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.”