certnz

Q3

JULY_TO_SEPTEMBER_2022

CYBER SECURITY INSIGHTS

Don't know what you've **lost** till it's gone

IN THIS ISSUE

Te Kāwanatanga o Aotearoa
New Zealand Government

Q3 CYBER SECURITY INSIGHTS

Director's message

Rob Pope, Director

We set a new record this quarter: the highest financial loss ever reported to CERT NZ in a three-month period.

It's an unhappy record. That $8.9 million of loss represents hundreds of individual New Zealanders and businesses out of pocket to criminals; over 90% going to scams and fraud.

Some lost thousands and others lost just a few hundred dollars. It'd be wrong to dismiss the small amounts, though, because being out of pocket by $500 can have a significant effect on many of us.

The impact scams can have on individuals isn't just financial. There's the stress, confusion, embarrassment and, potentially, reputational damage that can also occur.

But we're here to help. In this Cyber Security Insights Report, we focus on areas where we've seen increased incidents and associated losses and give you tips and advice on how to avoid the scammers.

During this time of the year, we're all looking for great deals online; the scammers know it and they're creating very convincing fake shopping sites. To help, we've outlined some of the things you can keep an eye out for when you're online.

We've also seen more incidents happening via social media marketplaces, where scammers look for people who might fall for investment, romance, and fake rental scams. You need to keep your wits about you with offers that are too good to be true or that ask for an upfront payment.

We also look at unauthorised access and how to stop it by using some simple security steps.

I hate being the bearer of bad news at Christmas, but I hope, by highlighting these issues, CERT NZ is able to ensure every New Zealander, with their friends and whānau, have a safe holiday season online.

AT A GLANCE...

Average incidents reported per quarter

2,166

Average loss reported per quarter

$4.5m

Losses reported to CERT NZ from previous eight quarters

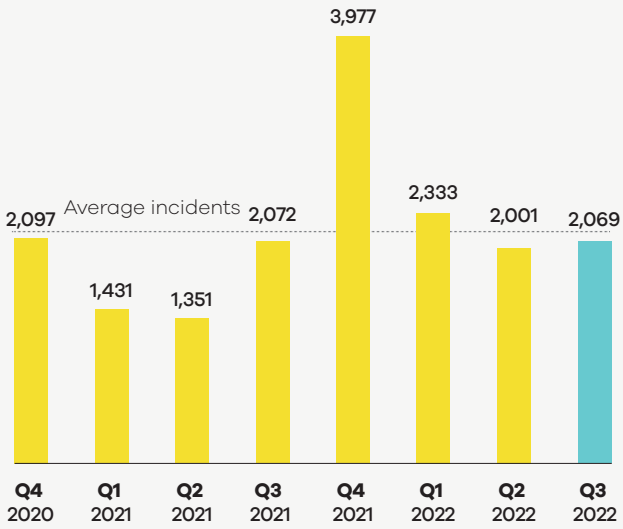
$36.1m

Figures based on previous eight quarters

INCIDENTS RESPONDED TO BY CERT NZ

2,069
incidents were responded to by CERT NZ in Q3 2022.

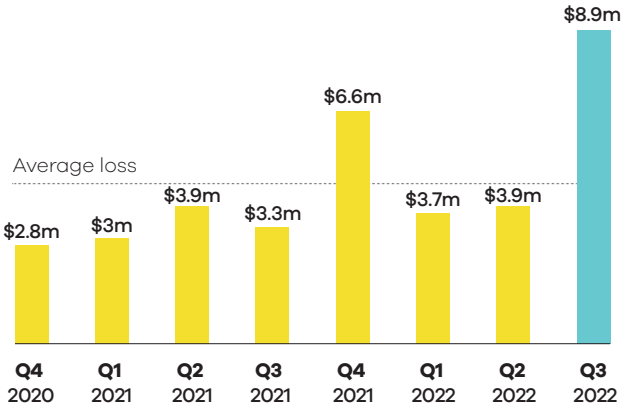
▲3%
increase from Q2 2022.



