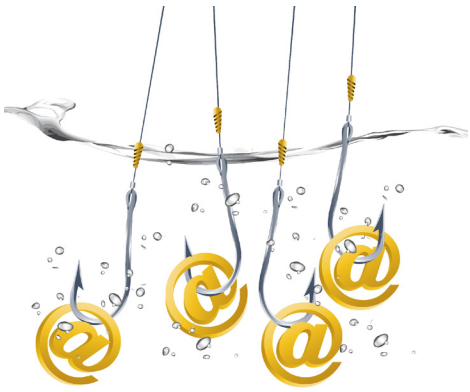
Common scams

INTERNAL AFFAIRS
Te Tari Taiwhenua

Scammers will do anything to rip you off, so it's important to be aware of the different kinds of scams circulating - especially if you use email or a mobile phone.

Phishing/banking scams



Phishing scams are emails that pretend to come from banks or other financial institutions. They urge you to click on links and enter your bank account details, credit card information, password, passport information, home address, or even your IRD number.

Many websites are clever fakes, and typing in your details could result in your bank account being emptied by fraudsters. Don't click on links in phishing emails as your computer could become infected with a virus.

If you have an account with the bank mentioned in the email, call the bank and verify the authenticity of the email. Remember that banks don't contact customers by email and ask them to confirm personal financial information. Most banks have information on their websites about reporting phishing or banking scams. Check out this information and make sure you alert the bank.

Example

From: ASB Bank [mailto:asbcacat17@admin.net]
Sent: Saturday, 22 September 2012 10:13 a.m.
Subject: ASB Online Locked - Support Update: Suspicious Activity
Dear ASB Customer,
Your ASB Online has been locked and is waitting for your response. If you do not take further action your account status will change to "Blocked" in 24 hours and automatically update to "Closed" in 48 hours. We found suspicious activity on your account and we need to confirm some transactions with you. Please confirm here: [website link removed]
Best Regards,
ASB Customers Department

Hints that it's a scam

- Email address is wrong - it should end '@asb.co.nz'
- Website link is wrong - it should link to 'www.asb.co.nz'
- It's not addressed to an individual ("ASB Customer")
- It has spelling mistakes ("waitting")
- If the bank needs to contact you they will call or post a letter to you

Report scams

Email: scam@antispam.govt.nz
TXT: Forward the message to our free shortcode 7726 (SPAM)
Phone: (04) 495 9314
Fax: (04) 495 9314

Job offer scams

If you receive an offer for a job you didn't apply for - don't believe a word of it. Scammers will do anything to get you to respond with your personal details. Scam job offers tempt you with easy work for great pay and flexible hours.

A genuine job offer will not require you to pay a fee to accept the offer.

If you are asked to deposit a cheque into your bank account and wire the money back to the sender or an alternative contact via a money transfer service* (for example Western Union or Money Gram) - don't do it. You will be helping the scammer to launder money.

Genuine mystery shopper companies do not recruit by sending unsolicited emails or letters. They ask you to register with the store of interest, provide a profile and you will be contacted when work is available.

*Many money transfer services are legitimate businesses but they are often used by scammers to make illegal transactions around the world.

Example

Subject: Start Now, Immediate Opening(Part Time)
Greetings,
A position is currently available for any individual in the UK&DE&AT who is interested in becoming an evaluator/Secret shopper. To become a mystery shopper with Clenco you must be over the age of 18 and all you needs to do is to register with us today by providing your details below and start shopping Evaluation!
Full Name...
Full Address ...
Postcode....
Mobile/Home number (s)...
Email Address....
You do not need previous experience, also you would be paid 100pounds For Two Surveys Per Day; 300pounds for 3days surveys completed in a week
NB: Only participants who replies or responds with their informations above would get further information.
Warm Regards.
Clement Conor
Clenco Survey Investment

Hints that it's a scam

- The recipient didn't sign-up to become a mystery shopper - this email came out of the blue
- The email requests the recipient's personal information
- It contains spelling mistakes and grammatical errors

Report scams

Email: scam@antispam.govt.nz
TXT: Forward the message to our free shortcode 7726 (SPAM)
Phone: (04) 495 9314
Fax: (04) 495 9314

Death threat scams

Death-threat scams (commonly sent by email) are hoaxes designed to play on people's fears and extract money from them. They are most often sent by email.

The Anti-Spam Compliance Unit regularly receives complaints about threatening emails that people have received from 'contract killers'.

Never respond to these messages. Responding will only inform the sender that your email address is active, and you are likely to receive more messages as a result.

Complain to the Department of Internal Affairs about death-threat scams and delete them.

Example

Subject: You can RUN but can never HIDE
Hello am i am a professional hired killer
You don't know me but I know you because i am paid to kill you, your and your entire family Everything about you I have been told this is What I do for a living There is only one way you can help yourself if you want to live again That is why am WRITING you
Note: this do not involve the police or let any one know about this, If you do I have no choice but kill you Don't be surprise why am letting you know I want to help you if you will co-operate with me Contact my email if you want to live But if you don't have respect 4 life, be prepare to dance to the music of the dead. I am very sorry for you , It is a pity that this is how your life is going to end as soon as you don't comply. As you can see there is no need for me introducing myself to you because I don't have any business with you, my duty as I am mailing you now is just to (KILL YOU) and I have to do it as I have already been paid for that. I have sent my men to track you down in Location and they have carried out the necessary investigation needed for the operation on you Lucky You

Hints that it's a scam

- The email requests money
- It contains spelling mistakes and grammatical errors

Report scams

Email: scam@antispam.govt.nz
TXT: Forward the message to our free shortcode 7726 (SPAM)
Phone: (04) 495 9314
Fax: (04) 495 9314

Inheritance scams

You're contacted out of the blue and told to act fast to claim a large sum of money from an unknown, distant relative who has died and left you a fortune.

The scammer usually pretends to be the deceased person's lawyer or a representative from a bank, and the figure quoted is often listed in foreign currency.

The scammer says he or she needs your personal details, or that you need to pay a fee (for taxes or other administrative costs) before you can claim your inheritance.

These scams can be very elaborate. Often the scammer will send you fake legal documents in an attempt to convince you that it is real.

Example

Subject: URGENT CLAIM OF YOUR PAYMENT BENEFICIARY!!!!
Dear Beneficiary
My name is Dr. Kingsley C. Moghalu,the deputy governor CBN.I was mandated by the President Federal Republic in conjunction with the Federal Executive Council (FEC), the Senate Committee on Foreign Debts Reconciliation and Implementation Panel on Contract/inheritance/compensation funds to complete all the unpaid Contract/inheritance/lottery fund. You are required as a matter of urgency to reconfirm your information including your name, phone number and your address for verification and immediate payment within 24 hours.
To this effect, the sum of TEN MILLION, SEVEN HUNDRED THOUSAND UNITED STATES DOLLARS (US$10.7m) has approved for you. We apologize for any delay you might have encountered in the past, your payment is now 100% Guaranteedd
Kindly choose from these three modes of payment (wire transfer, diplomatic cash payment and ATM card). I can be reached on this number anytime: [phone number removed].
Call me for more details, Dr. Kingsley Moghalu Deputy Governor CBN

Hints that it's a scam

- The sender is unknown to the recipient and the message came out of the blue
- The email requests the recipient's personal information
- It contains spelling mistakes and grammatical errors

Report scams

Email: scam@antispam.govt.nz
TXT: Forward the message to our free shortcode 7726 (SPAM)
Phone: (04) 495 9314
Fax: (04) 495 9314