Little BLACK BOOK of SCAMS

Live sorted

netsafe
netsafe.org.nz

Contents

Fraud fighting 101

Learn to fight fraud
This booklet includes some 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.

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 computer.

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.

Report it
Anyone can be targeted, from teenagers, to grandparents, to senior corporate officers. The best thing you can do is 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. **netsafe.org.nz**

Netsafe's **new** weapon

Scammers are so clever, it can be hard to tell what is real and what is fake. So, to try and help you sort the good deals from the good-for-nothings, Netsafe has a smart new tool – **checknetsafe.nz**.

Type in or copy and paste the web address link you want to check – within seconds you will know if the link is a scam or legitimate.

Investment scams

Are you a target?

Investment scams are becoming more sophisticated. Fraudsters are smart, 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 for.

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

Watch for investments that are being promoted or endorsed by "celebrities" – these are also more than likely a scam.

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 with the caller as they will use their skill to persuade you to part with your money.

Contact the Financial Markets Authority (FMA)
fma.govt.nz

Tips to protect yourself:

1. Before you invest – investigate.
2. Run the company website address through **checknetsafe.nz**
3. Find out the legal name of the business you are dealing with.
4. Check that the business/individual is regulated by FMA.
5. If the business is not based in New Zealand, find out who regulates them.
6. Check the regulators warning lists. **iosco.org/investor_protection/?subsection=investor_alerts_portal**
7. If you have lost money to a scam, you are highly likely to be targeted again – stay alert.

Phishing & 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.

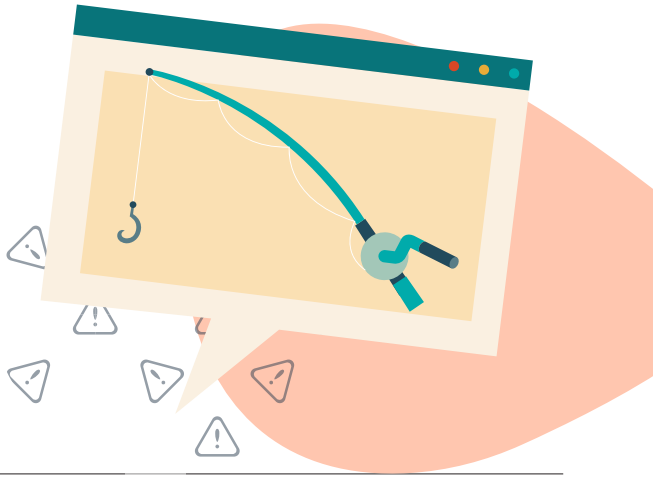
Phishing is when you get an unsolicited email that claims to be from a legitimate organisation, such as financial institutions, businesses or government agencies. Scammers ask you to provide or verify either via email or by clicking on a web link, personal or financial information, like your credit card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

SMISHing (SMS phishing) is the same thing, except it occurs via text messages. They use scare tactics to trick you into paying a fake toll, or overdue invoice.

Remember, scammers are constantly evolving their tactics, so it's important to stay vigilant and adapt to new threats. Don't be an easy target.

Tips to protect yourself:

1. Be vigilant and cautious. Always maintain a healthy level of scepticism when dealing with emails, messages, or websites that ask for your personal or sensitive information.
2. Double check the sender's email address, domain, or contact details to ensure they are legitimate. Best idea is to pick up the phone and talk to the organisation directly to confirm.
3. Don't click on or open suspicious links: hover your mouse over links in emails or messages to check their actual destination before clicking on them. Copy and paste into **checknetsafe.nz** to double check.
4. Be cautious with attachments: be wary of opening email attachments. Malicious attachments can contain viruses or malware that can compromise your computer security.
5. Keep your software up to date: regularly update your operating systems, web browsers and security software.
6. Don't reply to spam messages even to unsubscribe.



Romance scams

Who is really behind the keyboard?

Romance scammers are good at what they do and can spend months building up trust before they start to ask for sums of money. There's no fail-proof way to identify a romance scam, but there are signs to look out for.

A scammer pretends to be in a relationship with someone online in order to scam them out of their money. They do this through email, social media, dating websites and other websites and apps. Usually these scammers are pretending to be someone they're not, using stolen photos and identities of people they've found online. Netsafe have had cases of romance scams reported to them where people have lost substantial amounts of money ranging from a few hundred through to millions of dollars.

The scammers may move quickly, confessing their love or strong feelings within a short time of meeting. They pretend to be in a desperate situation and need your help. They might ask for money to help with airfares to come and see you or to help them with sick family members. They will prey on your empathy and compassion.

