certnz

Quarterly Report: Highlights

Q4 2019

1 October - 31 December, 2019

New Zealand Government

Director's message

"It's only by coming together that we'll make New Zealand stronger and more resilient to the cyber threats that present challenges to us."

Rob Pope, Director

In the last quarter of 2019 it seemed that everywhere you turned there were stories about cyber security having real-life impacts on people. From health records being breached to ransomware attacks, cyber security issues are part of our everyday lives.

New Zealanders are known for our 'she'll be right' attitude, but when things go wrong we need to know where we can go to get the help we need to recover. At CERT NZ, we see a large number of New Zealanders reaching out to us for help each quarter, however we know that there are more people who are impacted, and not getting the help that they need. As we see out 2019 and look forward to the year ahead, that's what we're encouraging with all Kiwis – if you see something, say something. Whether you need our help, or just want us to know that you've experienced an incident and have got it under control, we're only a phone call away.

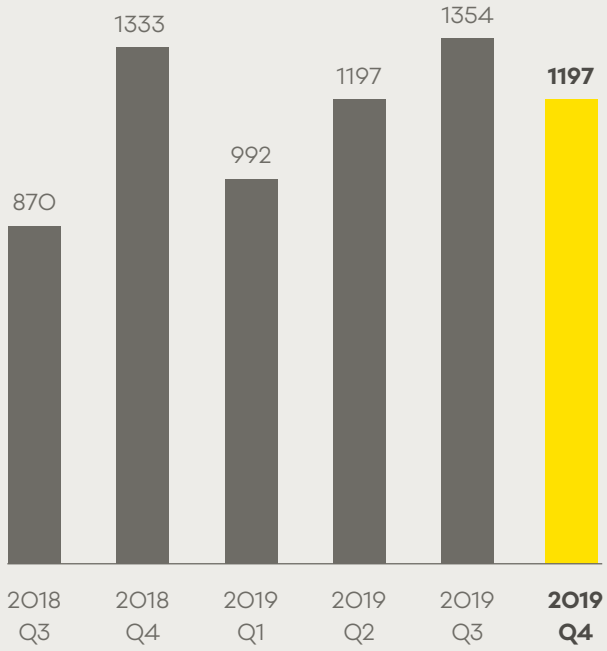
Kiwis love to be empowered to help ourselves, and at CERT NZ we want to continue encouraging that mindset. So as part of our work we're also focused on building cyber resilience in the community at large. One of the ways we do this is through our national awareness week, Cyber Smart Week, which was also in quarter four of 2019. Now in its third year, we saw another increase in partners coming on board, with over 120 partners promoting cyber resilience for all New Zealanders.

It's only by coming together that we'll make new Zealand stronger and more resilient to the cyber threats that present challenges to us: whether that's by teaming up to support each other when something bad happens, or banding together to become more protected in advance, we all make a bigger impact when we work together.

