Are Technical Support Scams Getting More Advanced?

Gabor Szathmari
Business Justice & Behavioural Sciences
Charles Sturt University
Sydney, NSW, Australia

***Abstract*—Technical support scams (TSS) are responsible for a growing amount of financial losses year after year. Nevertheless, while the victims are losing more money than ever, the number of interactions between criminals and victims is decreasing. Why? Because the scammers are getting better at what they do. In this paper, I demonstrate through examples how the TSS practices have become more advanced recently. First, the criminals improved their existing methodologies. Second, they introduced new practices to make the TSS schemes more lucrative. One of these improvements is the transition to robocalls, which enables TSS call centres to engage more people than ever. This shift to the auto-dialler approach allows call centres to find people more susceptible to TSS. The second significant change affects the management of online advertisements. The magnitude of TSS advertising campaigns assumes large-scale infrastructures, software logic and automation capable of delivering the pop-up ads more effectively. Also, TSSs borrow practices like code obfuscation and context-aware evasion practices from the malware world to improve their advertisements further. Other additions to the TSS industry include specialisation and the division of labour. TSS operations were found to divide their business up into advertising and call centre divisions. This segregation of duties allows the entities to optimise their core business processes. For example, call centres now employ English tutors to improve their staff members' communication and English-language skills. In conclusion, my discoveries demonstrate how TSSs can trick more money out of the victims than before. Also, the number of interactions between scammers and their victims is shrinking because TSSs can engage the more gullible.**

***Index Terms*—Technical Support Scams, Remote Support, Fraud, Scam, Computer Crime, Cybersecurity**

I. Introduction

Social engineering, scams, and fraud are well-known criminal activities that eventually found their way into cyberspace. These crimes are not only responsible for direct financial losses but also foster fear and distrust within internet users. In other words, netizens are less likely to trust individuals, businesses, organisations, and governments online because of the fear of becoming the target of a scam.

One category of online crimes is the technical support scam (TSS). This computer-enabled fraud combines confidence tricks and social engineering practices disguising itself as a legitimate technical support service. A typical scam aims to trick the victim into paying for a computer support service that fixes a non-existent problem. In a TSS, the scammer persuades the victim that their computer needs immediate professional attention. For instance, the criminal would run remote commands on the victim's personal computer (PC) to 'demonstrate' that the computer is ridden with malware or has a 'hacker infection'. Once the victim is convinced, the scammer pressures them into paying a sum of money for the cleanup. Once the victim pays, the perpetrators may not even pretend to remediate the non-existing problems. Instead, the money is quickly separated from the victim to prevent any reversal of the money exchange afterwards.

TSS has been an ever-growing problem since its first appearance in 2008 [1]. According to in-depth research on TSS operations, victims were more likely to lose money to TSS in 2021 than in 2018 [2]. The Microsoft [2] study reveals that TSS crime affects Australia, particularly as Australians were more likely to lose money than the global average. Also, the report draws attention to a contradiction. Although the absolute number of 'interactions' between TSS scammers and the victims is slowly decreasing, the losses keep increasing [2]. What is the explanation for the rising profits within the TSS industry while fewer people get engaged?

There is a potential explanation for this contradiction. I hypothesise that two things drive the rising TSS profits: the growing sophistication of existing TSS practices and the new additions to TSS schemes. In plain English, TSS business operations are simply getting better at doing their core business (i.e. scams). It means that TSS business entities have been perfecting their techniques and introducing a range of innovations to their TSS operations. Even though the growing prosperity within the TSS industry, I did not manage to identify a study to confirm my hypothesis. Although I found a few academic papers, industry reports and other sources of information stating the prosperity of TSS scams, a definitive answer is never provided to the why. Nonetheless, I believe it is crucial to understand what drives the success of TSS because more informed decisions can be made to fight TSS.

Therefore, I performed a literature review to understand what business and technology innovations have been introduced to the TSS industry lately. I identified possible reasons, including automation, black hat SEO, malware-like tactics, and sound business practices contributing to the TSS's prosperity. Furthermore, I analyse how these additions enabled TSS operations to grow and prosper. The research concludes that TSS businesses have become highly specialised and professionalised in recent years, which explains the record of TSS profits amid declining engagements.

II. METHODOLOGY

I undertook a literature review to explore how the sophistication of TSS has grown in recent years. As a result, I managed to shortlist twelve academic papers through Google Scholar and general internet searches. I chose these papers because of their relevance to TSS and the scambaiting phenomenon. Furthermore, because these papers have a high academic reputation, I decided to include some of their arguments presented in this paper. Search criteria included: 'technical support scams', 'tech support scams' and 'scambaiting'. My final paper includes four of the original set of academic literature.

In addition to these academic papers, I chose other sources of information to support the main arguments of this research. These sources of information include blog articles of security researchers, YouTube videos of well-known scambaiters and podcasts covering TSS. Even though I know these sources may have poor academic reputations compared to scholarly articles, the information value of these non-academic publications is high. Firstly, TSS fraud is relatively new compared to other variations of online scams; As a result, academic publications covering contemporary TSS innovations are scarce. Secondly, the tools and techniques of TSS rapidly evolve as law enforcement and the scambaiting community catches up with the latest extortion practices. Due to the fast-changing nature of TSS schemes, I found that these non-academic sources' information is generally more informed and up-to-date than the academic ones.

