certnz

Q3

JULY_TO_SEPTEMBER_2023

CYBER SECURITY INSIGHTS

Seems legit

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q3 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

Our numbers are telling us that scammers are thriving by evolving and adapting their methods.

After a brief respite in quarter two of this year, reports to CERT NZ rose again between July and September. The number of reports about scams and fraud increased by 32% from the previous quarter. In particular, the number of reports on scams involving buying or selling goods online went up by 70%.

The increase in reports came with an 11% rise in financial loss to $4.7 million. Of these, 11 incidents reported a loss of $100,000 or more and five were scams relating to a job, business or investment opportunity. This is something we've been seeing increasingly in 2023.

With that in mind, this report focuses on the evolving methods used by malicious actors to plan and execute investment scams. We have seen fake investment websites that look legitimate, with physical addresses, business registration numbers and even messenger-app groups with 'peers', all created to build trust, keep their target invested and steal as much money as possible.

In our Insights section, we look at job offer scams and how scammers target people by preying on their immediate needs. We also look at how artificial intelligence (AI) can be used to help attackers dupe people into handing over money or details. So far, CERT NZ has not received any specific reports of AI tools being used here for scams, however, this is an emerging area of concern and New Zealand will inevitably be affected by AI technology sooner or later.

Finally, CERT NZ is excited to announce the launch of our new website: Own Your Online (ownyouronline.govt.nz). The new site simplifies the world of cyber security, making it easier for individuals and small businesses to understand. Own Your Online has resources on how to safeguard yourself and your business against online threats including what to do if you become the target of an online attack.

Have a lovely holiday season and own your online, Aotearoa!

AT A GLANCE...

Average incidents reported per quarter

2,274

Average loss reported per quarter

$5.2m

Losses reported to CERT NZ

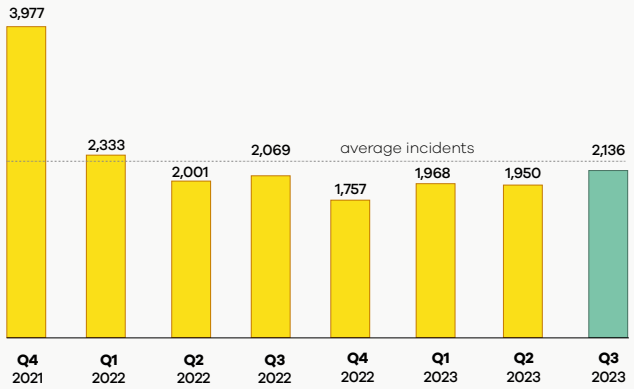
$41.3m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

