certnz

Q1

JANUARY_TO_MARCH_2024

CYBER SECURITY INSIGHTS

Battling breaches

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q1 CYBER SECURITY INSIGHTS

Director's message

Sue Critchlow, Acting Director

We saw a significant decrease in the number of incidents reported to us in the first quarter of 2024. The biggest drop was in reports about Phishing and Credential Harvesting, which remains our most common category.

A drop in incidents sounds like encouraging news, but we know cybercrime is significantly underreported.

Reporting common incidents such as phishing might seem like a waste of time because even when you forward phishing messages to concerned authorities, new ones keep popping up in your inbox. But every incident you report helps us in understanding the threats New Zealanders face online and in mitigating these threats. In this issue, we explain how reporting helps protect you and those around you from future threats.

You will see in this report financial loss increased by 84% from the last quarter, with more New Zealanders reporting they lost money online. The number of reported scams while buying and selling online has also gone up. People caught up in these scams experience significant emotional harm along with financial loss.

But it's not all doom and gloom. A recent survey report released by CERT NZ showed New Zealanders are becoming increasingly aware of cyber security threats and are taking action to protect themselves online.

In other news, we are sad to farewell Rob Pope, after he resigned from his role as CERT NZ Director. We are immensely grateful to Rob for all his work since the establishment of CERT NZ in 2017 and wish him the very best for his future.

Meanwhile, significant progress has been made in integrating CERT NZ and the National Cyber Security Centre (NCSC). The objective of the integration is to have a single, lead cyber agency that will look after the online security of all of Aotearoa, from individuals and small businesses to the country's largest institutions.

As we step up our efforts against online attacks, we need your reports to help us stay ahead of online attackers who will adapt and improvise. Together, we can make a more cyber-resilient Aotearoa.

AT A GLANCE...

Average incidents reported per quarter

1,915*

Average loss reported per quarter

$5.1m

Losses reported to CERT NZ

$41.1m

Figures based on previous eight quarters

*This number was revised in August 2024 following an internal data review process.

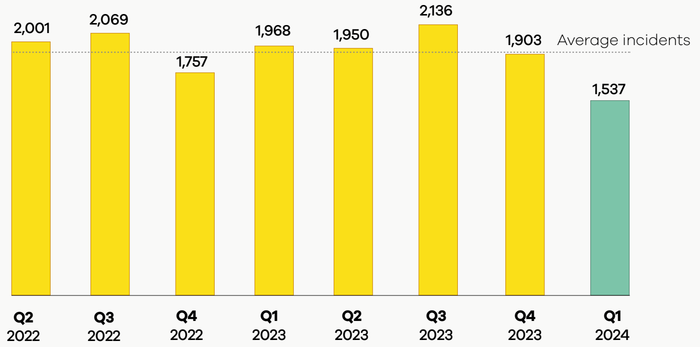
INCIDENTS RESPONDED TO BY CERT NZ

1,537*

incidents were responded to by CERT NZ in Q1 2024

▼19%

decrease from Q4 2023



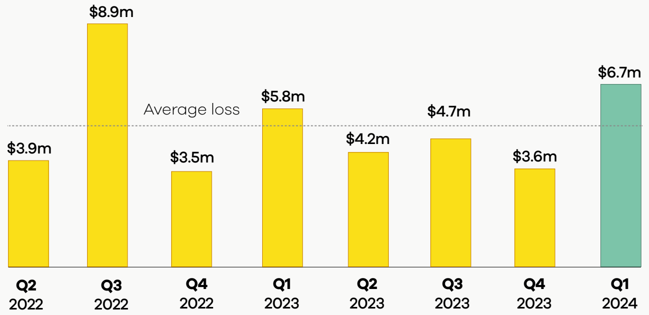
DIRECT FINANCIAL LOSS

$6.6m

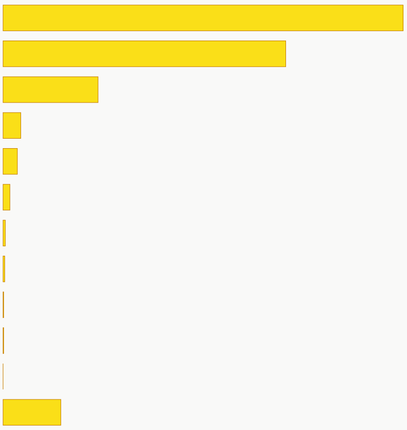
in direct financial loss was reported in Q1 2024

