Review of Momo attack in WhatsApp

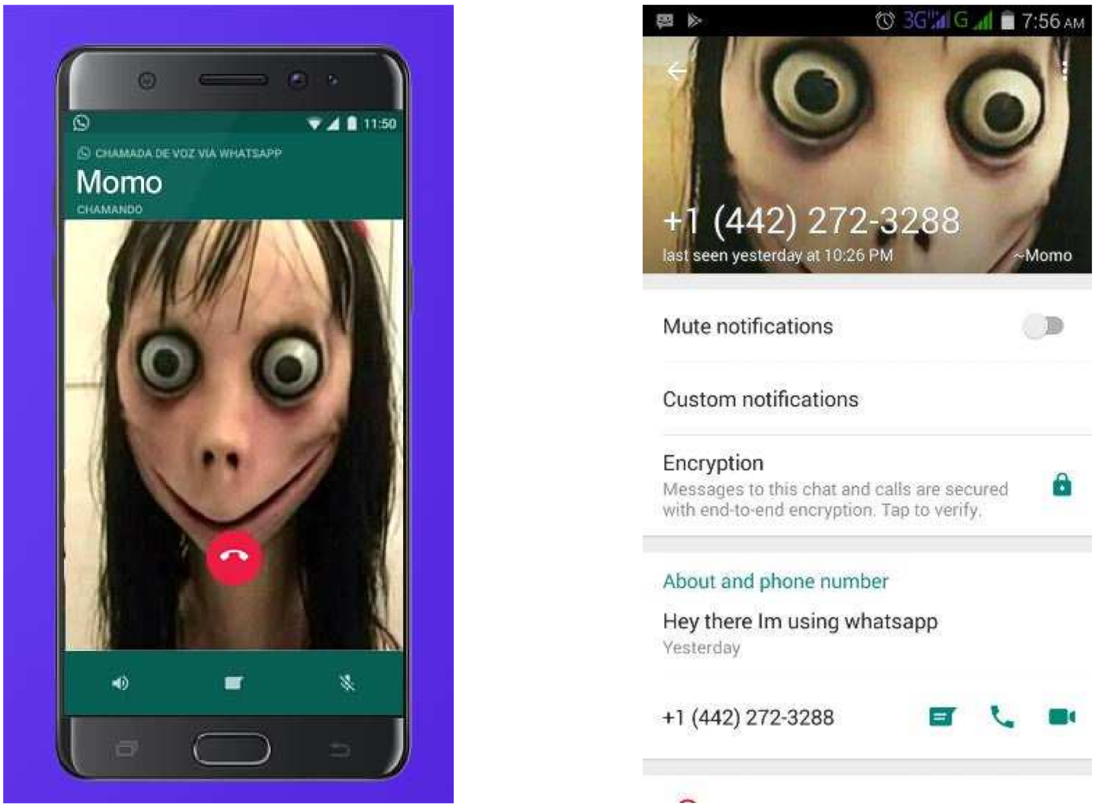
Mr. S. Manikandan
Assistant Professor & HoD, Deptartment of Information Technology
E.G.S. Pillay Engineering College, Nagapattinam, Tamil Nadu, India
manikandan@egspec.org

1. WHAT IS Momo?

Today the day to day life begins with mobile phone and 90% of peoples from the world using social media apps such as WhatsApp, Facebook, Twitter, Instagram, etc. Regular chatting and surfing at any place and sharing text, audio, image, video to others. The important of mobile usage now changed to sharing and chatting like video call, online sharing, shopping, etc. Recent days the we receive unknown message with the name of ‘Momo’ and they tell all the details of your details. So we suddenly shocked and get outdated details. Momo is not a attack and is the person already you known or unknown person creates duplicate account in the name other country person or other county numbers using mobile app and registered mobile OTP access. Normally the human minds set the unknown messages are received from WhatsApp and they shared your all the detail means we afraid and chat with Momo. Momo is not an attack it is private message or individual message from unknown number by your known person.

2. SOCIAL CHALLENGE

A recent social engineering scheme has spread across Latin America and could hit the borders of the United States. A WhatsApp contact called, “Momo WhatsApp” was posted on social media sites and has a Japanese area code and a photo displaying a bulging-eyed girl. Claims that interacting with the profile can incite youth suicide through coercion have been circulating around the Internet for days.



