

## **‘Don’t trust email’ Half-a-billion lost to scams in 2018, ACCC says**

---

**MATTHEW ELMAS** / Monday, April 29, 2019

Small businesses were the most-scammed corporate cohort last year, accounting for more than half of the \$7.2 million businesses lost to fraudsters, according to figures released by the ACCC today.

More than 3,000 small businesses lost more than \$4.5 million to scam activity last year, with false billing, investment scams, hacking and phishing emerging as the most successful schemes targeted at businesses.

The ACCC said businesses likely lost \$60 million to email compromise scams when Australian Cybercrime Online Reporting Network (ACORN) data is included, a 170% increase on last year.

Globally, US\$12.5 billion (\$1.77 billion) was lost to similar scams between 2013 and 2018, according to Federal **Bureau of Investigation (FBI) figures.**

**The scam involves fraudsters accessing business email or IT systems and then either extorting high ranking managers or financial officers for money or impersonating the firm in dealings with suppliers to scam them.**

**“Scammers are using pressure and fear tactics combined with technology to trick people into parting with their money,”** ACCC deputy chair Delia Rickard said in a statement circulated on Monday.

In one case, a business was scammed out of \$190,000 after a hacked supplier requested a change in bank details.

“The scammers sent us invoices with amended bank details as well as the prior email trail to and from the supplier so they must have been in their IT system,” the business told the ACCC.

“Everything was a perfect copy of a real version of the invoices we were so used to. We didn’t notice the difference.

“Thinking it was real we sent an amount of \$190,000 but the real supplier never received it.”

### **Can email be trusted?**

Cyber security experts have previously warned high-profile data breaches are fuelling increased scam activity because hackers have cheaper information at their disposal.

Andrew Bycroft, chief executive of the international cyber resilience institute, says he’s not surprised by the increase in scam losses, particularly through email.

“The bad guys have found new tactics that aren’t monitored so well,” he tells *SmartCompany*.

“For a while there were a lot of email security programs that did a good job of stopping spam, but we’ve become over-reliant on them.”

- **Bycroft says ultimately email is a platform “we can’t trust”.**

**“Even if you get an email from someone you believe is a friend it could have come from anywhere.”**

### **“Tip of the iceberg”**

When consumers are included more than \$489 million was lost to scams in 2018, an increase of \$149 million on last year. **Rickard says the figures are likely understated though because many scams go unreported.**

“These record losses are likely just the tip of the iceberg,” she said.

“These extraordinary losses show that scammers are causing significant financial and emotional harm to many Australians,” Rickard said.

**“Scammers are adapting old scams to new technology, seeking payment through unusual methods and automating scam calls to increase their reach to potential victims.”**

**There’s a sharp age difference in scam reports and losses. Fewer than 10% of reports were lodged by people under 24 years old, while those over the age of 55 accounted for almost half of all reports and 39% of losses.**

