The webinar will start shortly…

National Cyber Security Centre

own your online

Own Your Online and the NCSC

How to protect your business against business email compromise

National Cyber Security Centre

own your online

Who we are?

Tom Roberts

Team Leader

Threat and incident response

John Mollo

Team Leader

Engagement and Partnerships

About the National Cyber Security Centre

The NCSC is the Government's lead agency for cyber security.

- We provide advice and education to all New Zealanders, from businesses to individuals to nationally significant organisations.

- We also provide incident response and support to anyone who needs it.

- The Own Your Online website has easy to understand resources and guides to help educate all New Zealanders about cyber security and stay ahead of the latest scams and threats.

own
your
online

Scale of incidents across the country

- 7122 Total incident reports recorded by the NCSC
- 110 indicated links to suspected state-sponsored actors
- $21.6m - Total financial loss reported to the NCSC in incidents handled through the NCSC’s general triage process

Online security incidents affect us all

New Zealanders lose more than $198 million to scams and frauds each year – $3.8m every week.

- They are also stressful and time consuming
- They affect our confidence to operate online
- Information and data loss may affect you, even if you personally have not experienced a cyber attack.

own
your
online

Businesses are a target

Cyber resiliency is essential at a business level, no matter the size of the business.

- 36% experienced a cyber attack in last six month
- 55% say cyber security is a top priority for them
- 48% describe their organisation as prepared when it comes to preventing a cyber security incident
- 30% think a cyber incident affecting them is unlikely

Scamming is a business

Cyber criminals don't exactly work a 9-5 job, but it's not anything like this

They are looking for low-cost solutions to target the largest amount of people.

