certnz

Q1

JANUARY_TO_MARCH_2023

CYBER SECURITY INSIGHTS

Reversal of fortune

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q1 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

In the first quarter of this year, CERT NZ has seen report numbers creep back up, compared with the last quarter of 2022, along with, unfortunately, financial loss.

Reports are up 12% but losses are up 66% from last quarter to almost $6 million. Among those reports, we've again seen an increase in scams this quarter, going up 23%.

These figures are much higher than the average number for the past two years. While it's not the highest number of scam reports we've ever seen, the trend is that scams are on the rise.

At CERT NZ, we've been analysing all the incidents from the first few months of the year and we're seeing new ways of doing old scams.

Investment scams never went away, but scammers have changed their tactics, using search engine ads and professional-looking documentation. One scam campaign in February cost New Zealanders millions in a short time, which reflects how quickly someone can lose their assets if they're not alert.

Again, CERT NZ is asking New Zealanders to be vigilant online. In this report, we list red flags to look out for.

To complicate things, new tools are available that scammers can use, specifically artificial intelligence (AI).

AI has been discussed a lot in the media recently, and the cyber security world is taking notice. Scammers can use AI to write more convincing phishing emails in various languages, to create malicious code, and to even impersonate people in live chats.

We haven't seen many AI scams reported to CERT NZ yet, but it's only a matter of time.

Although AI may be lessening the workload for cyber criminals, for now, the results are the same kind of scams we've been seeing for years.

It's essential to be vigilant, take your time when you see investment opportunities online, verify exactly who you're talking to, don't give away your personal information and keep yourself secure online.

AT A GLANCE...

Average incidents reported per quarter

2,191

Average loss reported per quarter

$4.9m

Losses reported to CERT NZ

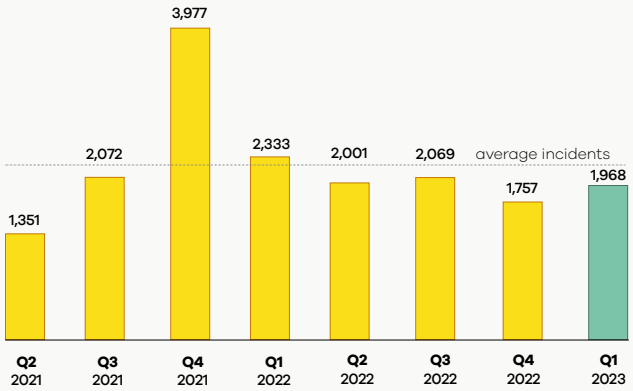
$39.6m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

1,968
incidents were responded to by CERT NZ in Q1 2023.

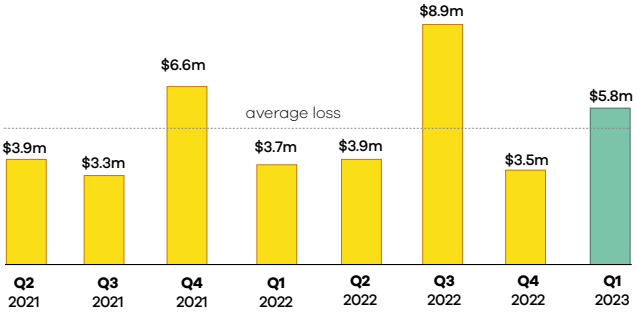
▲12%
increase from Q4 2022.



DIRECT FINANCIAL LOSS

$5.8m
in direct financial loss was reported in Q1 2023.

▲66%
increase from Q4 2022, with 30% of incidents reporting financial loss.



