certnz

Quarterly Report: Highlights

Q3 2019

1 July - 30 September, 2019

New Zealand Government

Director's message

"Whether you've been affected by a cyber security incident or want to know how to protect against one, the team at CERT NZ is here to help you make cyber security your business and improve your online resilience."

Rob Pope, Director

Cyber security might seem like a topic best left to those in information security and IT, but in this day and age it's everyone's business.

At CERT NZ, we learn more about New Zealand's threat landscape with every report we receive, and we're seeing that security issues are impacting people and organisations all over New Zealand. From teens to CEOs, incidents are experienced across the board. This quarter we've received the highest number of reports to date.

And it's not just at CERT NZ, we are seeing more headlines about cyber security than ever before. Media stories of everyday people receiving phishing emails through to big business experiencing data breaches show that cyber incidents are increasingly affecting us at work and at home.

In an environment where these issues are so relevant, and have great impact on the way we live and do business, it's important to know where to go for help and advice—even when the prospect of cyber security can feel overwhelming.

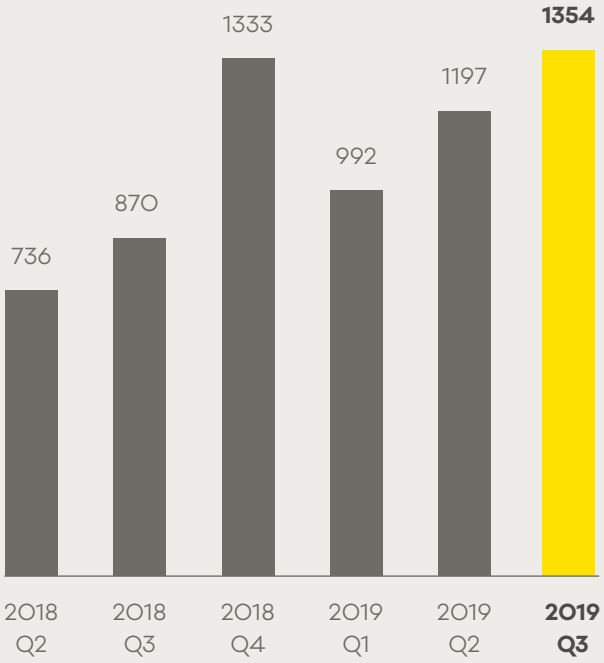
Whether you've been affected by a cyber security incident or want to know how to protect against one, the team at CERT NZ is here to help you make cyber security your business and improve your online resilience.

In this report, we unpack the security issues affecting all New Zealanders and share information to help better understand and protect against them. I know many of you will be able to directly relate to at least one of the issues covered, or know someone who has been affected.

Q3 highlights

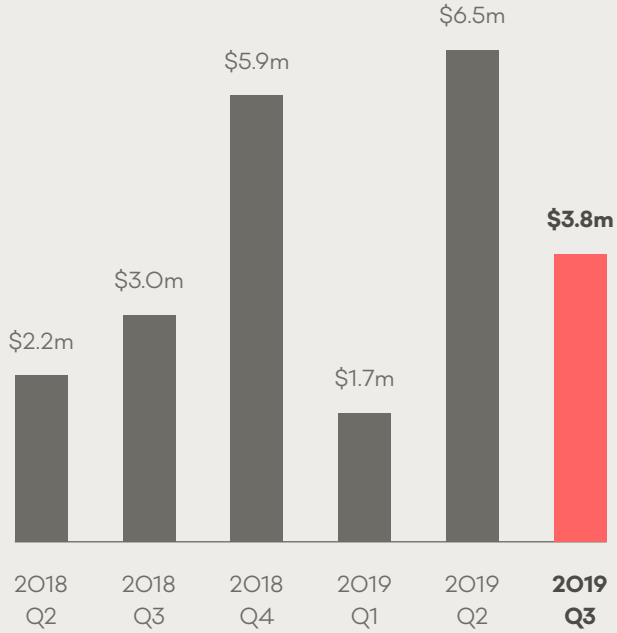
1,354 incidents

were reported in Q3 2019, up 13% from Q2.

