certnz

Quarterly Report: Highlights

Q1 2019

Q1 1 January - 31 March

New Zealand Government

Director's message

"This quarter, we've worked with close to 1,000 Kiwis, from Invercargill to the Bay of Islands, to help them recover from cyber security incidents and build their resilience."

Rob Pope, Director

As the old adage goes, change is the only constant. We see this refrain clearly in cyber security as CERT NZ enters its second year of operation and we continue to see the evolution of the cyber threat landscape and its impact on New Zealanders.

Technology and cyber security work hand-in-hand in our modern lives. As technology becomes increasingly normalised into the processes that we use every day, the need for a security overlay increases. Consider email, it's at the core of many businesses, but it also introduces risk to those businesses.

This quarter we've seen an increase in reports of unauthorised access of both business and personal email accounts, and new variations of email extortion scams. In both of these cases, attackers rely on exploiting the trust we have in our email accounts and contacts which can result in loss of finances and private information.

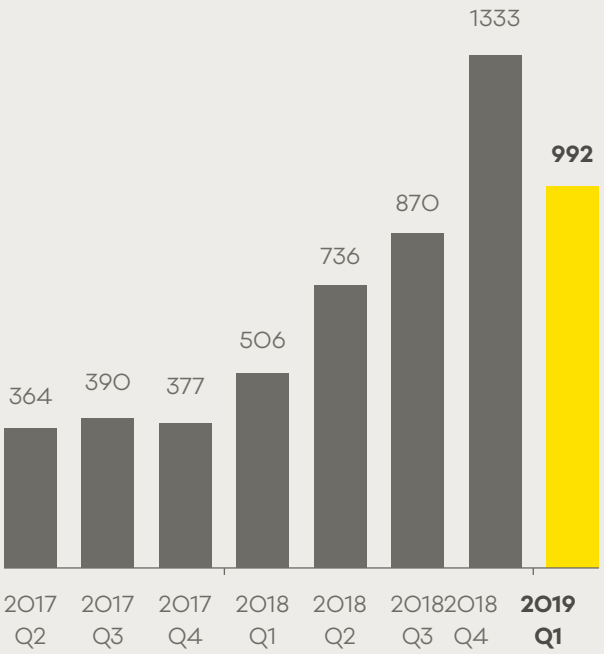
It's more important than ever that New Zealanders have a trusted source of timely information and actionable advice to help protect against and recover from these threats. Helping people keep safe online and improving cyber security in New Zealand is at the centre of what we do at CERT NZ, and that's why we're continuing to expand the way we work to have a greater understanding of the threats and vulnerabilities that can affect New Zealanders, at work and at home.

This quarter, we've worked with close to 1,000 Kiwis, from Invercargill to the Bay of Islands, to help them recover from cyber security incidents and build their resilience to new and evolving cyber security threats. In 2019, we're focused on building that resilience even further.