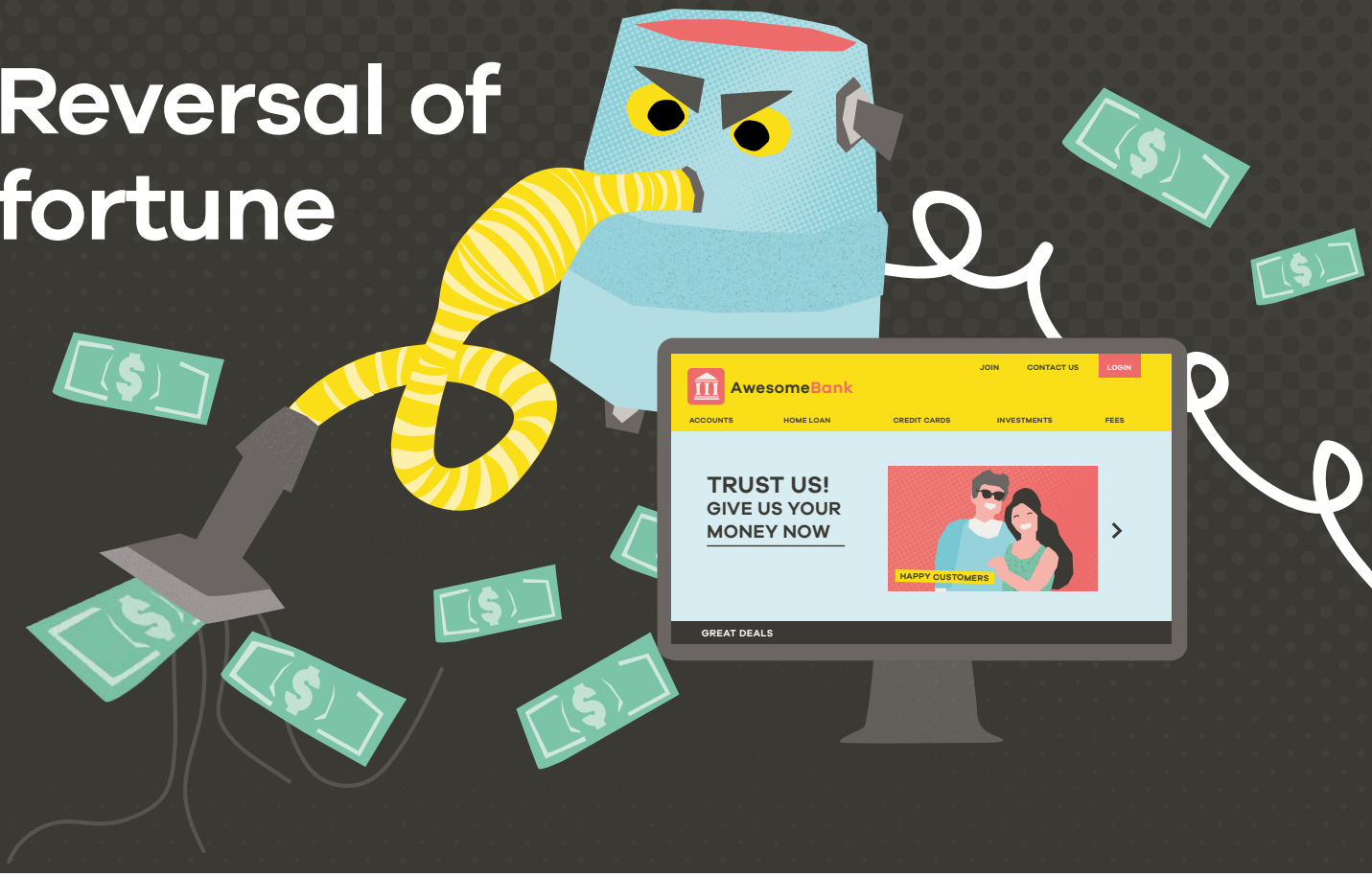
BREAKDOWN BY INCIDENT CATEGORY

Despite a decrease in reports across most categories in Q1, financial loss has increased 66% compared with the last quarter (Q4 2022).

		From previous quarter
Phishing and credential harvesting	946	▲ 5%
Scams and fraud	625	▲ 23%
Unauthorised access	240	▲ 35%
Malware	28	▼ 35%
Website compromise	13	▼ 13%
Suspicious network traffic	2	▲ 100%
Ransomware	12	▼ 67%
Botnet traffic	3	▼ 40%
Denial of Service	2	▲ -
C and C server hosting	0	▼ 22%
Attack on a system	0	● 0%
Other	97	▲ 56%

For more on the New Zealand threat landscape in Q1 2023, see the CERT NZ Quarterly Report: Data Landscape.