own your online

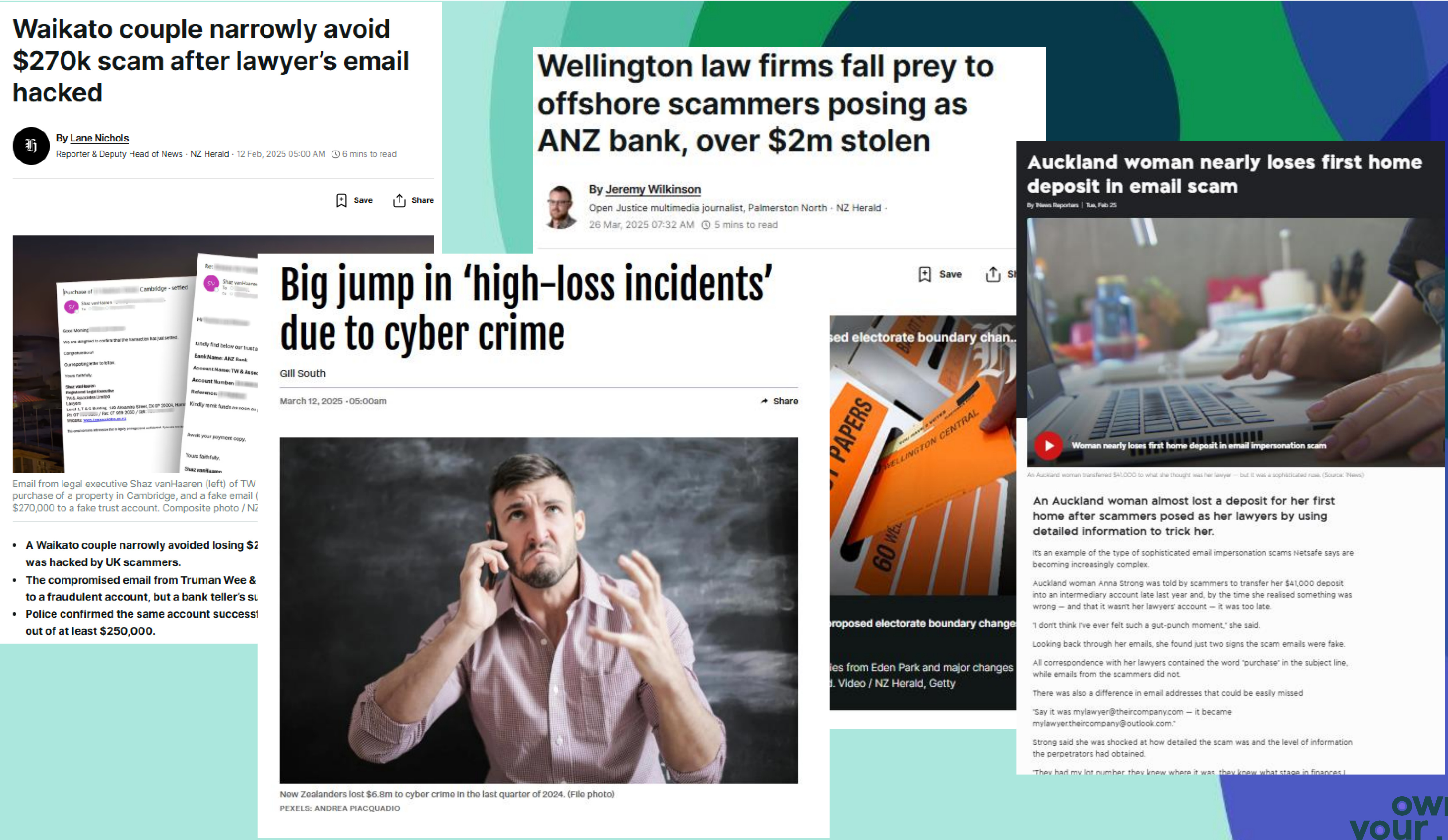
Common threats

- Phishing and credential harvesting
- Investment scams
- Recovery room scams
- Business email compromise
- Spoofing

own your online

Let’s dive in: Business email compromise (BEC)

own
your
online



Waikato couple narrowly avoid $270k scam after lawyer's email hacked

By Lane Nichols
Reporter & Deputy Head of News · NZ Herald · 12 Feb, 2025 05:00 AM · 6 mins to read

Email from legal executive Shaz vanHaaren (left) of TW
purchase of a property in Cambridge, and a fake email (
$270,000 to a fake trust account. Composite photo / NZ

- A Waikato couple narrowly avoided losing $2
was hacked by UK scammers.
- The compromised email from Truman Wee &
to a fraudulent account, but a bank teller's su
- Police confirmed the same account successf
out of at least $250,000.

Wellington law firms fall prey to offshore scammers posing as ANZ bank, over $2m stolen

By Jeremy Wilkinson
Open Justice multimedia journalist, Palmerston North · NZ Herald ·
26 Mar, 2025 07:32 AM · 5 mins to read

sed electorate boundary chan...

roposed electorate boundary change

les from Eden Park and major changes
l. Video / NZ Herald, Getty

Big jump in 'high-loss incidents' due to cyber crime

Gill South

March 12, 2025 ·05:00am

New Zealanders lost $6.8m to cyber crime in the last quarter of 2024. (File photo)
PEXELS: ANDREA PIACQUADIO

Auckland woman nearly loses first home deposit in email scam

By 1News Reporters | Tue, Feb 25

Woman nearly loses first home deposit in email impersonation scam

An Auckland woman transferred $41,000 to what she thought was her lawyer — but it was a sophisticated ruse. (Source: 1News)

An Auckland woman almost lost a deposit for her first home after scammers posed as her lawyers by using detailed information to trick her.

It's an example of the type of sophisticated email impersonation scams Netsafe says are becoming increasingly complex.

Auckland woman Anna Strong was told by scammers to transfer her $41,000 deposit into an intermediary account late last year and, by the time she realised something was wrong — and that it wasn't her lawyers' account — it was too late.

"I don't think I've ever felt such a gut-punch moment," she said.

Looking back through her emails, she found just two signs the scam emails were fake.

All correspondence with her lawyers contained the word "purchase" in the subject line, while emails from the scammers did not.

There was also a difference in email addresses that could be easily missed

"Say it was mylawyer@theircompany.com — it became mylawyer.theircompany@outlook.com."

Strong said she was shocked at how detailed the scam was and the level of information the perpetrators had obtained.

"They had my lot number, they knew where it was, they knew what stage in finances I

own
your
online

What is BEC?

- BEC is when an attacker gets access to someone’s work email account without their permission, to carry out attacks or scams.
- Can also be known as unauthorised access.

own your online

How it works?

