

Victims of a scam - on Facebook!

[Send to a friend](#) [Print](#)

Like millions of others, Natasha thought her Facebook presence was harmless enough - until her account was hacked.



Natasha Cann, 32

Clicking through the pictures on the screen, I smiled when I saw the beautiful bride. Thank God for Facebook, I thought. It was September 7, 2009, and I was on Facebook looking through photos of a friend's wedding. She lived overseas and I couldn't make it to her big day. But at least I could look at her pics.

After spending an hour online, I logged off and got started on my Sunday chores. At 8pm, I was about to settle into bed with a magazine when I was interrupted by a phone call.

'Are you okay?' my friend Sam* bellowed down the line. 'You

didn't tell me you were in London!

'What?' I replied, confused. 'I'm not in London.'

'Well that's what it says on your Facebook page. I got a message from you saying you'd been assaulted and robbed at gunpoint and urgently needed money to get home. You've put your bank-account details on there and everything.'

'What?' I stuttered, feeling overwhelmed. 'No, that didn't happen. Someone must have hacked into my account.'

'Are you on Facebook now?' Sam asked.

'No,' I said.

'Then I must be chatting to someone posing as you.'

Reassuring Sam I was fine, I hung up and immediately tried logging onto Facebook.

'Damn it,' I muttered as my password was rejected. 'Why can't I get on?'

I called my friend Lisa* and got her login details. Using her account to sign in, I clicked onto my profile page. Sure enough, it was full of messages from friends asking if I was okay.

My account has been hacked. This is a scam, I posted.

Sighing, I was glad I'd put a stop to the hackers' plans and hoped all my friends would see the message. But as soon as my message came up it was deleted. 'No!' I cried, as the hackers also blocked Lisa's account so I couldn't see my profile.

I started panicking, knowing I needed to get the message out to my friends that I was fine. I didn't want any of them putting their money in this bank account, which clearly had nothing to do with me.

I had 400 friends on Facebook and most lived overseas. I didn't have a lot of their phone numbers.

So I logged onto my Twitter page and posted a status update. My Facebook account has been hacked, I wrote. Don't send any money.

Then I started ringing the friends whose numbers I did have to tell them what had happened. I also logged a complaint with Facebook, saying my account had been compromised and I wanted it shut down.

All through the night I got calls from friends asking if I was all right. I felt so guilty for worrying everyone. 'Just make sure no-one puts money into that account,' I told them.

It was scary to know there was someone out there preying on my friends' good nature.

Waking up the next morning, I tried again to log onto my account. But it was still blocked. Suddenly, I got another call. 'Thank God I got in contact,' my friend Paul* said. 'I saw your message on Facebook and sent you money. Do you need more?'

'Oh no,' I said, upset. I thought I'd told everyone about the scam. 'How much did you send?' I asked hesitantly.

'\$1000,' he answered.

I gulped. Even though I'd done nothing wrong, I still felt horribly guilty. 'I'll get your money back,' I replied, explaining about the hackers.

Paul was really good about it but I could tell he was annoyed. 'At least you're okay,' he sighed.

After talking to him I called the police who transferred me to their cyber-crime squad.

'Unfortunately there's nothing we can do,' an officer said. 'This happens all the time and the hackers would have collected the money by now.'

'But how did it happen?' I asked. The officer explained the hackers use software that puts random passwords into your account until they get a match. 'These people are very hard to track,' he said.

He told me that in future, I should change my password every month and only use one computer to log on.

'I'm so sorry Paul,' I said when I told him the bad news.

'Never mind,' he sighed. 'I've learnt a valuable lesson from all this.'

Today, it's been three months since the scam and despite all that has happened, I still have a Facebook account.

I think it's a great way to stay in contact with friends. It's only these criminals who ruin the experience. And while I never found out who hacked into my account, I did get to see how much my friends care for me. If I do ever need their help though, they now know I'll be phoning them.

HOW TO STAY SAFE ONLINE

Detective Inspector Brian Hay from the Qld Police Fraud Squad has these tips to stay safe online.

1. Never give out too much information. If you use a social-networking site such as Facebook, don't give your full name. Just use initials or a nickname - and don't enter your date of birth.
2. Change passwords every month and only use one computer to log onto your accounts.
3. Discriminate - don't let everyone be your friend on Facebook and don't open emails from people you don't know.
4. Ensure your accounts are on the highest privacy settings.
5. The sure-fire way to spot a scam is when someone overseas

requests cash be sent to them. If this happens to you, call your local police station and they can put you in contact with your state's computer-crime unit.

COMMON CYBER CONS



BANK SURVEY EMAILS

You receive an email that looks like it's from your bank asking you to complete a survey. For this you need to put in your account details and password and it says you'll be paid for your time. Of course you won't. Instead, money will be stolen from your account.



FAKE LOTTERY

You receive an email saying you've won a large sum of money in a lottery you haven't entered. But to receive the payment you must first pay an admin fee to get the money released.



ONLINE ROMANCE

A person, usually from overseas or who can't speak English well, befriends you online and starts up a relationship. They'll then ask for money to be sent to an overseas location because they find themselves in some kind of trouble.

Find out more on how to stay safe online with our tips - [CLICK HERE](#).

Have you been a victim of an online scam? Let us know by leaving a comment below.