A particularly nasty twist is the 'pig butchering' scam. Scammers create fake accounts on dating and social media platforms to target victims to invest in cryptocurrency. They build trust and intimacy with their victims before stealing their crypto or money.

Tips to protect yourself:

1. Be wary if they ask you to move off the platform you started on.
2. Never send money or give financial details on a dating site.
3. Don't respond to requests or hints for money or gift cards.
4. If you think you're being scammed stop all contact and avoid sending further payments.
5. Contact the team at **netsafe.org.nz** freephone: 0508 638 723

Identity theft

Help ensure your identity remains yours alone!

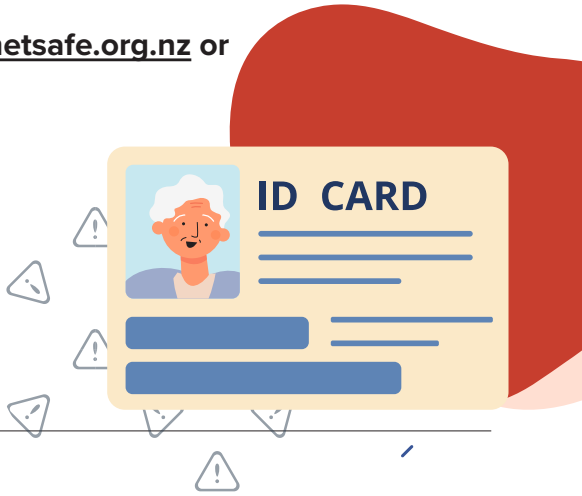
Scammers are always on the lookout to collect or reproduce your personal information to commit fraud. Thieves can make purchases using your accounts, apply for loans, receive government benefit and more. This could turn your life upside down.

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

Online, they can use spyware and viruses, as well as hacking and phishing, which is explained a little further on.

They look for credit card information, bank account details, full name and signature, date of birth, full address, mother's maiden name, online user names and passwords, drivers licence number and passport number.
Identity theft is a serious crime.

For more information contact netsafe.org.nz or idcare.org



Tips to protect yourself:

1. Never provide your personal information over the phone, via text message, email or internet. Unless you have initiated the action.
2. Avoid public computers or Wi-Fi hotspots to access or provide personal information.
3. Create strong and unique passwords for each of your online accounts, devices and home Wi-Fi network.
4. Use Multi Factor Authentication.
5. Update your computer operating system.
6. Use a secure and reputable payment service when buying online. Check the website through **checknetsafe.nz** before making any purchases.
7. Avoid giving out personal information on social media.
8. Always shield your PIN when using your card. If you hand it over to a cashier, never lose sight of it.
9. Shred and destroy documents with personal information.
10. Protect your mobile phone.

Emergency scams

Caring parents and grandparents, don't act too quickly.

Emergency frauds can target family members and even friends, taking advantage of their emotions to rob them of their money.

Scammers may impersonate family members claiming to have changed their number and asking you to save a new number into your phone.

The typical scam may start with a text message "Hi mum" and could provide several different reasons for why they are using a different phone number including switching providers or having lost or broken their phone.

A grandparent may receive a phone call from someone claiming to be their grandchild. The "grandchild" goes on to say that they're in trouble. Common misfortunes include having been in a car accident or even arrested and they need money immediately.

These schemes are designed to trick you into handing over money or financial information to a scammer.

Tips to protect yourself:

1. Take time to verify the story. Scammers are counting on you wanting to quickly help your loved ones in an emergency.
2. To steer clear of the “emergency” scam, it is advisable to make direct contact with your family member using their legitimate phone number and verify their situation before taking any further action. Additionally, reach out to other trusted family members or friends to confirm their actual whereabouts.
3. 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.
4. Never send money to anyone you don’t know and trust.
5. Never give out any personal information to the caller.

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 are 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 they call you to say that you owe Inland Revenue money and that you need to pay right away or else they will report you to the police.

If you do receive a call, letter, email or text saying that you owe money to Inland Revenue, contact Inland Revenue directly in the first instance and verify the situation.

Tips to protect yourself:

Inland Revenue will never:

- call you using aggressive or threatening language.
- threaten you with arrest or send the police to your home.
- ask for payments via prepaid credit cards or gift cards or cryptocurrency.
- 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 your address, mobile number, bank account details etc is in your secure online myIR account.

