Spirit Super has confirmed that 50,000 of its member records have been compromised following what the super fund described as a broad phishing attack campaign.

The member records date back to 2019 and 2020 and contain names, addresses, ages, emails, phone numbers, account numbers and balances.

However, according to the fund, the records do not include dates of birth, government identification numbers such as tax file numbers or driver’s licence details, or any bank account information.

The $26 billion industry super fund with 325,000 members said that members’ money remained safe following the incident and all those affected had been contacted.

“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,” Spirit Super said.

“Please be assured 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.”

Explaining the incident, Spirit Super said that an email account of one of its staff members was compromised on 19 May.

“In short, it was human error during a malicious email attack posing as official correspondence,” the fund said.

“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.”

Despite employing multi-factor authentication in addition to usernames and passwords, the super fund said the additional layer of protection had been thwarted by the attacker.

“Phishing attacks such as this are becoming increasingly sophisticated and common,” said Spirit Super.

“We have a skilled internal team focused on cyber security and protecting your information. This team detected the compromised account and acted quickly to contain and limit the impact of the breach. No further accounts or systems were impacted.”

Spirit Super said that it did not believe the attack was targeted and it remained unclear whether the attacker was aware that they had access to the personal information.  
Members have been told to remain vigilant to unsolicited emails, text messages or phone calls and to report any suspicious matters to the ACCC’s Scamwatch.

Those impacted by the breach have also been encouraged to not publicly share that their personal information may have been compromised to help avoid being targeted.

“Spirit Super takes your privacy and the security of our information and systems extremely seriously. Online threats are constantly evolving, and no organisation can completely mitigate these risks,” the fund said.

“We continue to invest in internal capability, technology, improved internal processes, and staff training to reduce the likelihood and severity of future data breach events.”

A phishing attack at Australian pension provider Spirit Super has resulted in “some personal details being compromised”.

The ‘super fund’ [confirmed that user data was breached](https://spiritsuper.com.au/privacy-breach-2022) on May 19, 2022 after an employee’s email account was accessed.

An investigation into the incident found that there was “unauthorized access to a mailbox containing personal data” that includes names and other sensitive information. Spirit Super said [approximately 50,000 individuals](https://spiritsuper.com.au/privacy-breach-2022#faq2) are affected.

Spirit Super manages $26 billion worth of funds on behalf of 325,000 members across [Australia](https://portswigger.net/daily-swig/australia).

Exposed data

A press release from the Tasmanian-based company reads: “The personal data that may have been compromised is similar to some information provided in an annual statement, including names, addresses, ages (as at 2019 and 2020), email addresses, telephone numbers, member account numbers, and member balances (as at 2019 and 2020).

“It is important to note that this data DOES NOT include dates of birth, [government](https://portswigger.net/daily-swig/government) identification numbers (such as tax file numbers or driver’s license details), or any bank account details.”

**DON’T MISS** [Volatile market for stolen credit card data shaken up by sanctions against Russia](https://portswigger.net/daily-swig/volatile-market-for-stolen-credit-card-data-shaken-up-by-sanctions-against-russia)

Spirit Super said it does not believe the attack was targeted, rather that it was “caught up” in a widespread phishing campaign.

The super fund detailed: “In short it was human error 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.”

The victim’s mailbox was compromised despite the deployment of [multi-factor authentication](https://portswigger.net/daily-swig/2fa) (MFA), said Spirit Super.

“We have a skilled internal team focused on cybersecurity and protecting your information,” it added. “This team detected the compromised account and acted quickly to contain and limit the impact of the breach. No further accounts or systems were impacted.”

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.”