Overview of Scams Activity for Businesses in ANZ

Cultivated from various reports in the past year, we have compiled a fact sheet detailing an overview of **Scams Activity** and **Email threats** for your business to be aware of. Many of these email threats stealthily slip past the gateway. Threats like ransomware, spear phishing, and account takeover put your organization and employees at significant risk. Request a **Email Threat Scan** to quickly and effectively finds social engineering attacks currently sitting in your Office 365 mailboxes.

Scam losses reported by businesses increased by 260% in 2020, to $18 million from $5 million in 2019.

Scams category

False Billing and Phishing Scams are the most reports made by businesses.

These scams typically involve a request for payment for a service or item that wasn't ordered or a scammer diverting money by impersonating the intended recipient of a payment.

Scam reports by business size

Micro and small businesses received the largest number of scam reports, with the majority originating from false billing, phishing and identity theft.

Large businesses experienced the highest losses with the most reported category being phishing.

Business Email Compromise is one of the top 3 scams causing the most financial harm to Australians in 2020.

Combined losses for business email compromise scams totalled **$128 million** in 2020.

Scamwatch received around 1,300 reports in 2020, with over $14 million in losses, compared to approximately 900 reports with $5 million in losses in 2019.

Source: Targeting scams: Report of the ACCC on scams activity 2020 (ACCC, 7 June 2021)

Top Two Sources of Breaches under the NDB scheme

Malicious or criminal attacks (including cyber incidents) remain the leading source of data breaches, accounting for **58%** of notifications.

Data breaches resulting from **human error** accounted for **38%** of notifications, up 18% from 173 notifications to 204.

Source: Notifiable Data Breaches Report: July-December 2020 (OAIC, 28 January 2021)

Cyber security incidents impacting organisations in New Zealand

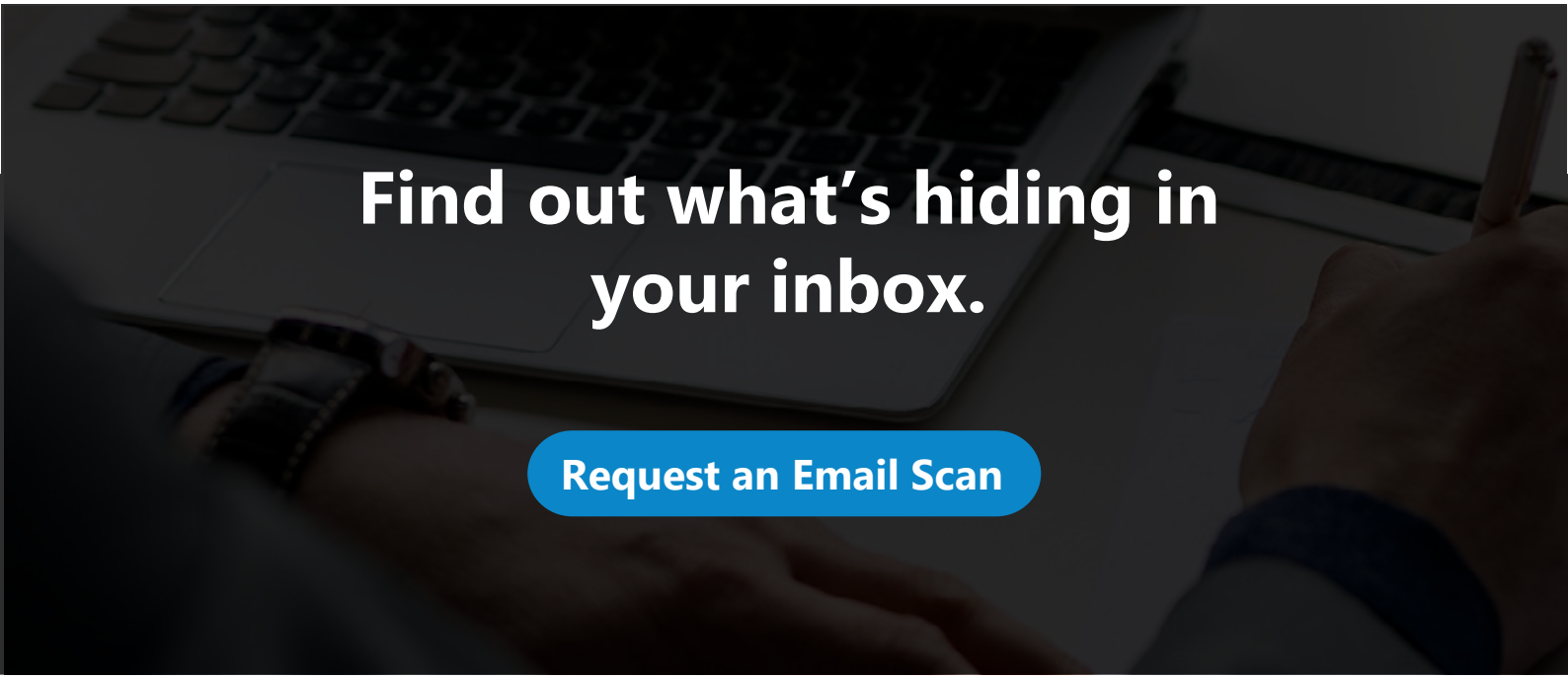
Phishing and credential harvesting is one of the most reported incident types to CERT NZ, making up **46%** of all incident reports.

Scams and fraud, and **unauthorised access** have increased significantly since Q4 2020; by 50% and 100% respectively.

Source: Quarterly Report - Data Landscape Q1 2021 (CERT NZ, 2021)

CERT NZ identified almost 500 vulnerable Microsoft Exchange email servers and over 100 compromised email servers. The **majority of the compromised mail servers belonged to small businesses.**

Source: Quarterly Report Highlights Q1 (CERT NZ, 2021)



mcr IT