III. RESULTS

This section is to showcase the latest innovations within the TSS industry. As the examples below demonstrate, each step of the TSS scheme has been improved in recent years. The changes affect the productivity, efficiency, and resiliency aspects of TSS.

In their podcast, Bhattacharjee and Benson [3] elaborate on how TSS call centres kept evolving their standard operating procedures. In one episode, Bhattacharjee and Benson [3] explain how criminals can dominate their victims over the phone and make them comply. According to the episode, the application of subliminal, neurolinguistic and other verbal practices are three factors that can manipulate the victims over the phone. For instance, they found that the scammers make the victims answer 'yes' to many innocuous questions at the beginning of the call [3]. Once the criminals establish a rapport with the victim, the victims are more likely to answer 'yes' to the payment demands later [3]. An additional domination trick of the trade is micromanagement. Bhattacharjee and Benson [3] cite an example when the victim was ordered to press the horn whilst driving en route for the payment cards. According to the researchers, the horn-honking demand intends to "dominate" the target and make them submit themselves to the scammer's will. The second central insight of Bhattacharjee and Benson is that the South Asia-based TSS call centres were found to employ English teachers. The purpose of the language tutors is to improve the conversation skills of the TSS call centre staff members. Thirdly, Bhattacharjee and Benson [3] claim that TSS call centres migrated from cold calls to robocalls in 2016. This robocall approach allows TSS operators to reach a higher number of potential victims than before and serves as a basic pre-screening process as well. Lastly, the podcast provides unprecedented insight into the money-laundering process of TSS payments. Bhattacharjee and Benson [3] describe how and why victims are ordered to buy 'stored value cards'. According to the podcast, these cards are converted to electronic fund transfers via a convoluted scheme involving 'general purpose cards' and money orders. The complexity of the payments is designed to distance the money from the victim as far as possible [3].

In their article, Zeltser [4] analyses how criminals abuse social media platforms to promote TSS scams. Zeltser explains how TSS call centres deceive unsuspecting users with bogus replies on Twitter. The researcher found that a TSS bot replies if a Twitter user publicly mentions a keyword like 'virus' or 'malware'. The mock response features a generic response and the phone number of a TSS call centre, Zeltser claims. For instance, when someone tweeted, "Show visitors your site is safe from hackers and malware", a bot replied: "Hey I just had the same problem as you I found these guys they fixed it fast the number is 855*408*699". However, the original tweet had the keyword 'malware', which triggered the bot to reply with a misleading response. According to the researcher, the phone number is associated with a known TSS call centre.

In their research, Srinivasan, Kountouras, Miramirkhani *et al.* [5] examine how TSS operations use black hat search engine optimisation (SEO) techniques to acquire new victims. Black hat SEO is a collection of questionable practices to manipulate search results. These practices can trick search engines (e.g., Google, Bing) into displaying TSS websites instead of legitimate pages within the search results. In plain English, if someone is seeking a solution to a computer problem, Google and Bing will display websites associated with TSS when black hat SEO practices are applied. The Srinivasan, Kountouras, Miramirkhani *et al.* [5] case study shows how large the TSS SEO campaigns can be. In their case study, the researchers found 452 support domain names, 662 final landing domain names, 216 internet protocol (IP) addresses and 521 unique phone numbers associated with just a single campaign. In addition to the large scale, Srinivasan, Kountouras, Miramirkhani *et al.* [5] find that TSS operations rely on complex hosting infrastructures to withstand website takedown and blocklisting requests. Other findings of Srinivasan, Kountouras, Miramirkhani *et al.* [5] point out the unusually short lifecycle of the domain names associated with TSS advertisements. The researchers found that the median lifetime of 40% of TSS domain names is nine days. The brief lifetime corresponds with Miramirkhani, Starov and Nikiforakis [6], as they found that 43% of the TSS domains point to malicious content for merely three days. In a nutshell, both papers conclude that the lifetime of some TSS domain names is abnormally brief.

In an analogous analysis of TSS web hosting infrastructures, Miramirkhani, Starov and Nikiforakis [6] explain how TSS operations evade unwanted research. During the data collection phase of the Miramirkhani, Starov and Nikiforakis [6] paper, the authors observed that TSS websites frequently refused to display any contact details when the researchers' web requests originated from a public cloud environment. The TSS websites under scrutiny were associated with deceptive pop-up ads mimicking fake Windows error messages and claiming fictitious problems with the potential victim's personal computer (PC). These pop-up ads usually claim a computer problem (e.g., malware infection) and promote a TSS phone number offering a remedy. When the researchers' web browsers connected from public cloud environments, the phone number was missing from the pop-up ads [6]. However, the contact details normally appeared when the web request was made from a residential internet protocol (IP) address. The second finding of Miramirkhani, Starov and Nikiforakis is how TSS-associated web pages feature advanced JavaScript code to tailor the advertisements to their target audience. The researchers found that a different phone number was displayed depending on the context of the web request. For example, the phone number varied depending on the website visitor's operating system, the web browser's make and model, and the computer's language settings [6]. Similarly, Chandrayan [7] also found various practices in the JavaScript code of TSS websites. The researchers found heavy code obfuscation techniques, presumably to evade the detection by security software and the analysis of cybersecurity researchers [7].

