Dr. Djalila Rahali
Clinical CyberPsychologist/ Researcher in cyberdelinquency , cybercriminality and cyberaddictions-
Ex Minister's advisor in e-communication / Consultant, trainer & Coach / Author and speaker
Global Goodwill Ambassador- TOP TEN 2018 of personalities contributing to the development of ICT & digitalization in her country (Algeria)
Email: fd.rahali@hotmail.com / LinkedIn: drrahalidjalila / Twitter:@Rahali_CybPsy / Website: http://www.rakm-conseil.com/equipe.php

TITLE:
How to detect psychological online NeuroPiracy used in "sextorsion" and "Online Romance Scam"?

Let us begin with a true story: Sarah was 60 when I first met her. She was a divorced pediatric surgeon living alone. A year ago, she came to me in tears asking for help in a shocking situation she couldn't understand. In fact, she virtually met an old French friend on Facebook she didn't see since university. He contacted her first and sent her some of his photos. He was an attractive man. A couple of days later he avowed her his feelings and she couldn't resist his charm and felt in love with him. It took just some hours since they became exchanging hot messages then had an intimate virtual relationship by exchanging intimate photos. At this point, another scenario began when the French man asked her money to help him, pretending he is visiting an African country (Congo). and his money has been stolen from his hotel. She effectively sent him 800 Euro. Then, a week after, he introduced his son to her then asked her to help him buying a beautiful birthday gift for his unique son who is settled in Congo. He pretended that he couldn't send money from France because his banking account was blocked by error. When she gently refused, he threatened if she doesn't send the money, he will publish her photos on Facebook. She was so chocked by the threatening message that she came to me saying: "If he does, I will kill myself". I knew she was not joking. Trapped in what we call "sextorsion" after being a victim of "Online Romance Scam" she went through a severe depression. In this article, we will see together how scammers act to manipulate vulnerable persons by love and I will give some elements that help everyone to detect a attempt of romance scamming or of a sextorsion.

Online Romance Scam and Social Engineering:

Criminologists and cybersecurity agents know that Online Romance Scam is one of the multitude techniques of Social engineering. The latter is a concept widely publicized and adopted by several disciplines such as management, sociology and even politics (political technology). In psychology, social engineering is a practice using techniques of psychological manipulation of the mind to harm or to heal a human. But by linking cybersecurity to psychology, social engineering can only refer to subversive psychological manipulation to obtain secret and delicate information whose purposes range from easy money gain to mere revenge.

The Online Romance Scams are ones of the most harmful cybercrimes as they cause big emotional damages as well as great financial loss. The cybervictims find themselves involved in love relationships where scammers hack their brains using a special cognitive process. The unbelievable love story Sarah had was a case from a million. The human behind the screen was a person who have usurp her friend's identity and used personal affinities and common values as empathy, altruism, compassion to nurture her romantic imagination to take control of her mind.

But, are all people vulnerable to this kind of scams?

This question takes us to profiling not only cybervictims but also cyberscammers. In fact, it has be proven the targeted persons, using online romance scam, are those who are vulnerable being lonely (divorced, widowed, elders..) looking for consideration, companionship and specially looking for deep and eternal love. Persons having good jobs and good social positions, presumed to be rich (i.e. doctors, industrials, engineers working for big companies, CEOs etc.), are targeted too but specially using the sextorsion method. The cybercriminal threaten his victim, who was looking specially for fun and sex pleasure when making relationships through the internet and specially on dating websites,

Before knowing the real objectives of her presumed lover, the cybervictim uses to develop a strong and dangerous attachment towards him/her. Encouraged to online intimacy the scammer uses the power of fantasmatic representations. At the point that the victim makes the mistake when sending photos or videos showing her in indecent image or posture, he reveals his true intention: having money or touching his victim's social reputation. But at this level, what the victim doesn't know is that this the scammers is just a member of a group organized to commit cybercrims.

