FRAUD SCAMS

Presented by Constable Sanders – Tauranga Police

Three main points to remember
1 – The Bank does not ring you. (Yes - there are a couple of exceptions to that but work off the principal that The Bank Does Not Ring You)
2 – If someone is asking for money then treat it like it's a scam
3 - Do not give out any personal details/passwords online or over the phone or click on any links sent to you where you cannot 100% verify who they are from.

Your Homework is to read the following website which covers off all types of scams going around and the two articles below.

https://netsafe.org.nz/advice/scams/

Serial fraudster who spent a decade targeting elderly jailed for more scams worth $371,000 | Stuff.co.nz

Phone reported stolen in London every six minutes - BBC News

https://www.bbc.com/news/technology-65486219

DO NOT CLICK ON ANY LINKS TEXT TO YOUR PHONE OR EMAIL ADDRESS

- Never open emails / text messages with attachments that your received unexpectedly
- Never open emails / text messages with attachments form people you don't know
- Never click on URL's (Website addresses) from people you don't know.
- Never forward emails / text messages with attachments unless you are sure the contents and the sender.

1. **Cellphones and Landline Phone Call Scams**

   If the phone number comes up saying the banks name E.G 0800 BNZ. It is an offender. Do not answer the call.
   If the bank does ring you it will normally be from a blocked number.

   If you do happen to answer a call from someone claiming to be from the bank, then tell them you cannot talk right now but will ring them back later. Ask for their name and contact number. **NB** DON'T ring them back on the number they give you.

   Ring the Banks 0800 listed number. Guarantee if it's an offender the person calling you will not want to give you a number to call them back on.

A line an offender will often say is “Someone is trying to use your credit card right now or that someone is trying to access your bank account or that your bank account has been compromised. In order for us to stop this we need some details from you” DO NOT EVER GIVE ANY DETAILS OVER THE PHONE.

If you stay on the phone too long then the offender will send you messages / links to your cell phone or email address and give you instructions or ask you to download software. Do not open or touch any of these. Hang up the phone immediately.

Landline phone calls will be simular but offenders may use something else you are familiar with the company Spark. E.G I am James and I work for Spark. In order for me to help you I need some details.

Hang up the phone call straight away.

My recommendation here is to always hang up and then ring the bank back yourself or go into a branch and see them and ask if someone was trying to contact you.

NB My home landline rings almost every night. I have caller ID set up. So I just look at the number. 8 times out of 10 its an overseas or weird number so I don’t answer it. I figure if its important they will leave a message. But guess what. No one ever leaves a message.

2. Credit Card Fraud & Bank Card Fraud

Be vigilant in checking your bank statements regularly. Keep an eye on any transactions you are not familiar with or aware of.

Just because you have your credit card in your wallet/purse does not mean someone else is using it right now!
This happens could be for a number of reasons.
1 – If making an online purchase make sure you use a website that has a Lock Icon on the top line. These sites are more secure than those who don’t have it. Offenders at times may hack into a company’s database and obtain credit card details which are kept on file.

2 - There may be a dishonest person working at premises who either uses or gives your card details to another offender.

3 - It’s my understanding that there are people overseas who have computer programmes running credit card numbers 24/7, and eventually when they get a hit on one that works, they will then sell it on the black market to someone who will then start using your credit card to go spending your dollars. For example, in your bank statement you may see a transaction for $0.01 or $1.00, something quite low initially. That’s where the offender is checking your card to make sure it works. Or it may something like Mircosoft $19.99. If you see that contact your bank straight away.

**Good news is your bank will generally (not always) refund any authorised transactions back to you. It may however take them up to a month to do so.

PAYWAVE CARDS - Banks automatically generally set up the Paywave option. My advice is if possible, cancel the Paywave option. This will prevent offenders from using your card and cleaning out your bank account should they get in possession of it.

Also I've been informed that your paywave card could be in your pocket or purse and the machine picks up your card for up to a metre or two away and the payment goes through without you even bringing your card out. Kathmandu sell covers to place your paywave card in that prevents the machines from picking up your paywave card.

3. Romance Scams

In Life people will often make things sounds or interpret things as to what they want to here.

A number of people are looking for companionship. Most people start doing that these days online. Children and Grandchildren usually do this.

There are two types of love scams.

1 – When you only ever have contact with the person online. As soon as they start asking for money it's a scam. End the relationship no matter how convincing they are.

2 – When you do meet them in person. Once again it takes time to get to know the person. Find out things about them. Don't be afraid to do Internet searches on their name, make enquires into their background to see they are telling the truth.
NB If they start asking for money then break the relationship off. If together for 2yrs or more the other person may be entitled to half of what you own.

4. Text Messages & Emails

The old saying "if it sounds too good to be true then it's too good to be true"

DO NOT CLICK ON ANY LINKS SENT TO YOUR PHONE OR EMAIL ADDRESS IF YOU DO NOT KNOW WHO THEY ARE FROM.

TEXT MESSAGES
You may get random text messages from time to time.
E.G One going around is one claiming to be from NZ Post.
Message may read " We have a courier package for you. But before we can deliver it we need you to pay the customs clearance fee of say $4.50". DO NOT PAY IT. If you do the offender will have your credit card details.