Q1 highlights

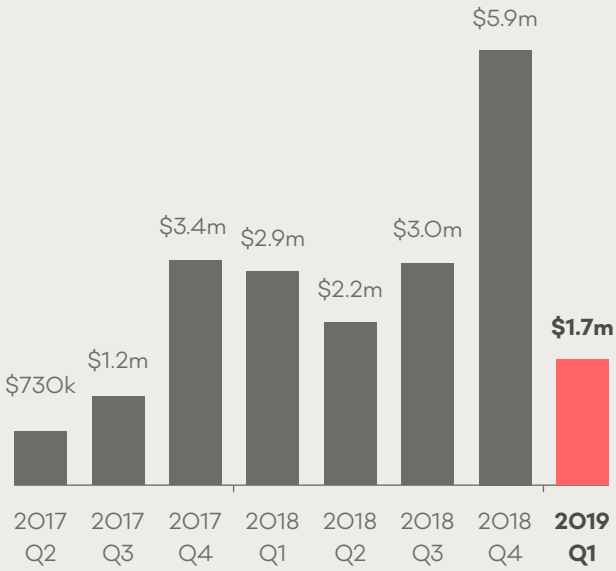
992 incidents

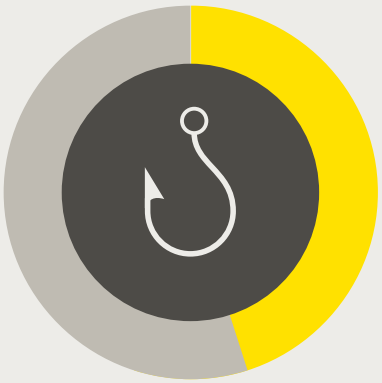
were reported in Q1 2019, the second highest after Q4, 2018.

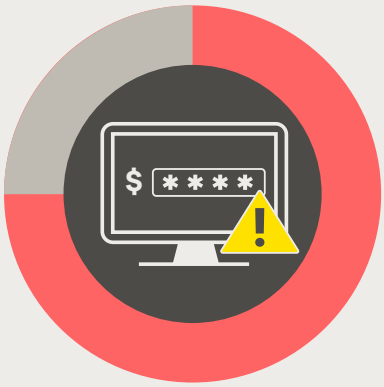


$1.7 million

in direct financial losses, with organisations reporting 61% of total financial loss.







45% phishing

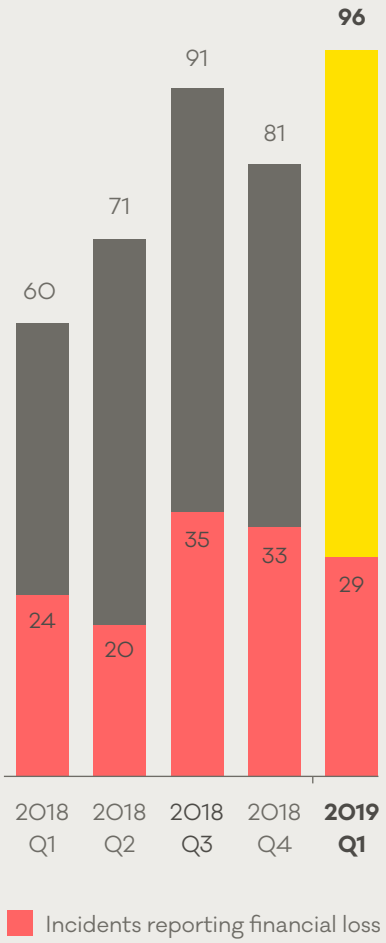
Phishing is the largest reported category, after previously being overtaken by scams and fraud in Q4, 2018.

Scams & fraud

accounted for 75% of financial losses.

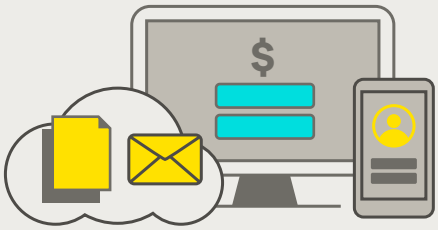
Increasing number of unauthorised access reports

In Q1, CERT NZ received the highest number of unauthorised access incidents in a quarter so far, with a 19% increase from the previous quarter. Just over two thirds of these incidents were about individuals.



$329,000

Unauthorised access can be costly, in this quarter 30% of these types of incidents reported financial losses, totalling $329,000.



Attackers targeted a range of account types like online banking, social media, cloud services and email. They do this for financial gain and to collect private information about the account holders and their contacts.

In this quarter's focus area we explore unauthorised access of business email accounts and how to protect against it.

For more on the New Zealand threat landscape in quarter one 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**.

Case study

Compromised cloud account used for phishing campaign

In Q1, CERT NZ received a report from an IT service provider. The IT service provider supported a business customer who had their Microsoft Office 365 (O365) account compromised. The attacker used the account to send thousands of phishing emails to the business' clients.

The compromised account belonged to an employee of the business, who had a large contact list. The attacker used their account to email their contacts a link to a document on a file hosting service, Microsoft OneDrive. If the recipient clicked on the link, they were taken to a legitimate-looking OneDrive login page asking them to enter their username and password.