These groups are often living in some African countries like Nigeria, Congo and Ivory Coast but can also be cyber delinquents from any country acting in a single way. For some they can be even students in colleges, cyberbullying their classmates and cyber blackmailing them using the Online Romance Scam. Thus, the nature of scammer's profile can be known only by analyzing his modus operandi, the words he uses, the way he talked about feelings and love, the way he writes (grammar, vocabulary which are generally poor).

Photo: Nigerian organized cybercriminals caught by Nigerian authorities

The power of the words:

I define psychological neuropiracy as a process through which a human mind is hacked till the loss of control in reasoning and feelings. Thus, the manipulated person becomes totally blinded by the emotions that the scammer anchors in her mental system. It is known that in the social engineering type attacks, words (said, written or symbolized) are the keys for perpetrating an intrusion into the human's neurological system as social language is the most important tool for the human being. Thus, in a received romantic message the scammer use impactful words. He anchors convincing representations in a context built on an irreproachable logic..

At a high level we can see that the mind intrusion uses the same elements as what is described in the book The ***Art Of War***, attributed to the ancient Chinese military strategist Sun Tzu in the 5th Century BC. Consequently, the social engineer uses to lure the victim by developing a whole ***stratagem*** after ***collecting information*** on her and then ***infiltrates*** her brain by a story rising from all sides. In this case, he may steal the identity of a person and may misuse stolen facts. At the last step, the offender may ***manipulate*** his target but does it only after establishing trust and confidence dispelling any mistrust by circumventing and destroying all his victim's defense mechanisms. At last, the cybercrime is operated ***furtively*** in a process of a ***jamming*** in the target's memories trail. Unlocking the target's system of logical reasoning is, in consequence, done by ***swarming*** his attention to diminish his vigilance until its annihilation.

Here is a model any person can use to detect rapidly if the person besides the screen is a real person or an online scammer.

The basic elements to detect a scamming temptation:

Any internet user should be very careful when meeting people in the virtual world. In private messages the main elements that should be looked at carefully are the following elements:

-1-Incredible virtual meeting (the first virtual contact)
-2-Incredible common things (values, hobbies, social position, bad..),
-3-The use of soft pressure and high one to make the victim feel guilty,
-4-Repeated demands of news about all the members of the family, one by one.
-5-The existence of a help offer then a request for help,
-6-Discussion about financial situation that is drawn by the scammer as a very bad.
-7-The repetition of divinity quotation (i.e. God Bless you, God Bless your family and protect you..),
-8-Repetitions of the same words and groups of words,
-9-Presence online all the day and sometimes disappear a couple of days and come back with a logical scenario.
-10-Many photos sent, personal and family ones .

Etc.

So, it is the prevalence of all these details in one person's text that should incite doubts and make any internet user very aware about what he should say and what he should do to verify the identity of the virtual person he is dealing with, this in one hand. In the other hand, the material received as videos, photos, pictures and audio file should be well seen to detect any anomaly in them and to detect the incongruent element in the story.

The power of image and sound on perception:

Social engineers (scammers) use generally the power of images and sounds by stealing other persons' identity on social networks. They copy fully their profile with personal and family photos, videos etc. They may make

changes on the collected photos using PhotoShop as well as audio software to cut of voice sequence, this to nest them in the scamming scenario. And here, the "(...), reality does not matter. Only perception counts, " as Yasmina Reza said in her book" (Dawn Dusk or Night). This is what adapts to the reality in the virtual world where the offender normalizes in his target's mind the wacky representations and imageries and even hallucinations. It happens that the causal relationship between the scammer and the victim is false and falsified but in the mind of the victim, it is very real one. She doesn't know that a psychological play is in the heart of the relationship as far as she maintains it with her presumed soul mate.

