Scammers hacked her phone and stole thousands - so how did they get her details?

Data breaches are getting so common that it can be hard to know how to react when it happens to you. It's often easy to shrug it off, but there's a risk. Being a victim of a data breach increases your chances of being targeted by criminals and scammers. Sue told the BBC how scammers went after her. We found her details had been leaked online.

Sue - a woman smiling while wearing a baseball cap - stands next to a horse. The horse is closer to the camera, with only it's eye and forehead visible beside her. Sue had her digital life hijacked by scammers She was a victim of what's known as a Sim swap attack - where scammers trick a network operator into thinking they're the account holder to get a new Sim card for a mobile device. They used it to take over almost all her online accounts through her phone. She said the experience was "horrible".

Sue also had a credit card opened in her name and the criminals purchased more than £3,000 in vouchers. It took several trips to the branches of her bank and mobile phone provider to get her accounts back. And the thieves weren't done.

"The criminals also did a sinister thing after breaking into my WhatsApp," she said. "They sent messages to horse riding groups I am in warning there were people on their way to stab the horses."

We searched hacker databases using online tools like haveibeenpwned.com and Constella Intelligence to see if Sue's details were previously compromised. Her phone number, email address, date of birth and physical address were all exposed in data breaches at gambling platform PaddyPower in 2010 and email validation tool Verifications.io in 2019. Other compilations of hacked records also included her details.

Hannah Baumgaertner, from cyber firm Silobreaker, said attackers likely used the personal data leaked in previous breaches to conduct the Sim swap attack. "Once they had access to Sue's phone number they were were able to intercept any security codes sent to verify her identity for her Gmail account," she said.

But scammers aren't always targeting big payouts. Fran from Brazil told the BBC she found a user had registered to her Netflix account - and increased her monthly subscription. "I was charged $9.90 (£7.50) on my payment card, even though I hadn't made this purchase," she said.

"I immediately contacted my family to find out if anyone had added another profile to the account we share, but they all said no." Fran was a victim of a common scam where her Netflix account was hijacked by a freeloader. It's not known exactly how they got into her account and the murky world of cybercrime means it is difficult to pinpoint if a single data breach led to someone being scammed.

But we found Fran's email address had been exposed in at least four data breaches including hacks of Internet Archive (2024), Trellov (2024), Descomplica (2021) and

Wattpad (2020) according to the website haveibeenpwned.com. The password she used for her Netflix account is not in publicly known databases but might be in others.

"There is a huge market for cracked Netflix, Disney and Spotify accounts", said Alon Gal, co founder of cyber security company Hudson Rock. It's a low-barrier entry point for cybercrime, turning one company's data leak into widespread, ongoing abuse."

Scammers often combine stolen private information with public information. Leah, who didn't want to give her real name, runs a small business using Facebook adverts and was recently targeted in a long running scam apparently originating from Vietnam.

"I got a phishing email from 'notifications@facebookmail.com' saying that I was due a refund. I clicked on the link and entered my details on the fake Meta page and the scammers were able to take over my business account even though I had 2 factor authentication. They then posted child sexual abuse videos under my name which got me blocked. I was even barred from using Messenger to complain to Meta." In the three days it took Leah to get back her business account back the scammers had run hundreds of pounds of adverts paid for by her. She eventually got the money back.

Alberto Casares from Constella Intelligence searched hacker databases and found Leah's email address and other details were taken in data breaches at Gravatar (2020) and this year's Qantas (third-party breach). "It looks like the attackers used a common technique of linking up Leah's private stolen email address with her publicly listed business number to launch a targeted phishing attack against the email account". They could have done this themselves or used a data broker to pay for a number of potential targets he said.