Reversal of fortune



A new scamming technique has caught out many New Zealanders.

Typically, scammers contact their target using a phishing email, text message or even a phone call. Phishing remains the number one cyber incident reported to CERT NZ.

However, in 2023, new methodologies are being used that have people actually approaching scammers.

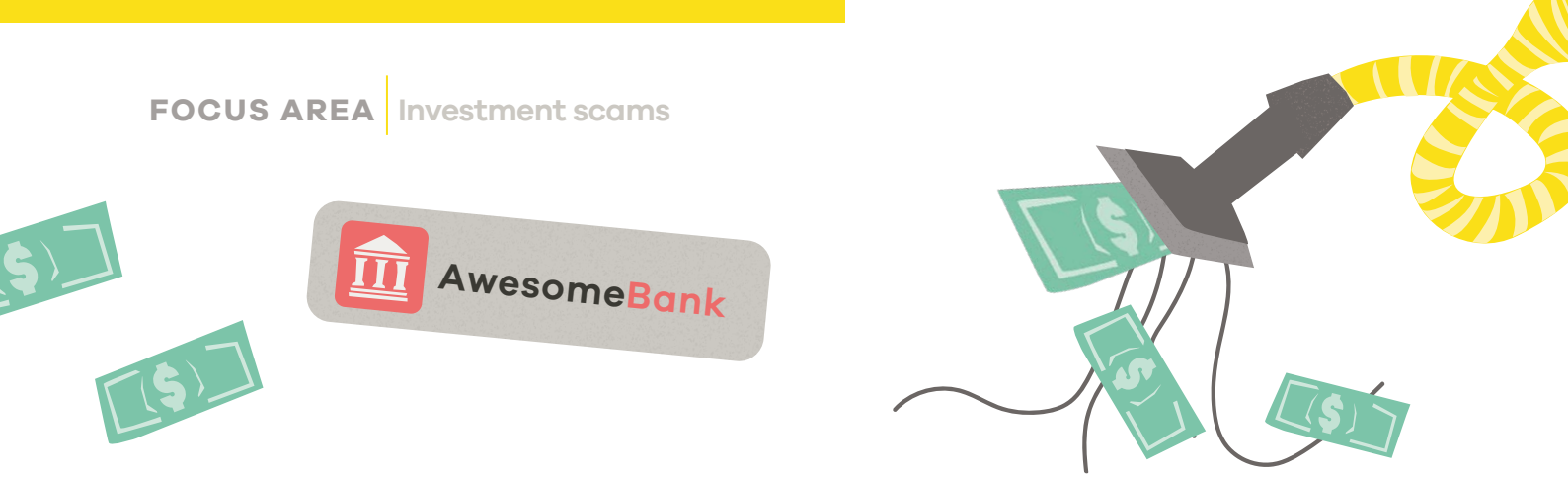
SEARCHING FOR SCAMS

CERT NZ has seen scammers setting up malicious websites and using key search terms to ensure their website appears high in the results of search engines, like Google. These websites usually mimic large organisations like banks, investment firms or large exporters.

How it works:

A person goes searching for an investment comparison website or a website to purchase and export certain products.

The top results contain malicious sites alongside the legitimate sites, depending on the terms searched by the person, and serve as an initial point of contact between this person and the scammer.



The person sends their details to the scammer through the fake site. Typically, this is via an email address (on another domain set up by the scammer to make the email address look legitimate) or a phone number. When the scammer gets a phone number, the interactions often move to platforms such as WhatsApp.

During the contact phase, scammers may even provide documents like investment comparisons or product catalogues. These documents look convincing and often includes branding of legitimate businesses and organisations.

Once people are convinced, they are provided with bank details to pay their 'investment' or the cost of the products they are looking to export. Unfortunately, these people may not realise this is a scam until the funds have been transferred and time has passed without any further contact from the scammer. This is often too late for the banks to be able to recover funds.

