Guidepost

SOCIAL MEDIA UNMASKING: REMOVING ANONYMITY FROM DIGITAL BULLIES AND CYBER CRIMINALS

Whether or not Elon Musk's recent acquisition of Twitter is a good thing or bad thing for the future of social media (Twitter accepts buyout, giving Elon Musk total control of the company – The Verge), one aspect of social media is unlikely to change: the abuse of social media platforms, by seemingly anonymous users, to harass, threaten, disparage, humiliate, scam, or falsely accuse individuals or companies of a panoply of hot button social issues. Often times, the victims and recipients of these attacks feel as if there is little recourse other than blocking or ignoring the user. After all, how could you possibly identify the real person behind the account @SolitaryPenguin388?

Scenario One – Unrequited Love

An on-air personality was receiving unsolicited Instagram messages from several accounts wherein the user was vacillating between professing his undying love and admiration for her presentation and coverage of events to vitriol-filled messages to her, her husband, and her staff regarding alleged promiscuity and adulterous behavior. Although the victim had blocked these accounts from messaging her, new accounts were created, and the messages continued. Given that her personal brand required social media interaction, creating a new account, or stepping away from social media altogether was not an option.

Our team reviewed several key data points from the current and former harassing Instagram accounts, and noted that many of the claims, language used, and time stamps of messages were similar suggesting there was a single user behind multiple accounts. These accounts also had overlap in followers and interests and we were able to identify the real users behind some of these followers, which happened to be family members. On-the-ground interviews with the family members revealed that their elderly father was behind these various accounts and had become enamored with the on-air personality after the death of their mother several months ago. A visit to the father's residence with local law enforcement helped the father to see the error of his ways and the harassing messages ceased.

Scenario Two – Fake News

A professional in the crypto space had been receiving a barrage of "fake news" accusations from a popular Twitter profile. This profile was making false accusations that the client, and their company, were involved in various crypto related scams and the business was seeing a significant loss of revenue. The popular Twitter account purposefully avoided disclosing personal details but did like to share photos of him and his female companion at various tourist destinations or sporting events. The photos were either taken from the rear, not showing their faces, or were taken from the front with graphics obscuring their faces.

Our team was able to locate fan-posted images and video from a championship game where the individual had shared a photo. From a composite of these images, we were able to see the "face" of the subject and his significant other but that did not provide an identity. A key finding was some very distinct tattoos on the woman's arms and legs, and so we focused our attention on her. She was easier to locate on social media, as her tagline was "Spouse of @XXXX," the subject of the investigation. Her digital hygiene was much less robust than the subjects and included references to an ethnic affiliation business owners' group and an alumni association. From these points, we identified a potential candidate, and looked into the social media of her family members. Her mother was very active on Facebook and shared photos of her daughter and her boyfriend, who had the same face as the individual identified at the sporting event. The mom also shared his first name. From there, it was an easy path to identify the user behind the public account and the client was able to initiate litigation from our research.

Scenario Three – NFT Theft

A client had an NFT stolen due to some poor digital security practices and wanted to identify the thief to recover their NFT. Due to blockchain technology, the account holding the NFT was easy to locate, but identifying the user was another matter. During our investigation, a Twitter account popular in the NFT space began sharing details about acquiring an NFT through a set of circumstances that echoed the events in which the NFT was stolen. This Twitter account had good digital security and was mostly absent of any personally identifiable information. However, mostly is not completely, and we were able to identify that the Twitter account was renamed from a previous username several years earlier. This username was associated with several other historic accounts including Pinterest, FourSquare, and other less popular social media platforms.

Through our research, we identified a connected account on a photo sharing website, and this account was kept current. The account shared a recent photo from a residential balcony that overlooked a body of water. Comments from fellow photographers complimented the shot and asked where it was taken. The user stated only that it was in a certain region of a European country. Through imagery analysis of visible landmarks and satellite photos from Google Earth, we were able to identify the exact angle from which the photo was taken. When plugging the latitude and longitude into Google maps, an address was found, and a short search later identified the address as an Airbnb rental. On-the-ground interviews with neighbors and the villa's owner ultimately identified the guest staying at the Airbnb when the photo was taken. Law enforcement involvement followed soon thereafter.

Privacy matters. Reputation more so. Executives and companies who face unwanted harassment, or negative publicity

from “anonymous” users need to be aware of the resources available to unmask those who hide behind their keyboards. Similarly, executives should be well aware of what information is available in the public domain about them and their families. Seek a security consultant with a global presence who can combine online research with boots on the ground investigation and liaison work. For certain U.S. clients, understanding your digital footprint and remediating security gaps may be part of a larger tax deductible security study.

CODY SHULTZ PCI, CCI

Director, Investigations & Private Client Protection

Cody Shultz serves as a director of investigations and private client protection for Guidepost Solutions and is based in the D.C. office. Having served with the Central Intelligence Agency, he is now sought out as an expert on reputation and identity management for ultra-high net worth clients and family offices. He holds a Professional Certified Investigator certification through ASIS International and is a Certified Cryptocurrency Investigator.