certnz

# Quarterly Report: Highlights

## Q2 2019

1 April - 30 June, 2019

New Zealand Government

# Director's message

**"At CERT NZ, we work to provide the best advice and mitigations to help people get the best out of the technology they rely on, while minimising the risks it can carry with it."**

**Rob Pope, Director**

It's easy to look to the bad when you're in this business, but as we all know online systems and services have hugely improved the way many of us run our professional and personal lives. That's why at CERT NZ, we work to provide the best advice and mitigations to help people get the best out of the technology they rely on, while minimising the risks it can carry with it.

We do this by analysing the data we receive in reports, by proactively seeking threat information as well as collaborating with other cyber security agencies in New Zealand and around the globe. We take this information, distil it and share with New Zealanders, at work and at home, through the likes of this report, our critical controls and Cyber Smart campaigns to help New Zealanders build resilience to cyber threats, protect against loss and keep safe online.

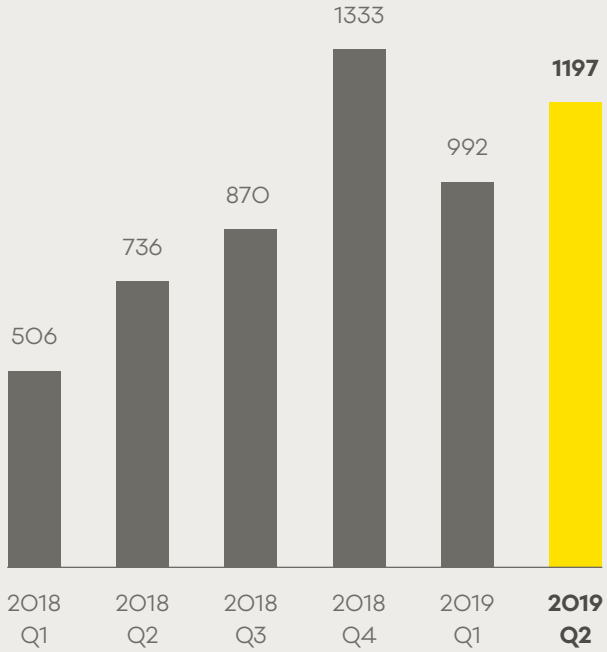
This quarter, CERT NZ received close to 1,200 reports, a 20% jump from last quarter. While the number of reports has increased, we also continue to see a breadth in the types of incidents that New Zealanders are faced with in their professional and personal lives, from file-encrypting ransomware to online shopping scams, all of which bring different challenges and impacts.

One of the big impacts we see is financial. With reports of direct financial loss in the millions of dollars, it's evident that cyber incidents can be costly. But as reports also show, financial loss is not the only impact businesses and individuals experience as a result of a cyber incident. In this report, we unpack how cyber attacks can also cause reputational risk, impact day-to-day lives and put a strain on resources, and offer actionable advice to help New Zealanders protect against them.

## Q2 highlights

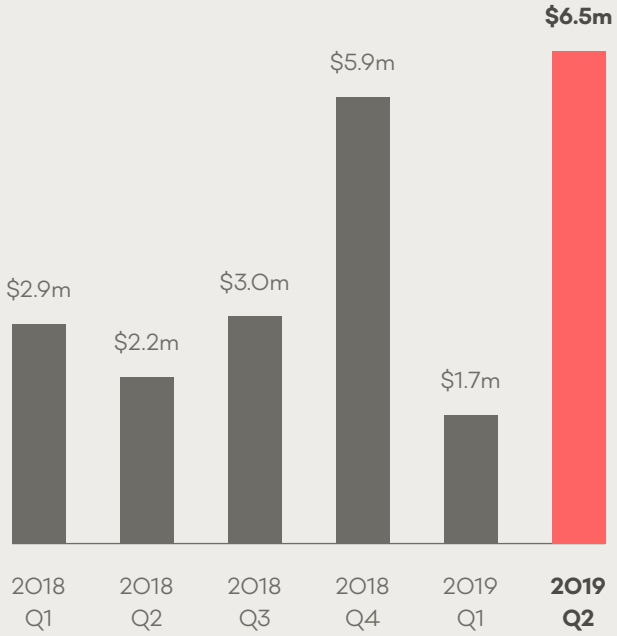
# 1197 incidents

were reported in Q2 2019, a 21% increase on Q1.