▲84%

increase from Q4 2023, with 27% of incidents reporting financial loss



BREAKDOWN BY INCIDENT CATEGORY



			From previous quarter
Phishing and credential harvesting	699	▼	36%
Scams and fraud	494*	▲	1%
Unauthorised access	166	▲	1%
Malware	31	●	
Website compromise	25	▲	32%
Ransomware	12	▲	50%
Denial of Service	4	▲	300%
Suspicious network traffic	3	▲	50%
C and C server hosting	1	●	
Botnet traffic	1	●	
Attack on a system	0	▼	-100%
Other	101	▲	9%

*This number was revised in August 2024 following an internal data review process.

For more on the New Zealand threat landscape in Q1 2024, see the CERT NZ Quarterly Report: Data Landscape.

Battling breaches

Data breaches are a significant concern for organisations of all sizes and their clients and customers.

A data breach occurs when an unauthorised person gets access to information they shouldn't have. This can include anything from names and email addresses to credit card details, passwords and intellectual property.

A data breach can affect your organisation in many ways.

- **Financial:** your organisation could incur costs such as legal fees, penalties and the cost of remediation.
- **Reputational:** a data breach can erode customer trust and affect brand credibility.
- **Legal:** if you are a business owner, you are obligated by the Privacy Act 2020 to protect peoples' personal data and to report breaches promptly.
- **Personal:** stolen personal data can lead to identity theft, financial fraud and other malicious acts.
- **More phishing:** people whose information has been leaked may become the target of more phishing attacks.

How it happens

Data breaches can happen because of an intentional attack or unintended error.

- Cybercriminals can exploit vulnerabilities in systems or networks to access your data.
- Someone in your organisation may be targeted in a phishing attack and tricked into revealing important information, such as their login details.
- Insider threats can be a source of a data breach. Anyone with authorised access could misuse their privilege or intentionally leak information.
- Data can also be leaked through human error, such as in an email to the wrong person, or through misplaced or stolen devices containing sensitive information.

DRUM UP YOUR DEFENCES

Good security practice is your best defence against potential attacks. Add layers of protection around the data you store to protect it from those who try their best to get their hands on it.

Only collect essential data from your customers. The more you collect, the more valuable it is to an attacker and the bigger the impact if it's made public.

If you're collecting data, make sure you're encrypting it to prevent unauthorised access. This includes while it's:

- in transit – for example, collecting data from your customers through a web form, and
- at rest – when it's stored in a database.

Make sure that two-factor authentication (2FA) is required to access any data you keep, to add an extra layer of security.

Make sure your software applications and systems are up to date by installing the latest updates from the vendor.

Train employees on best practices, including recognising phishing attempts and handling data securely.

Limit access to sensitive information by making sure your employees only have access to what they need to do their job.

Regularly back up data to secure locations. While this won't help prevent attacks, it can minimise the impact of data loss.

CASE STUDY: JAMES AND THE GIANT BREACH

James* is the IT manager of a shoe and clothing store chain called Centipod*, which has forty employees across eight stores in New Zealand. He is alerted to a post on an online forum threatening to sell his company data, with the attacker claiming that 10,000 records are available. James realises that someone has gained unauthorised access to the database of the store's customers.

His next actions will be crucial in deciding how the company meets this challenge. James has had previous experience of a data breach and he takes the following steps.

Containment

James identifies which system has been affected and isolates it by taking it offline. He changes the password on the administrator account and instructs all employees to do the same on theirs to prevent further unauthorised access.

