CHAPTER VII

Virtual Kidnapping: An Emerging Threat

"Authored By - Shagun Singh"

- **INTRODUCTION:**

With an ever-increasing growth in science and technology, our reliance on the internet and the various features that it offers is increasing and undoubtedly it is going to grow more and more indispensable. Our dependence on the internet and technology is justified because of the reason that is created for fulfilling our needs and making our lives easygoing. But we never know when that ease could turn out to be a havoc to our security and dignity. Internet these days is no safer and instead of most of the precautions that are available to us, we fall prey to such crimes which occur over the internet.

Cybercrimes are a threat to our digital identity and our sources and resources that we use in our daily lives. Crimes over the internet are collectively known as cybercrimes and the internet is flooded with such crime. To name a few, phishing, identity theft, hacking, spoofing, email junk, distributing child pornography, cyber scams, account theft, etc. Virtual kidnapping is one such cybercrime which is becoming a major threat and is a burning issue in most parts of the world. Unlike traditional kidnappers, these virtual kidnappers do not actually kidnap the victim but rather fake it and make the other people believe that they are being kidnapped.

- **MEANING:**

Virtual kidnapping may be defined as an act of extortion in which a person is made to be believed to be kidnapped or abducted by the kidnapper and in return, a ransom amount is claimed for setting free the kidnapped or abducted person, whereas in reality no such person has actually been kidnapped. Usually, the identity a person is used which involves calling from the mobile number of the person and a threated call is made to the family or relatives that the person has been kidnapped/abducted and if the ransom amount is not being paid, the victim may be hurt or killed.

There is no such a precise definition of virtual definition but attempts have been made by various organisations and sources to describe it. To name a few: Pcmag.com defines virtual kidnapping as an extortion scheme wherein people receive phone class telling them that their loved one has been kidnapped and will be killed or harmed if they do not immediately go to the bank and wire money. They may be fake crying in the background, but the kidnapped victims are not allowed to speak, and the call is never made from their phones.

Ahtins.com defines virtual kidnapping as an act where no victim is actually abducted or kidnapped during a virtual kidnapping but ransom amounts are being demanded and paid by the distraught family members or others, typically through wire transfer.

- **BACKGROUND:**

Though the number of cases of virtual kidnapping has suddenly hit a rise in the graph, the crime has been prevalent since the last two to three decades. Virtual

kidnapping is developing and changing for the past five years and is prevalent in most of the developed nations including Mexico, Latin America, the United States of America, China, and more seriously in Australia.

The original method followed by the kidnappers is as follows: a thousand of people are randomly called. Upon connecting with them, the extortionist makes the person called believed that their loved ones have been kidnapped or abducted and that now they are a victim to him. They would fake the sound of the victim and would even send them videos of the victim being tied and wrapped in tapes and being caged and tortured but those photographs and videos are extracted from the victim itself beforehand in the name of they being a government agency and that they are being held for a crime and that they have to send photos and videos of themselves being caught and held. Without allowing any verification, the caller would claim that they were in possession of a loved one before demanding a relatively small ransom for their safe release with a short deadline to pay the required amount.

In a concerning evolution of the crime, 'kidnappers' now use the initial phone call to coerce their victim into simulating their own kidnap. Victims answer the phone, only to be threatened that they are being shadowed by someone who will kill them unless they follow instructions. The victim is directed to a private place to pose for photographs that simulate their own imprisonment before these are sent to family members as proof of capture. The same process is then followed, keeping the victim on the phone so they cannot be contacted until the 'ransom' is received. The term 'virtual kidnap' is perhaps a misnomer - it is much better understood as a traditional form of extortion. Knowing this, it is important to consider what

makes this organised extortion scam effective. In its present form – self-isolation – its success is largely predicated on the victim's fear of dangers within the place they are presently operating; travelers or contractors working away from home are the usual targets.