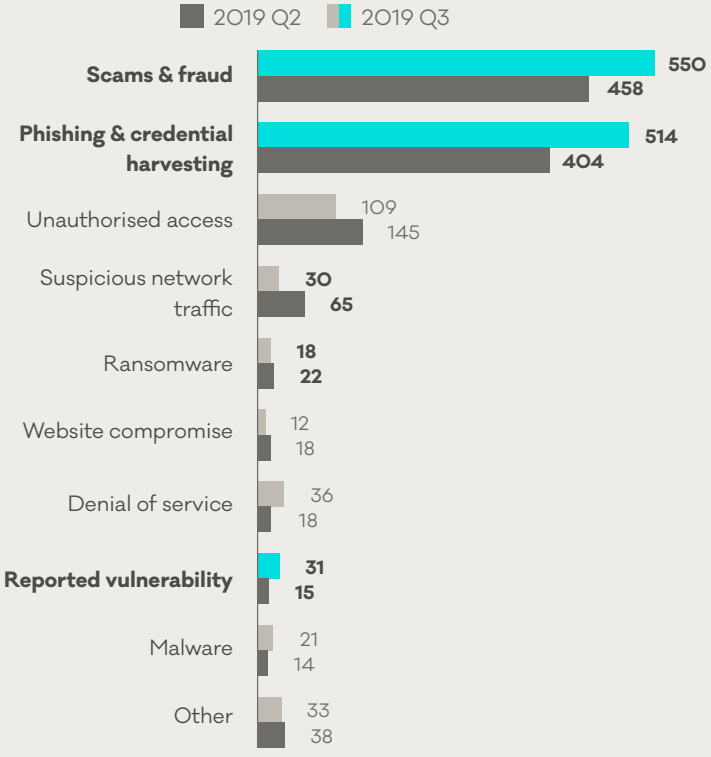


$3.8 million

in direct financial loss reported in Q3, with 18% of all incidents reporting some form of loss.



Breakdown by incident category



20% increase in scam and fraud reports from Q2.

27% increase in phishing and credential harvesting reports from Q2.

107% increase in reported vulnerabilities from Q2.

Know your phish

Phishing is consistently one of the highest incident categories reported to CERT NZ—making up 38% of all reports this quarter.

Since CERT NZ launched in 2017, we've:

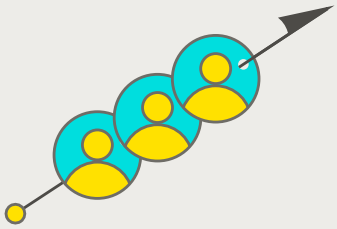
- received more than 3,000 phishing reports
- worked with organisations and individuals to help them recover
- helped take down phishing websites and disrupted campaigns
- investigated the software attackers use to distribute phishing campaigns and used the findings to develop preventions and mitigations to help protect against them.

Phishing may seem harmless, but it has a big impact on New Zealanders, the organisations they work for and businesses they run. It's often a precursor to more serious attacks.

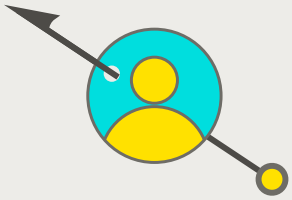
Attackers use a variety of phishing techniques in an attempt to trick recipients into sharing their private information, make financial transactions, or to open malicious attachments or files.

Types of phishing

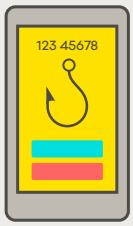
Phishing emails are sent to large email lists to reach as many people as possible. They can be hard to spot as attackers often make them look like they're from a well-known organisation. The emails usually replicate the organisation's branding, use similar language and URLs, and spoof the email address to appear legitimate.



Spear phishing emails are more targeted than generic phishing emails and can be a precursor to business email compromise. Attackers often have specific knowledge about the recipient or their organisation—usually found by researching websites and social media—making them seemingly more legitimate and harder to spot.

