

APRIL TO JUNE 2024

Q2

# CYBER SECURITY INSIGHTS



## Spoof and Spam

### IN THIS ISSUE

Focus: Spoof and spam P4

Insight: Beyond SMS P7

Insight: Progressive web apps P9

# Q2

# QUARTERLY SUMMARY

**New Zealanders reported to CERT NZ \$6.8m in financial loss due to cyber crime between 1 April and 30 June this year (Q2). This is a slight increase on the \$6.6m in the last quarter and a 61% increase on the \$4.2m reported to us in the same quarter last year.**

This is despite the number of recorded incidents continuing to drop over the last nine months. Just 1,203 incidents were reported this quarter, compared with 1,537 last quarter (Q1 2024). The numbers are also much lower than for the same period last year (1,950 in Q2 2023).

Unauthorised access accounted for more than half of all financial loss reported (\$3.6m). This highlights just how damaging incidents of unauthorised

access can be. It also underlines the need to have two-factor authentication (2FA) on all your online accounts. Along with passkeys, 2FA is the best protection against this type of incident.

In this quarterly report, we look at evolving methods cyber criminals are using to target people for their money, data and personal information. This includes spoofing and phishing tactics that take advantage of new technologies, such as rich communication services and progressive web apps.

We strongly encourage people and organisations to report incidents of any type, no matter how big or small. Your reports help us act against the threats New Zealanders face online and help others avoid being caught out.

## Combining forces

CERT NZ recently integrated with the National Cyber Security Centre (NCSC) to form the New Zealand Government's lead operational cyber security agency. The combined agency is located within the Government Communications Security Bureau (GCSB).

The NCSC now provides cyber security services to all New Zealanders, from individuals and small

businesses to government agencies and nationally significant organisations. We assess the cyber threat landscape and respond to cyber security incidents, disrupt cyber security attacks and work to improve New Zealand's resilience to online threats. The NCSC's vision is a New Zealand where good cyber security happens everywhere, all the time, by everyone.

## INCIDENTS REPORTED VIA THE CERT NZ REPORTING TOOL

# 1,203

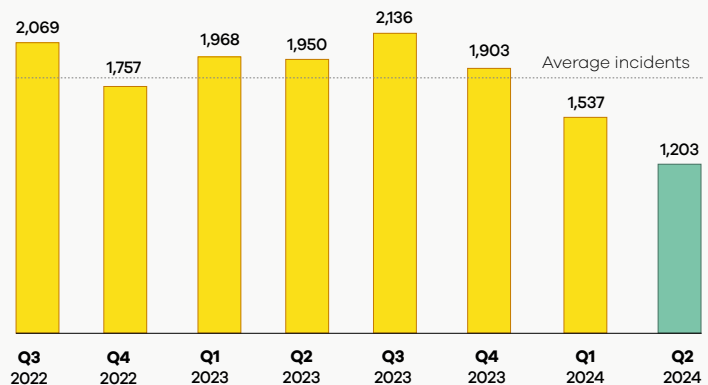
incidents were responded to by CERT NZ in Q2 2024

# ▼ 22%

decrease from Q1 2024

# 1,815

average incidents reported per quarter (based on previous eight quarters)



## DIRECT FINANCIAL LOSS

**\$6.8m**

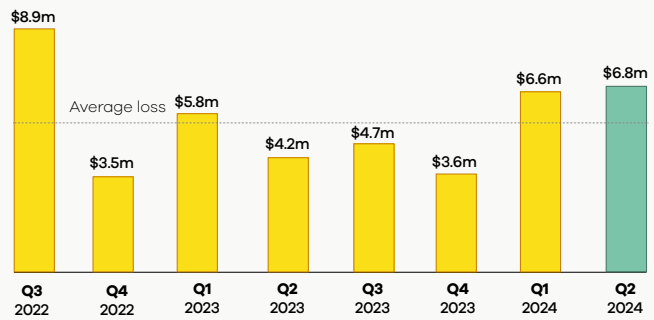
in direct financial losses were reported