Q4 highlights

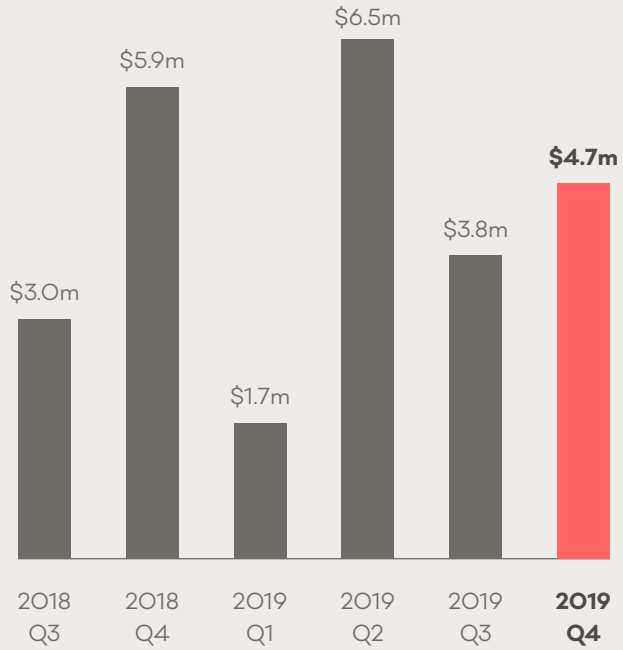
1,197 incidents

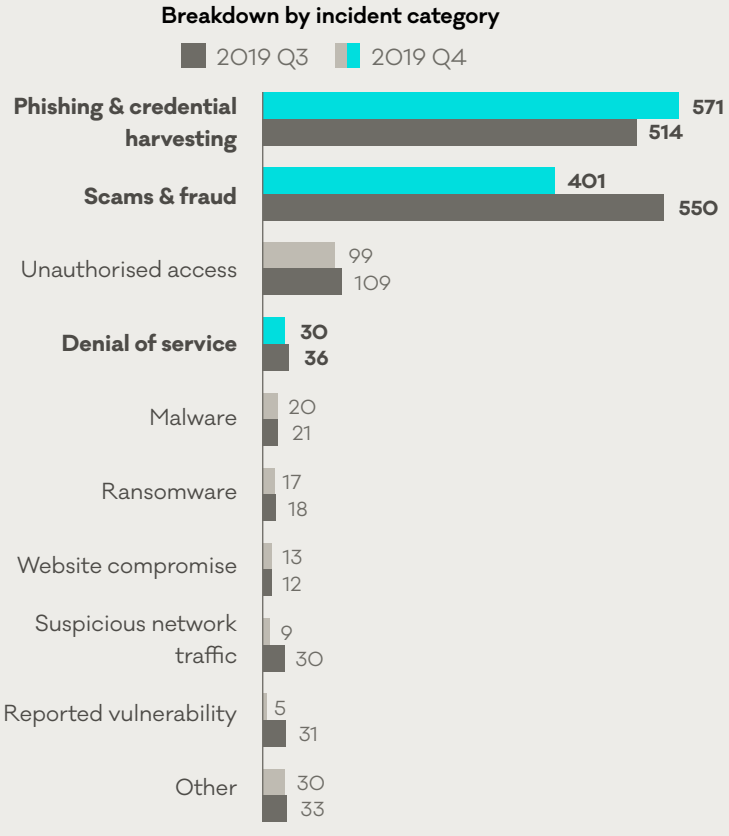
were reported in Q4 2019, down 12% from Q3.



$4.7 million

in direct financial loss reported in Q4, with 15% of incidents reporting financial loss.





11% increase

in **phishing and credential harvesting** reports from Q3.

27% decrease

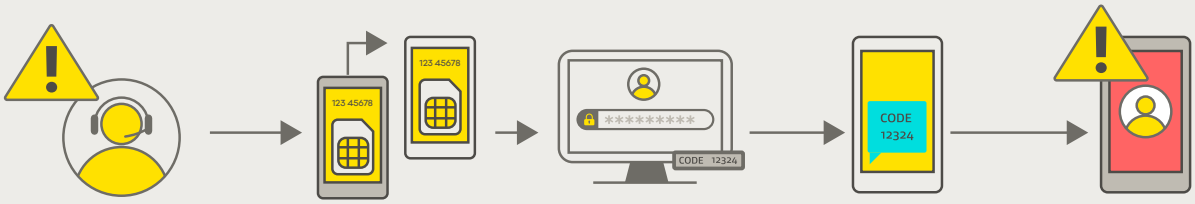
in **scam and fraud** reports from Q3.

Denial of service reports were higher in 2019, averaging **22 incidents per quarter** compared to an average of 4 in 2018.

SIM swapping attacks

SIM swapping attacks have been getting international exposure and media coverage for some time, but until recently we hadn't received many reports here in New Zealand. In Q4 this changed, and we received a small cluster of reports, some including significant financial loss. Given the potential impact of this type of attack we want to share how to protect yourself and your business.

What is a SIM swap attack?