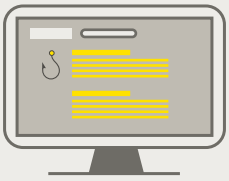


Whaling is similar to spear phishing, but usually targets senior executives within a business to trick them into sharing high-level information and making financial transactions.



Vishing (voice phishing) is phishing attempted via a phone call. The attackers pretend to be from well-known organisations and usually say they are calling to help the recipient with a service like their computer software, finances or tax refund—you might have heard of the 'Microsoft tech support' vishing scams.

Smishing (SMS phishing) is phishing distributed via SMS or text message. These campaigns are low cost and low effort for attackers who send out masses of text messages to blocks of phone numbers. Like generic phishing, they're large scale and less targeted—the SMS or text aims to trick recipients to click on a URL, visit the phishing website and enter their credentials.



Search engine phishing is when attackers use search engine optimisation techniques to 'promote' their phishing websites to the top of search results, where they can be mistaken for legitimate versions of websites. These can be difficult to tell apart from the real websites as they often copy the branding and use similar-looking URLs.

Phishing trends

At CERT NZ we see certain sectors and organisations targeted at different times by different phishing techniques.

The most reported type is generic phishing emails, likely due to the low effort required by attackers to target large numbers of people.

In quarter three, there was an increase in phishing and vishing pretending to be from Inland Revenue and trying to trick recipients into sharing their financial information.

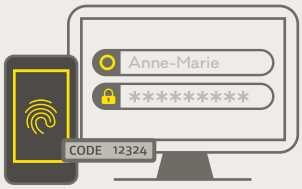
Another campaign on the rise is courier phishing emails. These pretend to be about a pending parcel delivery and request the recipient to click a link to accept.

CERT NZ anticipates seeing an increase in this campaign over the upcoming holiday season due to the higher demand for courier services.

The holiday season is also likely to bring an increase search engine phishing, with scam websites pretending to be well-known retail brands to target online shoppers—one key indicator of these sites is high-value consumer goods offered at a fraction of the price.

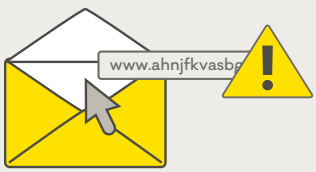
Protecting yourself from phishing

As phishing techniques change over time, it's a good idea to stay up-to-date with simple steps to help spot and protect yourself from them. These include:

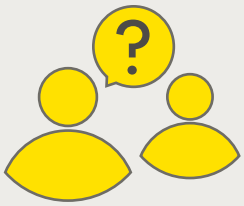


Use **unique passwords** on all your online accounts (and password managers to help remember them)—that way if you lose your account information in a phishing attack, your other accounts won't be impacted and you'll only need to update the password for the compromised account.

Use **multi-factor authentication** (MFA) on accounts where possible. Including this additional login step provides an extra layer of security to help protect your personal and financial information. That way, even if someone got your password, they'd still need to get past this additional security.



Check the links. If you're unsure about an email you've received, hover over the links in the email to check if they'll go to a legitimate website. If the email looks to be from someone you know, check the sender's email address is correct.



Ask someone. If you're unsure about a message you've received, it's a good idea to check it with a colleague, friend or family member. There's no shame in asking for help.

Report it. If you've received a phishing email or you've responded to one, get help quickly by reporting it confidentially to CERT NZ[2]. We'll help you work out the steps you need to secure your accounts, and your report means we can get the message out to help protect others.

See CERT NZ's website for more information about phishing.[2]

1. https://www.cert.govt.nz/report
2. https://www.cert.govt.nz/business/common-threats/phishing-scams-and-your-business/

Insight

Webcam blackmail scam reports steadily increase

In quarter three last year, CERT NZ received a spike in the numbers of reports about an email extortion scam variant.

The email claimed to have accessed the recipient's webcam and recorded them in the privacy of their home. The email demanded that the recipient pay money to prevent the recording being sent to their contact list.

Our latest data shows that, despite the increase in public awareness, the scam continues to affect New Zealanders, with some incidents reporting financial loss.