11:50
CHAMADA DE VOZ VIA WHATSAPP
Momo
CHAMANDO

7:56 AM
+1 (442) 272-3288
last seen yesterday at 10:26 PM
~Momo

Mute notifications

Custom notifications

Encryption
Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

About and phone number
Hey there Im using whatsapp
Yesterday

+1 (442) 272-3288

Figure 1: Mo Mo Person details

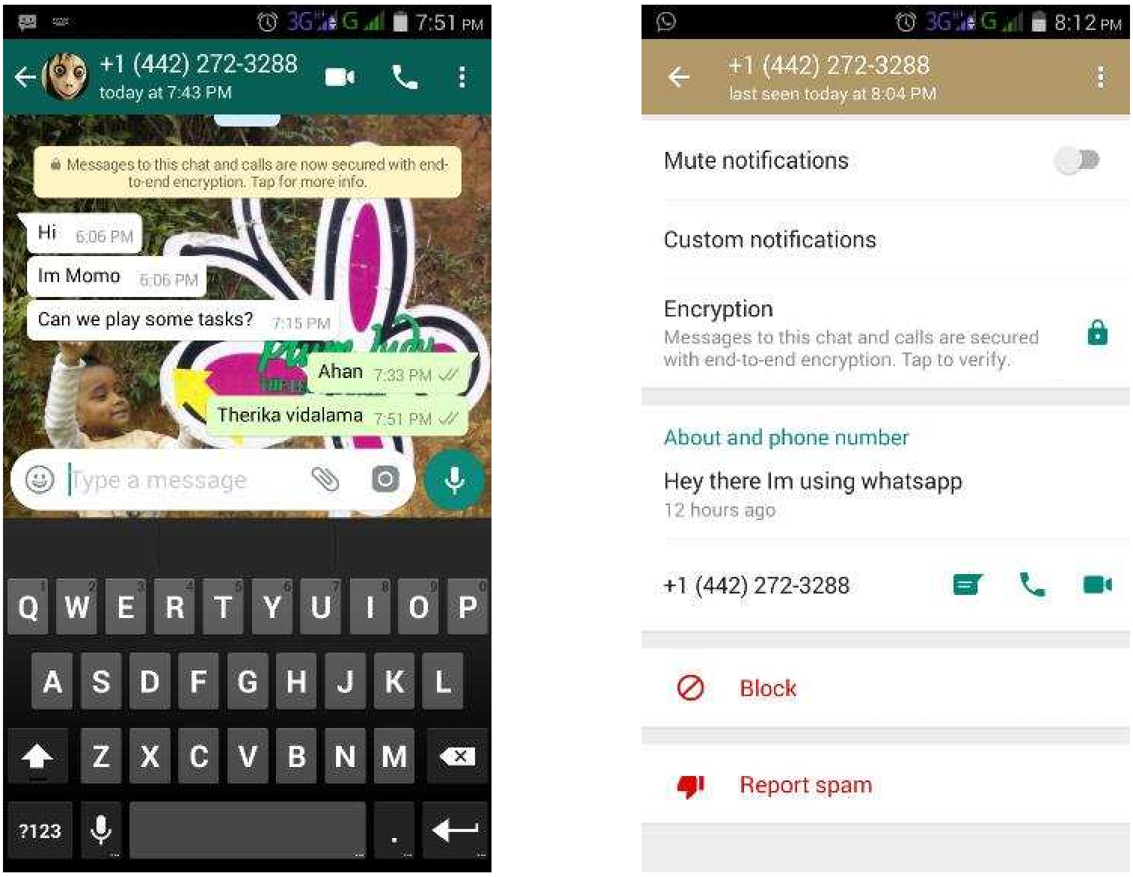
The above Figure 1. Shows that the details of Mo Mo and the number represents as other country details

Frightfully, points of interest of the Momo WhatsApp episode reverberate reports of the Blue Whale Challenge that circulated around the web in 2016, which has been bantered as a scam. Logical paranormal examiner, Ben Radford, set that the Blue Whale Challenge is a legend, propagated by the weight on experts to put forth official expressions on gossipy tidbits. Radford expresses, "Every urban legend have a component of shallow believability about them; that is the reason they are broadly shared and cautioned about."

Everything began as a dim test on a web discussion: who can make the most unnerving paranormal pictures on Photoshop? The test rapidly got on, and soon, a character of unmistakable fear was conceived. An anecdotal character, beyond any doubt, yet positively one sufficiently aggravating to put Stephen King and the Brothers Grimm bankrupt. Our security specialists at dfndr lab added the claimed Momo number to WhatsApp and got no reaction with endeavors at contact. We've verified that few profiles have developed all through the world utilizing this same photograph, so it's unrealistic to state with assurance that the maker of the first contact has made the dangers, or that they even exist. "From the minute this contact wound up viral via web-based networking media destinations, a few terrible performing artists are exploiting the dread and making new profiles to startle individuals, additionally expanding alert and empowering activities that could prompt damage," cautions the chief of dfndr lab, Emílio Simoni.