Anatomy of a real scam

In February 2023, CERT NZ was made aware of a major investment scam where someone searching terms such as 'term deposit comparison nz' on Google would be shown a search page that included ads paid for by scammers and linked to fake websites.

People who sent details to these sites were called by the scammers, claiming to be from the investment team at a New Zealand-based financial institution. These people were given professional-looking fake prospectus documents and details on how to transfer money to be 'invested'.

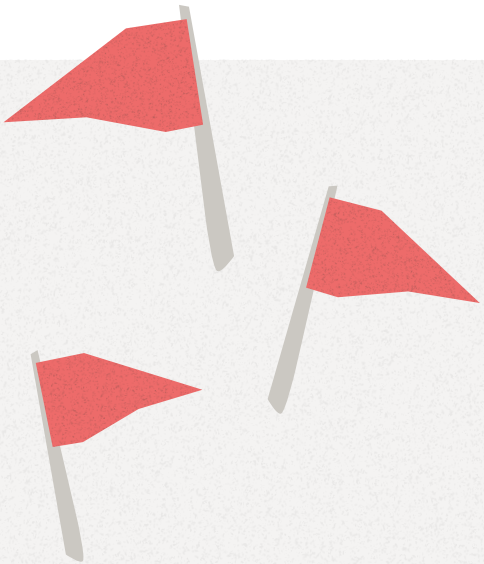
Some individuals were also given a fake investment portfolio website to check their investments. This fake site was sophisticated and required a login before showing a balance specific to the target. By showing fake growth, the scammers were able to ask for further money.

This campaign was able to steal millions of dollars over the course of a month.

CERT NZ and Google worked closely to have these malicious URLs removed. CERT NZ also worked with local banks to communicate to the public that this was happening and to contact the banks directly regarding investments.

During the contact phase, scammers may even provide documents like investment comparisons or product catalogues.

RED FLAGS AND WHAT TO LOOK FOR



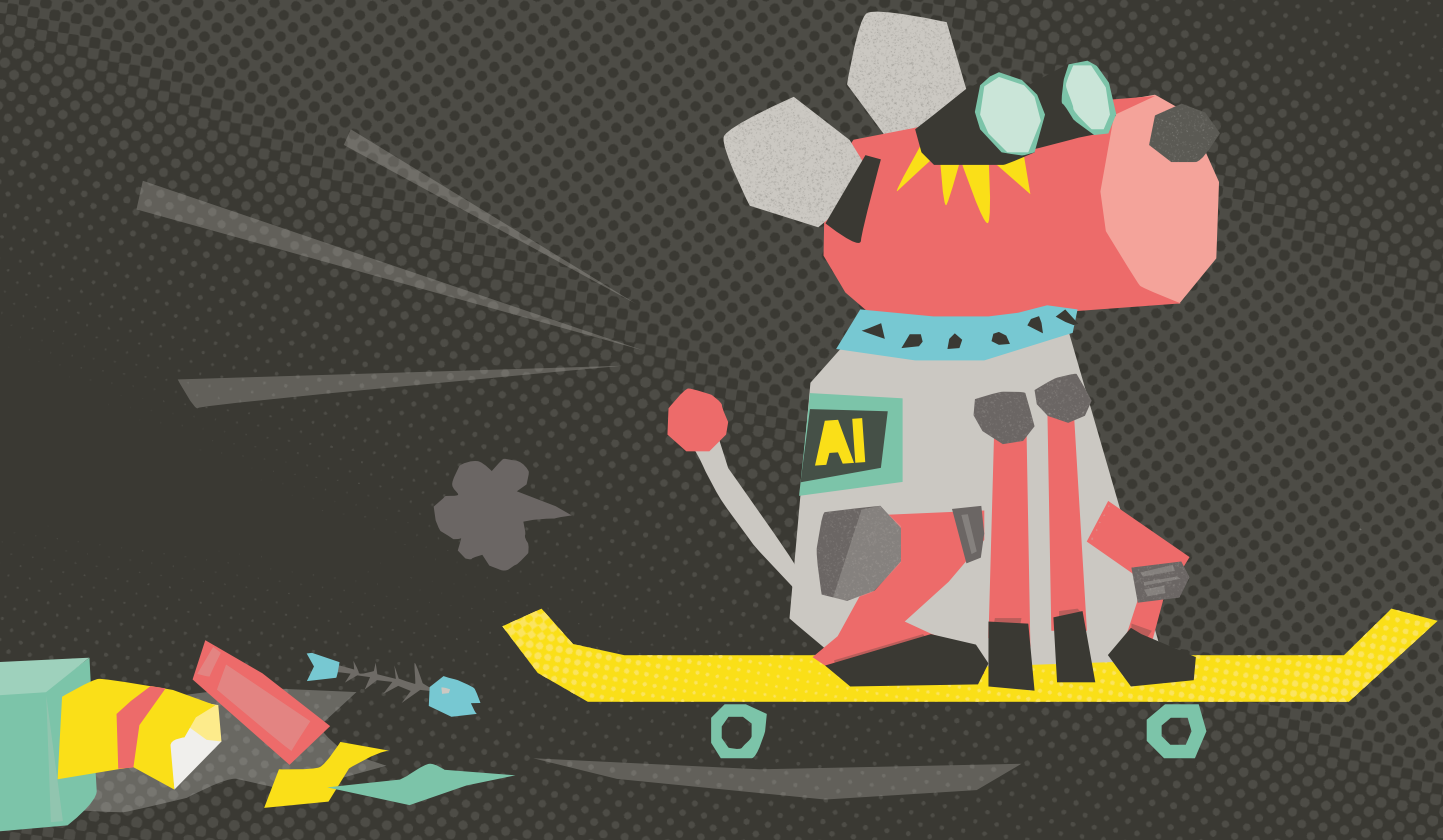
Staying vigilant is still the best defence. Healthy scepticism is a good way to keep yourself safe online. Treating every investment opportunity as suspicious will mean you are much less likely to lose funds to scammers. Investment returns that are too good to be true are always a red flag.