**▲ 3%**

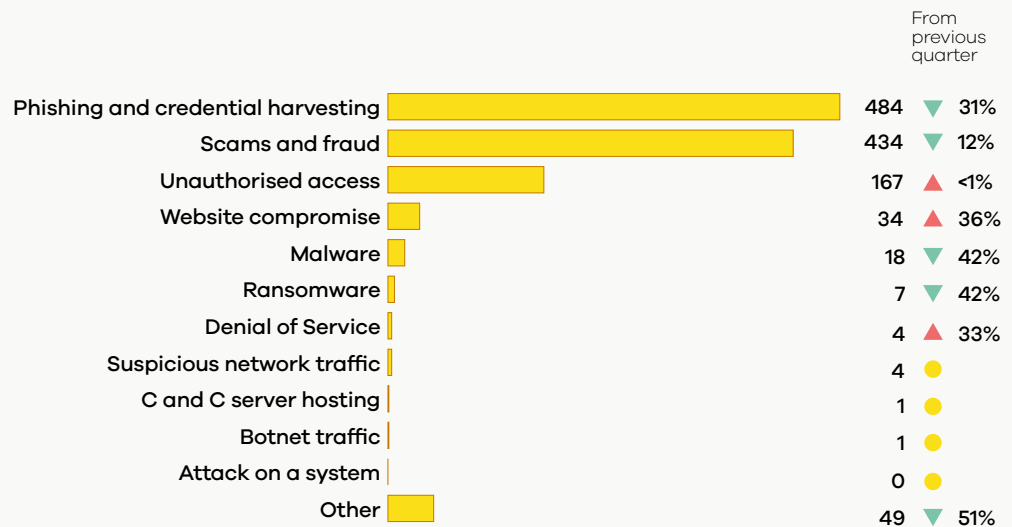
increase from Q1 2024, with 28% of incidents reporting financial loss

**\$5.5m**

average loss reported per quarter  
(based on previous eight quarters)



## BREAKDOWN BY INCIDENT CATEGORY



## INCIDENTS OF POTENTIAL NATIONAL SIGNIFICANCE

The NCSC responds to incidents affecting nationally significant organisations or with potential to cause national harm. We triage these into a scale that considers the organisational impact and the severity of the incident.

In Q2, there were 121 incidents with potential national significance.



*Note: As an integrated NCSC, one of our key priorities is determining the best ways to receive, categorise, and report on incidents. As such the way we report our numbers may change in the upcoming quarterly reports.*

There were no incidents that were categorised as Highly Significant (C2) or National Emergency (C1).



# Spoof and Spam

**Email spoofing is the practice of making an email look like it came from someone else.**

For example, if you own a business, an online attacker could impersonate your web address and send out emails that look like they came from you. If your personal account is spoofed, an attacker may send emails to people you know, pretending to be you.

## TYPES OF SPOOFING

---



### Sender name is a trusted source

When you receive an email that is spoofed, the sender's name may show up as someone you know but the email address does not match that of the sender. The from field could look something like this:  
**Sam Smith <rl20776v@example.com>**



### 'From' field is a close match

At other times, the email address in the 'from' field looks similar to that of the business they are impersonating. So, you might get an email from sender@example.org when the actual email address is sender@example.com. This is called domain impersonation and scammers frequently do this when sending out phishing links.



### 'From' field is an exact match

This type of spoofed email is the hardest to identify because it appears to come from the same email address as that of the sender it is impersonating. Online attackers can do this when the sender's email provider does not have the right controls in place to stop spoofing. You can spot this in some cases because the email address you are replying to changes when you respond to the message.

## WHY DO ATTACKERS SPOOF EMAILS?

Scammers send out emails pretending to be someone you know and trust so they can get your personal information, your passwords and, eventually, your money.

Some online scammers spoof your email address to extort money from you. When this happens, you will see a message in your inbox that appears to have come from your own email. The sender claims they have hacked into your account and recorded your internet activity. They threaten to make your videos or internet search history public if you don't pay them. While it can be easy to believe an email like this, it is usually a bluff. You can read more about extortion scams on Own Your Online.<sup>1</sup>

In a less common scenario, scammers can spoof your email and target you with spam or phishing emails. Because these messages have come from your own email address, you will not be able to block them.