Assessment

He assesses the extent of the breach and determines that information of around 10,000 customers has been compromised, validating the hacker's claim. The attacker couldn't get credit card details, but they may have obtained customers' email addresses, phone numbers and past invoices.

Notification

James notifies the office of the Privacy Commissioner within 72 hours, as stipulated in the Commissioner's Privacy Breach Guidelines. He also reports the incident to CERT NZ, which advises him on next steps and how to inform his employees and customers of the breach.[1]

Investigation

James starts to investigate how this breach happened. He discovers that a phishing email had been sent to a shared inbox claiming to come from their accounting firm. An employee had clicked on the link, which took them to a page that collected their login credentials. James decides to schedule a security training workshop for all employees.

Communication

Over the next few days, Centipod employees respond to queries from customers and stakeholders, telling them how they have been affected and what they can do. Centipod also co-ordinates with CERT NZ to put up messages across its social media platforms and prepares an incident response plan to be more prepared for future incidents.

*This case study uses fictitious names to illustrate typical incidents of data breach reported to us.

[1] https://www.cert.govt.nz/about/resources/#commsframework

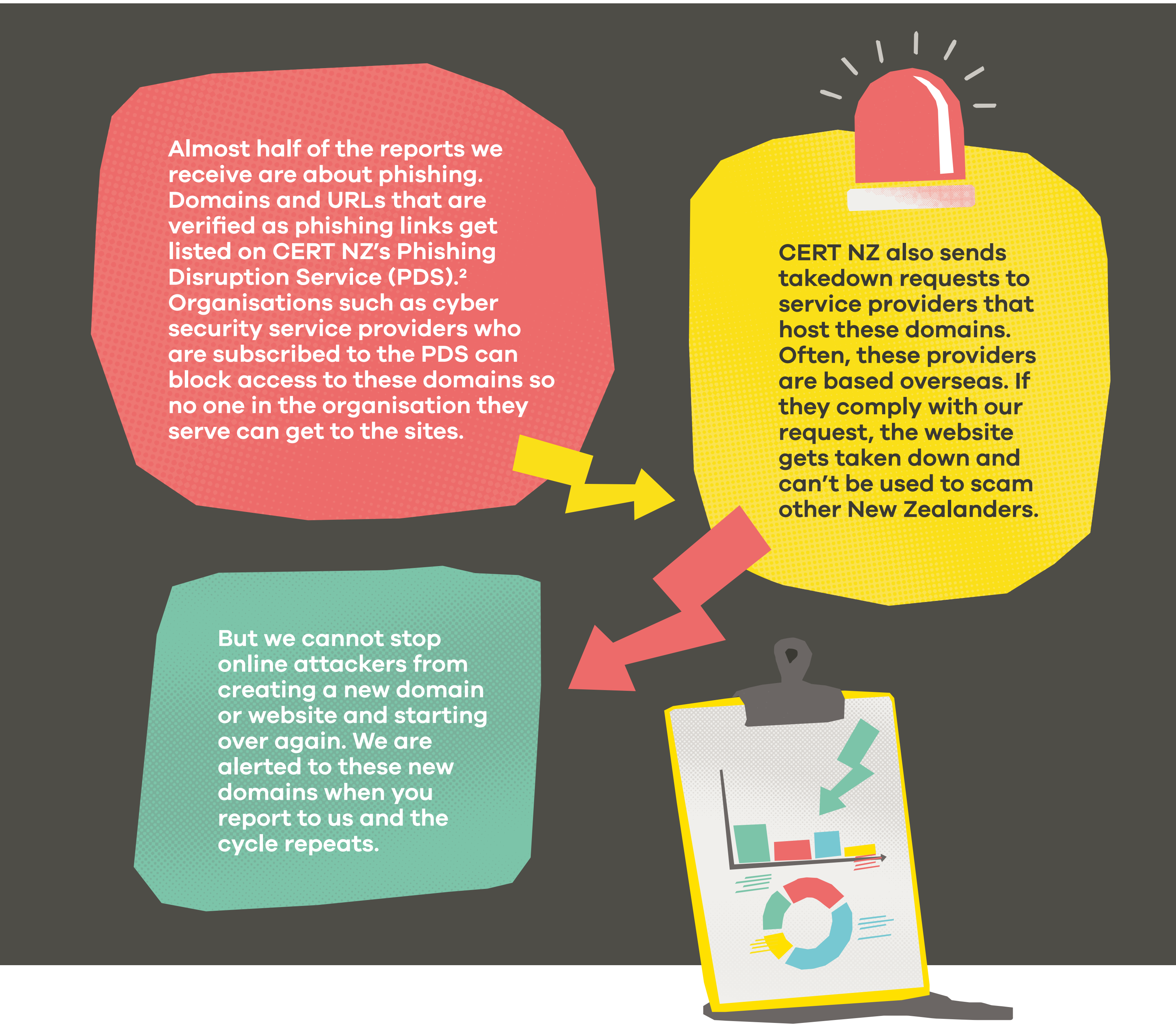
A report on reports

Nearly all of CERT NZ's information comes from the general public – people like you.

When businesses and individuals report online incidents to us, we know what scam and malware campaigns are affecting New Zealand. In this way, every report not only helps you but all Kiwi.

You can report any cyber incident confidentially. If you're locked out of your accounts, suspect you have been targeted in a scam, or if your organisation suffers a data breach, you can report it to us using the reporting tool on CERT NZ's website.

WHAT'S HAPPENING BEHIND THE SCENES?



