Alan Michael Simmons

Professor Miro, Edward

CSCI 019

26 March, 2022

Final Draft: What are scammers, and who would stop them?

What if I were to tell you a story about a youtube channel who dedicated themselves to hacking into scam call centers across the world? This person has been able to hack into phone lines, into scam call center CCTV and uploaded viruses on the people who often call poor individuals and try to scam them out of their money. This YouTuber is known only as Jim Browning, a hero among people who have lost hundreds of dollars to scam callers and what he does in order to make sure everyone affected does not end up losing money.

Let’s start things off with why scam callers go out of their way to ruin the lives of innocent people who did not know any better. Most scam callers use this robotic voice and warn you about some message that could very well be irrelevant like “we came to talk to you about your car’s extended warranty”, “critical alert from Microsoft”, or “this is a call from the IRS”. These scam callers can ultimately rip people off of their money or worse, give the scammers access to a person’s bank account information, credit cards, home addresses, IP addresses, social security numbers, cameras, phone lines, and even their full computers then deleting their files like music, pictures, audio then go to that person’s computer, go online and see all their saved passwords and history. We’ll go over a brief summary for each of these and why a person should not let this sort of information slip out.

Scammers - Malicious people who go out of their way to exploit the unaware by taking all their information and money. These people are basically thieves who somehow get away with it. While younger audiences will easily see that a “random caller that sounds like a robot with no idea what your name is”, more elderly individuals especially in the 60’s or higher, are unfortunately more susceptible to these vicious attacks since they would be none the wiser.

Bank account information - A person’s bank account is where all their money is kept, a scam caller with access to things like the account number, credit card, expiration date, security code, and even the person’s home address that is assigned to the bank account. This is bad since fake “SWAT” calls can be made to your house which can scare you for no reason however we can be glad this doesn’t always happen.

Credit cards - The money that is in your account, this is oftentimes the most sought after object of the hacker who wants to make money. They often will get as much money as they can, robbing people of all of their money until there is nothing left. Since most scam call centers are based in India, there is no way local authorities can help in this either. The only way to effectively shut down a scam call center is to have a professional hacker do it, and this professional hacker that I will speak of soon will be very important to the subject as he has done many things to stop these scammers.

Home addresses - This is not normally what is sought after, but especially malicious scammers will use other means to get your money like sending false bills, sending dangerous packages, or sending a SWAT call like I mentioned earlier. This is especially sad considering it is the same person who most likely already lost all their money that is getting affected in real life by these attacks.

IP addresses - This is especially accessible to a scammer who is trying to get information out of you, giving them your IP addresses can effectively mean many viruses can and will be sent to your computer, often in the forms of emails or digital security attacks. Not only this, but especially vicious scammers will be able to find your town or city that you live in with this.

Social security numbers - This is without a doubt the worst thing a person can lose to a scammer. Your social security number is essentially your identity, if you lose this to a scammer then that person can commit a crime known as identity theft and ultimately use it to commit terrible crimes in your name or impersonate you to access all your other banks and steal the money from there too. If the scammer is out of the country, then they can use it to get into the United States of America.

Cameras - This is not nearly as bad, however scammers can use it to create a fake ID and combined with the social security number can be used to enter the state. Only other dangerous factor is that the scammer will know your household pets and family members and could use them to get you. This is bad for many privacy reasons but it ultimately has the least effect compared to the other topics I noted.

Computers - This is the most common threat besides losing your money, hackers will get on your computer and start deleting everything on it without any care about what you think. This can include videos of good movies you watched, pictures of family or pets you saved, music you liked and wanted to listen to again, and video games that you play all the time. The worst thing the hackers can do however above all that, is to go online and look at your saved passwords for all other sites. If they were that malicious enough, they can even go ahead and destroy anything on those sites too. This is why it is important to get two-step verification, except a hacker has access to your email and will be able to undo that anyway.

Now, onto the main subject, a hero among people who has gone out of his way time and time again to stop these vicious scammers from stealing the information of these victims. Jim Browning is a YouTuber who goes out of his way to bait scammers into giving access to his computer, only to run a program that not only prevents that but gives him access to the scammer’s computers instead. Not only that, but he himself has managed to get into the CCTV of these scammers as well and keep track of the people who are trying to scam Jim, often saying things to scare the scammers like saying what color of shirt they are wearing, or who is standing next to them.