**Spoofing is different from business email compromise.**

**When your email address is spoofed, the attacker has made it appear like the email came from you but does not actually have access to your account.**

**A business email compromise happens when an online attacker succeeds in getting access to your organisation's email. They can then target your contacts to try to get money or personal details.<sup>2</sup>**

<sup>1</sup> <https://www.ownyouronline.govt.nz/personal/know-the-risks/common-risks-and-threats/extortion-scams/>

<sup>2</sup> <https://www.ownyouronline.govt.nz/business/know-the-risks/common-risks-and-threats-for-business/business-email-compromise/>

## SPOT A SPOOFED EMAIL

If you get an email from a friend, an agency or a company you know that is asking you to make a payment or to click on a link, your first instinct is to check the email address. But if the address has been spoofed, it can be easy to mistake it for a genuine message. Before you click on a link or send money to anyone – even someone you know – watch out for these common red flags.



**Were you expecting a message from this person or organisation? If it has appeared unexpectedly, it may be a scam.**



**If the email has an embedded link that it's asking you to click, it may be a phishing email. Mark the link as spam and do not click on it.**



**If you are unsure, contact the sender by another means, such as a telephone call, to confirm if they sent you the invoice or email.**



## STOP YOUR EMAIL FROM BEING SPOOFED

If your organisation's email is being spoofed to send emails to your customers, you need to make sure your SPF, DKIM and DMARC protections are configured correctly (see box opposite).<sup>3</sup>

Talk to your IT provider, if you need help with this.

If your personal email is being spoofed, you can report it to your email provider. If you receive extortion messages from your own email address, do not pay the ransom amount. You can report the incident to us using the online reporting form.<sup>4</sup>

### SPF (Sender Policy Framework)

allows you to tell others what servers are approved to send emails using your organisation's domain name.

### DKIM (Domain Keys Identified Mail)

allows your mail server to sign emails you send with a special key that is used to check that you created the email and others haven't modified it.

### DMARC (Domain-based Message Authentication, Reporting and Conformance)

allows you to tell others what you want to happen if they receive an email claiming to be from you but it doesn't pass SPF or DKIM checks.

<sup>3</sup> <https://www.ownyouronline.govt.nz/business/get-protected/guides/preventing-your-email-from-being-spoofed/>

<sup>4</sup> <https://www.cert.govt.nz/individuals/report-an-issue/>



# Beyond SMS

**The technology behind text messaging is constantly changing and the bad guys are keeping up.**

Scammers sending out phishing texts are harnessing the new features of modern messaging platforms like Rich Communication Services (RCS) and iMessage.

RCS is a feature that uses your phone's messaging app to send messages that are visually more interesting and interactive. The technology is available on most smartphones on the market today and can be used to send messages over most mobile phone networks.

RCS lets you send emojis and GIFs, react to messages, see when the other person is typing or has seen your messages, and share media and location. It also allows group texting. In short, you can do everything you can on a messaging app like WhatsApp without installing any third-party application.



**iMessage, Apple's native messaging app, also lets you send interactive messages over Wi-Fi networks to other Apple devices. It allows users to send a message that displays an email ID in the sender field instead of a phone number. Messages between Apple and other devices are sent as traditional SMS texts but with Apple expected to incorporate RCS soon, you will be able to send interactive messages and share files on all phones.**

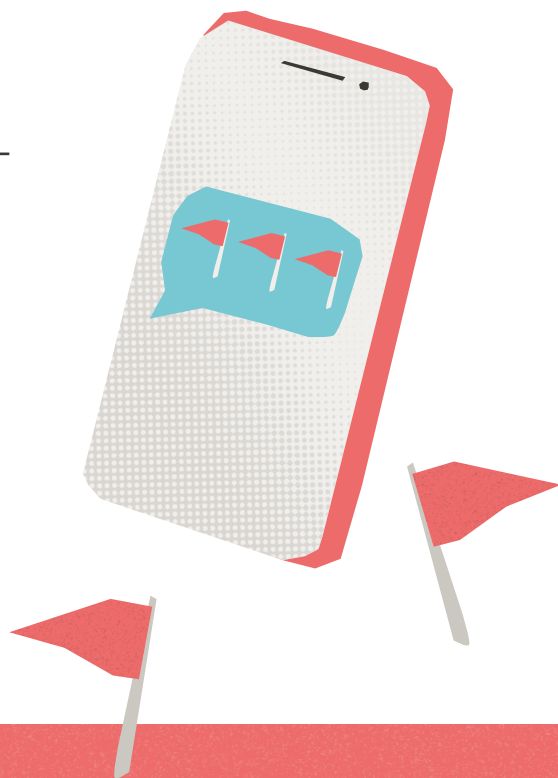
## WHAT'S NOT TO LIKE?