1. Attacker calls target's mobile provider and requests that the target's mobile number is transferred

2. Number is transferred to a different SIM, target unaware

3. Attacker tries to access target's account, either using stolen credentials or requesting a password reset

4. The 2FA code is sent via SMS to the attacker and they can access the account

5. Target only becomes aware when their phone is disconnected or they're locked out of an account

SIM swap attacks (also known as SIM porting or SIM hijacking) are where an attacker uses social engineering techniques to manipulate a mobile phone provider into porting a mobile phone number from a genuine customer's SIM card to the attacker's SIM card. The attacker can then receive all SMS messages and voice calls intended for that customer.

Given the amount of effort required, the incidents we see are motivated attackers focused on particular individuals.

Once the attacker has the victim's mobile phone number on their SIM card, they try to access their accounts, such as bank accounts, using stolen or guessed credentials. When prompted for a two-factor authentication code, the attacker uses the stolen number to receive two-factor authentication by SMS – working around the security control.

There is a significant risk to the people and businesses targeted by these attacks because the attacker can perform sensitive tasks, like changing passwords or authorising financial transactions.

Anecdotal reports show that incidents of SIM swapping are increasing, as motivated attackers find ways to circumvent additional security controls.

During Q4, CERT NZ received multiple reports of SIM swap attacks – the first of this type of attack for over a year. In these reports, attackers were able to gain access to the online bank accounts of the victims in all cases.

While there was only a small number of reports (less than 10), the average financial loss from SIM swapping attacks reported to CERT NZ in Q4 2019 was $30,000.

Average financial loss of
$30,000

How can I reduce the impact of SIM swapping?

It's difficult for an individual to prevent or detect SIM swapping. Attackers can contact mobile phone service providers and have numbers transferred without the user's knowledge.

There are ways to prevent or reduce your chances of being a target of successful SIM swapping, including:

Be careful where you share identity information

Your personal information can be used to impersonate you, particularly when it's used as part of the identity confirmation process. If you know that your mobile phone provider confirms your identity by asking for personal information, make sure it's hard to find online. For example, you may be asked for your date of birth so make sure you're not sharing it on your public social media accounts.

When there's a choice, don't use SMS two-factor authentication

SMS two-factor authentication is better than a password alone, but there are stronger options available. Ask your bank or service provider if they offer other forms of two-factor authentication for account access. For example, this might be an app-based authenticator that generates a new code every 60 seconds or sends you a push notification.

Be creative with account recovery questions

For some services, when you set up your account you'll be asked to provide answers to a set of security questions. These are generally used as a way to identify you if you forget your password and need a prompt — like your mother's maiden name. Unfortunately, these are also easy things for an attacker to find out, and could be used to gain access to your accounts without your knowledge. Where you can, make up something memorable but untrue that an attacker couldn't find through a simple search of your name. You can use a password manager to store these answers too.

Get notifications

Check with your bank or service provider about whether they have a system to notify you about suspicious account activity – like sending you an email any time there's a request for a transaction over a certain value.

How will I know if I'm affected and what should I do?

If you notice suspicious activity like un-prompted password reset notifications, or if your phone unexpectedly loses connection to the mobile network, you may be affected by a SIM swap attack.

If you're affected, take the following steps immediately:

1. Report it to CERT NZ, we can help with advice to secure yourself. With your permission we can also work with the New Zealand Police.
2. Reset passwords for your important online accounts. Online banking and email should be a priority.
3. Report it to your mobile phone provider and check if your mobile phone number has been transferred to another SIM.

I'm a business – what should I do?

Businesses who are responsible for customer accounts and data should consider the controls they have available.

Protect your customers by:

- Using our Critical Controls when designing and implementing your systems.
- Using app-based or hardware two-factor authentication for customer access to your services where possible.

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

Case study

SMS phishing on the hook

This quarter we saw a large SMS phishing campaign targeting the customers of a New Zealand bank.

The campaign used an online bulk text messaging service to send text messages to 27,000 New Zealand mobile phone numbers. About 12,000 of these people were customers of the affected bank.