DIRECT FINANCIAL LOSS

$8.9m
in direct financial loss was reported in Q3 2022.

▲128%
increase from Q2 2022, with 30% of incidents reporting financial loss.



BREAKDOWN BY INCIDENT CATEGORY

In Q3, an increase in reports occurred in most categories. Financial loss is at a record high, increasing 128% from the last quarter (Q2 2022).

		From previous quarter
Phishing and credential harvesting	924	▼ 17%
Scams and fraud	695	▲ 32%
Unauthorised access	295	▲ 28%
Malware	39	▼ 37%
Website compromise	15	▲ 15%
Suspicious network traffic	7	▲ -
Ransomware	6	▲ 20%
Botnet traffic	4	▲ 100%
Denial of service	4	▲ 100%
C and C server hosting	1	● 0%
Attack on system	0	● 0%
Other	79	▲ 80%

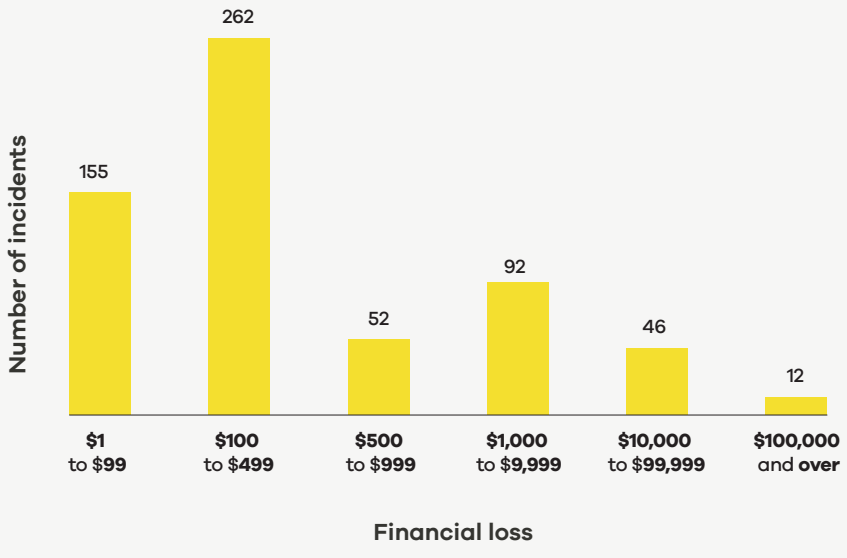
For more on the New Zealand threat landscape in Q3 2022, see the CERT NZ Quarter Three Report: Data Landscape.

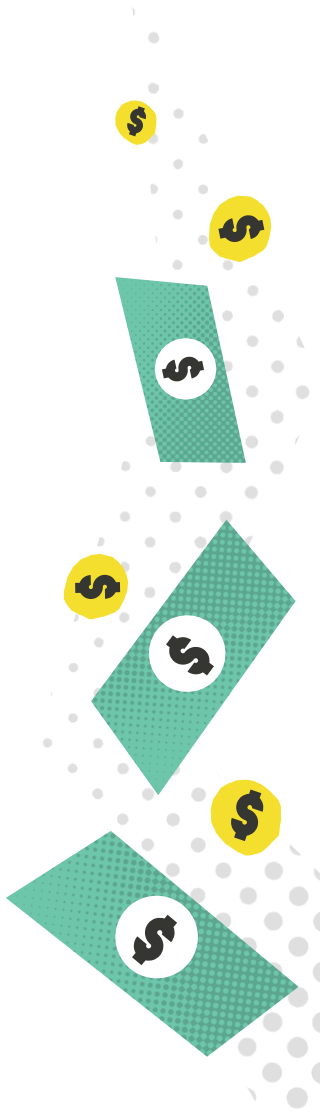
Don't know what you've **lost** till it's gone

New Zealanders lost close to $9 million to online incidents in quarter three this year, more than any previous quarter. Over 600 individuals carried most of this loss, including almost $7.5m lost to scams and fraud alone.

