# 6 **news**

# How the scammer worked

Scammer posted job advertisements on Facebook and Carousell offering part-time work, which involved replying to texts.



(2) 1460426380

 $\bigcirc$ 

WE HOR.

SMS with "Y" to receive

49293.Security

49991083934

When victims replied to the ads with their cellphones, they were told they would receive a text confirming purchase of game credits. They were told to reply "Y" for "yes", generating a code which they sent to the scammer.



In November last year, there was a spate of scams involving con men pretending to call from major software companies. They tricked people into paying for additional software and got them to download malware. They even had victims give out their credit card details.

social networks.

phone calls.



## I thought to myself, at least I can still try to work and pay off my debts. **But what about** the young girl?

- Miss Lin on a 15-yearold victim of the same scam.

# Easy job? Conjob

# Man, 19, arrested over fake job scam, victims cheated of \$14,000 in total

**Reports by ELIZABETH LAW** lawsm@sph.com.sg

She thought it was a way to earn a quick buck — getting paid just to reply to texts. ed up the victim of an elaborate Internet scam

Instead of earning the \$150 to \$200 she was promised for the job, Miss would be reimbursed and the credits Lin Siew Khim, 21, was left saddled would be erased," she said. with a \$1,100 phone bill.

She is one of more than 20 people **DELETED** - most of them students - who fell When she called him to sort out the prey to a 19-year-old con man.

will be charged today with cheating. line accounts had been deleted. Two weeks ago, Miss Lin saw an

advertisement on Carousell, a local online marketplace, for two days of work. All that was needed was a Sing- Carousell, which suspended it. But tel mobile phone line with monthly the con man quickly set up another billing.

Miss Lin was told she just had to in gaming credits, which could be people," Miss Lin said. used in online games like Maple Story, League of Legends, and on popular gaming platform, Steam.

its asking to confirm if she was buy- still try to work and pay off my debts She replied yes, and was sent an- Lin said.

other text message with a security Another victim, who wanted to be code that was to be activated on the known only as Mr Wong, said he saw gaming website.

"The guy (who put up the job list- page on Oct 31. ing) said I just had to take a screenshot He had previously found work on and send it to him, which I did," Miss the page, serving at a banquet and Lin told The New Paper yesterday.

This went on 11 more times, result- the ad was legitimate. ing credits.

She said: "As I was replying to these messages, I kept having a bad feeling that I could be cheated, because it's happened to me before on Carousell, but I didn't think too much about it.' The next day, a Singtel represent-But less than 12 hours later, she end- ative called and told her she had chalked up a \$1,100 mobile phone bill. "I was shocked because the man

who offered me the job told me I

situation, his mobile phone was off He was arrested on Monday and and he could not be reached. His on-

> Miss Lin made a police report that afternoon.

She also reported the account to account

"Whenever I saw a similar ad on TRICKED: acknowledge text messages from GX Carousell, I would report it so that Miss Lin was Credits, an online store specialising he couldn't go round cheating other scammed

She said she reported the scammer at least twice.

Two other victims contacted her – Shortly after she agreed, she re- one of whom was a 15-year-old girl. ceived a text message from GX Cred- "I thought to myself, at least I can ing more than \$100 worth of credits. But what about the young girl?" Miss

the job advertisement on a Facebook

working as an usher, so he believed

ing in a total of \$1,100 worth of gam- Mr Wong was promised \$200 for his work. But after spending \$600 on credits, the man behind the post could not be contacted.

Mr Wong also made a police report. In a news release yesterday, the police said at least 25 people had made reports of a similar nature, falling victim to elaborate "job scams" involving GX Credits.

After the victims provided their credits were then sold online.

Police estimate the man has cheated people of some \$14,000.

Working with the Commercial Affairs Department and the Technolo- ful with her online dealings, said: gy Crime Investigation Branch of the "When you think something doesn't Criminal Investigation Department, sound right, talk to your parents. Or police managed to track down the if you're unsure, do what I'm doing suspect.

He was arrested at about 2pm ment) agency."

on Monday at Kay Siang Road, just off Dempsey Road. Several mobile phones, SIM cards, bank tokens and cash amounting to \$7,500 were seized

He will be charged with cheating in court today.

Police Lian Ghim Hua, Commandmobile phone numbers and sent er of Ang Mo Kio Division: "Mem-

Miss Lin, who is now more care-

Said Assistant Commissioner of screenshots of the game codes, the bers of the public are advised to be scammer would disappear. These wary of online advertisements where deals might appear to be too good to be true. Personal information also

should not be offered to strangers." now and get a job through a (place-

# 8 1189

TNP PHOTO: JONATHAN CHOO

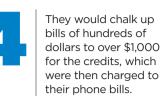
into buying

credits

via text

messages.

Victims were told they would be reimbursed for the money they spent on the credits, and they would be paid for their work via bank transfers.





When the victims tried to contact the scammer about the reimbursement, he would be unreachable and they were left saddled with the bills.

# **Other common scams**

# **SOFTWARE SCAM**

This led to some computers getting remotely controlled and used for illegal online activities.

# **INTERNET LOVE SCAM**

Con men. mostly claiming to be from the UK, target women searching for love on dating sites or

Once they befriend the victim. they correspond through e-mail or

In some cases, the scammer says he intends to visit Singapore to propose. On the stated day of arrival, he will call to say he has been detained by Customs for

carrying excess cash, and he asks the victim to transfer funds to secure his release

In other cases, the suspect will claim to send valuable items such as designer bags and watches. The victim will be asked to transfer funds to clear penalty charges on the items

### **PAYPAL E-MAIL SCAM** Scammers, who typically claim to

be located overseas, place orders with online sellers.

The scammers will send fake e-mails, usually from Paypal, notifying sellers that payment has been received. The victims will then send the items to the overseas addresses.

## **ONLINE CREDIT SCAM**

Con men convince male victims to buy gift cards or online shopping credit in exchange for a meet-up, date or sexual liaison. The scammers typically insist

the victims buy the cards from AXS machines or convenience stores before sending images of the receipts, along with the PIN, for them to claim the credit.

Victims were befriended on social media platforms such as WeChat and iAround and they communicated through online messaging and phone calls.

### **PURCHASE CARD** VIRTUAL CREDIT SCAM

Scammers gain access to a person's mobile messaging app account to impersonate him

They will send requests to buy gift cards to the account holder's friends or family members. These cards are meant for redeeming nonetary credits online.

Scammers will then ask the victim's friends and family to send messages or photos containing the redemption codes over mobile messaging apps.

They redeem all the value of the

gift cards before the victims realise their mistake

### **MULTIPLE PAYMENT ONLINE PURCHASE** SCAM

People posing as sellers ask buyers for further payments on the pretext of mistaken delivery orders. Victims typically accede to the request, but do not receive the items

The payments made by the victims are quickly transferred out of local bank accounts to overseas accounts, making it difficult to trace and get back the stolen funds.

## **CYBER EXTORTION**

In typical cases, a female scammer befriends her victim, usually male. The scammer coaxes the victim into undressing and performing indecent acts in front of a webcam.

The scammer video records the act and blackmails the victim.