2,136
incidents were responded to by CERT NZ in Q3 2023

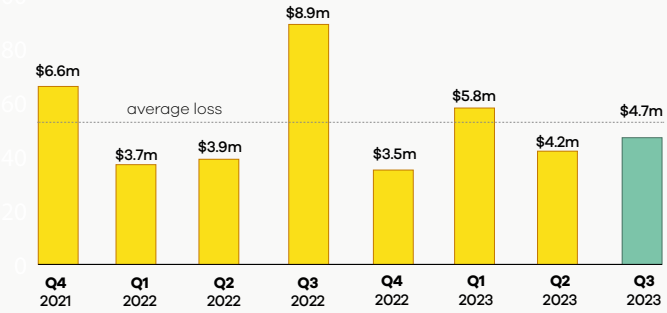
▲10%
increase from Q2 2023



DIRECT FINANCIAL LOSS

$4.7m
in direct financial loss was reported in Q3 2023

▲11%
increase from Q2 2023, with 27% of incidents reporting financial loss

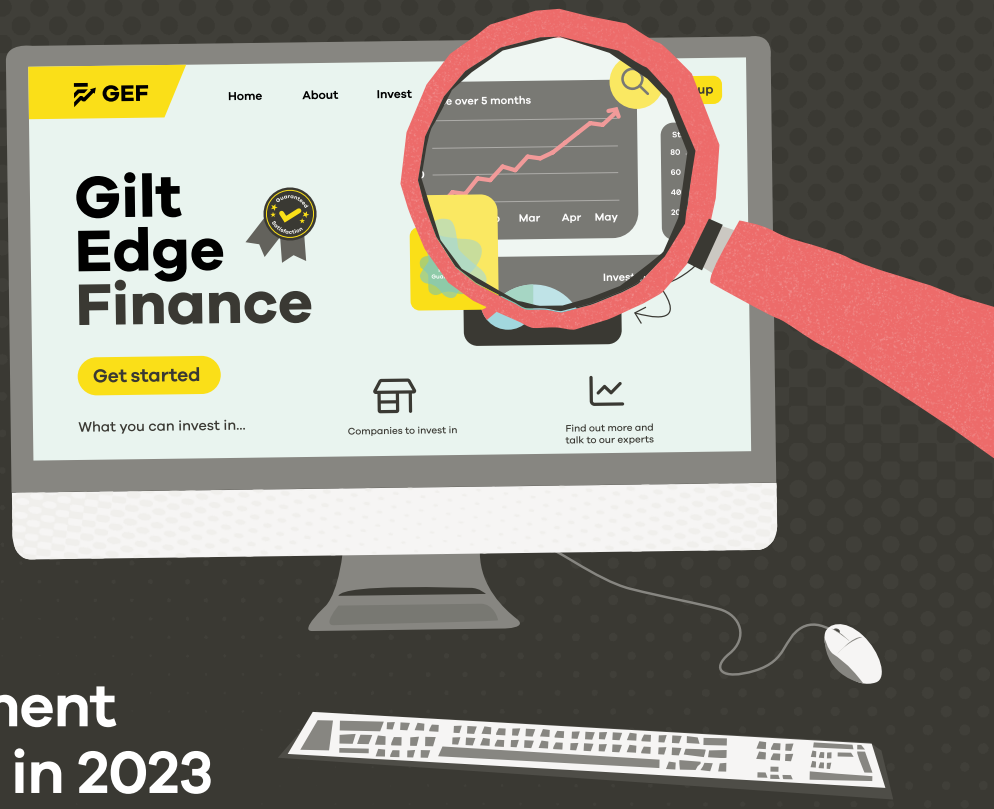


BREAKDOWN BY INCIDENT CATEGORY

After a dip in Q2, the number of incidents reported to CERT NZ rose again in Q3. In particular, scams and fraud went up by 32% compared with the last quarter.

		From previous quarter
Phishing and credential harvesting	1,181	▼ 1%
Scams and fraud	626	▲ 32%
Unauthorised access	184	▲ 6%
Malware	51	▲ 34%
Website compromise	11	▼ 39%
Ransomware	10	▼ 23%
Denial of Service	3	▲ -
Botnet traffic	1	●
C and C server hosting	0	▼ 100%
Suspicious network traffic	0	▼ 100%
Other	69	▲ 77%

For more on the New Zealand threat landscape in Q3 2023, see the CERT NZ Quarterly Report: Data Landscape.



Seems legit — what investment scams look like in 2023

If there's one thing a scammer likes, it's a large sum of money in one place. This is why New Zealanders looking to maximise returns on their savings are being targeted. Scammers create 'investment opportunities' that look legitimate and lucrative, reeling in potential targets.

Because the goal is to steal a lifetime's worth of savings, investment scams frequently have high losses. In Q3, CERT NZ received 11 reports where individuals reported losing over $100,000.

"LOOKS ALL RIGHT!"

For the scammer to pull off a plan of this scale, it is crucial that they build trust. This is done through well-planned communication and an appearance of legitimacy.

To make everything look legitimate, scammers set up physical and email addresses, phone numbers, messaging apps and online groups. Historically, scammers would contact targets via an unprompted email or call. They may lead with a lucrative investment opportunity or strike up casual conversation to establish a rapport. But, more recently, these conversations are increasingly taking place over a text message or messaging apps. They could also take a passive approach, putting up an advertisement online and waiting for someone to contact them. Sometimes, scammers will use just one 'persona', such as an investment advisor or overseas investor. At other times, they may create multiple accounts pretending to be an entire team of people.

Once they've turned the discussion to investment, they present some kind of business to invest in, to lend it legitimacy. They may create entire websites or even investing apps. Websites may be entirely fictional or based on real companies.

The difference of a dash

Fake websites can have URLs that closely resemble the website of an actual company. For example, in this case study report that CERT NZ received, the website the scammer provided had a difference of a dash. **[www.investment-group.com** instead of **www.investmentgroup.com]**

Case study

The person (we'll call them Alex) saw an advertisement for a trading platform that claimed to leverage AI tools and expert advice to find investment opportunities. The ad touted very high and reliable returns – almost too good to be true. They had a professional website and appeared to be licensed overseas, and so Alex registered an account.