In their publication, Miramirkhani, Starov and Nikiforakis [6] also explore the various confidence tricks TSS practitioners apply to deceive and exploit the victims. The study elaborates on how TSS call centres misrepresent the built-in Windows features to convince future victims that something is wrong with their computers. For example, once the scammer connects to the victim's PC with a remote management tool, they open the Windows Event Viewer first [6]. Then, the scammer claims that the high-severity Windows alerts can be attributed to 'hacker activity' and that the PC needs immediate attention [6]. A similar practice is running benign system utilities like `netstat` and `dir` to claim a problem [6]. A similar study by Rauti and Leppanen [8] confirms the misrepresentation of system utilities as a common trick of TSS schemes. In their paper, Rauti and Leppanen [8] found that the Windows Event Viewer and the Windows command-line tools are the two most commonly used methods for deception. Finally, the authors identified virtual machine detection practices aiming to determine if the victim is a scambaiter or not [8].

Lastly, court documents of *USA v. Anjum* [9] reveal how TSSs began to specialise in their business affairs. According to the documents, three distinct business entities are affiliated with TSS schemes: 'publishers', 'brokers', and 'call centres'. As *USA v. Anjum* [9] reveals, each business entity specialises in one or more areas within the TSS operation. For example, the publishers are responsible for creating and operating the advertising campaigns (e.g. deceptive pop-up ads, black hat SEO). In parallel, the call centre group performs the scam itself. Finally, brokers function as the intermediaries between publishers and TSS call centres. The brokers purchase phone calls of the victims from the publishers on behalf of the call centres and route the calls via the internet. In summary, each business entity operates independently of the other. The publisher is responsible for the acquisition of phone calls, the call centre for the TSS fraud itself, and the broker facilitates the trade and routing of phone calls between the other two, according to *USA v. Anjum* [9].

IV. Discussion

A. The Transition to Automated Diallers

In general, businesses can benefit from automation. Because machines can perform tasks faster and more accurately than humans, automation can make businesses more productive and efficient. As the TSS industry is no exception to this rule, automation can also enable TSS organisations to maximise their revenues and profits. Numerous examples indicate how TSS operators have automated high-effort and low-yield business processes in recent years.

One of these innovations is the computerisation of the customer outreach process with *robocalls* (i.e. software diallers). The perpetrators discovered that the automation of cold calls could enable their call centres to access a larger pool of victims. From the humble beginnings of TSS, human operators used to dial random telephone numbers from the phone book to find the next victim [10]. However, this cold-calling approach was a wasteful exercise because of the low success rates. Because many randomly selected people knew that the call was a scam, the targets hung up the phone before the scam could proceed. In addition, as this cold calling approach required human operators, the TSS call centre had to make a large volume of calls until they found someone gullible. In short, the customer outreach procedure was a laborious and uneconomical routine in the past.

This resource-intensive errand underwent a significant transformation in 2016 when TSS call centres added robocalls to their modus operandi [10]. What happened in 2016 was that TSS operators were introducing software dialling systems to their call centres. The change was a significant transformation of the labour-intensive customer outreach process into a highly-automated one. Consequently, call centres could begin to flood the telephone network with TSS calls on a much larger scale [10]. As a result, call centres began making tens of thousands of phone calls daily, according to Bhattacharjee and Benson.

Furthermore, the automation does not stop at the dialling process. As [10] explain, when someone answers a robocall, the software dialler plays a pre-recorded message to the victim. For example, a voice would claim that the victim is entitled to a refund from a reputable business like Microsoft, Google, or Amazon. The victim is then asked to press '1' on the dialpad if they wish to proceed with the claim. Once the victim proceeds by pressing '1', they are connected to a human operator from the TSS call centre, and the usual TSS scam takes place [10]. Because the recorded message does not require a TSS call centre employee on the line, the automation can generate and process far more calls than human operators can ever do.

The benefits of the robocall approach are two-fold. First, scammers can generate a much higher number of outbound calls with automation. In other words, offenders can engage more people than before 2016 [10]. Second, automation increases the success rate of the scam because it doubles as a simple pre-screening mechanism. When the victim is asked to press '1' to continue, only those with gullible tendencies remain on the line, as Bhattacharjee and Benson [10] explain. In summary, the 2016 switch to robocalls has lowered human resource requirements, improved success rates, and increased the victim numbers of TSS call centres.

