



QUESTIONS & ANSWERS REMOTE ACCESS TO EMAILS & THE PORTAL

March 2018

Following are some questions, and answers relating to the current problems with remotely accessing work emails and the Portal.

What happened?

Fire and Emergency have experienced an IT email issue, which we are investigating.

We noticed an increase in the number of spam emails being delivered to our system, containing links that generated more spam.

As a precautionary measure we suspended remote access to our email system through the internet (the Portal). It did not affect our normal access to our emails.

Remote access was still available for personnel with Fire and Emergency owned phones and laptops. Email is accessible on stations and at offices as normal.

This has not impacted on our operations.

This as a timely reminder to not to click on emails if you don't know the origin.

What was the nature of the spam? Do you know the country of origin?

A number of spam emails were created that were trapped and removed. It was an international address, but we cannot disclose the actual origin as this investigation is still ongoing.

Did it have any affect on public safety?

No.

When was the remote email access suspended, and for how long?

In early March we noticed an increase in spam emails. Only remote access to email, through the internet, was suspended as a precautionary measure, a week after we first noticed the spam email increase.

What was the volume of spam received?

We noticed an increase in spam emails and a handful were opened and a link clicked – this then generated more spam emails.

We are unable to disclose the number of spam emails received – but it is normal for organisations like ours to receive thousands of spam emails a week.

This is a timely reminder not to click on emails if you do not know the origin.

How many email addresses were affected, and how long were the out of action for?

Emails on station and in offices were not affected. As a precautionary measure we disabled remote email access to our system.

Everyone gets spam emails, but don't need to suspend email access. What was the volume of spam emails, and what happened when people clicked on it?

Suspending remote access to emails was done as a precautionary measure, because we noticed the number of spam emails had increased.

Email access was not suspended, remote access through the internet was. We received more than usual spam emails and when a link was clicked it then generated more spam emails.

Do you know when normal email service might resume?

Normal email service has not been affected.

Why was the level of security not sufficient?

Our ability to detect and stop spam is a constant focus and, like all New Zealanders who have home computers, they face the same issue through their internet provider.

What security measures have been put in place to combat the problem?

Extra security measures have been put in place. We cannot disclose the exact security measures we have taken, because disclosing this information could put security at risk.

This is standard practice when dealing with this sort of thing. We are adopting measures to try and discourage - not encourage - spammers to try to compromise our security process.

We continuously work to ensure our systems are safe. We have put in already put in place 7 of the [top 10 controls](#) that CertNZ has identified as being most likely to mitigate, or better contain, information security incidents.

The remaining 3 are underway:

	✓ Patch your software
	✓ Upgrade or replace legacy systems
	✓ Disable unused services and protocols
	✓ Implement application whitelisting
	✓ Change default credentials
In progress	Enforce multi-factor authentication
	✓ Enforce the principle of least privilege
	✓ Implement and test backups
In progress	Configure centralised logging
In progress	Manage your mobile devices.

Why was the GSCE involved?

GCSB were not involved. We always report spam issues through a central government system to ensure that other organisations are aware that this activity is taking place. This is normal practice as is it common for spam attacks to be targeted against many agencies.

MORE INFORMATION

You can find out more about how to keep safe online at:

- Netsafe helps New Zealand internet users stay safe - <https://www.netsafe.org.nz/>
- Cert NZ works with other government agencies and organisations to respond to cyber security threats in New Zealand - www.cert.govt.nz

If you need ICT support to access work emails from your Fire and Emergency phone or other device, contact:

- ICT Helpdesk - 0800 374 843