certnz

Q4

OCTOBER_TO_DECEMBER_2023

CYBER SECURITY INSIGHTS

Part and Parcel

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q4 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

There's plenty of positives to take from the final quarter of 2023. Reported financial loss was $3.6 million, a 24% decrease from the previous quarter. The number of scams came down by a notable 22% from the previous quarter and there was a significant decline in scams involving selling, buying or donating goods online.

But that doesn't mean scammers are taking a break.

There was a marked increase in the number of fraudulent phone calls. Most were phishing calls claiming to be from Immigration New Zealand and collecting visa information from people who spoke Mandarin. While fraudulent calls relating to immigration aren't new, this campaign targeted a specific group of people. This tells us that scams are continuously evolving.

We've received over a thousand reports of phishing and credential harvesting for three quarters in a row. In Q4, we saw scammers take advantage of the holiday season with phishing text messages claiming to be from NZ Post. In December alone, we saw 436 indicators of compromise relating to NZ Post, compared with 272 in the first six months of the year.

But Q4 was also an exciting time for us at CERT NZ.

We launched our new website Own Your Online as part of our campaign to make New Zealand more cyber resilient. Cyber Smart Week, held from 30 October to 5 November, saw a record 1,214 organisations sign up as supporters, a 514 increase from the previous year.

We continue to mahi tahi with other agencies internationally and within Aotearoa, sharing knowledge and learning from each other's experiences. For this report, we worked with the Financial Markets Authority (FMA) to bring you an insight into so-called 'recovery room scams' aka 'follow-up fraud'. These are scams that revictimise those who have already been scammed while purporting to help them recover their money.

In a world where scams are becoming more sophisticated, we cannot stress enough the need to take every step to fortify our online defences. Together let's bring those numbers down even further!

AT A GLANCE...

Average incidents reported per quarter

2,012

Average loss reported per quarter

$4.8m

Losses reported to CERT NZ

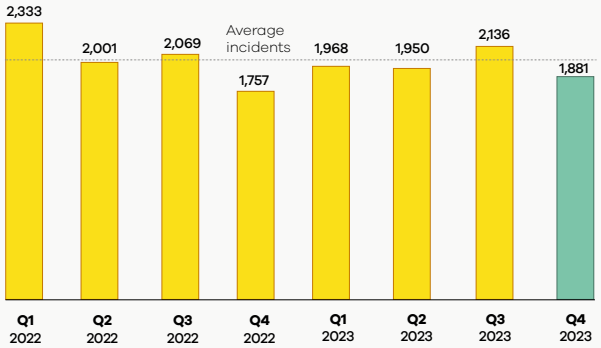
$38.2m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

1,881
incidents were responded to by CERT NZ in Q4 2023

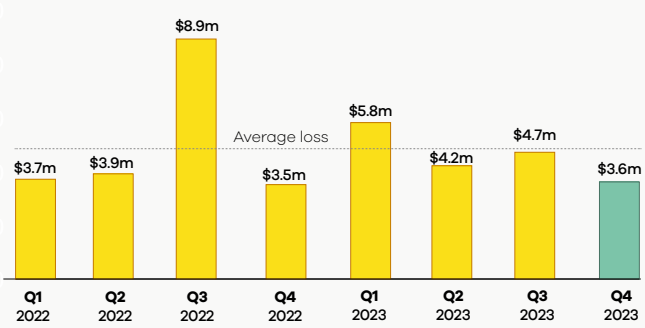
▼12%
decrease from Q3 2023



DIRECT FINANCIAL LOSS

$3.6m
in direct financial loss was reported in Q4 2023

▼24%
decrease from Q3 2023, with 19% of incidents reporting financial loss



BREAKDOWN BY INCIDENT CATEGORY

We saw a decrease in the number of reports across categories in Q4. An exception was website compromise which went up by 73% compared with the last quarter. There was also a marked increase in the number of scam calls.

		From previous quarter
Phishing and credential harvesting	1,091	▼ 8%
Scams and fraud	486	▼ 22%
Unauthorised access	164	▼ 11%
Malware	30	▼ 41%
Website compromise	19	▲ 73%
Ransomware	8	▼ 20%
Denial of service	2	▼ 33%
Suspicious network traffic	1	▲ -
C and C server hosting	1	▲ -
Botnet traffic	1	● 0%
Attack on a system	1	▲ -
Other	77	▲ 12%

For more on the New Zealand threat landscape in Q4 2023, see the CERT NZ Quarterly Report: Data Landscape.