However the page was fake, and for every recipient who entered their username and password, the attacker was able to access their email account as well. The scam went undetected for many recipients who clicked on the link and entered their details as it seemed like a regular download process.

Fortunately, the IT service provider noticed an unusually high volume of emails being sent. This alerted them to the attack and they reported it to CERT NZ.

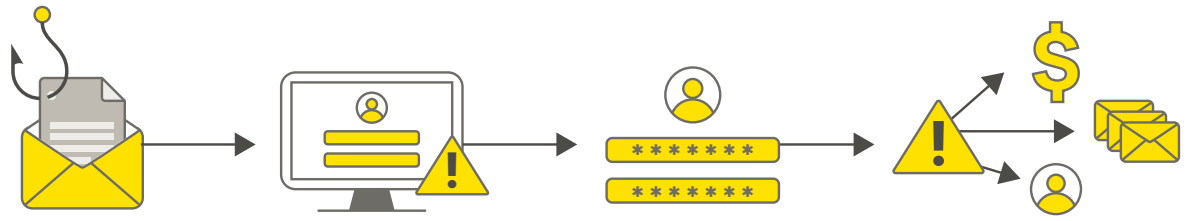
CERT NZ worked with the IT service provider and the business to alert those on the contact list, help the business secure their account, and prevent the attackers from sending further emails. CERT NZ recommended the business set up two-factor authentication (2FA) on their email and cloud service accounts to help prevent future compromise.

CERT NZ also received reports from the recipients of the phishing email who had followed the link and entered their username and password. We provided them with assistance to help secure their accounts.

As a result of the business acting quickly and seeking assistance from CERT NZ, they minimised the financial impact to the email recipients, and mitigated any potential negative impact on their reputation.

These reports and others have helped us to develop new website content and advice dedicated to helping New Zealanders and their businesses stay safe online. [1]

Our counterparts NCSC UK have produced an O365 specific guide that is also available on their website. [2]



Attacker sends phishing emails, with a link to an O365 or Google Docs document, to business employees.

If the employee clicks the link, they are taken to a real-looking login page.

When the employee enters their details, they are sent to the attacker.

The attacker can then steal money, send more phishing emails to the employee's contacts, and compromise more accounts.

[1] https://www.cert.govt.nz/business
[2] https://www.ncsc.gov.uk/news/rise-microsoft-office-365-compromise

Focus area

Business email compromise

Unauthorised access is consistently the third largest incident category reported to CERT NZ. One of the most common types of unauthorised access is business email compromise.

This is when an attacker gains access to an employee's email account and carries out a range of scams or attacks, like sending phishing emails or fake invoices to the business's contacts, usually to access private or financial information. The impact can be wide reaching, impacting not just the business but their suppliers and customers as well.

A common way that attackers gain access to a business email is by acquiring an employee's password. Attackers obtain passwords a number of ways, including guessing weak passwords, acquiring them from a previous phishing campaign or through a data breach that results in a credentials dump – where cyber criminals buy and sell lists of usernames and passwords online.

A recurring type of business email compromise is attacks on cloud-based services, like Microsoft Office 365 and Google G-Suite, to send phishing campaigns. If employees enter their workplace credentials into the fake site, attackers can use them to gain access to the business' wider network, making them vulnerable to more attacks. As more and more businesses move to cloud services, CERT NZ predicts that attacks on these platforms will increase.

Another common scenario is when attackers gain access to an employee's email account to monitor both payment-related emails from goods and service providers, and the business' billing cycles. The attackers then replicate and send legitimate-looking invoices mirroring the business' behaviour. These invoices can be hard to detect as often the only difference is that the bank account details have been swapped out to direct the payment to the attacker's account instead.

Applying two-factor authentication (2FA) to cloud and email accounts is the best mitigation for these types of attacks.

Other mitigations include checking invoices and reviewing your business processes to make sure they don't only rely on email. Verify payments to new or different accounts by phone before making a bill payment to help prevent losses.