B. The Manipulation of Search Engines

Besides TSS call centres reaching out to the victims, they have other means to acquire new victims for the scam. The other way is tricking the victims into dialling the TSS call centre. One way to make the victims dial is by manipulating search engines to display TSS links on the search engine results page (SERP). In their research, Srinivasan, Kountouras, Miramirkhani *et al.* [5] elaborate on how TSS businesses use various practices to manipulate the page rank of TSS-related sites. The second finding of the researchers is how immense and complex the SERP manipulation techniques got in recent times.

The Srinivasan, Kountouras, Miramirkhani *et al.* paper introduces the *black hat search engine optimisation (SEO)* technique as the technology behind the search results hijacking trick. The goal of the black hat SEO is to get more victims for the TSSs via the search results pages on Google or Bing. In short, if someone is searching for a solution to a computer problem in a popular search engine, the links on the SERP would take the victim to a website associated with TSS – thanks to black hat SEO [5]. These websites look like legitimate technical support businesses, but the phone number rings at one of the TSS call centres. If the person with the computer problem dials the number, the usual TSS takes place.

Google is aware of the problem and has fought black hat SEO practices since the beginning. For instance, Penguin is the name of one of the internal projects at Google targeting SEO fraud. It was launched in 2012 to penalise websites using black hat SEO [11]. The Google Penguin algorithm had gone through several iterations until 2016, when it became an integral part of the core search engine algorithm [11]. However, since black hat SEO practices are still flourishing per Srinivasan, Kountouras, Miramirkhani *et al.* [5], the criminals managed to outsmart every iteration of the tech giant's Penguin algorithm presumably.

In addition, Srinivasan, Kountouras, Miramirkhani *et al.* [5] found that it is not unusual for black hat SEO campaigns to manifest on a broad scale. For example, Srinivasan, Kountouras, Miramirkhani *et al.* [5] describe hundreds of telephone numbers, domain names, and IP addresses all associated with one black hat SEO campaign promoting a TSS. The sheer magnitude suggests a complex supporting infrastructure behind the scenes. To illustrate, the most extensive black hat SEO campaign from the Srinivasan, Kountouras, Miramirkhani *et al.* [5] case study features almost 2,000 phone numbers, domain names, and IPs in total. The scale of the SEO campaigns means that TSSs must have a sophisticated software environment capable of managing the supporting infrastructure of advertising affairs.

Moreover, both Srinivasan, Kountouras, Miramirkhani *et al.* [5] and Miramirkhani, Starov and Nikiforakis [6] point out that domain names associated with the campaigns tend to have an unusually short lifecycle. Both research groups found that the TSS domain names are often blocked or taken down due to blocklisting and domain abuse requests. Because of the volatile nature of domain names, TSS operators must keep registering them to keep the SEO campaigns running. It means that the high churn rate of the domain names also implies software automation in the background. In addition, the automation must be advanced enough to manage the TSS domains' entire lifecycle on this enormous scale.

In short, TSS businesses rely on black hat SEO practices to manipulate SERPs of the most popular search engines. As a result, people looking for a solution for a computer problem receive search results associated with TSS instead of legitimate helpdesk businesses. Furthermore, circumstantial evidence suggests that the black hat SEO campaigns require a large-scale supporting infrastructure due to the magnitude and ephemeral nature of the moving parts. Therefore, TSS must rely on a complex automation solution that can build, maintain, and operate search engine manipulation campaigns. Also, the circumvention of the Google Penguin algorithm assumes a high level of expertise within the TSS advertising circles.

C. Borrowing Ideas From Malware Tactics

Besides the black hat SEO campaigns, TSS criminals rely on other advanced strategies to obtain new victims. One of these acquisition channels is pop-up advertisements. These unsolicited ads often use scare tactics to make people dial the phone number in the pop-up. Usually, the pop-up features a false claim (e.g. the PC is infected with a computer virus) along with a phone number offering an immediate remedy [12]. Unsurprisingly, the phone number rings at a TSS call centre instead of a legitimate business offering genuine help [12].

In addition, TSS schemes rely on malware technologies to deliver these pop-up ads. For instance, Miramirkhani, Starov and Nikiforakis [6] found that TSS pop-up adverts did not appear under certain conditions. They found the ads remained hidden when the source IP of the researchers' web browser was associated with a public cloud service like Linode and Amazon Web Services (AWS). In other words, Miramirkhani, Starov and Nikiforakis [6] found that TSS advertisements only show up when the visitor is browsing the internet from a residential IP address. This defensive behaviour resembles context-aware malware *evasion techniques* capable of hiding any malicious code from antimalware solutions and security researchers. According to Miramirkhani, Starov and Nikiforakis [6], TSS advertising campaigns also use these malware-like evasion techniques to avoid scrutiny by security software and cyber professionals.