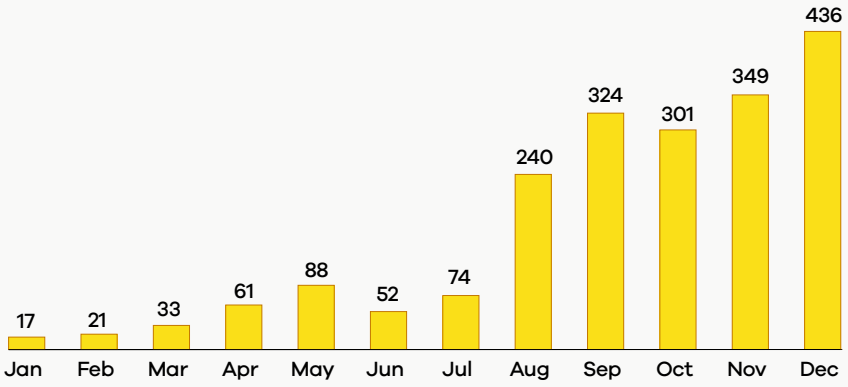
Part and parcel

It's a scam most of us are familiar with. You get a text saying there's a problem with your parcel, it can't be delivered, delivery fees are pending, or your information is not up to date. Then it tells you to click on a link.

Many of us have learnt to identify this as phishing and ignore it. But it's hard to be a sceptic all the time. What if you have purchased something online and are expecting a parcel? Or what if it's the festive season and someone could be sending you a gift? You click on the link and the landing page asks you for details: name, address, sometimes even credit card information. You enter all that only to realise there is no parcel. There never was.

While reports of such parcel-delivery scams are common throughout the year, CERT NZ noticed that the number increased significantly in the last quarter of 2023 as the holiday season approached. Between October and December, CERT NZ's Phishing Disruption Service received 1,086 reports of websites impersonating NZ Post. This made NZ Post the most impersonated brand in New Zealand in this period. These phishing messages might also claim to come from other postal companies operating in New Zealand.

INDICATORS OF COMPROMISE REPORTED TO CERT NZ IN 2023 IMPERSONATING NZ POST



HOW IT WORKS

To appear legitimate and credible, scammers like to impersonate well-known brands. The most common way of doing this is to create domains that closely resemble the website of the company they are looking to impersonate.

Phishing messages also seek to create a sense of urgency. A common lure is the use of words like 'track-alert' or 'missed-my-parcel' in the URL path.

Some malicious links hide behind URL-shortening services such as Tinyurl or Bitly.

Imitation is flattery

It is worth mentioning here that the company or agency that scammers impersonate is not to blame for these scams. Scammers go after reputable companies because their customer base is large and that lets them cast their net wide.

WHY DO SCAMMERS WANT YOUR INFO?

The most common objective for phishing is to harvest credentials. If you enter a password into a fake site, scammers can use that to access your account on the real website or to hack into your other accounts, especially if you use the same password across multiple accounts.

The end goal of scammers is to steal money. Phishing sites will sometimes ask you to make a small payment using your credit card or online banking. While this initial amount appears insignificant, scammers can use the details they have collected for a larger scam in the future.

In many cases, scammers may also try to install malware on your device after you click on these phishing links. The malware could potentially log your activity and collect more information.

SOME URLS IMPERSONATING NZ POST

nz-nzpost.jer-gdkad.shop
https://nz-nzpost.jer-mgnfd.shop/track.php?id=739801
https://nz-nzpost.hoq-qdacx.shop/track.php?id=539962
https://nz-nzpost.byt-trwvf.shop/track?id=541392
https://nz-nzpost.ter-yrgdf.shop/track?id=99707
https://nz-nzpost.byt-khnog.shop/track.php?id=159295
nz-nzpost.byt-jfgnk.shop
https://nz-nzpost.jer-gdkad.shop/track.php?id=136810
https://nz-nzpost.ter-huinj.shop/

HOW WE FOIL PHISHING ATTEMPTS

CERT NZ works to stop phishing campaigns through the Phishing Disruption Service. If you get a phishing text or email, you can submit the URL to the Phishing Disruption Service by sending it in an email to **phishpond@ops.cert.govt.nz**. CERT NZ collates and verifies the links and sends them out to subscribed organisations which can then block access, preventing the phishing scams from reaching people in the first place.

CERT NZ recommends that organisations set expectations with customers on how you will contact them. For example, promote that you will not send text messages, so if a customer receives a text claiming to be from your organisation, they will know it is a phishing attempt.

> If you get a phishing text or email, you can submit the URL to the Phishing Disruption Service by sending it in an email to phishpond@ops.cert.govt.nz.

NZ Post has the following advice on its website for New Zealanders who get a message claiming to be from the company.

NZ Post will never:

- ask for any of your personal information by email or text (including usernames, financial information, including password, credit card details or account information)
- send you an email from a domain other than nzpost.co.nz
- send you a text message from a phone number outside of New Zealand
- use a messaging app like WhatsApp to communicate with our customers.

