The one letter of the alphabet that cost this couple $284,000

Once the scam is discovered, it is often too late. Banerjee didn’t realise he had been robbed until just before settlement day, more than a week after the money had been sent to the wrong account.

So far, none of the money has been recovered. They managed to keep their new house in Kellyville Ridge, north-west of Sydney, thanks to friends and family, whom they now owe over $150,000.

Tanmoy Banerjee now realises there were red flags in his dealings with scammers.*Credit: Rhett Wyman*

“It was a shock,” said Banerjee. “The first reaction was that we will not be able to buy the house.”

Banerjee believes more should be done to help first home buyers who fall victim to these scams, particularly by the banks who are used to handle illegitimate funds.

He also questions why the risk falls entirely on the property purchasers.

“We have health insurance, we have accident insurance, but I think there is nothing that I can actually get some protection from if something like this happens,” he said.

Related Article

As someone who works in software consulting, Banerjee considers himself pretty savvy when it comes to technology. He's now kicking himself that he missed signs that things weren't right.

Initially, Banerjee agreed to pay the deposit for his new property into a shortfall account with his mortgage provider, NAB. But the scammers, hijacking the email thread and pretending to be the conveyancer, suggested a new way.

They told Banerjee to pay the money directly into PEXA, the online exchange network used by banks and conveyancers to lodge documents and complete financial settlement of properties.

To complete the ruse, there was a forged document from PEXA that included the details of a Commonwealth Bank account.

Crucially, the document was an attachment from the conveyancer's original email address. Banerjee now believes that scammers had gained access to the account and were able to send emails from it.

The *Sunday Age* and *Sun-Herald* have chosen not to name the conveyancer, who says he was the victim of a cyberattack and has passed the matter onto his insurer.

When Banerjee questioned the request to send the money to PEXA in December, the same business email responded that they were having difficulties with certain banks, which had resulted in breaches of contract.

Soon after, the fraudulent email address with an S on the end began sending and receiving the emails, to prevent the conveyancer from realising what was going on.

"Please disregard my previous emails," they wrote.

Related Article

After sending an initial test payment of $100, Banerjee made a string of payments over a week totalling $284,000. After each transfer, he was sent a receipt on PEXA letterhead to show the money had been received.

In all likelihood, the money was then sent offshore or into cryptocurrency and is out of reach of authorities.

The transfers ended on December 15. On December 27, Banerjee asked how the keys would be handed over the following day. He was still unaware of the hackers' email address and never heard back.

Hours later, he received an alarming message from his conveyancer's correct email address. NAB had noticed there were insufficient funds in Banerjee's shortfall account to complete settlement.

Related Article

Neither NAB nor Commonwealth Bank were able to comment directly on the case for privacy reasons. Both pointed to efforts under way to prevent scammers from impersonating businesses.

Commonwealth Bank has implemented NameCheck, which compares account details with names and highlights potential differences.

"Once money has left an account, unfortunately it can often be very difficult to recover," said Chris Sheehan, NAB's head of investigations and fraud.

"Before you make a payment to a business, we encourage everyone to call and double-check payment details before hitting send."

The Australian banking industry recently announced it was introducing "confirmation of payee" technology, which would prevent people from making transfers where the account name doesn't match.

The United Kingdom has had those rules since 2020 and recently introduced new laws to force banks to reimburse scam victims up to a maximum of £415,000 ($803,214).