---

While RCS makes the average user's texting experience richer, scammers can use these platforms to embed brand logos, attach forms and documents, buttons and link previews. The texts can look convincing and increase the risk of impulsive actions.

RCS messages can be sent over the internet even when there's no cellular network. A scammer can send hundreds or thousands of texts and it won't cost them a cent. No additional charges are incurred for sending international messages or for roaming.






According to the Department of Internal Affairs (DIA),<sup>5</sup> RCS and iMessages are not visible over the mobile network. This means New Zealand telecommunication providers cannot monitor them in the same way as with SMS messages. This causes issues when it comes to combating RCS and iMessage phishing attacks.

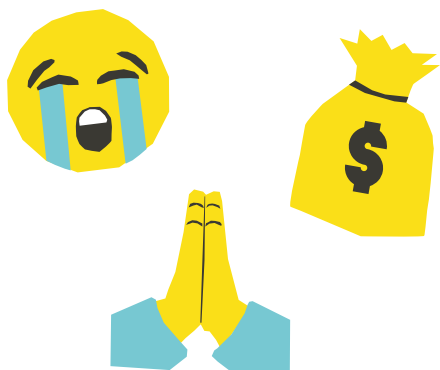


## SPOT A PHISHING TEXT

---

No matter the technology used, the intent of phishing texts messages remains the same: to steal your information and money. RCS texts reported to CERT NZ include texts about missed parcels, pending road tolls and texts with fake invoices. You can identify a phishing text from these telltale signs.

-  You receive a message unexpectedly.
-  The message is from an international number or an email address.
-  The sender creates a sense of urgency.
-  The sender asks you to click on a link or to download an attachment.
-  The sender asks you for personal information.



## ADVICE FROM THE DIA

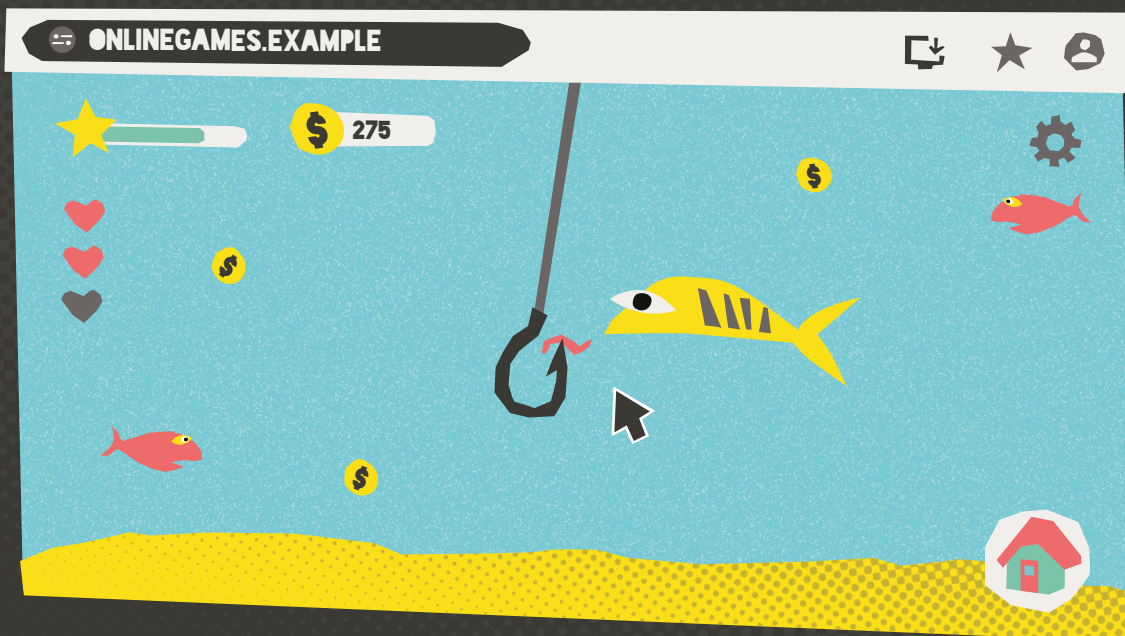
---

If you receive a scam message via RCS or iMessage, take the same action you would with an SMS message.