The Psychological play: A manipulative roles' play

To understand the psychological game that scammers use for manipulative purposes, we have to know that everything is based on roles. In fact, the online romance scammer plays a role like a movie actor. He immerses himself in the role he has created for himself than immerses his victim in the role he chooses for her according to the information he collected about her. The scammer also uses to play several roles and this according to each script he has prepared or will invent. Transactional analysis in psychology can help us understanding the psychological game in order to be able to detect it from the beginning of the story. Thus, we should see Karpman's theory. The latter speaks about three roles in any manipulation process through communication. He talked about "the dramatic triangle" with the existence of three roles in manipulation: Executioner, Savior and Victim roles.

In scenarios created by the offender, the Savior appears to assist the victim not by helping her to think and defend herself but by taking away all her energy to act in her behalf and showing her that he is the one who will do all the work at her place. The Savior role consists to show a kind superiority. He misleads the victim by creating a superhero image of himself in the victim's mind and encourages her to rely totally on him. While the Executioner, he use to attack and humiliate the victim by considering her as inferior and therefore will harass her in the virtual world. In the role of the Victim the scammer may presume being disarrayed so his target feels pity on him. He positions himself in an inferior status with regard to his target to seek his compassion and his help. He can also put his prey in the role of a Victim so that he plays the role of the Savior. He attracts her, annoys her, excites her and urges her to financially help him in some incredible scenario.

What cyberpsychology teaches us about all of these roles is the fact that they are rooted in our childhood. In the various ego states in Transactional Analysis, we have the Child Ego, the Parent Ego and the adult Ego. So those who communicate via their Child Ego are the most likely to be scammed by social engineers since they are dependents, feeling to be inferior to others and needing help and especially psychological support .

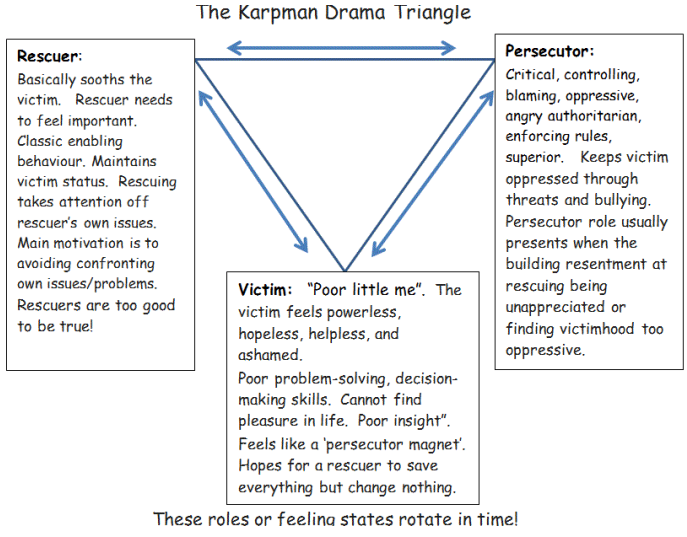

Figure1: The drama Triangle of Karpman

Important questions to detect a attempt of online romance scam by texting:

Any person who begins having feelings towards a virtual person should ask himself the following questions to be sure that he won't go through a attempt of a romance scam or sextorsion: These questions are:

- How does the other person start the relationship (incredible story, gift she wants to offer, old classmate etc.?)?
- What happens after my reaction (manifestation of a rapid falling in love?)?

- What is the hidden message the other is trying to give me (he cannot live without me/ he is searching for that greater love/ he finds me the most charming and the smartest person in the world/ he loves too much my profession, my house even my dog ?)?
- What is the secret message I want to explain him (I have some feelings towards him but still don't understand why he felt in love with me so rapidly and so deeply as he says?)?
- How does every texting conversation end each time (Makes prayers for me/ asks me to be online more often/ sends lot of special emoticons and emojiis of love, or roses bouquets/ HE tells me he cannot wait till the next conversation but never inform me about his silence periods ?)?
- How do I feel after each conversation (good/ happy/ sad/ eager to text/ more powerful when he is besides me and into my life/ better in my mind but still do not understanding the strong feelings he has for me?)?