Organisations that discover they are being impersonated can report to CERT NZ. We can offer advice on how to send out advisories to their customers and other steps to take.

WATCH OUT FOR THESE

Check the URL. New Zealand courier companies usually have websites ending in ".co.nz".

Some URLS also have the IP as a hostname. This is definitely a red flag. For example: http://46.23.109.9/.

Messages from unrecognised overseas phone numbers are most likely a scam.

If you are expecting a parcel or delivery and you get a message, you can call the postal company to verify it.

Do not give away your information, including your address or sensitive information such as credit card details.

Visa-vis

While scammers prefer a widespread campaign, hoping to catch anyone who is unaware, they sometimes home in on specific groups they see as susceptible to their messages. We saw a targeted scam of this type in the last quarter of 2023 aimed at Mandarin speakers living in New Zealand on a visa.

Starting in early November, a spate of calls occurred from a source impersonating Immigration New Zealand, telling recipients there were serious problems with their visas. While calls of this nature - pretending to be from a government agency and targeting people who would interact with that agency - are not new, this particular series was remarkably high in number. CERT NZ and Immigration New Zealand together received over 800 reports across a span of six weeks. Because most incidents go unreported, we estimate the actual number of phone calls to be much higher.

The callers did not start with the knowledge of people's immigration status or their background. So, while the content of the scam was targeting a certain demographic, anyone with a New Zealand phone number could have received the call.

> CERT NZ and Immigration New Zealand together received over 800 reports across a span of six weeks.

THE NATURE OF THE CALL

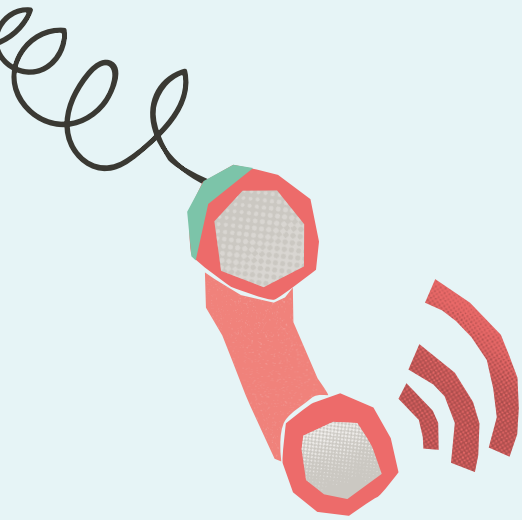
This scheme was specifically designed to target Mandarin speakers. The callers masked their originating numbers by 'spoofing' (see below) the phone numbers of unsuspecting individuals. The call started with a voice message asking the recipient to choose a language: English or Chinese. Selecting English ended the call. Those who selected Chinese were directed to a scammer who told them that there were issues with their visas and in some cases asked them to return promptly to China.

The callers collected personal and sensitive information (including visa numbers), and sometimes asked for payment to help sort out visa problems.

Those who selected Chinese were directed to a scammer who told them that there were issues with their visas and in some cases, asked them to return promptly to China.

GETTING THE MESSAGE OUT

CERT NZ worked with Immigration New Zealand which used its platform and connections to get the message out to people who could be targeted. The Chinese consulate also engaged with us and promptly disseminated information in the community. The number of reports reduced significantly in December and eventually died out, with the last case reported to us on 23 December.



What is spoofing?

Spoofing is the practice of making your phone number look like a different one. So, even blocking or reporting the number won't work because it's not the real source. Scammers can do this by using cheap and easily available software and the owner of the phone they are spoofing will not know that their number is being used.

"WE HAVE A PROBLEM WITH YOUR VISA."

Adding insult to injury:

Recovery room scams

Imagine someone who has lost tens of thousands of dollars to an online scam. Soon after, they get a call from an online agency offering to help them get all or most of their money back. The upfront fee of a few thousand dollars sounds like a small amount compared with what the person has lost. But once the fee is paid, the 'online agency' goes silent, leaving the victim to realise they have been scammed again.

This is a quintessential recovery room scam, a practice where malicious actors revictimise someone recovering from a hard-hitting scam.

HOW THEY WORK

Recovery room scams target individuals or organisations that have already been scammed. They may do this by trawling social media or forums for people who post about being scammed.