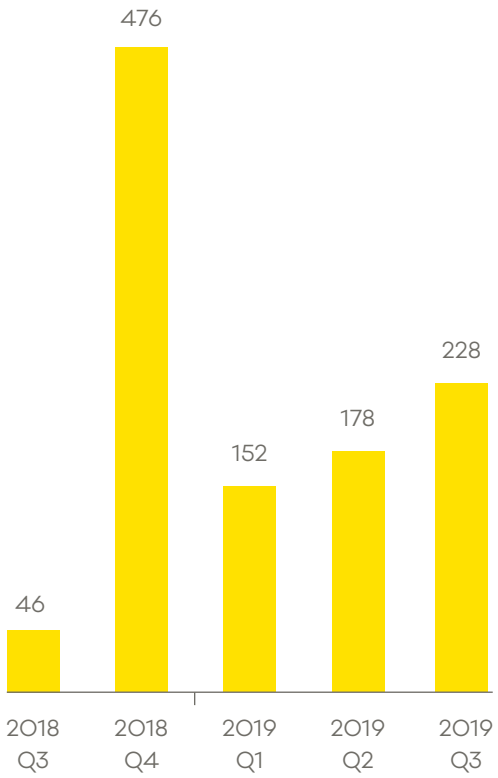
So far this year, we've received 560 webcam blackmail scam reports (Q1 - Q3), compared with 522 for the whole of 2018. This quarter, we received 228 new reports, showing a continued rise in reports through 2019. These figures indicate that this scam is likely to continue into 2020.

When the first surge of webcam blackmail scams hit in October 2018, CERT NZ released an advisory with preventions and mitigations to raise awareness and help New Zealanders protect against the scam.[3]

The advisory includes the following key mitigations:

- do not respond to the email
- do not pay the sender
- report the email confidentially to CERT NZ.

Number of webcam blackmail scam reports



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

3. https://www.cert.govt.nz/individuals/alerts/webcam-and-password-blackmail-scam/

Case study

CERT NZ works with researchers and vendors to resolve vulnerabilities

CERT NZ's coordinated vulnerability disclosure (CVD) process helps researchers and finders communicate vulnerabilities with the affected vendors and have them resolved.

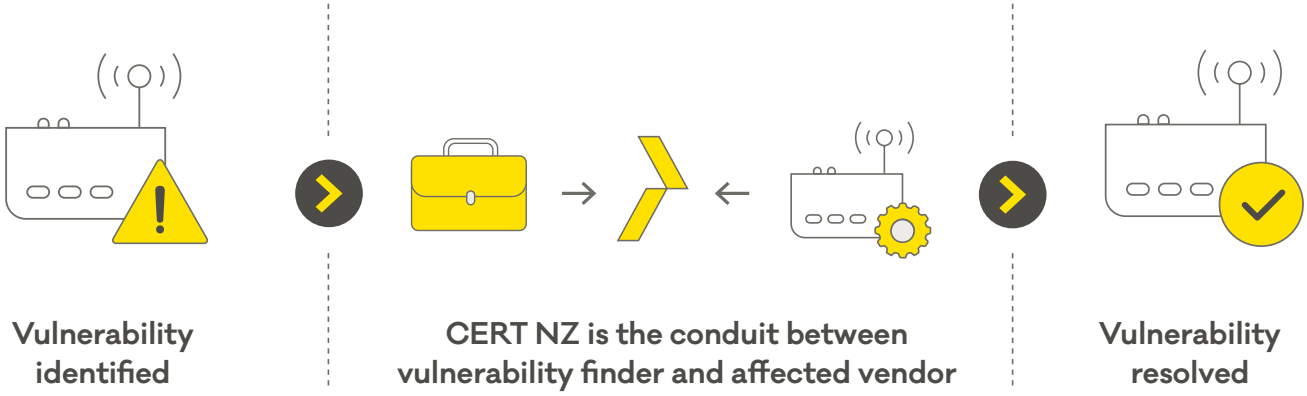
A vulnerability is a weakness in software, hardware, or online services that attackers can exploit. We encourage people who find vulnerabilities to disclose them to the vendor directly. If the finder has difficulty contacting the vendor or would prefer to stay anonymous, they can report them to CERT NZ via our CVD policy and we'll work as a safe, trusted conduit of information.