Similar malware-like behaviour of TSSs is *code obfuscation*. In their paper, Miramirkhani, Starov and Nikiforakis [6] describe how heavily TSS advertising campaigns depend on client-side JavaScript code. They reveal that TSS campaigns use JavaScript to fine-tune the deceptive pop-up ads based on the visitor's location, operating system and system language. These optimisations allow the pop-ups to be tailored to the visitor, making them more attractive for the victims to click. The problem is that this JavaScript code needs to be fetched to the visitor's web browser. Therefore, the code is prone to inspection by antimalware solutions and security researchers. In their article, Chandrayan [7] explains that TSS campaigns apply multiple layers of code obfuscation as a defence mechanism to avert detection and code analysis. On top of that, Chandrayan [7] points out how the obfuscation techniques are improving. According to the researcher, the latest variations of the TSS campaigns rely on symmetric encryption and double-obfuscation algorithms to stay hidden from prying eyes [7]. In summary, code obfuscation is integral in successfully delivering pop-up ads.

Numerous examples illustrate how TSS advertising uses progressive technologies such as software code evasion and obfuscation techniques. I found that TSSs borrowed these reliable techniques from the malware world and successfully adapted to the online advertising aspect of TSS. Both evasion and obfuscation allow the delivery of more ads without security software and security practitioners disrupting the campaigns.

D. The Exploitation of Social Media

Besides the search engines and pop-up advertisements, TSS call centres were also caught abusing other promotion channels than the web. In their article, Zeltser [4] illustrates how automated bots made their way to social media to promote TSS scams. According to Zeltser, if someone talks about viruses or malware on Twitter, a bot responds with a message promoting TSS services [4]. To illustrate, when someone tweeted, "Show visitors your site is safe from hackers and malware", a bot replied: "Hey I just had the same problem as you I found these guys they fixed it fast the number is 855*408*6991" [4]. The phone number in the reply is associated with a TSS call centre, as claimed by the researcher.

Furthermore, Zeltser points out that the textual replies are not written and reviewed by humans. To give an example, the author found that a tweet mentioning the Ebola virus also received a reply from a TSS bot advising them to call the helpdesk service. The bogus reply means that the criminals use automation to identify tweets looking for a technical problem and reply to them [4].

Lastly, the findings of Zeltser suggest two innovations. One is that the criminals began utilising new media platforms for promoting TSS. Second, criminals have invested in automation to push their social media campaigns effectively. These two innovations demonstrate how TSS schemes can adapt to the changing media environment and optimise their promotion strategies for maximum impact.

E. Business Professionalisation and Optimisation

A different aspect of the growing sophistication of TSS schemes is the appearance of business *specialisation*. In his 1776 masterpiece, Smith [13] wrote that the *division of labour* is the key success factor of economic prosperity. Smith suggested that workers mastering a task can enable businesses to achieve higher productivity and lower production costs. For instance, specialisation and the division of labour allow businesses to shrink training budgets because workers only need to learn a simple task instead of the whole process [13]. Consequently, specialisation and the division of labour increase productivity while production expenses decrease.

In recent news, TSS is no exception to Smith's groundbreaking idea. TSSs often run as registered businesses, and recent court documents reveal how they enjoy the economic benefits of specialisation. In 2020, the Department of Justice [14] announced the court appearance of Abrar Anjum, an individual responsible for the operation of multiple TSS call centres in India. Because of the public court documents of *USA v. Anjum* [9], we have unprecedented insight into the latest business model of TSSs. According to the papers, TSS schemes are split into three key entities: 'publishers', 'brokers', and 'call centres' [9]. While the first group, 'publishers', are responsible for the customer (victim) acquisition, 'call centres' specialise in executing the scam [9]. Finally, the third group, 'brokers', are guilty of facilitating trade between the other two TSS entities [9].

The multi-tier business model alights with Smith's thoughts about specialisation and the division of labour. The split between 'publishers', 'brokers', and 'call centres' means that each entity can focus on its core business activity and outsource nonessential processes to the others. For instance, 'publishers' can perfect their pop-up campaigns to achieve high click-through rates thanks to specialisation. This separation of duties between the three entities resembles some recent changes in the ransomware industry. Similar to TSS, criminals in the ransomware business also began to specialise in their affairs. The first entity, called 'ransomware operators', is responsible for the ransomware code and its hosting infrastructure [15]. The second group, known as 'ransomware affiliates', became experts in delivering malicious code to the victim's computer or network [15]. The two-tier structure is known as the Ransomware-as-a-Business (RaaS) model, allowing 'ransomware operators' to write better ransomware code. At the same time, the 'ransomware affiliates' tier can perfect their methods to deliver the ransomware code with more success. The increasing ransomware profits prove that this specialisation approach works [15]. As the RaaS model is successful, TSS businesses can benefit from the division as well.

In a nutshell, the *USA v. Anjum* [9] case demonstrates how TSS business models became more profitable by embracing a refined business operation model. The division of business processes is nothing new, as Smith already pointed out the benefits in the 18th century. Furthermore, the RaaS model demonstrates that illegal businesses can also benefit from specialisation and the division of labour. Following the success of the RaaS model, TSS also embraced the concept of Smith. As a result of the business model change, highly-specialised TSS operations can achieve higher revenues and larger profit margins.