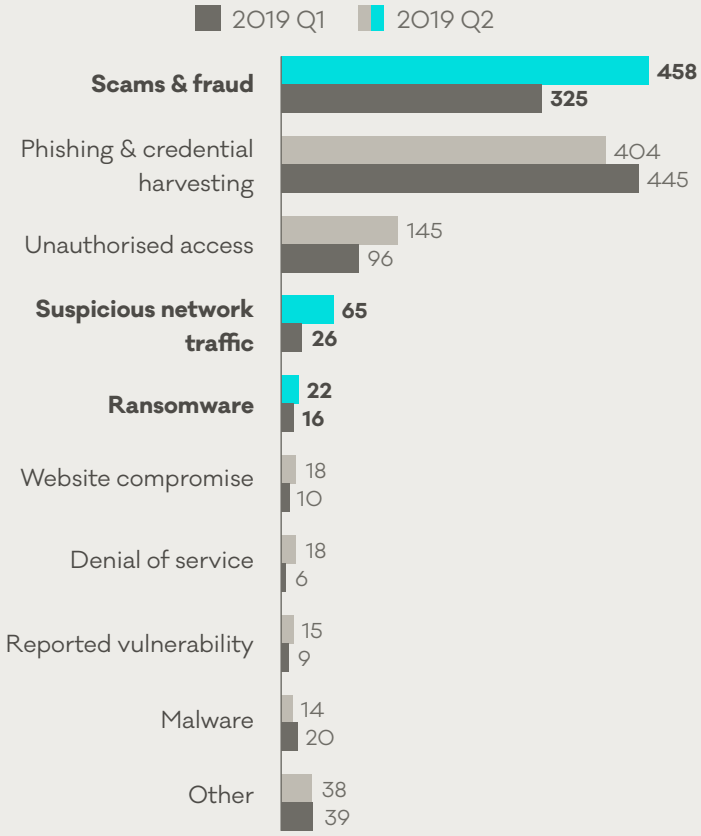



# $6.5 million

reported in direct financial loss in Q2, with 23% of incidents reporting some type of loss.




### Breakdown by incident category




**41%** increase in scam and fraud reports, from Q1.

**150%** increase in suspicious network traffic, from Q1.

**38%** increase in ransomware, from Q1.

Insight

# Buyer beware: online shopping scams on the rise

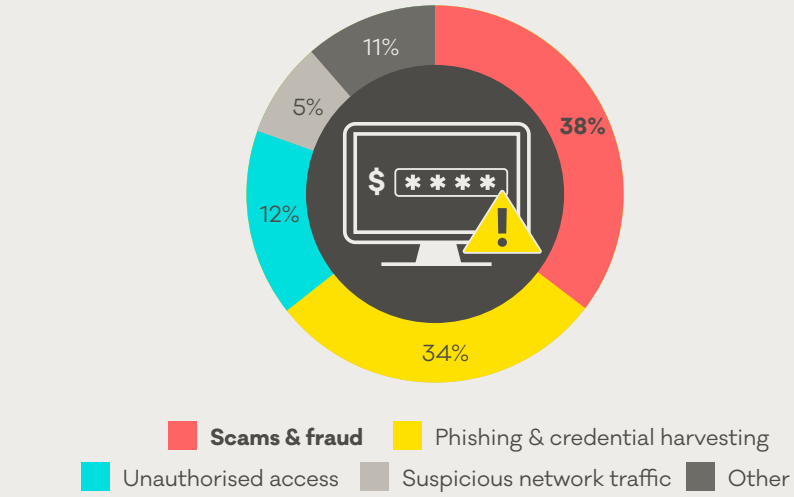
This quarter, 38% of all reports were about scams and fraud, making it the highest incident category in quarter two.

Scams relating to buying and selling goods online make up a high proportion of these reports, totalling 19% of all scam and fraud reports in quarter two.

