Black Book of Scams, giving rise to our own edition here in New Zealand.

KNOWLEDGE IS POWER!

cffc.govt.nz

Commission for Financial Capability (CFFC)
Level 15, 19 Victoria Street W, Auckland Central, 1010
PO Box 106-056, Auckland City 1143
Office phone: +64 9 356 0052 | Office email: office@cffc.govt.nz

cffc.govt.nz | sorted.org.nz | moneyweek.org.nz