The most common way business email compromise happens is when a scammer gets access to an employee’s email. This can happen in a number of ways:

- Guessing or code cracking weak passwords
- Finding log in details in credentials dumps
- Collecting account login information
through phishing campaigns.

own
your
online

Then what…

Attackers can carry out a range of attacks including:

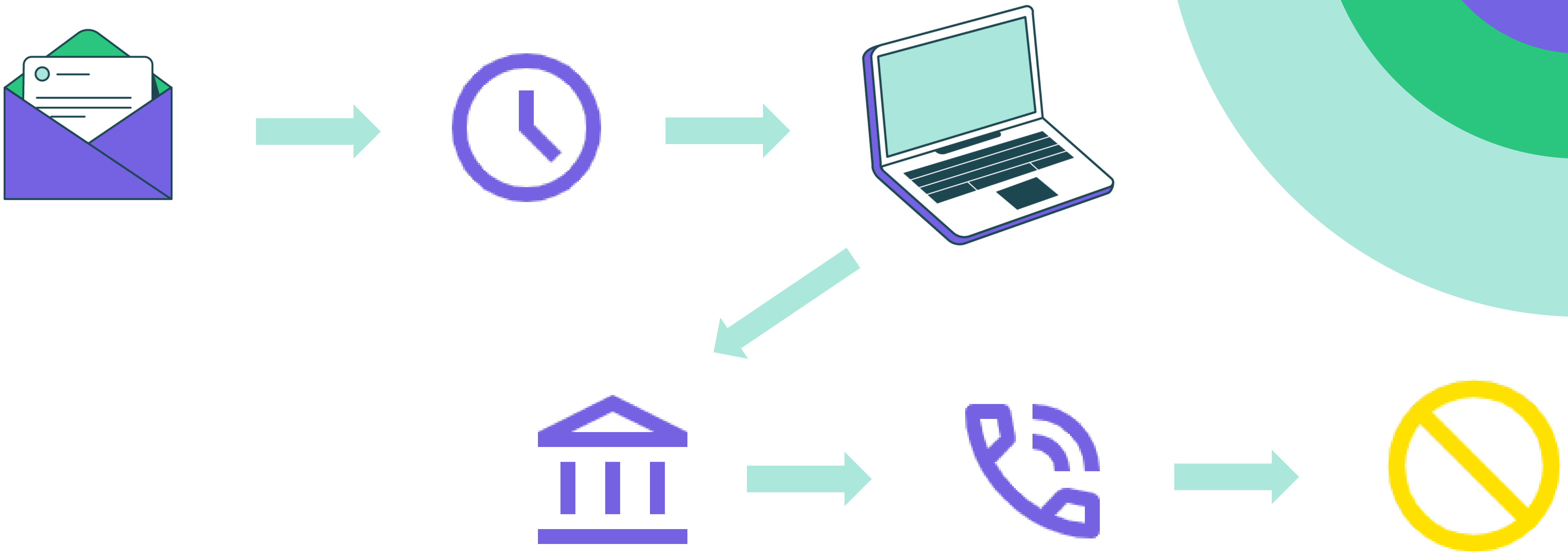
- Invoice scams – these are common and involve sending fake invoices pretending to be from a business.

- Intercepting legitimate invoices and changing the payment details to redirect payments to their bank account.

- Sending phishing emails.

- Sending malware.
- Espionage and information gain

Case study: law firm BEC



own
your
online

What to look out for

BEC can be an incredibly sophisticated attack and hard to detect. Monitoring your business email is important and sometime you may need your IT provider to help with this. You should check for:

- auto-forwarding rules on email accounts, especially those relating to accounts receivable,
- auto-filtering rules on email accounts to see if there are any rules that you did not set up, and
- email access logs to look for any unusual login behaviour like a change in log in times and an unexpected or foreign IP address.

How to protect your business from BEC

own
your
online

Turn on two-factor authentication (2FA)

- 2FA is an additional security step on top of your username and password that helps keep other people out of your online accounts.
- 2FA is a way of ensuring that it's really you logging into an account.
- With 2FA enabled, an attacker would usually need access to another device or a token to be able to log in to your system, even if they managed to crack a username and password.

own your online

All 2FA is not created equal

- The most basic form is a unique code sent to your phone.
- There are also 'authenticator apps' that generate codes for you.
- Biometrics.
- A physical key that you plug into your device.

Pick two…

Something you know.

- Passwords, PIN numbers, security questions.

Something you have.

- Your phone, a security key, another device.

Something you are.

- Voice, fingerprint, face, "biometrics"

own
your
online

Use long, strong and unique passwords

- Longest is strongest: use at least 16 characters.
- Use a passphrase of four or more random words.
  - PumpkinTreeBlueMap
- Avoid common patterns and personal information.
- Don’t use the same password across accounts.
- A password manager can help.
- Check if your password or email account has been compromised at www.haveibeenpwned.com.

own your online

Set up logs

- Logs record all the actions that people take when they access your website or server. They can help you detect when an incident happens and establish the full scope of the incident.