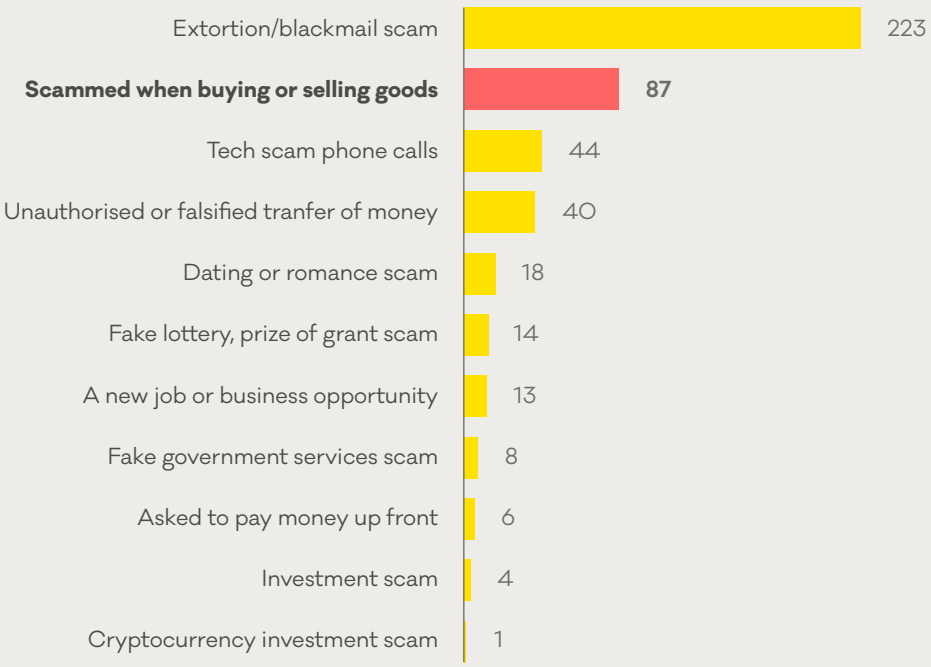
The incidents reported show how online shopping scams can operate across various platforms like social media, scam websites and sometimes through legitimate auction sites. These scams can result in financial loss when goods don't show up, or don't match the description and can also lead to other types of incidents like identity theft.

In one case, an online shopper reported a fake website that was posing as a reseller of an international clothing brand. The shopper was close to completing their transaction when they realised that the website URL didn't use HTTPS and decided to contact the site first to check it was legitimate. The website didn't have any contact information listed so they reported it to CERT NZ. We were able to quickly identify it was a scam website, and worked with the hosting provider to have the site taken down, protecting other shoppers from the scam.

**Breakdown by incident category**




**Breakdown of scam and fraud reports**




For more on the New Zealand threat landscape in quarter two 2019, see CERT NZ Quarterly Report: Data Landscape.
If you have experienced a cyber security issue, report it to CERT NZ at **www.cert.govt.nz**.

Focus area

# Ransomware impacts

Ransomware has significant and wide-ranging impacts on affected organisations, their staff and customers.

Ransomware incidents have remained steady since CERT NZ launched in 2017, making up 2-3% of total reports received. This quarter, we received 22 ransomware reports, mostly from businesses.

Ransomware is a type of malicious software that can get into a computer system in a number of ways, like a bad link or attachment in an email, or through out-of-date software. Once the ransomware has infected the computer, it encrypts files so they can't be read or accessed, and demands money to recover them.

**CERT NZ does not recommend paying the ransom. Although it may seem like the quickest solution to recovering files, the payment does not guarantee that they'll be returned or decrypted.**

Paying the ransom could also lead to further attacks, and further financial loss.

We've seen a number of ransomware campaigns impacting New Zealanders. One of the first was WannaCry, which exploited Microsoft systems. More recently, the wide-spread GandCrab, which reportedly infected over 1.5 million computers globally, impacting public services and disrupting the lives of many people.

Over time, attackers modify ransomware and release new variants. New types of ransomware are released to exploit newly identified software vulnerabilities. CERT NZ predicts that ransomware will be released to take advantage of Windows 7 when support for this operating system ends in January 2020.

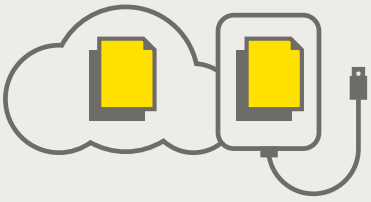
The total direct financial loss from ransomware reported to CERT NZ is just over $127, 000, mostly from ransoms being paid. The costs of ransomware also go beyond direct financial loss. Cases we have seen report losses like reputation, data, and customer information. Of the total 160 ransomware incidents reported, over 70% reported one or more of these loss types.