- Remember, a high return in a web search doesn't mean a site is legitimate.
- Check email and web domains closely. You can look on an organisation's legitimate site for email addresses companies will use.
- Communicating over an app, such as WhatsApp, is a sign they may not be legitimate.
- Check the companies register for a business's legitimate website. New Zealand Companies Register (companiesoffice.govt.nz)
- Check the Financial Markets Authority (FMA) website for warnings about malicious investment sites. Home | Financial Markets Authority (fma.govt.nz)
- Check with your bank and other organisations, such as the FMA, before investing any money. This will give you a good sense about whether a particular opportunity may be a scam or not.
- If the person you're speaking to becomes agitated or angry when you say you might leave, that is a good sign you **should** leave.
- You are under no obligation to invest money, and if something feels wrong, you should walk away with your money in hand.

PIG BUTCHERING

It's not the nicest term but, thankfully, it's not a scam involving animals. This term has been coined to represent a situation where aspects of different scams are combined to get the most from a target.

Most commonly, scammers will use the social engineering aspects of a romance scam to build trust with a victim before switching to an investment or cryptocurrency scam.



New dog, old tricks

The newest threat in the cyber landscape is artificial intelligence (AI), and how it's being used by scammers.

Overall, the AI tools available to scammers haven't yet significantly changed the mechanics of scams, but they have made the lives of scammers easier by simplifying some of the work required to create and run a scam.

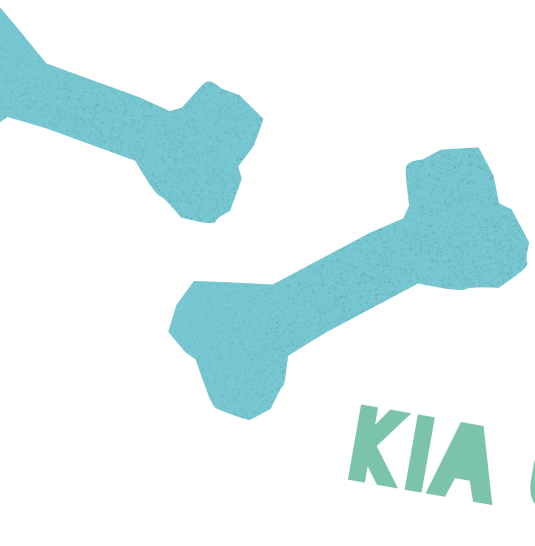
The tools at their disposal mean attackers can quickly create more believable online content.