3. MO MO CHAT DETAILS WITH MY CONTACT

I received message from the unknown number to my whatsapp and following are screenshot for chatting information


+1 (442) 272-3288
today at 7:43 PM

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

Hi 6:06 PM

Im Momo 6:06 PM

Can we play some tasks? 7:15 PM

Ahan 7:33 PM

Therika vidalama 7:51 PM

+1 (442) 272-3288
last seen today at 8:04 PM

Mute notifications

Custom notifications

Encryption
Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

About and phone number
Hey there Im using whatsapp
12 hours ago

+1 (442) 272-3288

Block

Report spam

Figure 2: First Chat Details and Contact Information

The above figure 2 shows that the first message received from unknown number and I replied as normal chat and verified by using true caller apps it shows information as the unknown number are registered as other than Indian country contest.

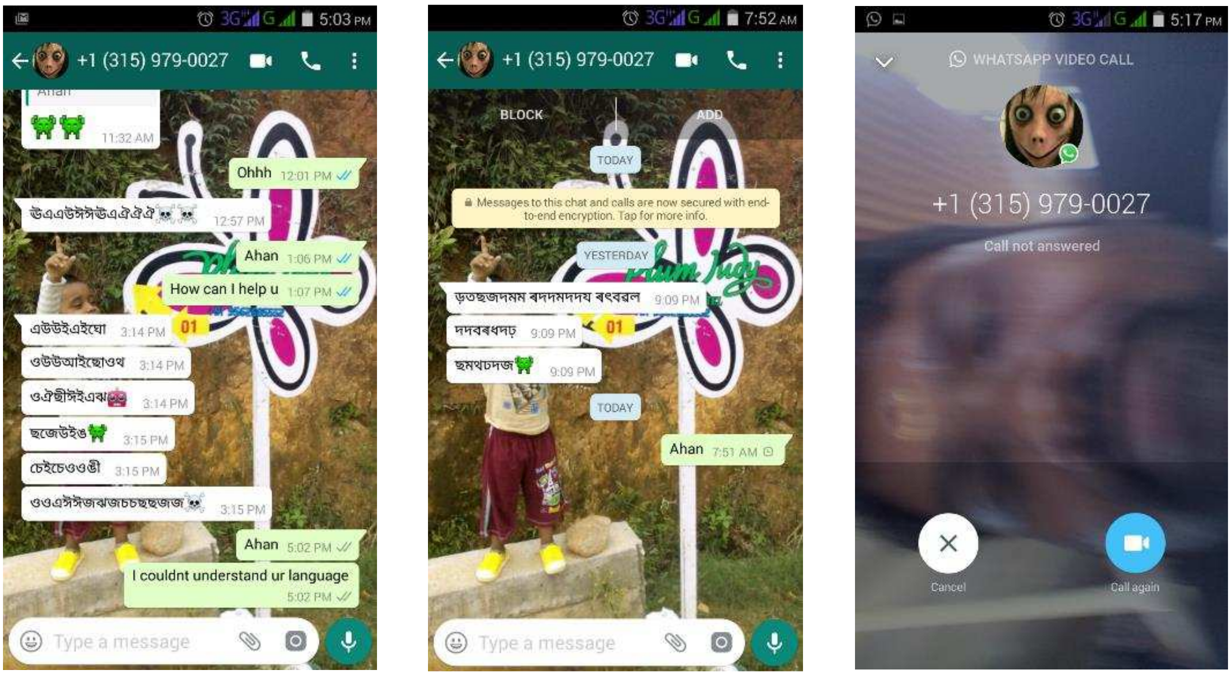
1. Keep contact records straightforward. Empower parental controls by securing your kid's contacts list. Guarantee they are not trading data with individuals they don't have the foggiest idea.

2. Focus on interpersonal organizations. Know about what your youngsters are sharing via web-based networking media accounts, particularly their telephone number. Keep in mind that a number can be gotten to and utilized by vindictive individuals.

3. Continuously utilize a decent antivirus. Ensure everybody in the family has antivirus assurance on their telephones, for example, dfndr security, A notice will fly up at whatever point your young person gets a pernicious connection in WhatsApp, SMS, and Facebook Messenger.