F. Communication Skills Improvements

Specialisation enables TSS businesses to perfect their tools and methodologies, as discussed. To give an example, one of these improvements concerns the communication skills of the TSS call centres. Contrary to popular belief, TSS call centre staff are fluent in English and constantly improve their language skills. In their podcast, Bhattacharjee and Benson [16] reveal that call centres in South Asia were found to employ English tutors on-site. The purpose of the language teachers is to make the TSS call centre staff speak English more fluently [16]. According to Bhattacharjee and Benson [16], better communication skills enable call centres to engage US-based victims more successfully.

Another benefit of specialisation is the application of subliminal, neurolinguistic and other *verbal practices* [17]. According to the Bhattacharjee and Benson [17] podcast episode, the scammers aim to establish a rapport with the victim early in the call. To do that, the call centre operator makes the target answer 'yes' to a range of innocuous questions as often as possible. The questions aim to develop a pattern of agreement between the scammer and the victim. Why? Because when the scammer orders the victim to hand the money over, the victim is more likely to comply [17]. Specialisation allows call centres to focus their resources on verbal manipulation techniques.

G. Scambaiting Evasion

Lastly, the division of labour allowed TSS call centres to develop standard operating procedures for identifying scambaiters. *Scambaiting* can damage any TSS business because they take time from the money-making scams and draw unwanted public attention to the operation. Therefore, TSS businesses began to screen their targets to ensure the person on the call was not associated with scambaiting.

Scambaiting is a phenomenon that aspires to fight online scams such as TSS [18]. An individual or several people can perform scambaiting acts as part of a scambaiting group. In short, a scambaiter typically contacts a TSS call centre and pretends to be a victim. Their purpose is to waste the TSS call centre's time or gather information for later naming and shaming the perpetrators [19]. Kitboga (a pseudonym) is a popular TSS scambaiter regularly performing on the YouTube and Twitch platforms [19]. Kitboga occasionally relies on driving simulation computer games to pretend they are driving to the nearest store for the payment cards. On one occasion, Kitboga wasted circa 16 hours of the criminals' time by pretending to drive to the nearest supermarket per the scammers' request [18]. In short, scambaiters are bad for the TSS business due to the time-wasting and unwanted attention aspects.

Therefore, TSS scammers developed a number of practices to ensure the person on the line was not a scambaiter. To illustrate, in one of Kitboga's videos, the scammer on the phone was asking Kitboga to operate the horn of their car [20]. This unusual request was there to prove Kitboga was driving an actual vehicle. As Kitboga is an experienced scambaiter, they tooted the virtual horn within the driving simulator instead. However, inexperienced scambaiters may fail this anti-scambaiter test. In contrast, Bhattacharjee and Benson [17] argue that the horn-blowing exercise is meant to assert dominance over the victim rather than weeding out scambaiters.

In their research, Rauti and Leppanen [8] showcase additional techniques aim to identify scambaiters. For example, the researchers found on a remote desktop session with a TSS call centre that the scammer opened the Google Chrome browser history and the Windows prefetch folder [8]. The scammer's purpose was to determine if the victim's PC was a real home computer or a virtual machine (VM) built for TSS research purposes [8]. Typically, home computers have a rich browser and application launch history, while VMs freshly built for research do not. This practice is common in the malware industry and is known as VM evasion or sandbox evasion techniques.

In conclusion, the growing popularity of scambaiting made TSS schemes to combat the phenomenon. Scammers can ask their victims to perform unusual things to prove they are not scambaiters. Also, TSS schemes can borrow battle-tested methods from the world of malware, like the VM inspection practices. These anti-scambaiting practices are evidence of the TSS operators' attention to detail and their ability to adapt to new changes and challenges.

H. Payment Processing Shenanigans

Finally, I found various enhancements in the TSS payment processing practices. For instance, the latest trend in TSS operations is to prefer *immutable and untraceable payment methods* over credit cards and PayPal transfers [2]. As a result, criminals embraced new payment methods and implemented complex money-laundering procedures. The purpose of these new additions is to increase profits and lower the chances of being caught.

In their report, Microsoft [2] found that TSS call centres are using new payment methods to extort money. Although the two most prominent payment options are still credit cards and PayPal, these two have fallen from favour since 2018 [2]. Instead, the research found that gift cards and electronic bank transfers (EFT) are growing in popularity [2].

When the scammer prefers the gift card method, the victims are pressured into buying them in a nearby supermarket. Once the cards are purchased, the victim is ordered to read the scratch codes from the back. Then the scammer redeems the codes online, and the victim has no option to get their money back. According to Microsoft, the gift card method is the fourth most abused payment option in 2021. However, one significant benefit of gift cards is the irreversible nature of the payments.

Furthermore, Microsoft [2] reports that 32% of the victims ended up paying via EFT, making bank transfers the third most abused choice. However, EFT can be reversible, but only for a limited time once the settlement is complete. According to Fillingham and Godyla [21], shifting to gift cards and EFT from PayPal and credit cards is a conscious decision of the criminals. The big financial institutions behind PayPal and credit cards can stop and reverse suspicious TSS payments and offer refunds when someone becomes a victim of fraud [21]. As a consequence, the perpetrators prefer payment methods without any robust consumer protection regime like gift cards and EFTs.