While those totals are eye-catching, it's important to note that most people (314) lost between $100 and $1,000, and those amounts can have a large impact on individuals.

FINANCIAL LOSS INCIDENTS





SCAMS AND FRAUD

As always scams and fraud accounted for the largest financial loss. Romance scams, fake job offers, investment and even rental property scams, are becoming more prevalent, especially in social media marketplaces.

While many people think of scammers as trying to get access to their bank account, the more devious scams don't need to. A new wave of scams is stinging people for an ongoing subscription disguised as a small one-off fee. See example below.

$4.8m!

The most noticeable fraud subcategory was the $4.8m New Zealanders lost to unauthorised money transfer.

(This is a separate incident type to unauthorised access.)

To learn more about unauthorised access and the effect it can have on businesses and individuals, see our insight on page 10.

Unauthorised money transfer example

A recent scam claiming to be from NZ Post asked recipients to put in their credit card details to pay a small fee to release a package from Customs. The transaction went through but also signed them up to a subscription of anywhere from $40 to $80 per month.

TYPES OF SCAMS AND FRAUD

	Incidents reported	Amount Lost
Buying, selling or donating goods	375	$280,000
Dating or romance scam	65	$590,000
Tech scam phone calls	61	<$1000
Unauthorised money transfer	60	$4,835,000
A new job or business opportunity offer	51	$1,170,000
Extortion/blackmail scam	29	$-
Scam phone calls	23	$19,000
Asked to pay money upfront	12	$390,000
Cryptocurrency investment	7	$455,000
Investment scams	6	$189,000
Fake lottery, prize or grant scam	4	<$1000
Buying, selling or donating services	2	<$1000

695
total incidents of scams and fraud

$7.9m
total dollar amount lost to scams and fraud

The most common type of scam is buying, selling, or donating goods. The number of reports in this category is up 50% from the previous quarter."

Other areas with notable losses include scams for cryptocurrency and non-fungible token (NFT)[1] investments, being asked to pay upfront for something, and romance scams. Only seven reports of crypto scams were made, but, these averaged to over $65,000 each, showing this type of investment scam is still losing New Zealanders thousands of dollars.

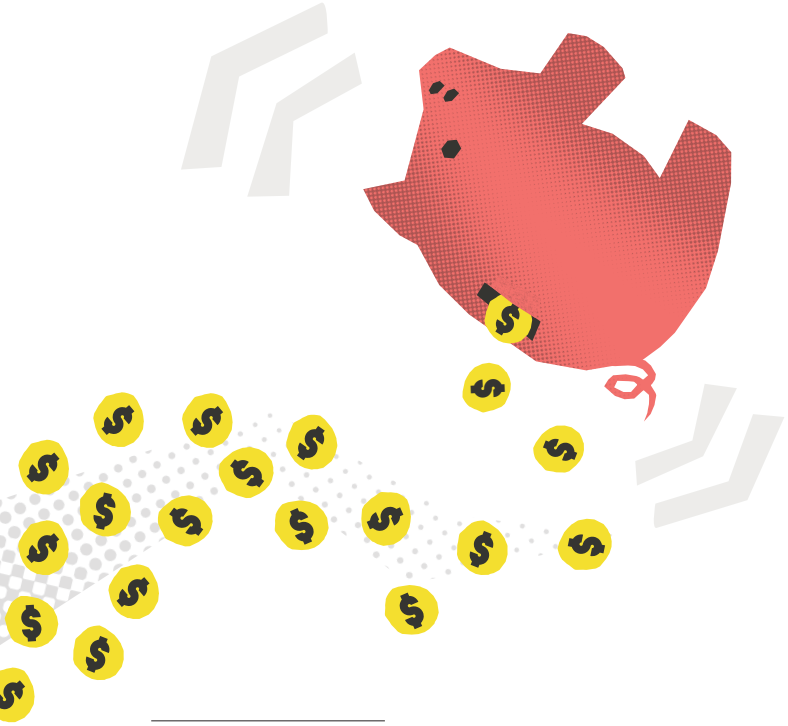
Upfront payment scams persist, with scammers targeting Facebook and other social sites. We've especially seen this on social media where a user may be approached with the offer of rental accommodation or something similar, and to get it they must pay up front. It's a scam that preys on an individual's needs, and often scammers find targets by reading public posts.

