Beware of Beijing scammers

HACKING

Australians tricked into paying thousands by 'sextortion' con

Claire Bickers, News Corp Australia Network
October 5, 2018 2:12pm
Subscriber only

EXCLUSIVE

SCAMMERS have tricked Australians into paying thousands of dollars with a “sextortion” con that threatens to expose footage of them watching pornography online if they don’t fork out.

A “well-renowned” Australian author and business leaders are among those who have been targeted so far by the email scam, in which fraudsters claim to have hacked an individual’s device and recorded footage of them watching pornography.

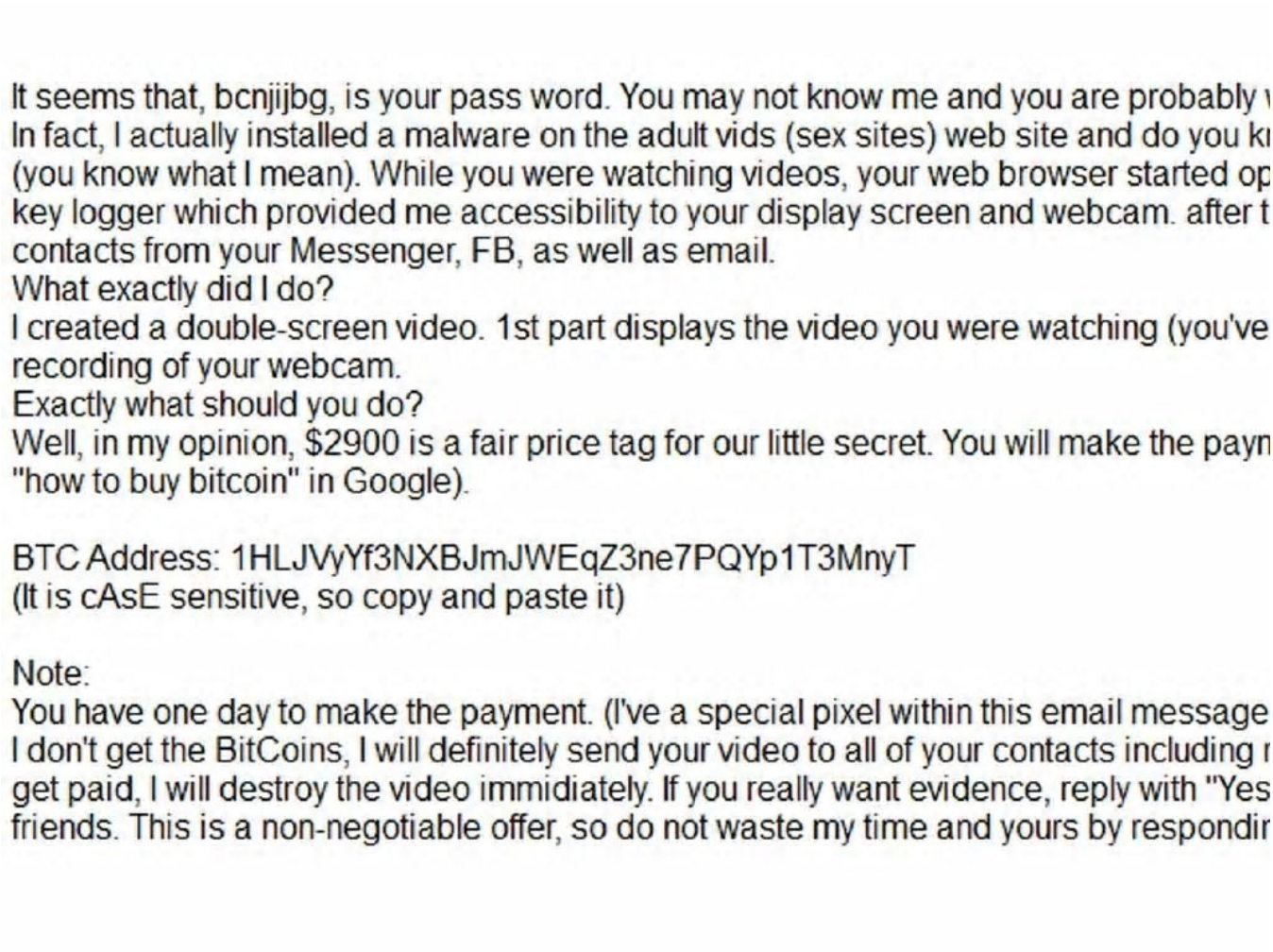
In a twist on an old phishing scam which makes the new con frighteningly realistic, the fraudsters appear to prove their threat by sending victims one of their current or old passwords.