4. NEXT STEP

Then the number is altered and received message from other number from different language perceptive



5:03 PM

+1 (315) 979-0027

11:32 AM

Ohhh 12:01 PM

উএএউঈঈউএঐঐঐ 12:57 PM

Ahan 1:06 PM

How can I help u 1:07 PM

এউউইএইঘো 3:14 PM

ওউউআইছোওথ 3:14 PM

ওঐছীঈইএঝ 3:14 PM

ছজেউইঙ 3:15 PM

চেইচেওওঙী 3:15 PM

ওওএঈঈজঝজচচছছজজ 3:15 PM

Ahan 5:02 PM

I couldnt understand ur language 5:02 PM

7:52 AM

+1 (315) 979-0027

TODAY

Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

YESTERDAY

ড়তছজদমম ৰদমদদয ৰৎৰৰল 9:09 PM

দদবৰধদঢ় 9:09 PM

ছমথঢদজ 9:09 PM

TODAY

Ahan 7:51 AM

5:17 PM

WHATSAPP VIDEO CALL

+1 (315) 979-0027

Call not answered

Figure 3: Mo Mo Message from other number and chat details

The above figure 3 shows that Momo message contact for other number as different language (Bengali) and registered unknown number as foreign or other country registered number. As the same time I chatted by our language as Tamil and Momo person understand the Tamil language and responded.

The most vulnerable victims to these types of social engineering attacks are young people. Even though the Blue Whale Challenge and Momo WhatsApp could be construed as urban myths, instances of cyberbullying and online harassment are very real. It can now and then be difficult to face your companions, so Childline offers the accompanying tips on the most proficient method to state no:

1) Say it with certainty: Be self-assured. It's your decision and you don't need to accomplish something which influences you to feel risky or uncomfortable.

2) Try not to judge them: By regarding their decisions, they should regard yours.

3) Spend time with companions who can state 'no': It takes certainty and bravery to state no to your companions. Invest energy with different companions who likewise aren't taking part.

4) Suggest another thing to do: On the off chance that you don't feel good doing what your companions are doing, propose another thing to do.

5. CONCLUSION

As per above discussion and chat the Momo is not attack or game. It is normal contact chat by known person registered by using other county sim card or app. Each and every chat the mentioned as mobile hacked or going to hack your mobile phone. As well as the mentioned all your details in each chat. So the user get confuse and suddenly we get panic. But we must understand Momo is chat based person to know your details and get to panic. In case any doubt or secure your phones you will register two step verification processes with mail to secure and unwanted access your phone details. The conclusion says that Momo is chat by unknown person to get afraid or to create panic to users. My personal opinion shows the Momo is not attack or hacker just chatting my using WhatsApp.

REFERENCES

https://www.thesun.co.uk/news/6922459/momo-whatsapp-suicide-challenge-parents-girl-death-argentina/

https://timesofindia.indiatimes.com/life-style/health-fitness/health-news/after-blue-whale-it-is-momo-whatsapp- suicide-game-thats-risking-your-teens/articleshow/65335762.cms

https://knowyourmeme.com/photos/1391967-momo

https://books.google.co.in/books?isbn=3642048463

https://www.facebook.com/allmissouriattack/

https://eisamay.indiatimes.com

About the author: S. Manikandan is working as Assistant Professor and Head of IT in E.G.S Pillay Engineering College, Nagapattinam. He completed M.E-CSE in Annamalai University with First class with Distinction, 2012 and BTech-IT in E.G.S Pillay Engineering College with First class with Distinction, 2010.

Currently he is doing PhD in Anna University, Chennai and his research work includes Artificial Intelligence, Network Security, Algorithms and Cloud Computing.

Popular types of social engineering attacks

1. **Baiting**: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive, in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.
2. **Phishing**: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
3. **Spear phishing**: Spear phishing is like phishing but tailored for a specific individual or organization.
4. **Vishing**: Vishing is also known as *voice phishing*, and it's the use of social engineering over the phone to gather personal and financial information from the target.
5. **Pretexting**: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
6. **Scareware:** Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.
7. **Water-holing**: A watering hole attack is when the attacker attempts to compromise a specific group of people by infecting websites they are known to visit and trust in order to gain network access.
8. **Diversion theft**: In this type of attack, the social engineers trick a delivery or courier company into going to the wrong pickup or drop-off location, thus intercepting the transaction.
9. **Quid pro quo**: A quid pro quo attack is one in which the social engineer pretends to provide something in exchange for the target's information or assistance. For instance, a hacker calls a selection of random numbers within an organization and pretends to be calling back from tech support. Eventually, the hacker will find someone with a legitimate tech issue who they will then pretend to help. Through this, the hacker can have the target type in the commands to launch malware or can collect password information.
10. **Honey trap**: An attack in which the social engineer pretends to be an attractive person to interact with a person online, fake an online relationship and gather sensitive information through that relationship.
11. **Tailgating**: Tailgating, sometimes called *piggybacking*, is when a hacker walks into a secured building by following someone with an authorized access card. This attack presumes the person with legitimate access to the building is courteous enough to hold the door open for the person behind them, assuming they are allowed to be there.
12. **Rogue**: Rogue security software is a type of malware that tricks targets into paying for the fake removal of malware.

Source & Courtesy: https://searchsecurity.techtarget.com/definition/social-engineering