The most common scam is related to buying, selling, or donating goods. Reports in this category are up 50% from the previous quarter. While the average loss isn't high, it's a constant threat and one that isn't easy to combat beyond realising that sometimes a deal is too good to be true.

IT'S NOT JUST MONEY

Financial loss is the simplest loss type to quantify, however, reports to CERT NZ also often include other types of losses. These can be areas that affect businesses such as operational, reputational and data loss.

Reputational loss, for example, can create long-term damage to a business or organisation. CERT NZ encourages businesses to think about these other kinds of losses when creating cyber security and incident response plans.



KEEPING SCAMMERS AT BAY

When doing anything online that requires money or personal details, act with an abundance of caution. Scammers want you to do things quickly and without thinking, by creating urgency.

Many scam tactics can be fended off with a small bit of research, taking your time to consider if an offer is legitimate, or contacting a company directly rather than clicking a link in a text message.

If you believe you have been the target of an online scam contact CERT NZ and, if you have lost money, contact your bank, immediately. The sooner you report it the more likely the loss can be minimised or even reversed.

[1] See Quarter One: Cyber Security Insights 2022 https://www.cert.govt.nz/about/quarterly-report/quarter-one-cyber-security-insights-2022/

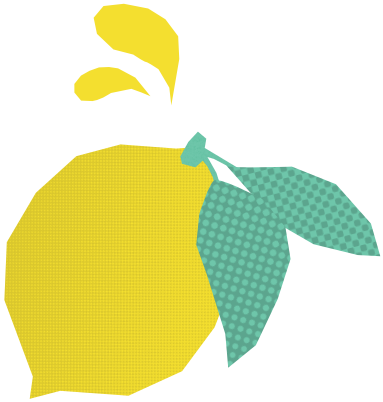
Buyer beware

This quarter, CERT NZ received the highest number of reports related to buying, selling and donating goods online for a single quarter (375). Most reports were about purchasing goods online that either didn't arrive or an inferior product was delivered instead.

You may think you're ordering collectible sneakers but receive a pair of cheap sunglasses. So how do you know before you buy?

The scammers are clever and use every trick in the book and hope bargain hunters will fall into their traps.

More and more, CERT NZ is seeing websites that imitate well-known brands but with a slight change to the URL in order to trick people. We have seen quite a few cases of adding 'outlet' or 'nz' to the domain name of a well-known shop (for example, www.HughsShoesOutletNZ.com).



HOW TO SPOT A DODGY WEBSITE

Gone are the days where looking for the padlock symbol next to the web address (URL) was the sign of a safe website to buy from. The lock and a URL containing 'https' mean the connection between your web browser and the website server is encrypted[2], it doesn't mean the site sells legitimate goods.

So, what do you look for?

A good place to check is the contact page on the website. Fake sites may not have a contact page, or if they do, the contacts may be overseas phone numbers or emails that don't align with the brand.

Check external reviews and feedback of the site. Googling the name of the site and 'reviews' may find more info than what's presented on the site itself because scammers are unlikely to leave bad reviews up.

For more info on the site you can use Whois.com, a website that will tell you who the domain is registered with, when it was registered and how long it was registered for. You can also establish if a website is legitimate by checking domain names at the Domain Name Commission register.

Scammers are also setting up websites for brands that don't sell online or otherwise have a strong web presence. Suddenly see something for sale online that was supposed to be an in-store purchase only? There's a good chance it's a scam. The letters NZ in a website's URL do not mean the site is necessarily based in Aotearoa, and this can mean they are not required to follow New Zealand consumer law.

IF YOU FIND A FAKE WEBSITE

Report all dodgy websites to CERT NZ; we can investigate them and potentially get them taken down. If the seller is using a platform such as Amazon or Facebook to sell their goods, then you can report them to that platform.