In quarter three, vulnerability reports more than doubled from the previous quarter, with a number being handled under the CVD process. In a recent case, a finder contacted CERT NZ reporting two vulnerabilities they'd found. The first was with an off-shore company. Because the finder wanted to remain anonymous, CERT NZ contacted the business on their behalf and notified them that a critical flaw in one of their products had been reported.

The business was not aware of the flaw and as a result of the CVD process, the vulnerability was successfully resolved.

The second CVD reported was about a New Zealand-based company, which provides internet-connected devices. The finder had identified a critical flaw in one of their products. CERT NZ worked with the finder to gather information about the vulnerability and sent it to the business. This vulnerability was a high risk for the business and its customers, potentially allowing an attacker to compromise personal networks.

With CERT NZ acting as the information conduit between the parties, the business found a solution and fully resolved the issue.



If you research vulnerabilities, or your organisation receives information about vulnerabilities in your products and systems, and you'd prefer to not deal with the organisation or finder directly, you can report them confidentially to CERT NZ[4] . We'll help address them, which in turn helps keeps online systems more secure for all New Zealanders.

CERT NZ's website has articles to help you deal with vulnerabilities:

- How to report a vulnerability to a business (https://www.cert.govt.nz/it-specialists/guides/how-to-report-a-vulnerability/)
- What to do if your business receives a vulnerability (https://www.cert.govt.nz/business/guides/responding-to-incidents/getting-a-vulnerability-report/)
- CERT NZ's coordinated vulnerability disclosure policy (https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/cert-nz-coordinated-vulnerability-disclosure-policy/)

4. https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/cert-nz-coordinated-vulnerability-disclosure-policy/

Insight

Over 65s' online resilience improving

This year, CERT NZ's data has shown a positive trend for the over 65 age group. Since Q1, there has been a 60% decrease in direct financial losses reported, while at the same time, a 20% increase in the number of reports about this age group.

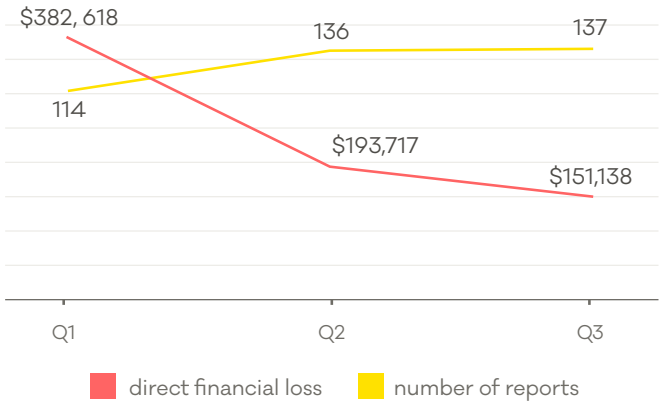
This positive trend indicates that although cyber attacks are on the rise, the over 65 age group are taking the simple security steps to help build their online resilience and increase their ability to protect themselves and their finances from scams and attacks.