The answers given between brackets after each question will help any person to understand which role the other wants him to play and how the roles change as the relationship develops.

How to detect fake profiles on social media platforms?

It is known that in social media, fake profiles are generally copied from true existing profiles with all their content, especially on Facebook and Linkedin. The latter has been infiltrated these last years in a more disturbing way. To recognize a fake profile anyone must verify the interactions and reactions of his/her owner as the "likes" and comments. He/she should also verify the dates and hours of all publications from the opening of the account. This because sometimes, scammers resort to the rapid filling of profiles information they use as a trap.

The suspicious profiles are generally accounts having a profile's photo showing a Caucasian woman, a very beautiful blonde who post professional applications searching for financial partnership to a presumed investment in any country or a profile used to attract men. For man's profile, the photo is this of a charming man, smiling or doing a sport, having a well built body. In the case of LinkedIn, the scammers present themselves as job/ training seekers. Furthermore, after the contact established with their victims, they begin playing the role of romance seekers and here a scenario starts where the scammer feels nothing and less guilty. But the question many ask themselves is about the feelings of a scammer when he is stealing an old woman fo exemple.

How do the scammers feel and how they perceive their act?

Social engineers using romance scam are generally very patient. This patience is one of the elements we see in the Flow state. Flow is described as the mental state of operation in which a person performing an activity is fully immersed in a feeling of energized focus, full involvement, and enjoyment in the process of the activity" (Wikipedia). This state of immersion is experienced by hackers not only them but also by all those who engage fully in any task by prioritizing it, to experience a great pleasure. Also, the flow can be experienced in the case of great dissatisfaction and the need for success to win a challenge a person has launched or has been launched out by others.

Social engineers have also **distortions in perception**. The disproportionate self-confidence they have about themselves approaches megalomania. They see themselves as smarter than al people and speciallymore intelligent than security agents and often make fun of security executives according to Raoul Chiesa's study in "Profiling Hackers" research. This perception of their super ego is also generalized on the victims they perceive as "idiots" having money they do not worth, thus, they have the right to put their hands in their pockets. Each kind of scammers has a reason that blocks the feeling of regret and remorse. They perceive their act as being a right on any race they perceive as an enemy: Blacks against whites, people of the East against the people of the West, Orientals against the West and vice versa. For example, cyber-scammers use the "neutralization of affect" factor to block guilt by rationalizing their behaviors. This leads them to feel a sense of supremacy and success in rendering a right by force. In any case of crime including those committed in cyber space, the factor of jealousy should not be forgotten in parallel with the revenge one.

Cyber scammers also present **cognitive distortions.** They believe or strive to believe that the Internet is unguarded, that they are free to do what they want (online disinhibition as John Suler described this behavior) and believe that people on the internet are all potential victims. They consider themselves heroes every time they succeed an attack. They believe that their furtiveness puts them in a state of perfect invisibility (in the majority of cases this is unfortunately true).

Scammers may be a part from an entity that employs them. Thus, they are considered as mere **employees executing the boss's orders** having a common moral contract towards the entity which employs them and

protect their act in a complete safety and in a common safe moral conscience (since it is the boss who wants and they are paid only to execute orders such as soldiers or factory employees).

Conclusion

The weakest link is the human, a fact recognized by the majority of experts in cybersecurity, so I suggest to experts and jurisprudence to go give more importance to cyberpsychology, victimology and behavioral sciences to better understand these attacks of human against the human.

Sextorsion and Online Romance Scam are both doing millions of victims and for some fragile persons they have committed suicide as the case of Amanda Todd. Fortunately, Sarah is still living after the difficult moments she went by that pushed her to the limits of depression. She is now sensitizing women in the social media platforms to be aware of such cybercrime whose perpetrators are just mercenaries of love.

January,2019