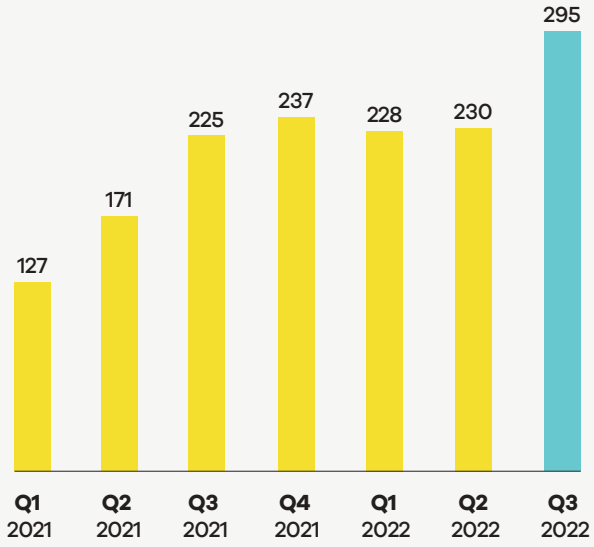
If you have been caught out by a scam website, contact your bank, to see if you can get the charges reversed.

[2] https://www.cert.govt.nz/business/guides/benefits-of-making-your-website-use-https/

Unauthorised access shut down with two steps

In quarter three, close to 300 reports were received about unauthorised access, a 28% increase on the same quarter last year, with a direct financial loss to New Zealanders of $734,000.

UNAUTHORISED ACCESS REPORTS STEADILY INCREASING



Unauthorised access is when an attacker gets access to an account without the account holder's permission, and can affect both individuals and businesses. Usually this is for financial gain or to gather personal information.

It can happen in several ways but most often it's due to easily guessed passwords or login details that have been leaked, stolen or gathered through a phishing campaign.

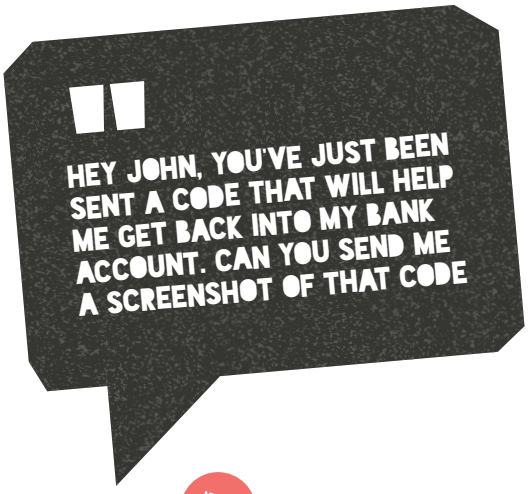
The best way to protect from unauthorised access is by enabling two-factor authentication. This is an extra layer of security on top of your password, usually a code generated by an app on your phone or a digital finger print.

HOW UNAUTHORISED ACCESS CAN AFFECT INDIVIDUALS

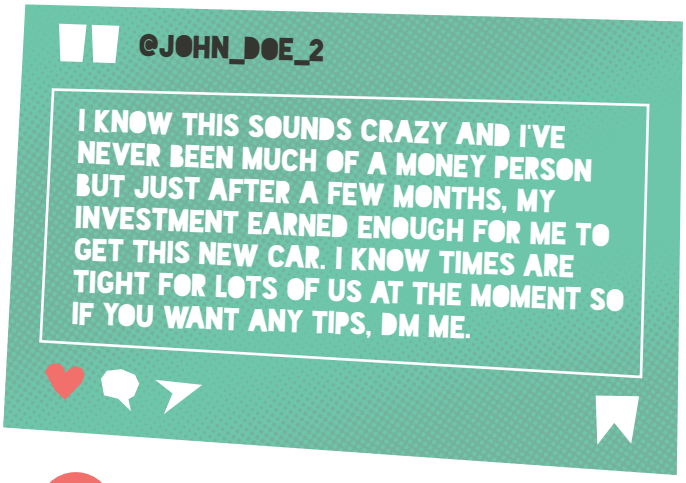
This quarter, individuals reported over $570,000 in direct financial loss through unauthorised access.