AI text generators can create far more realistic and error-free phishing scripts as well as descriptive content, while AI image generators can create a suite of photos of a particular person or a completely fictitious one. This makes it easier for scammers to create the type of fake profiles used in romance or investment scams at speed and in bulk.

Tools like ChatGPT can also be used during live chats, making the scammers seem even more legitimate.

AI makes some scams easier to pull off

- **Phishing** – more realistic wording in multiple languages
- **Investment scams** – realistic investment advice
- **Romance scams** – communications sound like a real person, including online chat, and can include realistic images



OTHER LANGUAGES

AI doesn't just help edit English, it can work across various languages. This means speakers of regional languages, who may not usually encounter cyber crime, are now potential targets.

CERT NZ is aware of scams occurring in te reo Māori. It's unclear if these were created using AI but the threat of that happening is increasing.

HOW TO STAY SAFE

The good news is while the tools make it easier for scammers, their methodologies are essentially the same. For example, they can set up a completely AI-generated social media profile, but they still need you to provide information, take some action on your device, click on a suspicious link or send them money.

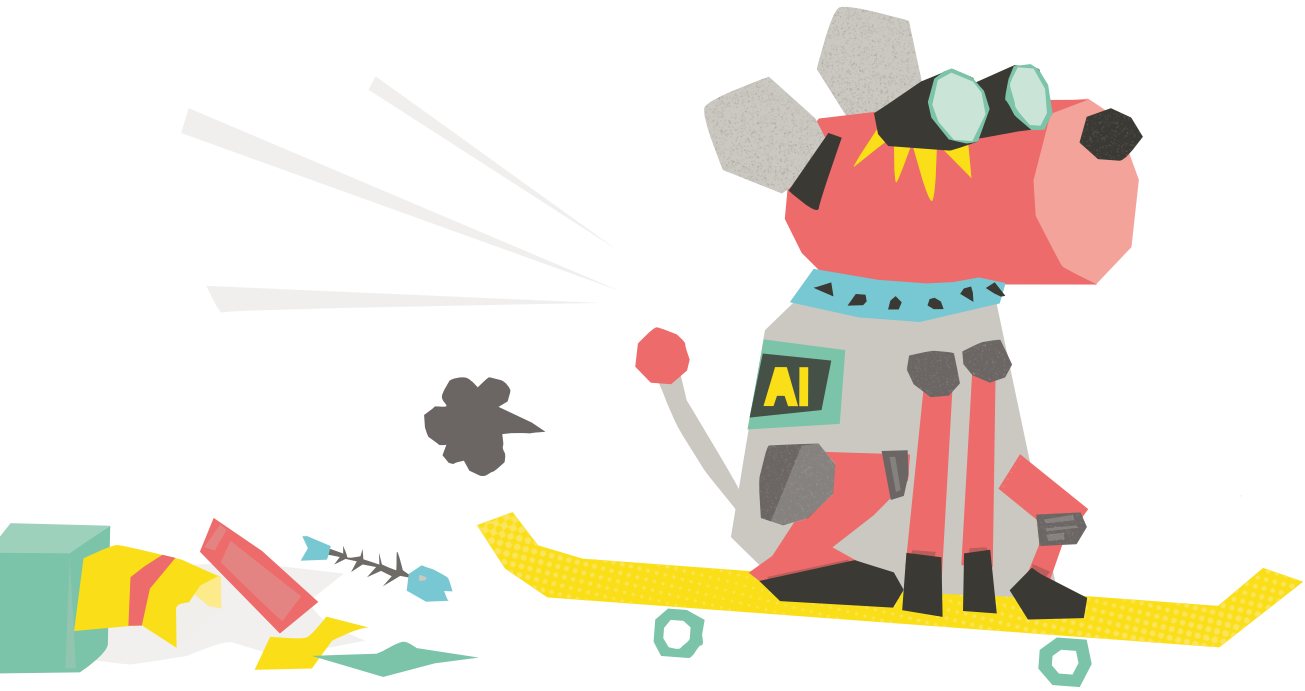
As always, be wary of who you're talking to online, take a second to check any links or details, and don't share passwords, authentication codes or personal information.