Almost half of the reports we receive are about phishing. Domains and URLs that are verified as phishing links get listed on CERT NZ's Phishing Disruption Service (PDS).[2] Organisations such as cyber security service providers who are subscribed to the PDS can block access to these domains so no one in the organisation they serve can get to the sites.

CERT NZ also sends takedown requests to service providers that host these domains. Often, these providers are based overseas. If they comply with our request, the website gets taken down and can't be used to scam other New Zealanders.

But we cannot stop online attackers from creating a new domain or website and starting over again. We are alerted to these new domains when you report to us and the cycle repeats.

HANDLING REPORTS

CERT NZ works with partner agencies, like the New Zealand Police, the Department of Internal Affairs, banks and telecommunication companies. If you need more help, and consent to it, we can forward your report to these agencies.

You don't have to experience an incident online to talk to us. If you think you or someone you know is being targeted in a scam, CERT NZ can provide technical advice.

[2] https://www.cert.govt.nz/about/phishing-disruption-service/

A case for passkeys

You might have heard some of the most popular phone apps are switching to or enabling passkeys to make logging in easier and more secure.

Passkeys are a way of logging in without passwords. They use something you have (like a USB key or your phone), or recognise who you are with your face scan, voice or fingerprint, to let you into your account. You may already have apps on your phone, such as your digital wallet, that use this form of authentication.

WHAT HAPPENED TO PASSWORDS?

Passwords are the most popular tool for authentication. But scammers are always trying to get their hands on them, and their jobs are made easier when people don't have strong passwords or use the same password for multiple accounts.

That's where passkeys have an advantage. Passkeys are device-specific, and your data is not saved on a website server. So even if the website suffers a data breach, scammers can't steal your credentials.

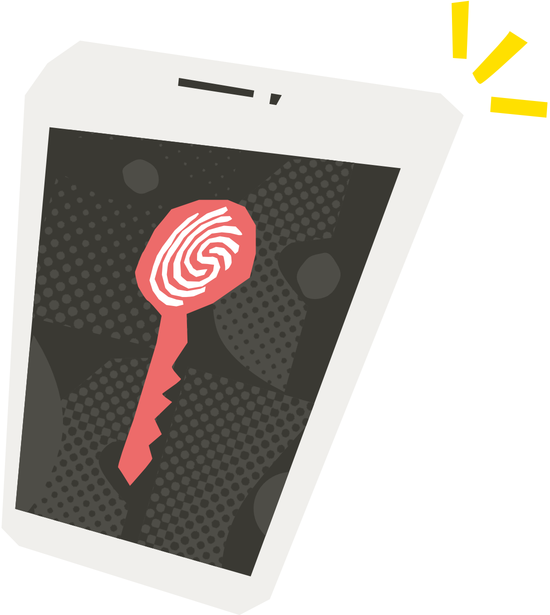
ARE PASSWORDS HISTORY?