The second improvement to the payment processing practices is the increased complexity. In their podcast episode, Bhattacharjee and Benson [22] describe how complicated it became to distance the victim from their money. Bhattacharjee and Benson explain that the victim has to buy one or more 'stored value cards' at the nearest shop first. Then the victim is ordered to scratch the back of the cards and read the numbers to the scammer. Then, using this code, an accomplice of the scammer transfers the money from the victim's 'stored value card' to a 'general purpose reloadable (GPR) card' in the criminal's possession. The GPR card is known as a Visa or MasterCard prepaid debit card. The next step is the accomplice buying a money order (e.g., Western Union, MoneyGram) with the GPR card. Then, the money order is deposited into a bank account, and the money can be transferred anywhere in the world. Bhattacharjee and Benson [22] suggest that this elaborate process is meant to distance the money from the victims as far as possible. According to the Department of Justice [23] press release, the scale of business operation from Bhattacharjee and Benson's story was in the "tens of millions of dollars".

These recent changes to payments enable TSS operations to permanently make the victims' money disappear within the financial system. First, the new payment methods warrant that the money exchange cannot be reversed even when the victim realises they got scammed. Second, the convoluted money laundering scheme ensures that the funds cannot be traced and recovered once the transaction is settled. In summary, specialisation allowed TSS schemes again to perfect their methodologies to become better at stealing and keeping the money scammed out from the victims.

V. Conclusion

In this paper, I have presented a literature review covering the latest innovations within the TSS industry. Unfortunately, my conclusion is that the sophistication of TSS schemes has increased in the past few years. This growing sophistication allows TSS businesses to steal more considerable sums of money. Furthermore, the additions target those more likely to fall for the scam. The drivers of this recent success of TSS are productivity improvements, specialisation, and professionalisation of the TSS business. In short, the growing sophistication allows TSSs to identify and engage more gullible people, who are more likely to get scammed.

Firstly, I found that automation enables a highly-professional approach to reaching out to potential victims. One significant change in the TSS call centres is the shift from cold calls to software diallers. This robocall method can reach more people and doubles down as a simple pre-screening technique. In addition, the online advertisements of TSS also underwent a major overhaul. Due to the recently implemented evasion and obfuscation techniques, the pop-up ads and TSS websites are more likely to display on the victims' computers. Further enhancements include black hat SEO practices, better resiliency to take down requests, and cybersecurity solutions. In short, the dialler campaigns and the online advertisements became much more effective.

The second factor of TSS's triumph is the business model's professionalisation. Following the centuries-old concept of specialisation and division of labour, TSSs split their operations into separate business entities. Consequently, each entity could optimise its core business processes for better performance. For example, TSS call centres were found to employ English tutors on-site to enhance the scammers' verbal skills. Therefore, better English skills could increase the chance of success of the TSS call centres. Further additions to the communication skill set include subliminal, neurolinguistic and psychological capabilities. In short, specialisation allows TSS businesses to develop new and innovative ways to maximise profits and operate more efficiently.

Last, I found that the recent payment processing changes are valuable additions to TSSs. For instance, TSS operations have developed long and convoluted payment chains that can distance the victims from their money more effectively. Furthermore, TSS schemes are gravitating towards new payment methods, such as gift cards and bank transfers, because these are quasi-irreversible compared to the old methods. These changes allow TSS businesses to safeguard the stolen funds from payment institutions and law enforcement.

My research findings demonstrate that TSS has become a ruthless and highly professional affair. Every aspect of TSSs transformed into an effective business venture using innovative tools and practices. As a result, TSS fraud is a striving industry with a competency to maximise its revenues and profits. Moreover, due to the more refined TSS, criminals can identify and target those more likely to fall for the scam. These factors explain the record incomes amid the declining number of engagements.

References

[1] Malwarebytes, 'The Anatomy of Tech Support Scams,' 18 Oct. 2016, p. 6. [Online]. Available: https://www.malwarebytes.com/pdf/white-papers/anatomytechsupportscams.pdf (visited on 30/09/2022).

[2] Microsoft, 'Global Tech Support Scam Research,' Jul. 2021. [Online]. Available: https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2021/07/MSFT-2021-Global-Tech-Support-Scam-Research-Report.pdf (visited on 02/10/2022).

[3] Y. Bhattacharjee and E. Benson, *Chameleon: Scam Likely*, 2022–. [Online]. Available: https://podcasts.apple.com/au/podcast/chameleon-scam-likely/id1532225667.

[4] L. Zeltser. 'Scammers Prescreen Victims for Tech Support Scams via Twitter and Phone.' (17 Mar. 2015), [Online]. Available: https://zeltser.com/prescreening-tech-support-scam/ (visited on 27/09/2022).

[5] B. Srinivasan, A. Kountouras, N. Miramirkhani *et al.*, 'By Hook or by Crook: Exposing the Diverse Abuse Tactics of Technical Support Scammers,' version 1, 2017. DOI: 10.48550/ARXIV.1709.08331. [Online]. Available: https://arxiv.org/abs/1709.08331 (visited on 26/08/2022).

