ACT Policing

Virtual Kidnapping Scam

ACT Policing guide to identify and protect from virtual kidnapping scams

What is Virtual Kidnapping?

Virtual kidnapping is a new and emerging scam, often targeting international students. Scammers will contact the victim by phone and typically impersonate a person in authority such as a police officer or government agency representative, often from their home country.

Scammers will advise the victim they have been identified as being involved in a crime and the call will be transferred to 'police', who are also part of the scam. Scammers may seek to appear genuine by knowing things about the victim and sending pictures of fake documents like an arrest warrant with the victim's name included. Scammers may also use phone
numbers linked with a Government agency. Scammers will require the victim to use online communication platforms to communicate, such as 'Skype' and 'WeChat' among others.

Scammers will eventually demand money be paid via online banking transfer, with threats accompanying the demands. The threats may include things like being arrested, having assets frozen, and/or deportation from Australia.

As the scam escalates, scammers will tell the victim to leave their home, university, friends and life. They will have the person withdraw cash and remove the SIM cards from their mobile
telephone to make the victim isolated. Scammers will provide advice to the victim on how to obtain funds, which usually involves having the victim stage their own (fake) kidnapping.

Once the victim is under the control of the scammer, the scammer will take control of the victim's social media accounts. They will then contact the victim's family advising of their
kidnapping. A ransom is then demanded to secure the release
of the victim and the victim is made to do things like taking photos to provide the appearance of a kidnapping. This can occurs usually without the victim ever meeting any third party or being kidnapped.

How to spot a scam?

Identifying a scam may be difficult to spot initially. Scammers may:

- Use technology to disguise what phone number they're using, appearing to call from and be contactable on an official phone number
- Pretend to be from an organisation or agency that is common or well known to use personal information
- Use information previously provided by you to obtain further information
- Ask you to download or use other communication platforms other than traditional telephone calls
- Inform you that you have been identified in criminal activity and that payment will need to be made
- Inform you the investigation is confidential and not to attend a police station
- Request you remove SIM cards, turn GPS off and distance yourself from friends and family
- Requesting to meet at a hotel

What you should NEVER do:

- Never make a bank transfer or payment to anyone , unless you have confirmed the person is who they say they are
- Never share information about yourself or others unless you know for certain who you are dealing with
- Never leave your camera on, tell someone where you are, or take photos or videos of yourself if asked by someone you don't know

What you SHOULD do:

- Check if the call is real or not by hanging up and calling the organisation they are claiming to be from. Use contact details you have found yourself. Do not use contact details provided to you by the caller
- If you're unsure or are being threatened by a caller, hang up the phone
- Report suspicious behaviour to police and Scam Watch
- Speak to friends and family about the incident for support
- Speak to your university for support
- Contact your Embassy or Consulate Office for advice

Need help?

For police assistance in the ACT you can call 24 hours, seven days a week, on 131 444 or go to your nearest police station. If it is a life threatening situation, telephone 000.

To report a scam, visit Scam Watch
www.scamwatch.gov.au/report-a-scam

ACT Policing

虚拟绑架骗局

澳大利亚首都直辖区警务指南：识别和防范虚拟绑架

什么是虚拟绑架？

虚拟绑架是一种新出现的骗局，通常以留学生为目标。骗子会通过电话联系受害人，通常会冒充警官或政府机构代表等权威人士，这些人通常来自受害人的祖国。

骗子会告知受害人他们已被确认参与犯罪，电话将被转接给 “警方”，而 “警方 “也是骗局的一部分。骗子可能会声称了解受害者的情况和发送伪造文件的图片（如包含受害者姓名的逮捕令） 以达到以假乱真的目的。骗子还可能使用与政府机构关联的电话号码。骗子会要求受害人使用网上通信平台进行交流，如 “Skype “ 和 “ 微信” 等。

骗子最终会要求通过网上银行转账付款，还会进行威胁。威胁内容可能包括被逮捕、资产被冻结和/或被驱逐出澳大利亚等。

随着骗局的升级，骗子会让受害者离开家、大学、朋友和生活。他们会让受害人提取现金，拔掉手机 SIM 卡，使受害人与世隔
绝。骗子会向受害人提供如何获得资金的建议，通常包括让受害人自己实施（虚假）绑架。

一旦受害者被骗子控制，骗子就会控制受害者的社交媒体账户。然后，他们会联系受害人的家人，告知他们受害人被绑架的消息。然后索要赎金，以确保受害人获释。受害人会被强迫做一些事情，比如拍照，以制造绑架的假象。受害人通常不会遇到任何第三方，也不会被绑架。

如何识别骗局？

识别骗局最初可能很难。骗子可能会：

- 利用技术手段掩盖他们使用的电话号码，让人以为他们是用官方电话号码拨打电话的，并且可以通过官方电话号码联系到他们
- 伪装成某个组织或机构的人员，而该组织或机构通常或众所周知是会使用个人信息的
- 利用你之前提供的信息获取更多信息
- 要求你下载或使用传统电话以外的其他通信平台
- 通知你，已确认你参与了犯罪活动并且需要付款
- 通知你，调查是保密的，不要去警察局
- 要求你拔掉 SIM 卡、关闭 GPS 并远离朋友和家人
- 要求在酒店会面

绝对不能做的事

- 切勿向任何人进行银行转账或付款，除你已确认对方的真实身份
- 切勿分享有关你自己或他人的信息，除非你确定与你打交道的人是谁
- 如果有不认识的人提出要求，切勿打开手机的相机、不要告诉别人你的位置或拍摄自己的照片或视频

你应该做的事

- 挂断电话并致电他们自称的组织，以确认电话是否真实。使用你自己找到的联系方式。不要使用来电者提供给你的联系方式
- 如果你不确定或受到来电者的威胁，请挂断电话
- 向警方和 “反诈骗中心 **(Scam Watch)**” 报告可疑行为
- 向朋友和家人讲述事件，寻求支持
- 告诉你就读的大学，寻求支持
- 请联系你本国的大使馆或领事馆以获取建议。

你需要帮助吗？

在澳大利亚首都直辖区，你可以每周 7 天、每天 24 小时拨
打 131 444 或前往最近的警察局寻求警方帮助。如果情况危及生命，请拨打 000。

如需举报诈骗，请访问反诈骗中心（Scam Watch）
www.scamwatch.gov.au/report-a-scam