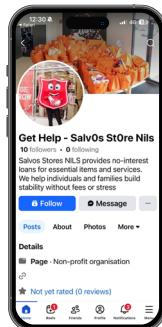




Charity impersonation scam on social media

Stop. Check. Protect.

A social media scammer impersonated a charity to get access to a customer's myGov account and steal their payment. Services Australia assisted the customer to recover their account and payment.



1 The lure

Samantha clicked a **Facebook ad** from 'Get Help – Salvo's St0re'. The ad was posted by a scammer pretending to be a real charity.

The ad offered **financial help with a No Interest Loan**.



2 The trap

The scammer sent a **private message**, asking Samantha to complete a **fake application form**.

Samantha completed the form with her **bank details, myGov username and password**.



3 How the scam worked

The scammer signed into myGov with Samantha's details. They asked Samantha for the **6 digit code sent by SMS**.

Samantha gave them the code.

The scammer got into her myGov and then her Centrelink online account. They **changed Samantha's bank account details and stole her next payment**.



4 The realisation

The scammer then asked Samantha to **open a bank account**. This raised suspicion and Samantha ended the chat.

Samantha called **1800 941 126** for help. The **Scams and Identity Theft Helpdesk** secured her myGov account and recovered her stolen payment.

For more information

If a scammer has contacted you about **myGov, Medicare, Centrelink** or **Child Support** and you've given them personal information, call our **Scams and Identity Theft Helpdesk**.

Let us know if you need an interpreter and we will arrange one for free.

 Call **1800 941 126**, Monday to Friday, **8 am – 5 pm**

 To report scams impersonating charities or other organisations, go to scamwatch.gov.au/report-a-scam

 For more information, go to servicesaustralia.gov.au/scams

 If you see social media scams about myGov, Medicare, Centrelink or Child Support you can report it by emailing reportascam@servicesaustralia.gov.au