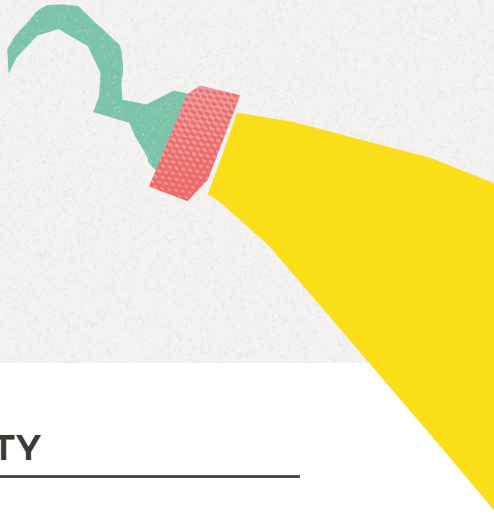
In some cases, the same actors responsible for the initial scam may go back to the victim purporting to be someone who can help them with recovering the money they lost.

Scammers sell details of their victims to other scammers. These lists contain contact details, the amount lost and the type of scam the person fell for.

Recovery room scammers will often setup and promote recovery companies online that show up in your search results. These websites look legitimate and it can be hard to recognise them as a scam.

Finding you from what you search for

Google lets advertisers target people based on their search and browsing history. If you search for help with recovering funds lost to a scam, your search engine algorithm may push sponsored ads of these companies that it thinks will be relevant to you.



ADVICE FROM THE FINANCIAL MARKETS AUTHORITY

In 2023, the FMA received 36 reports of recovery scams.

"We continue to receive significant reports. While most of the recovery scams are not in our remit as a regulator, we are alarmed by this current trend and feel we need to alert the public," FMA Senior Responsible Officer Peter Taylor says. "Be very suspicious of anyone who claims they can recover your stolen funds, it's hard to get your money back once it has been moved offshore. We recommend you talk to your bank if you think you are being scammed this way."

The FMA recommends the following.

- If you have been the victim of a scam, be on guard against follow-on scams. Also, consider getting a new phone number and email address. It is likely your contact details will be on a scam list.
- Be wary of a company that doesn't have a physical address or phone number. Note that many scams involve companies using false addresses and telephone numbers. It's important to verify these against the contact information provided.
- If someone claims to be a government employee, check that the organisation exists. If it does, contact the organisation using the details on its official website and ask to be transferred to the person named in the initial contact to verify that they contacted you. Taking these steps will likely make it clear if it is a scam.
- If you have given anyone remote access to your device and you now suspect it is a scam, disconnect your device from the internet to prevent access.

CERT NZ work

The seventh annual Cyber Smart Week was run between 30 October and 5 November 2023. We had seven key industry partners — Westpac, BNZ, ASB, Kiwibank, 2degrees, Harvey Norman and TradeMe — and over a thousand organisations sign up as supporters, to help share the message with their extensive customer base.

To launch Cyber Smart Week 2023, CERT NZ created *EXPOSED: Through the Lens of a Hacker*, a free public exhibition of photographs featuring real New Zealanders who have been affected by an online incident and want to share their experiences.

PACIFIC PROGRAMME

As part of its outreach work in the Pacific, CERT NZ attended the Pacific Cyber Capacity Building and Cooperation Conference (P4C), held in Nadi, Fiji in October. We also supported the Cook Islands during the 52nd Pacific Islands Forum annual leaders meeting in Rarotonga in November.

CERT NZ represented New Zealand at the Global Forum on Cyber Expertise (GFCE) Annual Meeting and the inaugural Global Conference on Cyber Capacity Building (GC3B) in November. A significant outcome of the event was the announcement of the Accra Call — a global action framework that supports countries in strengthening their cyber resilience.

International insights

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

Two international counterparts released their annual threat assessments in the final quarter of 2023: the Australian Cyber Security Centre (ACSC), which is a part of the Australian Signals Directorate (ASD), and the United Kingdom's National Cyber Security Centre (NCSC UK), which is a part of the Government Communications Headquarters. To follow are the main findings from their reports.

ASD 2023 Cyber Threat Report[1]

- ASD saw **94,000** cybercrime reports, up **23%** on the year before and representing an average of one report every six minutes.
- The average cost of cybercrime for a small business in Australia was AUD **$46,000**.
- The top three cybercrime types for business in Australia were email compromise, business email compromise, fraud and online banking fraud.

NCSC UK Annual Review 2023[2]

- NCSC UK's review has a focus on AI, with the artwork for the report generated using AI.
- The organisation received an all-time high of **2,005** incident reports. Ransomware remains one of the most acute threats for the United Kingdom, with data extortion attacks becoming more common.
- Incidents involved in the exfiltration and extortion of data totalled **327**, highlighting the value that criminals see in the data of users and businesses.

ASD's ACSC also published a new tool — Business Continuity in a Box[3] — which supports businesses to quickly set up critical business functions during or following a cyber incident.

[1] ASD 2023 Cyber Threat Report.
[2] NCSC Annual Review 2023.
[3] Business Continuity in a Box.