Losses extend to anyone digitally connected to the compromised account, because the access not only exposes the account holder to risk but also any of their contacts, including friends and whānau.

Many of the incidents reported were social media accounts being compromised and the real account holder being locked out. The attacker then pretended to be the account holder, trying to trick friends or family of the account holder into giving them money with either an urgent request or a fake investment opportunity.



Red flag - urgency



Red flag - too good to be true

HOW UNAUTHORISED ACCESS CAN IMPACT BUSINESSES

In quarter three, 21 businesses reported unauthorised access with a direct financial loss of almost $170,000.

For businesses, one of the most common types of unauthorised access is business email compromise. This is when an attacker gets access to an employee's email account without their permission to carry out malicious actions like:

- invoice scams
- intercepting communications
- changing details like banking details on an invoice, and
- distributing phishing emails or malware.

Just like a social media account, this can affect any contacts linked to the email account including clients, customers and suppliers.

Preventions

The impacts of unauthorised access can seem overwhelming; however, protecting from this type of incident doesn't need to be. There are some simple measures you can put in place to strengthen your business's online security. By taking these steps, it also means you're protecting your contacts from being affected too.

Change your password immediately if you receive a temporary code for an account you weren't trying to log in to. It could mean someone has your password and is trying to access that account without you knowing.

- **Enable two-factor authentication (2FA)** [3] to add an extra layer of security to your accounts. This means that, even if an attacker gets hold of your password, they still won't be able to get in.
- **Use strong, long and unique passwords** on all your accounts. If you're a business, encourage staff to use a password manager to help them remember all their passwords.
- **Don't give out personal information online**, whether on social media or by email.
- **Verify payments** with an SMS or call to the person or business that sent you the invoice.

[3] https://www.cert.govt.nz/individuals/guides/two-factor-authentication/

UPDATES

Cyber Smart Pacific – 2022 PaCSON awareness raising campaign launched

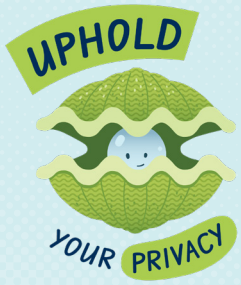
Cyber Smart Pacific was launched in October, in time for International Cyber Security Awareness Month. The campaign look, feel and messaging was developed collaboratively between **Pacific Cyber Security Operational Network (PaCSON)** members and CERT NZ, to encourage and engage people across the Pacific to be more secure online.

Four calls to action are characterised by sea creatures, commonly found in the Pacific, which encourage individuals and business to take on the four main cyber security steps.

UPSIZE your passwords – so they're long, strong and hard to crack.

UPGRADE to two-factor authentication – so your online accounts have double protection.

UPDATE your apps and software – to keep bugs and viruses out.



UPHOLD your privacy – to keep your personal information secure.

Incident communications framework

CERT NZ has created a communications framework for organisations to incorporate into their incident response plans. Based on the work of Jason Nurse and Richard Knight from the universities of Kent and Warwick, the framework is designed to help organisations communicate clearly and effectively with their staff, stakeholders and the media.

This type of guidance is often requested by organisations CERT NZ helps as part of incident response. Alongside the framework, CERT NZ has created templates and other resources to further make communications simpler for those who may only have technical expertise.

Announced at the 2022 PaCSON conference in September, CERT NZ's incident communications framework and the accompanying assets will be publicly available on the CERT NZ website soon.

International insights

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

The UK's National Cyber Security Centre (NCSC UK) has published new guidance to help organisations effectively assess and gain confidence in the cyber security of their supply chains.[4]

Supply chain attacks can cause far-reaching and costly disruption, yet the latest UK government data shows just over one in ten businesses review the risks posed by their immediate suppliers (13%), and the proportion for the wider supply chain is just 7%.

[4] How to assess and gain confidence in your supply chain cyber security - NCSC.GOV.UK: https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security