Prevent email spoofing

- Email spoofing is when an attacker sends an email appearing to come from your organisation’s domain . This can happen if your domain doesn't have SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication, Reporting, and Conformance), and DKIM (DomainKeys Identified Mail) security policies set.

Key takeaways

- Online security incidents affect us all, businesses of all sizes can be targets.
- Get the basics in place – having strong passwords and 2FA in place on emails, banking and main accounts.
- If you're concerned your business is affected by an online security incident report to CERT NZ (we'll show you how in the next slide).
- Head to www.ownyouronline.govt.nz to find more information about how to protect yourself from BEC.

Protect your business

Kia pare i tō pakihi ki te whakamōrea īmēra

Protect your business against email compromise

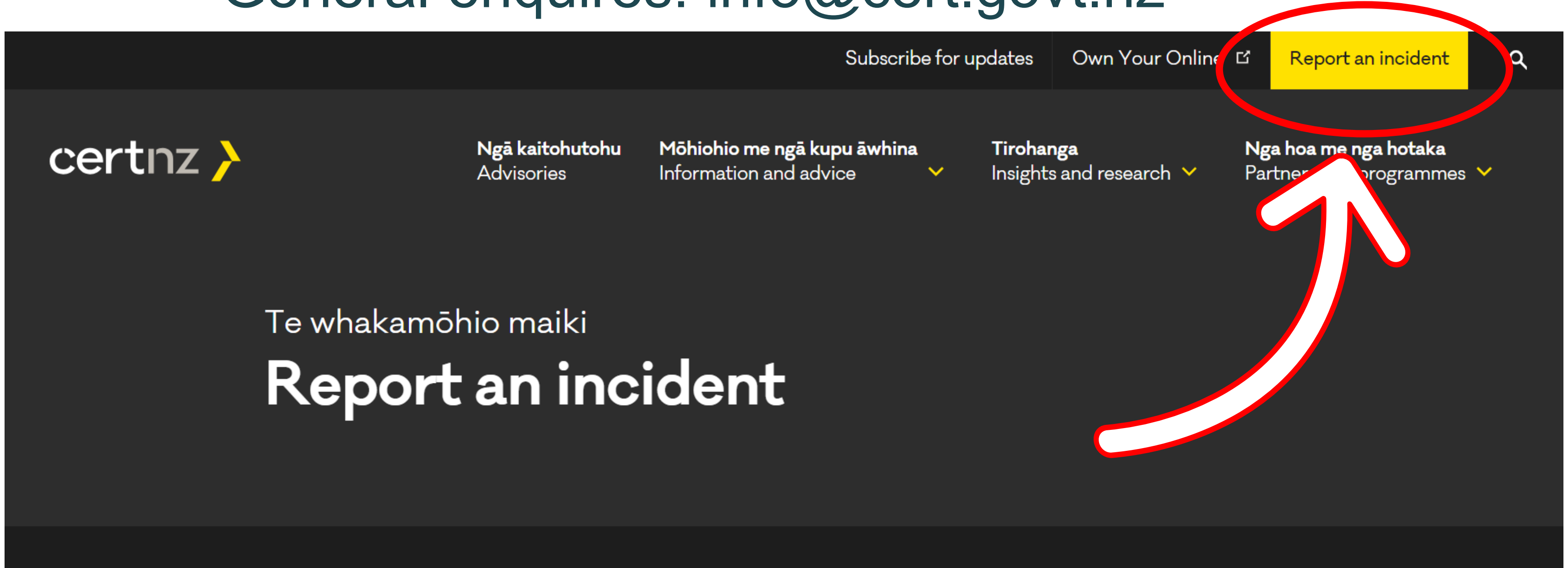
There are some simple measures you and your staff can put in place to strengthen your business email security.

own your online

Getting help

How to get in touch with us

- If there is a cyber security incident:
  - Website: https://www.cert.govt.nz/report/
  - Phone: 0800 2378 69
  - Email: incidents@ncsc.govt.nz
  - General enquires: info@cert.govt.nz



Subscribe for updates

Own Your Online

Report an incident

certnz

Ngā kaitohutohu
Advisories

Mōhiohio me ngā kupu āwhina
Information and advice

Tirohanga
Insights and research

Nga hoa me nga hotaka
Partner programmes

Te whakamōhio maiki

Report an incident

own your online

Thank you

National Cyber
Security Centre

own
your
online