- **Ignore the message and don't click any links.**
- **Forward the message for free to DIA's 7726 spam reporting service and follow all the prompts.**
- **If the message came to your text message inbox from an email address you can still report this to 7726. When asked for the sender's phone number, enter the email address instead.**

<sup>5</sup> <https://www.dia.govt.nz/Spam-NZ-Spam-Law>





# Phishing with Progressive Web Apps

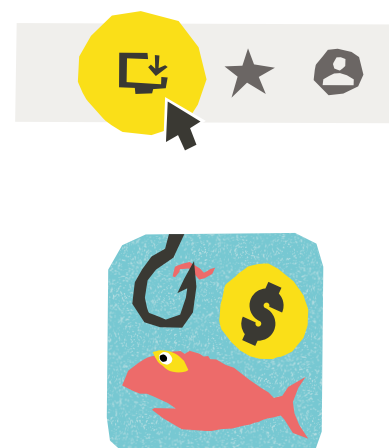
**Attackers are always looking for new opportunities or technologies they can take advantage of. This is the case with incidents involving Progressive Web Apps (PWAs). Globally, we are seeing PWAs increasingly being used as part of phishing toolkits to steal user information.**

## What are Progressive Web Apps?

PWAs are like regular apps but run in a browser. You can download and install them from the address bar of most websites you visit. Once installed, an icon is added to the home screen, but rather than launching a separate app, it will open in the browser with the standard controls hidden.

PWAs are often light and load faster than the full website. It takes fewer clicks to open the app from your screen or taskbar than it does to open a browser window and type in the address. They are also common. Blogging sites, dating apps, maps and ride-sharing apps, news portals, e-commerce sites, music apps and games use them to allow for easy browsing and enhance the user experience. Some apps allow push notifications and can work offline. PWAs of file-sharing websites can also sync files on your device and server while working in the background.

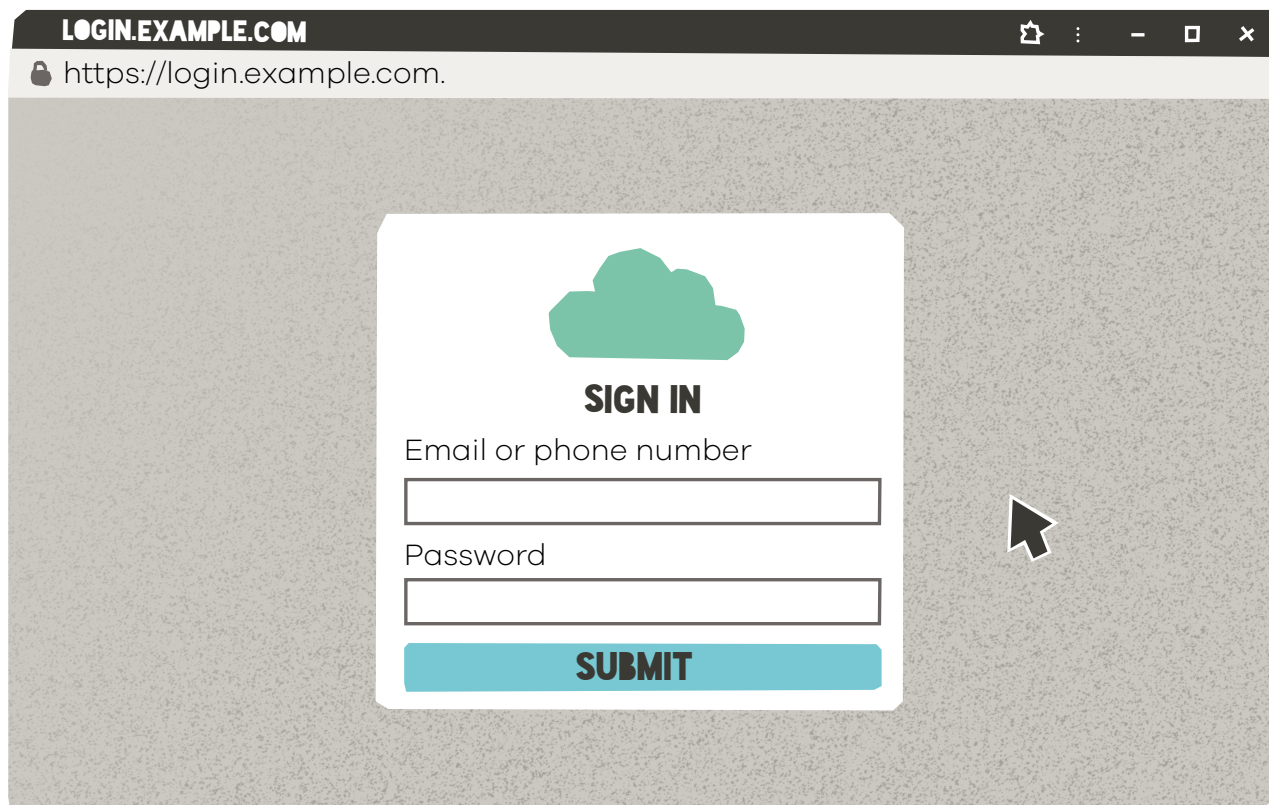
While PWAs have advantages for the user and developer, they are also a handy tool for phishing scammers.