It's also a good idea to lock down your social media profiles because scammers can take that information and feed it into AI tools to create more realistic fake accounts or use your publicly available information to target you.

AI BANNED FOR OTHER REASONS

AI is a tool and, like with any new tool, organisations must look at how it affects issues such as security, privacy, and data integrity.

AI tools have been banned in some organisations, but not always for security reasons. Some schools and other learning institutions have put a ban on AI to curb students using it to write assignment answers. Some organisations have created policy which blocks the use of AI to prevent documents with intellectual property from being uploaded and added to the AI learning database.



Scammed out of love

CERT NZ has again noticed an increase in dating and romance scams. These are some of the most financially and emotionally devastating types of scams online and they can be hard to spot.

WHO TO BELIEVE

Scammers can be so convincing that the first time a person realises they are being scammed is when they receive a warning from their bank.

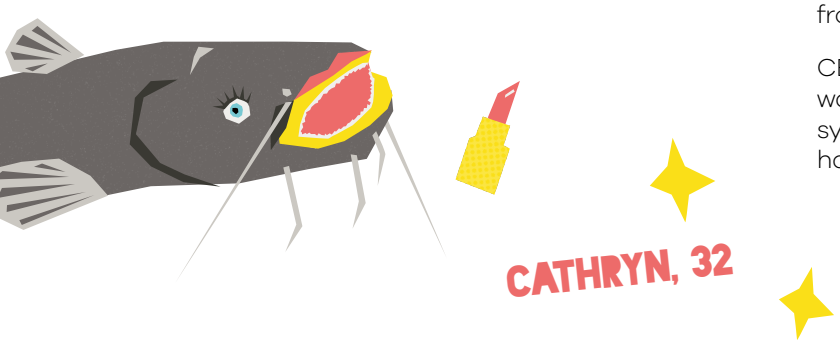
If you attempt to transfer money to someone and your bank advises against it, this is a good indication the person you are transferring money to may be trying to scam you. Banks are able to see some information that scammers can't hide, such as bank account activity.

A warning from your bank is also a good time to look back for any other potential red flags.

- Not wanting to talk on the phone or video chat.
- Sense of urgency around transferring them money.
- Images that don't seem to align with their descriptions.

You can then do other checks, such as using a reverse Google image search, to see if their photos are taken from another online account.

CERT NZ strongly recommends you listen to any warnings from your bank. The bank has formal systems set up to limit loss and fraud. And it is much harder for a scammer to scam a bank.



CRITICAL CONTROLS

CERT NZ has released its Critical Controls for the year which includes one new control: Building security awareness.

Your people play an important role in making sure your organisation and information are kept secure. Alongside implementing technical controls, investing in your people's security awareness and training is a long-term commitment to improving the security of your organisation. This will also flow into their personal lives, keeping their whānau safe online as well.

It's critical your people understand the security risks your organisation faces so they can play their part in the protection of your systems. You can empower them to do this by providing appropriate security awareness training, programmes, and tools.

> Your people play an important role in making sure your organisation and information are kept secure.

International insights

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

CERT NZ, alongside its international partners, has published 'Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default.' The joint guidance – created by the cybersecurity authorities of Australia, Canada, United States, United Kingdom, Germany, Netherlands, and New Zealand – urges software manufacturers to take on the steps necessary to ship products to customers that are secure-by-design and -default. [1]

The National Cyber Security Centre UK has published a blog on the risk and cyber security issues of the AI tool ChatGPT and large language models.[2]

[1] U.S. and International Partners Publish Secure-by-Design and -Default Principles and Approaches | CISA

[2] ChatGPT and LLMs: What's the risk - NCSC.GOV.UK