Not quite. Passwords are handy and if done right, they can be a strong line of defence. If you use long and unique passwords, attackers can't brute force their way into your account. CERT NZ strongly advises enabling two-factor or multi-factor authentication on your most important accounts such as banking, email and social media, to make them more secure.[3]

Most sites and apps that let you use a passkey also require you to have a backup password that helps you recover your account.

Not all devices can perform face or fingerprint scans, or take external keys, so passwords remain the most common method of verifying user identity.

CERT NZ has a guide on creating good passwords and protecting your online accounts.[4]

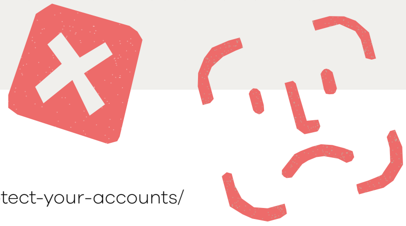


The upside:

- Using passkeys can make logging in faster.
- You don't have to create, or remember, complex passwords.
- Passkeys are phishing-resistant; scammers cannot remotely log in to your account with a password because there is none.

The downside:

- If you lost access to all your devices at once, it can be difficult to enter your own account.
- Biometric logins don't always work and may need you to use your password. For example, when trying to use a fingerprint scan with greasy or wet fingers, or a face scan in the dark.
- Devices that read fingerprints or that can recognise face scans can be more expensive. If you use an external key or a second device for authentication that is an additional cost as well.



[3] https://www.ownyouronline.govt.nz/personal/get-protected/guides/use-two-factor-authentication-to-protect-your-accounts/

[4] https://www.ownyouronline.govt.nz/personal/get-protected/guides/how-to-create-good-passwords/

CERT NZ updates

A lead cyber security agency

The process to integrate CERT NZ and the NCSC is now well under way, with kaimahi expecting to share a location by the end of this year. CERT NZ provides advice and support to everyday New Zealanders along with small-to-medium organisations, while the NCSC helps nationally significant organisations such as government agencies and critical infrastructure. Bringing the agencies together to form a lead national cyber security agency will result in improved collaboration and a single source of cyber security information and support from government.

Dates announced for Cyber Smart Week 2024

Cyber Smart Week 2024 will run from 21 to 27 October. Last year, we had a record 1,214 organisations sign up to become supporters, and we want even more this year. You can sign up to become a supporter and to receive advice and guidance on staying cyber smart all year round on our website.

Pacific partnership

CERT NZ's Pacific Partnership Programme, funded through the New Zealand Aid Programme, works with our Pacific partners to build local and regional cyber security capacity.

In February, the team met with the Solomon Islands Government and community organisations to discuss grassroot projects, technical support and network strengthening.

In March, the team met with counterparts in Tuvalu, to discuss steps towards building a cyber-secure digital nation, and in Fiji where Aotearoa New Zealand will be a partner in establishing a local establishing a local CERT, and building capacity and capability.

International insights

In this section, we cover news from our international partners.

The UK's National Cyber Security Centre (NCSC) has released a guide for CEOs in public and private sector organisations to manage a cyber security incident.[5]

NCSC UK has also released an assessment focusing on how artificial intelligence will affect the efficacy of cyber operations and the implications for the cyber threat over the next two years.[6]

Australia's National Office of Cyber Security has released the findings of its Lessons Learned Review into the co-ordination of the response to the HWL Ebsworth cyber incident. The incident was a breach of around four terabytes of data affecting HWL Ebsworth, a major law firm in Australia, along with a large number of federal and state government entities, as well as private sector organisations.[7]

[5] https://www.ncsc.gov.uk/guidance/ceos-responding-cyber-incidents

[6] https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#section_

[7] https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/nocs-hwl-ebsworth-lessons-learned-report.pdf