## MALICIOUS PROGRESSIVE WEB APPS

Attackers can use the PWA mechanism to issue prompt screens, asking people to log into an account. Because the web browser's standard controls may be invisible, and the address bar may be fake, it can be hard for the user to tell if this prompt is legitimate.



If you try to log in at this point, it won't take you anywhere and the credentials you entered will be captured by the phishing kit. The attacker could then use them to log into your real account and even try your password on other websites you use.

### Watch out for malicious Progressive Web Apps

- To avoid falling for malicious PWAs, only download software from websites you trust and frequently visit.
- Just like regular apps, PWAs may request permissions, and some of them may seem unreasonable. For example, if a PWA wants access to your microphone or your photo gallery, for example, you can always choose not to proceed.



# Phishing Disruption Service

The NCSC's Phishing Disruption Service (PDS) is free and provides a verified list of New Zealand-specific phishing indicators that organisations can act on and block from their network.

When you get a phishing link via text or email, you can forward it to [phishpond@ops.cert.govt.nz](mailto:phishpond@ops.cert.govt.nz). The incident response team then analyses the links it receives, also called phishing indicators, and publishes verified ones to the PDS. The NCSC's research team also proactively identifies phishing sites and blocks them before they can be used to target New Zealanders.

In Q2, the NCSC processed 11,278 phishing indicators of which 2,059 were published to the PDS. The NCSC proactively identified 325 indicators in Q2. The industry most impersonated by phishing scammers this quarter was postal agencies.

# Pacific partnerships

The NCSC's Pacific Partnership Programme, funded through the New Zealand Aid Programme, works with Pacific partners to build local and regional cyber security capacity. The team is currently supporting counterparts in Samoa with preparations for the Commonwealth Heads of Government Meeting (CHOGM), scheduled to be held in Apia in October.

In June, a member of the Pacific team, alongside a colleague from Kiribati, formed Team PaCSON and took part in the annual FIRSTCON Capture the Flag Competition in Fukuoka, Japan.<sup>6</sup>

Post Office NZ: Payment of import duty/tax & advance fee of \$1.99 is required for your shipment to be processed.  
Pay secured via: [nz-nspost.jer-gdkad.shop](https://nz-nspost.jer-gdkad.shop)



## International updates

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

The National Cyber Security Centre, together with our international partners from Australia, Canada, the UK and USA, released a joint advisory regarding deploying AI systems securely. The advisory outlines methodologies for protecting data and AI systems and responding to malicious activity.<sup>7</sup>

Our partner agencies also joined us in releasing guidance designed to inform organisations of secure-by-design considerations for the procurement of digital products and services, resulting in better-informed assessments and decisions. The advisory also informs manufacturers of secure-by-design considerations for digital products and services.<sup>8</sup>

<sup>6</sup> <https://pacson.org/news/first-conference-2024-fukuoka-japan>

<sup>7</sup> <https://www.ncsc.govt.nz/news/deploying-ai-systems-securely>

<sup>8</sup> <https://www.ncsc.govt.nz/news/choosing-secure-and-verifiable-technologies>