If you were unsure about any message you receive, then ring the company's. I can guarantee they won't know who you are.

Road Toll text message – it might say “Hey just to let you know your account is overdue by $2.50 – click here to pay the outstanding amount” Same principal apply’s. Don’t click on any link or reply to it.

IRD saying you owe them money. Ring IRD yourself to confirm.

**If in doubt about anything then I would ask someone you trust, should you ever receive anything you are unsure about. Waiting another 24 to 48hrs for the right answer is much better than making a rash decision you end up regretting where lots of money is lost.

EMAIL ADDRESS
You will get random emails with the promise that you may have won something or that you own someone money. The message will ask you to confirm or provide personal details. It will be a lie.
NB If you receive an email from an address, you do not know or are not expecting, delete it. Do not open it.

Once again some of these emails can be very convincing. The company email address may look correct but there may be a slight spelling difference of one letter to the actual correct one. E.G It is easy for offenders to use legitimate information to make it all look genuine such as Logos ect…

5. Business Fraud

Be aware that you or your business might receive an email from a customer or employees email account where it informs you that their bank account number has changed, so can you please pay the next invoice or paycheck into the new account. NB They may even send false invoices for you to pay.

Do Not make those changes. Ring the person requesting it to make sure that is correct. I can guarantee you it wont be.

Offenders can hack into a company or individuals email account so you think you are dealing with the company or person where it may be the offender.

6. Identification – Driver’s Licence

Whatever you do, DO NOT photograph and send a photo of your driver’s licence as proof of I.D. to anyone or any other form of Identification. Once someone has a copy of someone’s driver’s licence, they can then start applying for finance online in your name.

So if you are unlucky to be involved in a vehicle accident. Do not let anyone take a photo of your driver’s licence. You can give them some of your name, date of birth

and insurance company. But DO NOT let them get your 3 digit version number of your licence or your address.

7. **Trade Me**

Trade Me is generally very good and safe to deal with.
Unfortunately, we do get the odd instance where fraudulent people create a Trade Me account to sell things that don't exist.

If someone shows you their driver's licence or any form of ID to prove its them, then its likely false. Do not go through with the sale. Where possible, pay for any item when it's picked up.

Check their sales history and feedback – the more sales and good feedback the safer you should be. If they are new to Trade Me or basically have no sales against their name, then I would be reluctant to buy anything from that person if it was more than $50. (howmuch you are prepared to lose).

Offenders will often cut and paste a legimate advertised items for sale off someone else's sale page and advertise it on Trade Me. E.G Cellphones, Vehicles.

8. **Social Media – What's App / Facebook Messenger**

If you ever get a message from a family member or friend asking for money or credit card details. It's a scam. Do Not do it.

The offender has likely hacked your family member or friend's social media account and sent you a message.

E.G This year we had a mother's day scam that goes something like this - 'hey mum / my phones broken / lost, I urgently need a new one. Can you send me some money and I'll pay you back – here's my bank account number'.

Do Not send any personal information on these online forums.

Ring your loved one on their lost number. Guarantee it will still work.

9. **Door to Door - Random people coming to your address**

In the past a handful of offenders have gone to people's property's officer a service E.G to cut your hedge or mow your lawns. Do not accept what they are offering. They will likely become pushy and try and do the work right then. Use the excuse that you already have someone who does the work for you. Then contact a family member or friend to seek their advice if still unsure.

If they start doing work on your property or refuse to leave then ring the police straight away.

Also if you get a knock on your door, try and get an idea on who it may be before opening the door if you can. I've had police open the door for me at 2 a.m. in the morning just because I said I was a police office. They just assumed I was without checking.

10. Shopping

Be careful where you place/leave your handbag / cellphones, especially the ladies. Don't leave your handbag unattended in a shopping trolley. It only takes an offender a few seconds to grab it and run off with it.

11. Contactor at your address doing work

There will be a genuine contactor/s or persons at your address who may need to use toilet or be in certain rooms. Could be people who do home help for the elderly. Don't be afraid to keep an eye on them or remove valuable items out of that room before they arrive.

Most people should be fine, but you just never know. Don't always keep your valuable jewellery or cash in your bedside table or the normal places that you have always left them. Consider putting items in other locations in the home.

Also check all your doors and windows after the contactor has finished to make sure your home is all secure.

12. Facebook Marketplace - #1 Fraud place

Simply answer is - Do not buy anything on Facebook Marketplace unless you can pick it up and hand over the money at the same time.

There are numerous scams running. The main one's going on at the moment are on: cellphones, shipping containers, power tools, pets for sale, caravans.
These scams will generally advertise a product at a fair price that will save you money versus buying it form a company. It will appear a fair price to pay. E.g. a cellphone might retail for $2,000.00 but they're selling it for $1,600.00. A shipping container might cost you $8,000.00 but they're selling it for $6,000.00. Animals as well that could be unique or hard to get and so people will pay what they want for them.

The offenders will also say, I have a lot of people wanting this item. In order to secure it for you then pay a deposit. It's a scam.