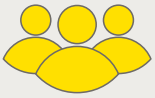
CERT NZ coordinated a joint response to the incident with the bank, New Zealand Police and the Department of Internal Affairs. As a result of this collaboration, measures were taken to protect the bank's customers and stop the campaign before further harm was done.

Because the incident report made to CERT NZ contained lots of actionable information, we were able to help the bank quickly identify how the attack occurred and mitigate some of the immediate threat. It also added important detail to our understanding of this type of attack in the threat landscape, and we use this information to keep more New Zealanders safe.

If you receive spam text messages, or text messages with suspicious links, forward them to the Department of Internal Affairs' text message spam reporting number: 7726

The campaign used
27,000
messages

About
12,000
of these people were customers of the reporting bank.

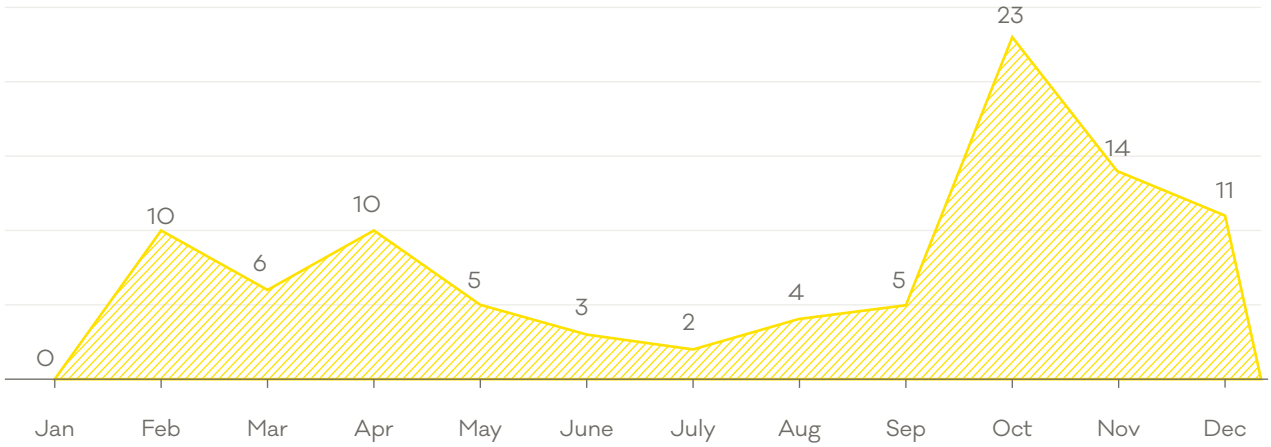


CERT NZ coordinated a joint response with the affected bank, New Zealand Police and the Department of Internal Affairs.

Insight

Scam calls spike in Quarter Four

Number of scam calls - 2019



CERT NZ has seen an increase in reports of scam calls trying to extract information from people. The graph above shows the numbers of scam call reports received over the last 12 months.

CERT NZ receives a wide variety of reports about scam calls. A large portion are familiar and well-documented tech support scams. Alongside these, robocalls are increasingly popular. These automated calls claim to offer credit card holders an increase on their credit limit or notify them of a supposed suspicious transaction. If you receive calls like these, hang up immediately and contact your bank.

New in this quarter, we've had reports of a scam call campaign claiming to be from the 'New Zealand Government Grants Department' that advises the victim that they've been awarded a $10,000 tax refund grant, subject to confirming some security questions. This scam is designed to harvest personal details to gain access to their accounts.

Scam calls need a coordinated response; they impact New Zealanders from all walks of life and they're hugely variable. To combat this, the Telecommunications Forum (TCF) have signed Memoranda of Understanding with key agencies, including CERT NZ and other government partners. By teaming up and sharing information with the TCF, we are seeing scam call campaigns stopped early so fewer New Zealanders are impacted by them.

If you think you've received a scam call, you can report it to CERT NZ:

www.cert.govt.nz/report

For more on the New Zealand threat landscape in quarter four 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/report**.