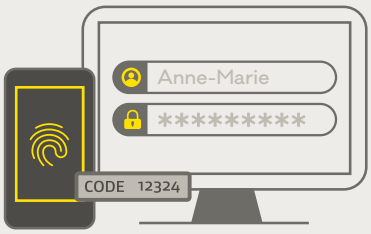
Protect your accounts with two-factor authentication (2FA)

What is 2FA?

To log in with 2FA you need your username and two other things — your password and something else — before you can access an account.

These two things can be:

- something you know, like a password
- something you have, like a token or an app on your phone, or
- something you are, like a fingerprint.



How it works.

When you log in to an email account, you use both your password and something else like a temporary access code from an app on your phone. Even if someone finds out what your password is, they can't get into your account with that alone. They also need to have physical access to your phone so they can get the code, which is less likely.

Scam & fraud incidents

As part of CERT NZ's ongoing efforts to improve our data, we have made changes to the way we record incidents. These changes provide a greater level of detail in our data.

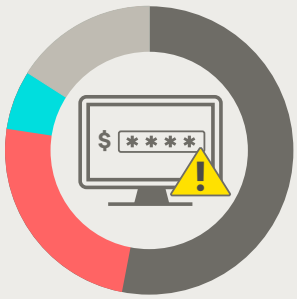
The changes include updating our scams and fraud category, and introducing ways to identify sub-types of online scams and fraud.

Overall, scam and fraud incidents decreased in Q1, to 33% of all reports received – down from 50% of all reports received in Q4, 2018. Despite the decline in reports, the financial losses experienced as a result of scams and fraud made up 80% of the total in Q1.

Compared to the previous quarter, there were fewer email extortion variants. The main variant reported in Q1 was a CIA-themed extortion threat — where scammers attempt to trick recipients into thinking they have been caught in an international CIA investigation involving child exploitation. Scammers demand a payment to 'remove' the recipient's information from the investigation.

CERT NZ expects to see these campaigns continue throughout the year, with new variants being introduced as people become aware of scammers tactics.

In Q1, the top three types of scam and fraud incidents were:



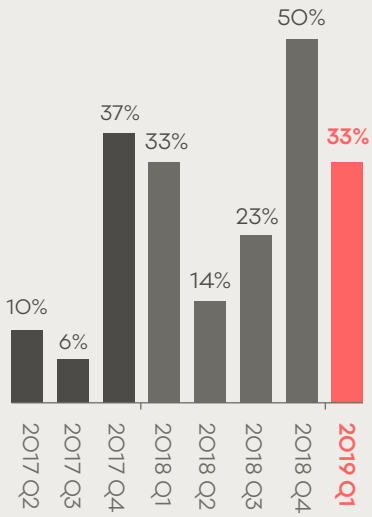
53%
Email extortion campaigns

24%
Scams related to buying and selling goods online

6% Invoice scams

17% Other scams

Percentage of scam and fraud incidents



Enriching incident data to help New Zealanders

CERT NZ is expanding the way we collect and extract threat information from the international landscape.

This enables us to better identify incidents that could affect New Zealand infrastructure and New Zealand system owners.

This increase in information:

- helps us manage intelligence and incidents more effectively
- significantly improves our ability to map relationships between threats and incidents
- improves the time and effort to extract and enrich threat data from incidents reported directly to CERT NZ.

In quarter one, we were able to identify 56 new incidents.

These incidents were raised because international organisations had observed New Zealand-based infrastructure performing suspicious activity.

CERT NZ worked with many of the system owners to resolve their issues. We continue to develop and refine this capability, and use the information generated to help protect more New Zealanders.

Of the 56 identified incidents:

37 involved phishing and credential harvesting attempts.

Many of these proactively identified compromised websites hosted in New Zealand or hosting phishing pages for some New Zealand brands as well as other well-known global brands.

19 were about suspicious network traffic from New Zealand-based sources.

These included port scanning and brute force attempts to gain unauthorised access.