Scammers use positions of authority to pressure you into trusting the information without verifying it

Alex was then added to a WhatsApp group of 'other investors', who were all in on the scam. The group shared regular trading news highlighting investment opportunities, asking for thousands or tens of thousands at a time. Some of the companies mentioned were real ones. However, instead of being invested in these companies, the money was going to the scammers.

Scammers may use urgency to push you into acting before thinking your investment through or talking it out . They may claim to have time-sensitive opportunities like 'pre-IPO investments'

Scammers create a sense of peer pressure to push you to participate

The scam continued for close to 18 months, until Alex wanted to get out. The scammers claimed that, to withdraw the money, a large fee needed to be paid first. Alex felt trapped and unsure of what to do.

Scammers create a sense of fear and confusion to dissuade people from getting support, often by claiming there is a large fee before you can withdraw your money

Scammers create a sense of complacency to keep you invested. This may be by showing you fake charts of your 'investments' going up in value, or offering alternative investments instead of getting your money out

After reporting to CERT NZ and talking to the bank, Alex was able to recover some of the money, but most of it was already gone.

BUILDING THE FAÇADE

Large investment scams work on a high-trust model. The scammer must appear knowledgeable, reliable and competent. Building that illusion requires patience and some smart steps.

Scammers use positions of authority to pressure you into trusting the information without verifying it (pretending to be an expert or several experts using multiple emails or accounts)

Scammers may use urgency to push you into acting before thinking your investment through or talking it out (claiming to have time-sensitive opportunities like 'pre-IPO investments')

Scammers create a sense of peer pressure to push you to participate (scammers may create entire group chats talking about 'successes').

Scammers create a sense of complacency to keep you invested. This may be by showing your 'investments' going up in value despite not existing, or offering alternative investments instead of getting your money out.

Scammers create a sense of fear and confusion to dissuade people from getting support, often by claiming there is a large fee before you can withdraw your money.

SNIFFING OUT INVESTMENT SCAMS

- Before you invest in something that sounds lucrative, check for investment alerts by the New Zealand Financial Markets Authority (FMA) or other equivalent overseas agencies. Many of the reports that come to CERT NZ involve 'companies' that these agencies have issued investor alerts on.
- Check the company's New Zealand Business Number (NZBN) against its registered name. This can be done on the NZBN website.
- Watch out for signs of peer pressure or created urgency. If something feels wrong, get a second opinion from someone outside the group.
- Remember — if it seems too good to be true, it probably is.

MORE TIPS ON FMA WEBSITE

The FMA website has advice for avoiding investment scams, including finding a reputable advisor and warnings about known fake investment websites.

https://fma.govt.nz/library/warnings-and-alerts/

Artificial IntelliScams

Artificial intelligence is a powerful technology, with the potential to revolutionise many aspects of our lives. But AI can also be used for malicious purposes and, unfortunately, scammers are increasingly using AI to create more sophisticated and convincing scams.

IMAGE AND VIDEO GENERATION

AI can generate realistic images or videos of people and places. It can create fake photos of a real person, or generate images of someone who doesn't actually exist. These images can be used to create entire social media accounts or dating profiles that look genuine. Scammers can then use these fake accounts to trick people into giving them money or sharing personal information.

CHATBOTS

Chatbots are computer programs that can simulate conversation with people. Most people have seen or even used one. Companies like banks and airlines use them to answer common questions that customers may have. But scammers, too, can use chatbots to create fake customer service representatives and trick someone into giving away personal or sensitive information, or into making a fraudulent payment.

VOICE IMITATION AND GENERATION

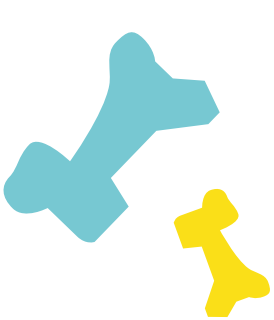
Reports overseas have noted where scammers used AI to imitate a person's voice, generally someone in authority or a loved one, to trick someone into parting with money or sensitive information. We have not had a case of voice imitation reported to CERT NZ but, as AI tools get more sophisticated, this type of scams remains a possibility.

