Q4 CERT NZ Quarterly Report /// October – December 2017

certnz

Results ///

Incidents reported to CERT NZ

377 incident reports received

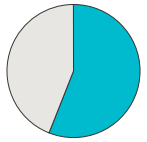
- **229** were responded to by **CERT NZ**
- **144** involved cyber crime and were referred to **NZ Police**
- **2** involved cyber bullying and were referred to **Netsafe**
- **2** were referred to **NCSC**

Incidents reported by type

Reports of scams and fraud have increased significantly to **139** in Q4 from **65** in Q3.

Unauthorised access

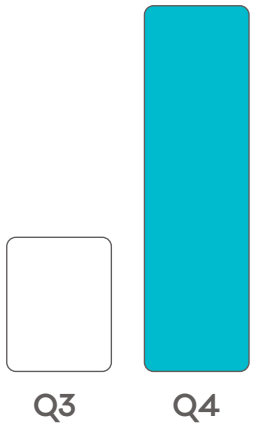
56% of unauthorised access incidents in Q4 involved some form of loss. This is the highest proportion recorded since reporting began.



Impacts ///

Over $3.4 M in financial loss reported.

This is more than double the losses reported in Q3.



High value losses

9 incidents involved losses of over **$100,000 each.**

$2.8 M in total loss from the 9 incidents

2017 Summary ///

1,131 incidents reported

Over $5.3 M in total financial loss reported in 2017

Notable trends

The most reported incident type in 2017 was phishing & credential harvesting.

There was a spike in ransomware reports during the Wannacry and NotPetya ransomware campaigns in Q2.

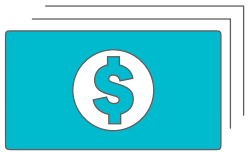
Reporting period: 1 October - 31 December 2017

Q4 CERT NZ Quarterly Report /// October – December 2017

certnz

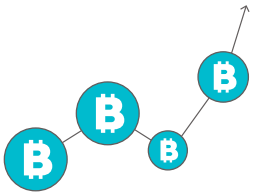
Focus area: Cryptocurrency scams ///

6%
of incidents reported to CERT NZ in Q4 involved cryptocurrency



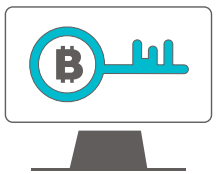
$262,323
financial loss from cryptocurrency reports (which represents 8% of the total loss this quarter)

Two main types of cryptocurrency reports in Q4



Cryptocurrency investment scams

These scams operate by sending out emails or setting up fake websites advertising cryptocurrency investment opportunities with attractive returns.



Stolen cryptocurrencies

These attacks use a fake website or applications to gain credentials or private keys. These are then used by the criminal to transfer the cryptocurrency.

Protect yourself

Two-factor authentication

2FA adds an extra security check on top of your password, making it a step harder for someone to access your wallet or exchange account.

Password

Set a strong, unique password to access your wallet and/or exchange account. We recommend using a long and strong password with 2FA to limit unauthorized access.

Backup

Risks like ransomware, accidental data loss or loss of device mean you should regularly backup your cryptocurrency wallet to offline storage.

Minimise risk

Reduce the amount of money in your cryptocurrency wallet to an amount you are willing to lose and keep the rest in offline storage.

Encryption

Ensuring that you have full disk encryption on all devices from laptop to mobiles, will reduce the risk that an attacker could extract your wallet.

Case Studies ///

Case Study – Don't download fake crypto-wallets

CERT NZ received a report about cryptocurrency stolen using a fake Electrum wallet. The individual had searched the term 'Electrum' and clicked on a link in the list returned without doing any further research. They downloaded and launched an application. Once they had entered their details they realised that something was wrong with the application. When they checked the blockchain, they saw that their cryptocurrency had been transferred to another address. The loss was over $100,000 at the time of the report. The case was referred to NZ Police.

Case Study – Watch our for fake 'security issues' emails

A cryptocurrency investor reported a bitcoin theft to CERT NZ. The investor received an email that said their bitcoin account had security issues, along with a link. They followed the link to a legitimate-looking website and logged on. The website requested further logons and the investor realised the email was a hoax, but by then their bitcoin had already been stolen from their account. Although CERT NZ referred the case to the NZ Police, it is unlikely the investor's bitcoin can be recovered.

More tips for staying safe online can be found at **www.cert.govt.nz**