TOPIC 1

Financial Losses From Scams and Fraud

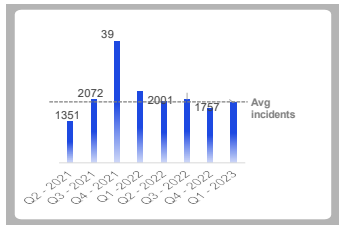
OVERVIEW

Overview of financial losses

Financial losses due to cybercrime rose by two-thirds in the first quarter of the year, figures from cyber security watchdog Computer Emergency Response Team (CERT NZ) show.

Nearly 2000 incidents of cybercrime were reported to the agency between January and March, up 12% on the previous three months.

A total of $5.8m in direct financial losses were reported, an increase of 66% on the prior quarter. In 16 cases, the victim lost over $100,000. One scam campaign in February cost Kiwis millions of dollars over the course of a month.



INCIDENT CATEGORY	Occurrences	CHANGE FROM PREVIOUS QUARTER
Phishing and credential harvesting	946	+5%
Scams and fraud	625	+23%
Unauthorised access	240	+35%
Malware	28	-28%
Website compromise	13	-13%
Suspicious network traffic	2	+100%
Ransomware	12	-67%
Botnet traffic	3	+40%
Denial service	2	0%
C and C server hosting	0	-22%
Attack on system	0	0%
Other	97	20%

1,968 incidents were responded to in Q1 2023.

CASE STUDY

Term deposit scam

CERT NZ acknowledge the reports they receive are likely to be the tip of the iceberg. Combined data from New Zealand banks showed customers lost $183m to scams in the year to September 2022.

> "In the February attack, cyber criminals used search engines and professional-looking documentation to scam New Zealanders looking to invest money."
> - CERT NZ said.

People searching terms such as 'term deposit comparison nz' would be directed to a page that included ads paid for by scammers and linked to fake websites.

If they sent details to these sites, victims would be called by scammers claiming to be from the investment team at a New Zealand-based financial institution.

Some were even given fake investment portfolio websites requiring a login to check their investments.

CERT NZ worked with Google to remove the malicious URLs, and the watchdog also worked with local banks to communicate with the public directly about the scam.

> "AI can be used to write more convincing phishing emails in various languages, to create malicious code, and to even impersonate people in live chats."

CASE STUDY

IRD scam

"The numbers of scams are increasing and so is their sophistication and the sums involved"

Nicola Sladden, Banking Ombudsman.

$60,000 In a recent phishing case, a bank customer lost $60,000 after receiving an email from what he thought was the IRD.

The customer entered his banking details and an SMS code to a fake website because he was convinced he was dealing with the tax department and his bank.

The Banking Ombudsman found the bank should reimburse the customer the full $60,000.

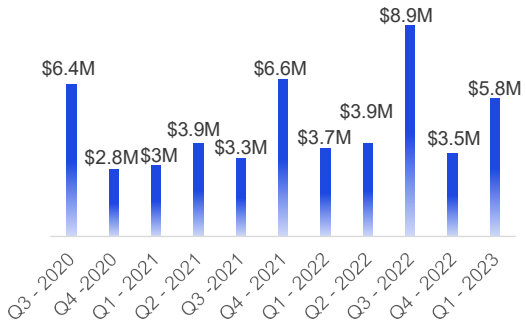
The customer thought the SMS code was related to his internet banking login, but was in fact to complete the mobile banking setup which allowed the scammer to withdraw the money.

> "If the SMS message had made the purpose of the code clearer, the customer may have been alerted to the scam, the Banking Ombudsman found."

IMPACTS

Direct financial loss

Direct financial losses totalled $5.8 million in Q1 2023, which is a significant increase (66.3%) compared to last quarter.



Types of loss

586 incidents of Financial Loss

This not only includes money lost as a direct result of the incident, but also includes the cost of recovery. For example, the cost of contracting IT security services or investing in new security systems following an incident. (Q4, 2022: 469).

67 incidents of Data Loss

Loss or unauthorised copying of data, business records, personal records and intellectual property. (Q4, 2022: 87).

15 incidents of Operational Impact

The time, staff and resources spent on recovering from an incident, taking people away from normal business operation. (Q4 2022: 18).

15 incidents of Reputational Loss

Damage to the reputation of an individual or organisation, as a result of the incident (Q4 2022: 29).