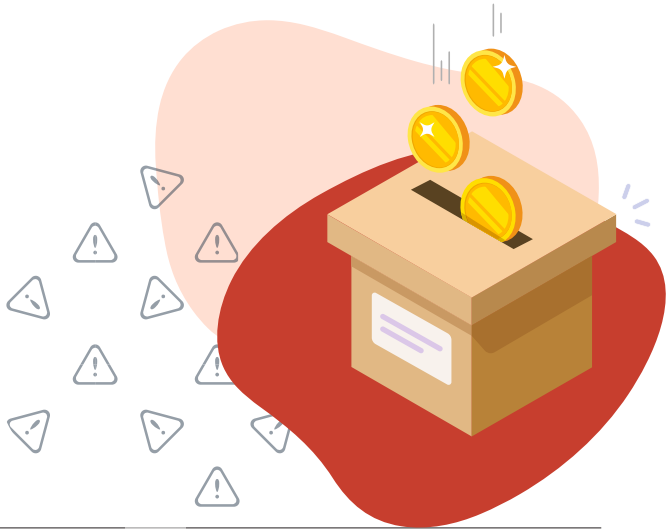
Door to door & charity scams

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 your business. 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:

1. Don't feel pressured to make a quick decision – take time to do some research on the seller and the products first.
2. Ask for photo ID, get the name of the person and of the company or charity they represent.
3. Check to see if the charity is registered. **register.charities.govt.nz/CharitiesRegister/Search**
4. Never share any personal information or copies of any bills or financial statements.
5. Only allow access to your property to people you trust.
6. Research before you invest. Don't sign anything and always read the fine print.
7. Know your rights. Contact Consumer Protection for more information on the Consumer Guarantees Act. **consumerprotection.govt.nz**
8. Use a DO NOT KNOCK sticker **consumer.org.nz/articles/do-not-knock/know-the-issue**

Health & medical scams

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

There are fraudsters out there who hope to take advantage of peoples' 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.

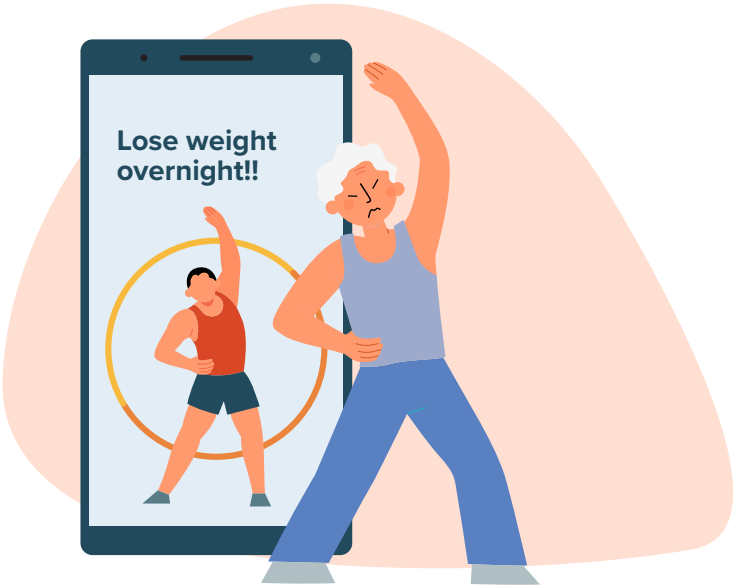
Some of these may seem to be endorsed by celebrities or promoted by testimonials of people claiming to have been cured.

Weight loss scams promise dramatic results with little or 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:

1. Remember that there are no magic pills or miracle cures for achieving quick weight loss or treating medical conditions.
2. Don't trust claims about medicines, supplements or other treatments. Get the facts straight from your healthcare professional.
3. Never commit to anything under pressure, especially if an advance payment or contract is required.
4. Know that if an online pharmacy is legitimate, it will require a valid prescription. Run the website address through **checknetsafe.nz** first.
5. Be sceptical of celebrity endorsements or testimonials.
6. Check with your doctor in the first instance.



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-aging 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:

1. Trust your instincts. If it's too good to be true, don't sign up.
2. 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. **consumerprotection.govt.nz**
3. 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.
4. If you go ahead with a free trial, keep all documentation, receipts, emails and text messages.
5. Regularly check your credit card statements for frequent or unknown charges.
6. If you have trouble cancelling your subscription, contact your credit card provider or your local consumer protection organisation.

Purchase of goods or services scams

Not all online vendors are reputable or all brands are who they say they are.

The surge in online shopping, prompted by the pandemic, has made it a popular pastime for many consumers. However, it's crucial to exercise caution as numerous online deals, ranging from inexpensive designer purses to significantly discounted electronic goods, are often too good to be true.

Brands get targeted too with copycat websites and fake ads.

Scammers employ various tactics, such as creating accounts on reputable auction sites like eBay or Trademe, as well as online marketplaces like Facebook. They entice buyers with low prices for their products, but the end result may be poor-quality items or disappointing imitations. Or even items not delivered.