Recovering from the impact of these attacks can be time consuming and significantly affect a business's day-to-day operations. However, there are simple prevention measures CERT NZ recommends to help protect against a ransomware attack.

## Protect from ransomware

### Keep your operating system and apps up-to-date

Update to new versions when they're available. You can set this up to happen automatically with major operating systems like Windows and MacOS, and common applications like Office.



### Make sure you back up your files regularly

You can use an external hard drive or cloud service. This includes the files on your computers, phones and any other devices.

### Install antivirus software

Running antivirus software and updating it regularly helps keep your device safe.

Case study

# Small business experiences the impacts of ransomware

Small businesses are increasingly experiencing the impacts of ransomware attacks, and the consequences are not always financial as one business recently experienced.

A gym with close to 1,000 clients was hit by a ransomware attack. The manager had purchased new gym equipment and soon after received an email claiming there was an outstanding invoice with a PDF invoice attached.

The manager thought the invoice was a mix up for the recent purchase and tried to open the attached PDF. Nothing happened, so he tried again. Thinking the download issue was a fault with the computer, he carried on with other work. When he went back to the computer and tried to access a document, all the files were locked and a ransom pop-up notice appeared demanding payment to unlock them.

**The manager immediately called his IT service provider and took the advice not to pay the ransom.**

The IT provider investigated and identified that the PDF attachment was a ransomware file that had infected the computer when it had been clicked on. The files had been encrypted with Locky ransomware and unfortunately couldn't be recovered.

The gym had been in business for ten years, and had not backed up or stored any data, so as a result client records and fitness programmes were lost. With the significant loss of customer information, the gym also faced a reputational risk. The manager let all clients know of the incident and that their files had been lost. Fortunately, the clients appreciated the open communication and the difficulty of the situation.

To recover, the gym had to start from scratch to rebuild records while maintaining day-to-day operations like classes and personal training services. This cost a lot of staff time and resources.

The gym is now following CERT NZ advice and taking steps to secure their systems by backing up all data regularly, and installing anti-virus software.

Focus area

# Suspicious network traffic increase

Last quarter, we introduced how CERT NZ is expanding the way we collect and extract threat information from the international landscape. This helps us better identify incidents that could affect New Zealand infrastructure and system owners.

In quarter two, this process has enabled us to identify more suspicious network traffic reports, up 150% from quarter one.

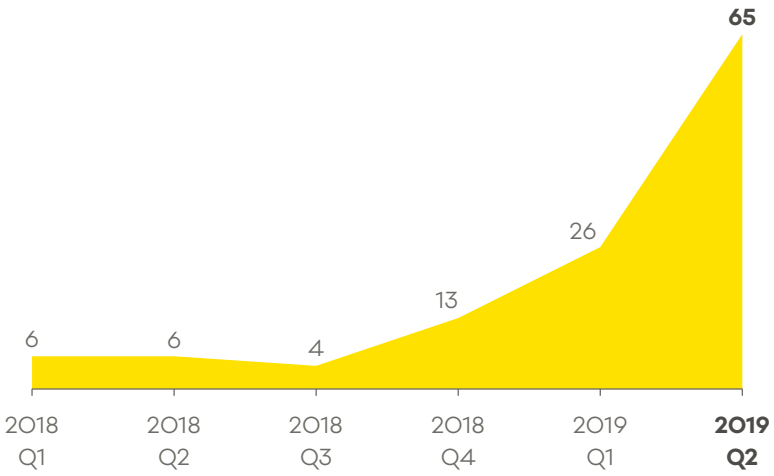
Suspicious network traffic is when an attacker attempts to find insecure points or vulnerabilities in networks, infrastructure or computers. 58 of the 65 incidents in this category were found by CERT NZ – more than three times the amount in quarter one.

If the threat information shows a New Zealand source is involved, CERT NZ checks the data, raises a report of suspicious network traffic, and notifies the ISP.

The most common type of suspicious network traffic CERT NZ has seen this quarter are brute force attempts, which are attempts to gain unauthorised access.