Dozens of Aussies have been targeted in the sophisticated scam.

Cyber security expect Michael Connory has had a dozen people contact his firm Security In Depth since July about the scam, including “CEOs” and a

“well-renowned Australian author who has written a considerable number of books”.

The individuals were sent emails demanding between $2900 and $5000 to be paid within 24 hours via digital currency bitcoin or a video of them doing “nasty things” would be sent to all of their email and Facebook contacts.



It seems that, bcnjijbg, is your pass word. You may not know me and you are probably
In fact, I actually installed a malware on the adult vids (sex sites) web site and do you k
(you know what I mean). While you were watching videos, your web browser started op
key logger which provided me accessibility to your display screen and webcam. after t
contacts from your Messenger, FB, as well as email.
What exactly did I do?
I created a double-screen video. 1st part displays the video you were watching (you've
recording of your webcam.
Exactly what should you do?
Well, in my opinion, $2900 is a fair price tag for our little secret. You will make the payn
"how to buy bitcoin" in Google).

BTC Address: 1HLJVyYf3NXBJmJWEqZ3ne7PQYp1T3MnyT
(It is cAsE sensitive, so copy and paste it)

Note:
You have one day to make the payment. (I've a special pixel within this email message
I don't get the BitCoins, I will definitely send your video to all of your contacts including
get paid, I will destroy the video immidiately. If you really want evidence, reply with "Yes
friends. This is a non-negotiable offer, so do not waste my time and yours by respondir

A sample of the email being sent by scammers.

One version reads: “While you were watching videos, your web browser started operating as a RDP (Remote Control Desktop) having a key logger which provided me accessibility to your display screen and webcam. After that, my software program collected every one of your contacts from your Messenger, [Facebook], as well as email. What exactly did I do?

Several people targeted in the sophisticated scam have paid up.

“I created a double-screen video. [First] part displays the video you were watching (you’ve got a fine taste omg), and next part displays the recording of your webcam.”

“Exactly what should you do? Well, in my opinion, $2900 is a fair price tag for our little secret.”

Mr Connory knows of at least three people who have paid up.

The ACCC and the eSafety Commission are warning Australians about the scam, urging them: “Do not pay any money or give in to other demands.”

“Because it’s got your password in the header, because they’ve addressed it directly to you and because the English is relatively good, it freaks a lot of people out,” Mr Connory told News Corp.

The scam is a “timely reminder” for Australians to update their passwords regularly.

He said one victim was extremely concerned when they called him because the scammers had obtained a password which was also used his bank account and “a whole range of things”.

Authorities are warning victims world-wide not to pay the ransom as they believe the passwords have been obtained by cyber criminals who purchased a database of stolen email addresses and passwords from hackers on the dark web.

Mr Connory said it was “very easy” for criminals to buy a hacked database. A database with about 100,000 emails and passwords could be purchased for 20 cents to $20 per record. If just 40 people paid the ransom, the criminals could make a “significant” profit, he said.

Reports of the scam first emerged in July.

Authorities are warning victims across the globe not to pay the ransom.

The Australian Competition and Consumer Commission and The Office of the eSafety Commissioner have confirmed they have received reports about the scam.

“It’s important for Australians to know that if they receive this email, it is a scam that may have scraped accurate passwords, but it is highly unlikely the scammer has intimate footage of the victim – do not pay any money or give in to other demands,” eSafety Commissioner Julie Inman Grant told News Corp.

“Although the passwords may be accurate, we’ve encountered no evidence that any person’s device has been hacked, or that the perpetrator has any intimate footage or details of their contacts.

“The disclosed password has likely been collected from previous data leaks – and demonstrates the level of targeted sophistication perpetrators behind sextortion scams are using to legitimise their demands.”

The Commissioner said the scam was a “timely reminder” for Australians to update their passwords regularly.

Mr Connory also warns that thousands of Australian companies are leaving themselves open to cyber attacks.

Research by Security in Depth shows 47 per cent of companies do not offer their staff training on cyber security threats and just 17 per cent of companies are prepared for a data breach.

Originally published as Porn scammers targeting Aussies