In some cases, fraudsters use sponsored links to redirect unsuspecting users to seemingly authentic websites. If you decide to make a purchase there, you won't receive the protection or services offered by legitimate websites.

It's important to note that there has been a rise in fraudsters using .co.nz domain names to sell counterfeit goods at seemingly realistic prices.

Tips to protect yourself:

1. Before purchasing run the website address through **checknetsafe.nz**
2. Buy from companies or individuals you know by reputation or from past experience.
3. Never make a deal outside the auction site.
4. Beware of sellers that have limited or no reviews. Sadly the scammers create fake reviews too – good or bad.
5. Beware of sellers that ask for payment in advance.
6. Use a credit card when shopping online and use a card with a reduced limit.
7. Read the refund and return policies carefully, including the fine print.
8. Ask the supplier questions and confirm service delivery timelines and total cost. Most will supply a legitimate tracking number for you.
9. Check if the website information matches the product they are selling.

Red flags, things to watch out for

Learn to recognise the signs that something is amiss

Overpayment:

When you are selling something – especially online – be wary of how you get paid. A fraudster may pay you more money than you expected and then ask for a refund of the overpayment. This is a way of the fraudsters laundering money.

Wire transfer:

Many scams involve a request to transfer money electronically using a money transfer service or using cryptocurrency such as Bitcoin. Remember that sending transfers through these services is like sending cash – once the amount is picked up it is almost impossible to get your money back.

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. Do not give out any information and hang up immediately. Then call the organisation yourself using the number from a trustworthy source, such as their website, invoice or statement. Have your bank's number pre-stored in your phone.

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, drivers licence or birth date, especially if you don't know the person.

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 you 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 of the 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 range from money to cars and trips. If you have not entered a contest, throw that card away. It's probably a scam. Check the website through **checknetsafe.nz**

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 this can lead to big profits for scammers.

Technology is ever-evolving

Take this scam vulnerability test:

1.	Are you aware of common scam tactics?	**yes**	**no**
2.	Do you regularly update your computer and mobile device's security software?	**yes**	**no**
3.	Do you use strong, unique passwords for all your online accounts?	**yes**	**no**
4.	Have you enabled two-factor authentication for your important accounts?	**yes**	**no**
5.	Do you carefully review website URLs before entering personal information?	**yes**	**no**
6.	Are you cautious about clicking on links or downloading attachments in suspicious emails?	**yes**	**no**
7.	Do you verify the legitimacy of requests for personal information or financial transactions over the phone or email?	**yes**	**no**
8.	Have you taken steps to protect your social media accounts' privacy settings?	**yes**	**no**

Take this scam vulnerability test:

9. Do you research and verify the credibility of charities or organisations before making donations?	**yes**	**no**
10. Are you cautious about sharing personal information on social media or other public platforms?	**yes**	**no**
11. Do you regularly review your bank and credit card statements for any unauthorised charges?	**yes**	**no**
12. Do you stay informed about the latest scams and fraud trends?	**yes**	**no**
13. Have you educated yourself about phishing techniques and how to recognise them?	**yes**	**no**
14. Do you have a trusted source or resource to report suspected scams or fraud?	**yes**	**no**
15. Have you discussed online safety and scams with your family or friends?	**yes**	**no**

If you answered YES to most of these questions you are well on the way to being a fraud fighting superhero. But remember that frauds and scams are constantly evolving and continual education is the key to keeping yourself safe. So stay up to date with the latest scams at **netsafe.org.nz**

Reporting a scam

Who to contact depends on what type of scam is involved. Whether you have 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 or make a report using NZ Police's non-urgent 105 reporting tool.
police.govt.nz/use-105

Cyber security scams:

You can report any cyber security issue to CERT NZ. They can help to identify the issue and give you advice about the next steps.
cert.govt.nz
0800 237 869

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

netsafe.org.nz

Freephone: 0508 638 723

Spam emails and text messages:

If you want to report email spam there are two easy options. Either fill out an online form **dia.govt.nz/Spam-Report-Spam** or forward the spam email to complaint@spam.govt.nz

TXT Spam – forward the offending TEXT message from your phone free of charge to SPAM (7726)

Identity theft:

- Contact ID Care for more information and assistance. **idcare.org** 0800 121 068

Credit reporting:

- Contact the 3 credit reporting companies and place a fraud alert on your credit reports.

Centrix
centrix.co.nz
0800 236 874

Equifax NZ
mycreditfile.co.nz
0800 692 733

Illion
checkyourcredit.co.nz

Financial and investment scams:

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

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 on your account statement or on the back of the card. Or contact them directly through secure messaging using internet banking.

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

Knowledge is power.

Live sorted

netsafe
netsafe.org.nz