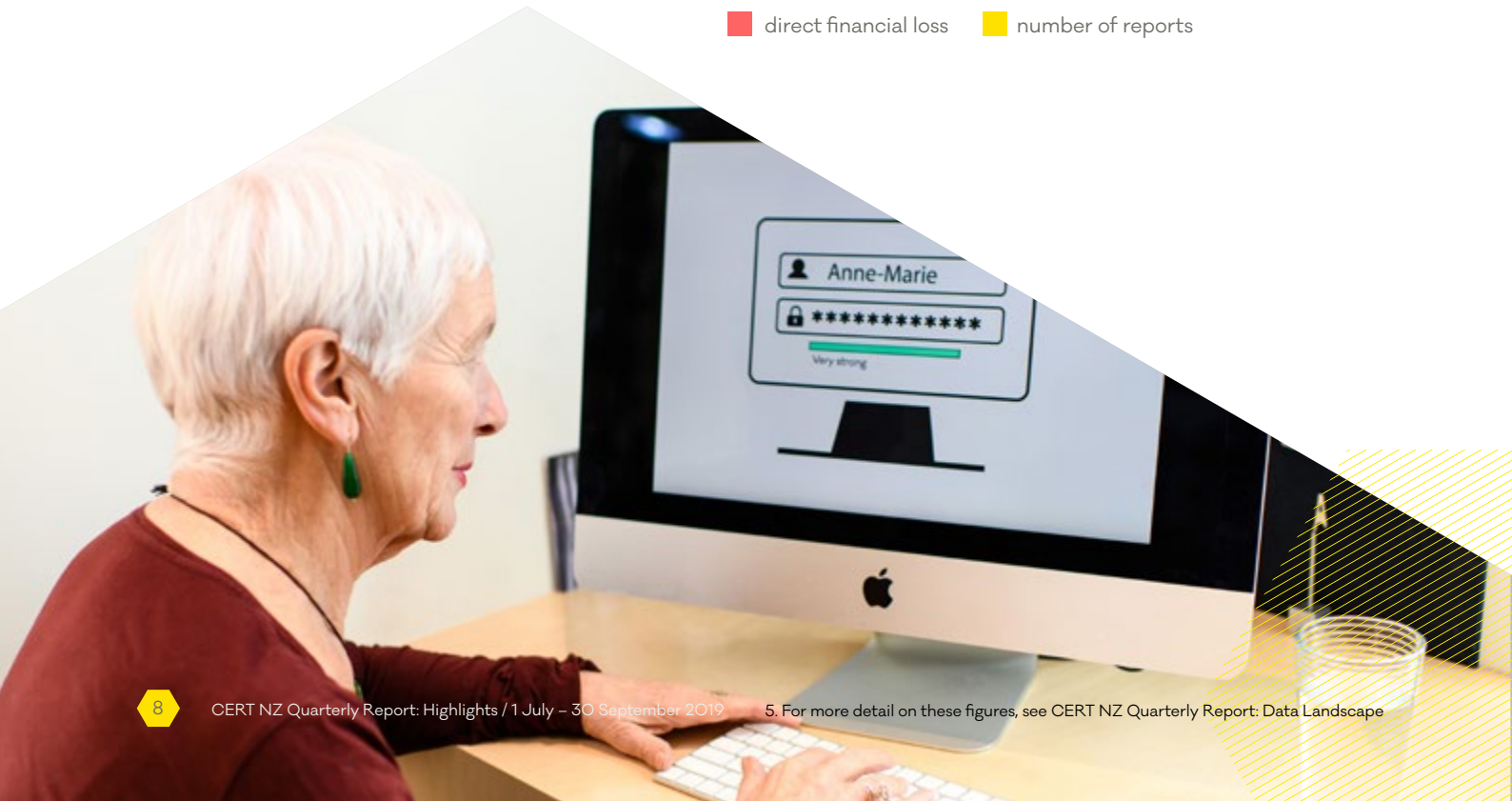
CERT NZ's targeted awareness programmes like Get Password Smart and our partnerships with national organisations including SeniorNet have been one of the ways we've worked with this age group to actively engage them in easy ways to keep secure online.

Although this is good news for the over 65s, our data shows that cyber attacks continue to make a big financial impact on every day New Zealanders. Losses reported by the 45 - 55 age group have climbed this year from $271,279 (Q1) to $1,112,012 (Q3), an increase of more than 300%. We've also seen increases of more than 79% in direct financial loss from the under 18 and 18 - 24 age groups—with scams and fraud remaining the largest category for both incidents and direct financial loss reported.[5]

Gathering data on age furthers our understanding of how cyber security incidents are impacting New Zealanders. It helps inform the focus of our upcoming campaigns and outreach programmes as we continue to engage all New Zealanders with simple security measures to help boost their online resilience.

Over 65s' financial loss and number of reports (Q1 - Q3 2019)





5. For more detail on these figures, see CERT NZ Quarterly Report: Data Landscape