STAYING SAFE

AI scams are a growing threat, but the same tactics that you use to protect yourself from other types of scams can also be used to protect yourself from AI scams. Be wary of unsolicited messages, never give out your personal information to someone you don't know and be sceptical of offers that seem too good to be true.

Be wary of requests from people you have only ever met online, and, if a request for financial help or sensitive information comes from someone you know, verify it with that person through a different means of communication.

> **Be wary of unsolicited messages, never give out your personal information to someone you don't know and be sceptical of offers that seem too good to be true.**



Too good an offer?

Online scammers use fake job advertisements to trick job hunters into sharing personal information such as their address, passport details, employment history or even financial details.

Fake job advertisements can look just like real ones. They may be posted on genuine job listing platforms or shared with victims directly through unsolicited emails or direct messages. Like other scams, these offers are often too good to be true. The fake roles are usually part time, completely online and come with very good compensation.

MALICIOUS METHODS

The methods of these scammers can change a bit between each scam. Once a person starts interacting with a scammer around a job opportunity, they will often get asked to engage on alternative platforms like WhatsApp. The scammer may also request sensitive, personal information much earlier than one would expect for a genuine job offer.

In some cases, the scammer will claim that the next stage of the interview process is an in-person interview and ask their target to deposit funds into a travel account for flights and accommodation, funds they claim will be refunded after the interview.

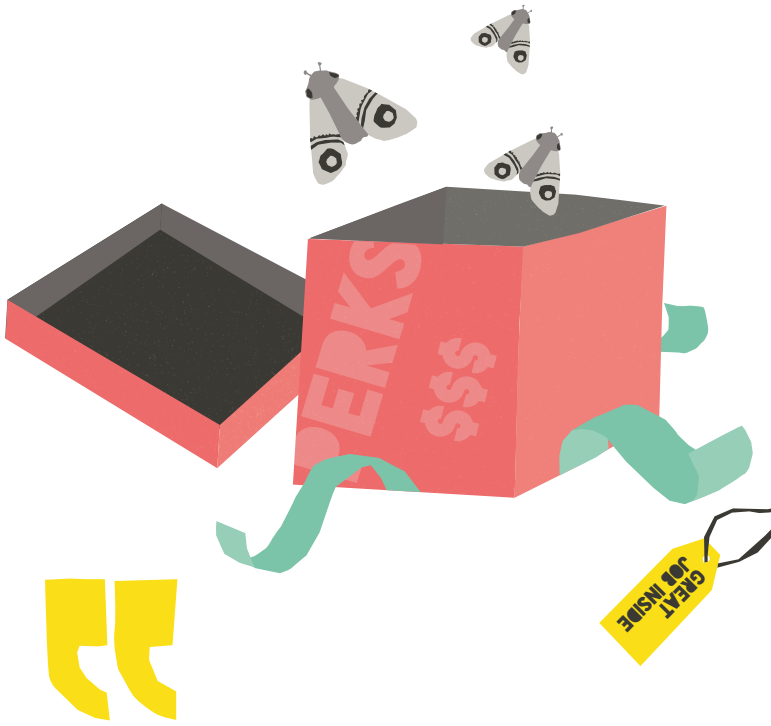
Once a scammer has obtained someone's personal information, they can use it to conduct a range of criminal activities, including online fraud and identity theft. This can have serious repercussions for the affected person, including financial loss or negative impacts on their credit rating.

Unfortunately, victims often don't realise it is a scam until they have provided their sensitive, personal information or deposited money, at which point the scammers will usually cut contact with the victim.

SPOT IT EARLY

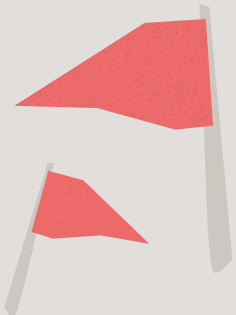
It can be difficult to tell the difference between a genuine job listing and a job scam, but you can look out for specifics.