CERT NZ strongly recommends building resilience to cyber attacks by implementing our Critical Controls across systems and networks.[1]

**Number of suspicious network traffic reports**




# Increase in incidents referred to NZ Police

CERT NZ operates as a central front door for New Zealanders to report cyber security incidents, handling some incidents on our own and working alongside partner agencies for incidents where they may be better placed to help. For example, incidents we receive about cyber crime are referred to New Zealand Police. This is one of the ways we work across the New Zealand cyber security landscape to make sure that all incidents are dealt with by the right agency for the best outcome.

This quarter, there was a 42% increase in the number of reports we referred to New Zealand Police. This increase was mostly due to the large rise in numbers scam and fraud reports, up 41% from quarter one. There were also 29 separate reports, totalling $62,000 in direct financial losses relating to the unauthorised access of a cryptocurrency exchange. Recent reporting suggests that losses could potentially be NZ$20-30 million, making it one of New Zealand's costliest cyber security incidents to date.



[1] https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/

Insight

# Cyber security incidents affect all ages

In quarter two, 59% of the reports CERT NZ received were about individuals.

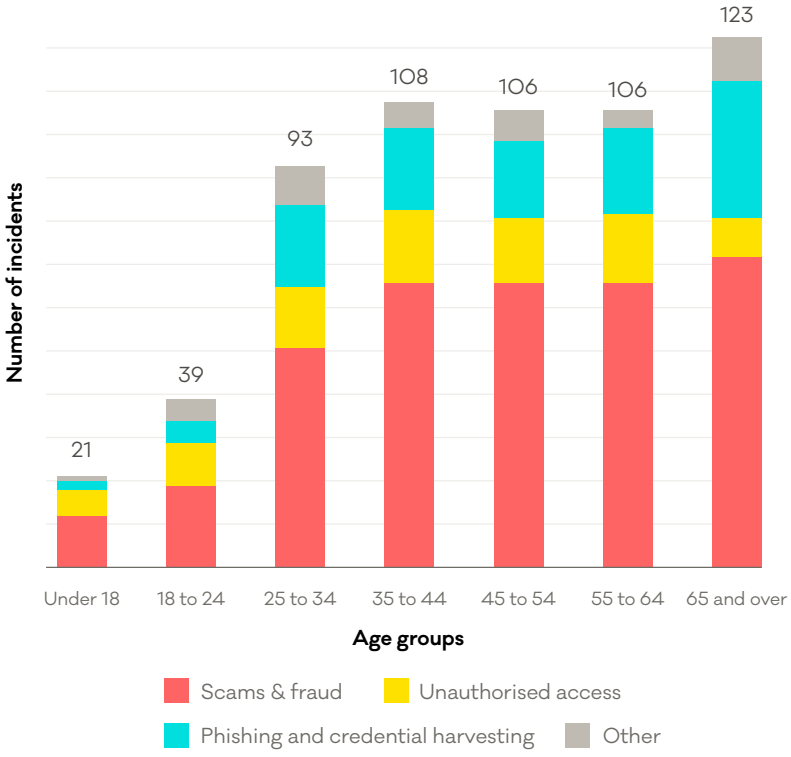
The number of incidents reported by individuals continues to be spread across all age groups, demonstrating that New Zealanders of all ages are affected by cyber security incidents.

Of the 712 incidents about individuals, 30% reported some type of loss, like financial, data and reputational. Scams and fraud was the highest reported category affecting individuals (56%), with a total direct financial loss of $4.5 million.

While all New Zealanders are affected by cyber security incidents, the 55 – 64 age group experienced the highest volume of financial loss in quarter two. This age group made up 89% of financial losses reported by individuals, mostly attributed to scams and fraud.

This data helps us understand what types of cyber security threats are impacting everyday New Zealanders. We use this information to develop specific outreach programmes, like our upcoming Cyber Smart Week in October, to raise awareness around the simple steps New Zealanders can take to stay safe online.

**Incidents affecting individuals by age group**



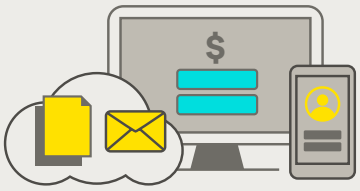

## Top three incidents affecting individuals


**401 (56%)**

Scams and fraud

**136 (19%)**

Phishing and credential harvesting




**122 (17%)**

Unauthorised access