Spirit Super confirmed this week that 50,000 of its member records have been compromised  following a data incident where a staff member's email account was hit by a [phishing attack](https://www.mybusiness.com.au/resources/news/fresh-warning-over-new-phishing-attack).

The super fund is investigating the extent of the breach which occurred on 19 May, and believes there was [unauthorised access](https://www.mybusiness.com.au/how-we-help/be-a-better-employer/managing-risk/the-ins-and-outs-of-data-breaches) to a mailbox containing personal data.

Spirit Super confirmed that the hacked mailbox contained names, addresses, ages, email addresses, phone numbers, super account numbers and the balances of Spirit Super members from the 2019-20 financial year, with about 50,000 of the fund's 330,000-odd total members potentially impacted.

However, no tax file numbers, driver's licence details or bank account details appeared to be stolen

Spirit Super believed this was not a targeted attack but that the fund had been caught up in a broad phishing attack campaign.

“The breach was the result of an email phishing activity, rather than a system error, regardless we are taking all reasonable steps to prevent this from happening again,” the company said in a statement.

“In short it was [human error](https://www.mybusiness.com.au/resources/news/human-error-a-major-factor-in-data-breaches) during a malicious email attack posing as official correspondence. This was not the result of a material security control weakness or technology failure. The malicious email resulted in a staff member's password being compromised.

“Spirit Super employs multi-factor authentication (MFA) in addition to a username and password to access our systems.

"Unfortunately, this additional layer of protection was overcome by the attacker and the mailbox was accessed. Phishing attacks such as this are becoming increasingly sophisticated and common.”

Spirit Super confirmed it had notified all the relevant authorities, including the Privacy Commissioner. It was now in the process of reviewing all data handling practices and staff training.

The superfund was also reviewing account activity and placing enhanced controls on accounts and had pledged to further strengthen its IT security and reduce the risk of cyber incidents.

“We are reviewing all our data handling practices and staff training. As a member-focused organisation, for various reasons our staff are required to handle member data. Regrettably, some of this data from 2019 to 2020 was contained within the compromised email mailbox,” Spirit Super said.

“While we know the malicious party had access to the mailbox, they may not be aware that they have this information. We cannot speculate on their motive for the original attack.

“Please be assured that investigations to date indicate that accounts have not been compromised. We have increased the levels of security to ensure our members’ accounts remain safe. Our investigation will continue.”

The company had also increased its security controls immediately following the breach.

“This includes increased identification steps on the accounts of impacted members,” Spirit Super said.

“We have proactively implemented a block to payments from these accounts as a precaution. Please contact us if you have a need to withdraw money from your account and are eligible to do so. We are not aware of any unauthorised activity to member accounts.”