- **RISE IN THE NUMBER OF CASES:**

In the past few five to ten years, the number of virtual kidnapping scams have reached a new record. The numbers are increasing at a much faster rate and they are posing a serious threat over for security purposes. This threat is spreading widely in the U.S., Australia, Mexico, and many other nations. FBI has even warned the people of the nation about its seriousness and has raised guidelines for creating awareness among the people. The cases were once limited to Mexico and Southwest nations, but now it has reached the U.S., warned the FBI.

Between 2013 and 2015, investigators in the FBI's Los Angeles Division were tracking virtual kidnapping calls from Mexico—almost all of these schemes originate from within Mexican prisons. The calls targeted specific individuals who were Spanish speakers. A majority of the victims were from the Los Angeles and Houston areas.

"In 2015, the calls started coming in English," said FBI Los Angeles Special Agent Erik Arbuthnot, "and something else happened: The criminals were no longer targeting specific individuals, such as doctors or just Spanish speakers. Now they were choosing various cities and cold-calling hundreds of numbers until innocent people fell for the scheme." In that year only, the investigation into the cases revealed that the total victims were around 80 in number and that the net ransom amount extracted was

around $87,000.

- **CURRENT SITUATION IN AUSTRALIA:**

The concern and attention have now being shifted to Australia when suddenly it was examined that the International students, basically Chinese have been held a victim of the virtual kidnapping scam. The cases have been recorded since May and the number is constantly increasing. Anonymous criminals seek to contact the parents of the students in China and demand for ransom money in the name of the threat that their child living out there in Australia has been held and is under their custody. The police in New South Wales has confirmed that there have been eight confirmed cases this year, with more than $2 million dollars being paid in ransom for abductions that never happened.

"The victims of virtual kidnappings we have engaged are traumatized by what has occurred, believing they have placed themselves, and their loved ones, in real danger," said Peter Thurtell, the assistant commissioner of the New South Wales police force.

The recent spree points to the evolution of a crime that exploits oversharing and fear for a distant loved one with digital savvy and old-fashioned coercion by con artists. Since the last 1990s, criminal gangs from Taiwan and China to Mexico and Cuba have been persuading families to pay ransom for simulated kidnappings, often with personal information provided intentionally or unintentionally by the victims.

Last year, extortionist called hotel rooms on the American side of the U.S.-Mexico border and convinced guests that armed enforcers were nearby and that they

needed to drive across the border and switch to a Mexican hotel, where they had to take a screenshot of themselves that the criminals then used to persuade loved ones to pay a ransom. There were 1,172 cases reported of what police calls "Chinese Authority" phone scams across Australia.

In the Sydney form of the scam, which the authorities said they first started seeing a few years ago, rob calls deliver messages to thousands of random phones purporting to be from a messenger service. It says a package needs to be delivered. Those who continue on the call are greeted by someone speaking Mandarin who asks for basic identity information — name, address, phone number, anything else of import — and promises to call back.

In one recent case from Sydney, a family paid 2 million Australian dollars in this case where their daughter was held to be a victim of virtual kidnapping.

- **GUIDELINES FOR THE PREVENTION OF VIRTUAL KIDNAPPING:**

FBI and various other agencies have issued guidelines to create awareness among the masses and to protect the people from falling into the prey of this cam. Some of the important guidelines are as follows:

1. **Contact the victim**: in cases like these, people go restless and they do not try to look at the other side of the story. In that case, the first thing to do is to call the victim and make sure of their current situation. In this way, complexities can be avoided.
2. **Report it**: as soon as one figures out that the call is a scam, one must immediately report it and bring it to the

notice of the authorities.

3. **Have a secret family code:** when such calls are made, try asking the kidnapper about the code or some sort of question. In that way, you can trick the kidnapper and get to confirm that about the scam. Scams like this fail as soon as they would be target realizes that their loved ones are safe.
4. **Trick them:** this is one effective method to slow and hunt them down. Tell them that you are busy, ask them to call back in a while, or give a callback or you can keep them talking too.
5. **Warn them that you know it is a scam call:** this thing would itself make the hunter into prey.

• • •