[6] N. Miramirkhani, O. Starov and N. Nikiforakis, 'Dial One for Scam: A Large-Scale Analysis of Technical Support Scams,' version 3, 2016. DOI: 10.48550/ARXIV.1607.06891. [Online]. Available: https://arxiv.org/abs/1607.06891 (visited on 13/08/2022).

[7] S. Chandrayan. 'Tech Support Scams Increasing in Complexity – Part 3.' (28 Nov. 2018), [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tech-support-scams-part-3 (visited on 27/09/2022).

[8] S. Rauti and V. Leppanen, '"You have a Potential Hacker's Infection": A Study on Technical Support Scams,' in *2017 IEEE International Conference on Computer and Information Technology (CIT)*, Helsinki: IEEE, Aug. 2017, pp. 197–203, ISBN: 978-1-5386-0958-3. DOI: 10.1109/CIT.2017.32. [Online]. Available: https://ieeexplore.ieee.org/document/8031474/ (visited on 26/08/2022).

[9] *Usa v. anjum*, 2020. [Online]. Available: https://www.pacermonitor.com/public/case/35844656/USA_v_Anjum.

[10] Y. Bhattacharjee and E. Benson, *Meet the Callers*, 8 Aug. 2022. [Online]. Available: https://podcasts.apple.com/au/podcast/scam-likely-episode-3-meet-the-callers/id1532225667?i=1000571611968.

[11] B. Schwartz. 'Google updates Penguin, says it now runs in real time within the core search algorithm,' Search Engine Land. (23 Sep. 2016), [Online]. Available: https://searchengineland.com/google-updates-penguin-says-now-real-time-part-core-algorithm-259302 (visited on 21/10/2022).

[12] David Harley. 'Tech Support Scams: Top of the Pop-Ups,' WeLiveSecurity. (7 Oct. 2015), [Online]. Available: https://www.welivesecurity.com/2015/10/07/tech-support-scams-top-pop-ups/ (visited on 09/10/2022).

[13] A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (Wordsworth Classics of World Literature). Ware: Wordsworth editions, 2012, 974 pp., ISBN: 978-1-84022-688-1.

[14] Department of Justice. 'Indian National Pleads Guilty in Telemarketing Scam.' (24 Aug. 2020), [Online]. Available: https://www.justice.gov/usao-ri/pr/indian-national-pleads-guilty-telemarketing-scam (visited on 28/09/2022).

[15] K. Baker. 'Ransomware as a Service (RaaS) Explained,' crowdstrike.com. (7 Feb. 2022), [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (visited on 11/10/2022).

[16] Y. Bhattacharjee and E. Benson, *Tell the Cops*, 22 Aug. 2022. [Online]. Available: https://podcasts.apple.com/au/podcast/scam-likely-episode-5-tell-the-cops/id1532225667?i=1000571612403.

[17] Y. Bhattacharjee and E. Benson, *Chase the Runners*, 1 Aug. 2022. [Online]. Available: https://podcasts.apple.com/au/podcast/scam-likely-episode-2-chase-the-runners/id1532225667?i=1000571611523.

[18] Kitboga, Ed., *I Tricked 2 Scammers Into Wasting 16 Hours - Ep. 1*, 18 Jul. 2020. [Online]. Available: https://www.youtube.com/watch?v=smgEacoxxYQ (visited on 01/10/2022).

[19] S. Laato and S. Rauti, 'Scambaiting as a Form of Online Video Entertainment: An Exploratory Study,' in *Proceedings of the 12th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2020)*, ser. Advances in Intelligent Systems and Computing, A. Abraham, Y. Ohsawa, N. Gandhi *et al.*, Eds., vol. 1383, Cham: Springer International Publishing, 2021, pp. 738–748, ISBN: 978-3-030-73689-7. DOI: 10.1007/978-3-030-73689-7_70. [Online]. Available: https://link.springer.com/10.1007/978-3-030-73689-7_70 (visited on 13/08/2022).

[20] Kitboga Shorts, Ed., *Kitboga Proves He's Using A "Real Car"*, 26 Aug. 2021. [Online]. Available: https://www.youtube.com/watch?v=o7y6dPsy_As (visited on 01/10/2022).

[21] N. Fillingham and N. Godyla, *Mary Had a Little Scam Report*, 5 Aug. 2021. [Online]. Available: https://thecyberwire.com/podcasts/security-unlocked/39/transcript.

[22] Y. Bhattacharjee and E. Benson, *Follow the Money*, 1 Aug. 2022. [Online]. Available: https://podcasts.apple.com/au/podcast/scam-likely-episode-1-follow-the-money/id1532225667?i=1000571607485.

[23] Department of Justice. 'Owner and Operator of India-Based Call Centers Sentenced to Prison for

Scamming U.S. Victims out of Millions of Dollars.' (30 Nov. 2020), [Online]. Available: https://www.justice.gov/opa/pr/owner-and-operator-india-based-call-centers-sentenced-prison-scamming-us-victims-out-millions (visited on 02/10/2022).