The scammers would often shut down their CCTV or the computer off, which you think that would be the end of it, but Jim keeps track of everyone’s real name and the fake alias they use (scammers will never reveal their true name to the people they will scam). Not only that, but he will even be able to access the information about all the scammers including who actually runs the project, who they call, their allies and their victims.

While most people do unfortunately get scammed, he uses his traces to find out who became a victim, and warns the victim if they are being scammed. I have noticed many times how a victim was able to defend themselves and not let the scammers get any money, saving another victim from an “Amazon purchase they never remembered purchasing” or a “Car’s extended warranty” and other stuff like that.

Scammers upload phone numbers of people who have been scammed before and even call about being a “Microsoft refund department”, ultimately to scam the same people who have already fallen victim to scams before. The scammers will give their scammer call numbers to bait them into calling again and start stealing their information. This is of course, what I meant earlier when I said scammers usually attempt to scam people who have already been scammed before again.

Jim was once able to hack into a scammer’s laptop that was used to scam. With the camera from his laptop, Jim was able to get a little bit of a layout of the entire call center. Unfortunately, YouTube’s recent policies state that faces and names are supposed to be blocked, regardless if the people who had their face blocked are literally criminals, but we can just blame that on YouTube’s policies which only help evil and malicious people like that.

Since the laptop is connected to a wireless network, Jim was able to get a decent clue as to where the scam call center is located. Jim was able to find the location Kolkata and followed the address to the image below, while this is bad for us if a scammer gets access to our location, this is great for Jim who can use the address to effectively scare off and ultimately shut down the scam call center.



Scammers are often working together, normally in an office building where they work together to scam as many people as possible. It’s also important to note that many scam call centers get traced back to India. You should be very careful when speaking to someone who claims to be a Police Officer, from Microsoft, calling about your car’s extended warranty and they also have an Indian accent. Not to say that all Indians are bad, but this reputation stems from the fact that many scam callers are from India where the police there do not try to find the scammers since the victims are in America.

A scammer did something very drastic, by offering a refund to immediately turning on her laptop’s camera, threatened her, grabbed pictures of her children, and tried to delete all of her files. The scammer will then make sure you don’t talk to the actual bankers and convince them that the scammer is doing what is right. Jim warns the individual by changing the audio file entirely that gets sent. Instead of the scammer’s audio: “Hi, we are calling you from the Microsoft refund department. If you remember you have a contract with us, for computer support and services, unfortunately we are closing business. So you can give us a call for the refund of the amount you paid. To claim your refund please call us on (747) ###-#### (purposefully redacted by me) or press 1 to talk with our executive. Thank you”. Jim will create his own audio: “Hello, this is an automated message being sent from scammers in India. They were going to try to scam you by claiming that you would get a refund from your computer maintenance company. However this is just a scam so that they can access your computer and will try to get money from your bank account. If you ever get a message like this, it is always a scam. Please do not mention that I have changed their message but if you would like to waste their time, you can speak to these scammers by pressing 1 on your telephone keypad.”

Jim reported that this was without a doubt his most effective way of getting a message to the scammers’ potential victims at the expense of the people making the calls, the scammers themselves. Jim then increased the rate of his calls, which drains the money of the scammers as much as he could. This is how much Jim was able to drain from the scammers while simultaneously giving the victims a message that protects them from the scammers.

This ultimately also slowed down the amount of money that the scammers would have gained from victims since the victims already know of their scams. The scammers also couldn’t pinpoint the problem since Jim asked the victims to not reveal that the message was changed, ultimately making it much harder for them to fix their issue. The scammers lost a lot of money over the weeks and figured out that their system was compromised and they figured out that there was something wrong with their audio.

Over the weeks, he also was still using the audio from the scammers and got all of their names. Jim then emailed the Kolkata cyber police and hoped that they would do something, however he explained that since they have not gotten back or mentioned anything, that they will do nothing to solve the issue. So that is why he uploaded this video to youtube.

[<https://www.youtube.com/watch?v=xb_rgQ4IDS8&ab_channel=JimBrowning>]

This was only one of many videos that has gone on YouTube. Jim Browning has over 3,600,000 subscribers (as of 26 March, 2022) and 89 videos spanning across 8 years. He has been able to take down many scam call centers and other scammers who have tried to rip the money off of honest people. He shows that it is possible for hackers to do the right thing by taking down scammers and makes a living off of it since it is his job. 