- Scammers often create fake websites with a URL similar to that of a genuine company. If in doubt, verify the company's webpage and navigate to the job listing from there.
- Check that the recruiter's email matches the company's domain name. As with URLs, some scam emails may look like they have come from a real company, such as **jobs@example-test.com**, when the real company's email is **jobs@exampletest.com.**

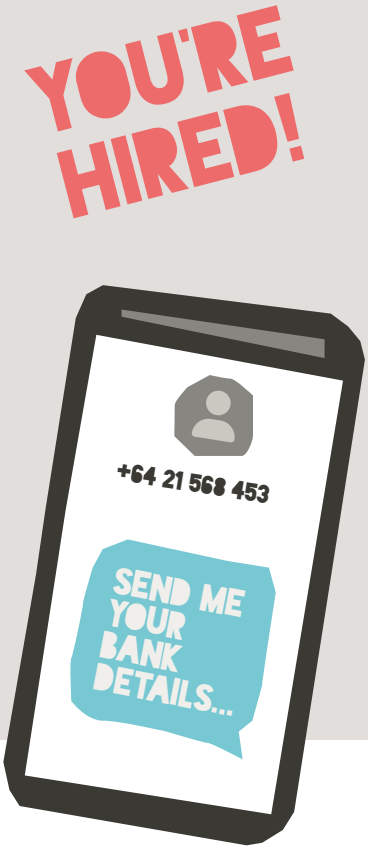


It can be difficult to tell the difference between a genuine job listing and a job scam, but you can look out for specifics.

RED FLAGS



- **The job listing is only on a single board.** Most recruitment agencies and organisations post their vacancies to several job boards to reach as many people as possible.
- **Communication moves quickly to an instant messenger service.** It's becoming more common for job interviews to take place over the phone or via video calls. However, you should be wary if your first interview is on an instant messenger service.
- **The employer contacts you out of the blue or offers an interview or a job straight away.**
- **The potential employer wants your personal information or bank account details early in the recruitment process.** A genuine employers won't need your bank account details until you have accepted a job.



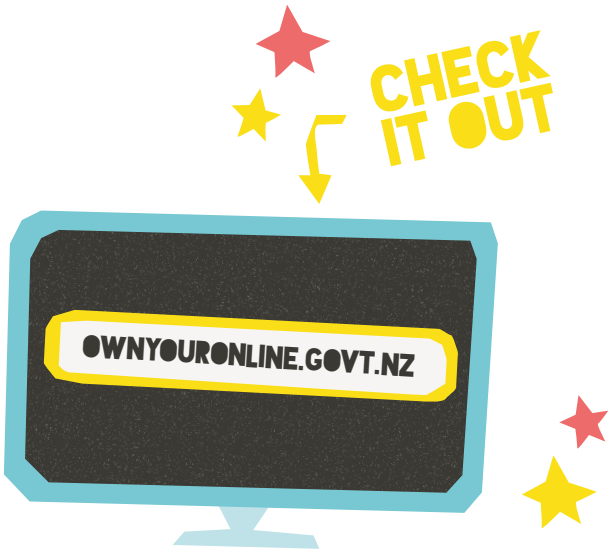
CERT NZ work

OWN YOUR ONLINE

CERT NZ has launched its new website Own Your Online **(ownyouronline.govt.nz)** to simplify cyber security and make it easier for individuals and small businesses to navigate.

The website contains handy guides and resources to help you:

- **learn about common risks and threats**
- **get protected from cyber attacks**
- **check if you've been scammed**
- **get help if you've been the target of an attack.**



PACSON AGM AND FIRST REGIONAL SYMPOSIUM FOR THE PACIFIC

In September the CERT NZ Pacific Partnerships Team attended the 2023 PaCSON (Pacific Cyber Security Operational Network) Annual General Meeting in Port Vila, Vanuatu. The AGM was followed by the FIRST Regional Symposium for the Pacific.

The meetings focused on opportunities to enhance cyber resilience across the Pacific region and tools to support respective communities in the evolving landscape of the online world.

International insights

In this section, we cover news from our international partners.

Artificial intelligence tools and security issues concerning them have remained a matter of interest for our international partners. The National Cyber Security Centre (NCSC) UK has published a blog delving into specific vulnerabilities associated with Large Language Model (LLMs) algorithms used by AI tools like ChatGPT and Google Bard.[1]

CERT NZ joined 17 international partners including the Cybersecurity and Infrastructure Security Agency (CISA), NCSC UK and agencies from across Europe and Asia Pacific in releasing a new joint guide *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*. The joint guidance urges software and technology manufacturers to ship products that are secure by design.[2]

[1] Thinking about the security of AI systems (https://www.ncsc.gov.uk/blog-post/thinking-about-security-ai-systems)

[2] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (https://www.cisa.gov/resources-tools/resources/secure-by-design)