Understanding, Measuring, and Detecting Modern Technical Support Scams

Jienan Liu*, Pooja Pun^, Phani Vadrevu^, Roberto Perdisci*

* University of Georgia
^ University of New Orleans

IEEE European Symposium of Security and Privacy (Euro S&P)
Delft, Netherlands, 2023
Technical Support Scams (TSS)
Technical Support Scams (TSS)
TSS defense: State-of-the-art

• “Text-based” detection approach [1].
  • Prone to false positives as search engines are also inherently “text-based”.
  • Scammers often “evolves” into multiple scam topics easily.

We need a robust, preferably scam-agnostic defensive approach based upon a deeper understanding of the TSS ecosystem!

[1] Exposing search and advertisement abuse tactics and infrastructure of technical support scammers, WWW 2018
Finding TSS Scammers...

Tech Support all calls
Public · 3.3K members · 10 posts a week
This group is about getting all tech support calls

Calls available according to new Google policies with good flow and quality for USA, UK and Australia besides this new updated tfn's of Zoom, Pbx and

Related groups
Tech Support kolkata business
Public · 2.2K members · 4 posts a day
GOOD NEWS FOR ALL TECH SUPPORT BUSINESS. If you are facing problems mentioned above then dont panic. We are offering a customize solution to your...

Tech Support calls..
Public · 7.6K members · 8 posts a month
Window Pop-up (Blue screen, Microsoft Security Essential) call available with relentless flow. These are high conversion of 30-65%.
Basis for Understanding TSS Ecosystem

• 10 Facebook groups, 13 WhatsApp groups
• Obtained multi-month data from these groups.
• The data that revealed day-to-day TSS business operations.

• We subject the data to Qualitative Analysis
TSS Operations Map

Each arrow indicates a category of post found on WhatsApp & Facebook groups.

The source of an arrow indicates which unit made a post on the group. The destination of the arrow indicates which unit the post was intended to.
TSS Agents: hiring ads

Openings for 10 Sales Agents in North & west Delhi.
We are hiring candidates on commission basis. Great incentives are also promised.
Candidate must have experience with Sales for any of Amazon Refund, Cash app, Zelle, banking calls, Paid Email, Refund and tech support Calls.
"Good call flow available."

$$$ Next day or Weekly payout also available. Unlimited earnings.
-5 days working
-great work environment
Minimum working experience: 6-12 Months
Call or whatsapp right now: 989-989-5800
Dm for more info
TSS web developers: live victim call sales

TSS Web developers promote TSS sites using Blackhat SEO techniques or search-based ads.
Toll-Free Number Providers

TFN/DID AVAILABLE
For Routing
For Own Center
One Month Guarantee
For Non Suspension

IF ANY THING HAPPEN WRONG
WITHIN A MONTH YOU WILL GET
ANOTHER TFN/DID WITHIN 5 MIN

TSS Website
Developers

Toll-Free Number
Providers

888-000-0000
888-111-2222
800-333-3333
888-444-4444

Call centers
Money laundering offers

whatsapp no update +1[redacted]
Genuine guy u can meet me if you want after u can start working with me DM for proofs,rates,query......

1. All major Giftcard blocking @goodrate
2. Physical wire 70% payout
3. Fedex 70% payout
4. Cashapp
5. Paypal
6. Gpay

Typical money laundering fees is around 30-40%
If you are looking for usa based data or leads your search ends here. We are providing almost all type of leads for international process. Following are leads type we are providing:

1) Tech Support Leads
   (sales leads, refund leads, hp leads, dell leads, raw data)

2) Payday Leads
   (Real time payday leads, Fresh pay day leads)

3) Old age leads
   (plus 60 years customer with all details)

Book your order now:

Often highlight data of seniors who are more vulnerable to these scams.
Miscellaneous: Announcements

Warnings about impending police raids or dishonest scam operators
## TSS Data Summary

<table>
<thead>
<tr>
<th>TSS category</th>
<th># Posts</th>
<th># Unique posts</th>
<th># Post authors</th>
<th># Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSS agent hiring</td>
<td>1322</td>
<td>516</td>
<td>245</td>
<td>1005</td>
</tr>
<tr>
<td>Money launderers</td>
<td>6677</td>
<td>1435</td>
<td>541</td>
<td>3097</td>
</tr>
<tr>
<td>TSS webmasters</td>
<td>5167</td>
<td>1411</td>
<td>525</td>
<td>1908</td>
</tr>
<tr>
<td>Toll-free number providers</td>
<td>1129</td>
<td>258</td>
<td>107</td>
<td>190</td>
</tr>
<tr>
<td>Victim data sales</td>
<td>951</td>
<td>311</td>
<td>121</td>
<td>129</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TSS category</th>
<th># Posts</th>
<th># Unique posts</th>
<th># Post authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSS agent hiring</td>
<td>161</td>
<td>104</td>
<td>57</td>
</tr>
<tr>
<td>Money launderers</td>
<td>8887</td>
<td>2138</td>
<td>787</td>
</tr>
<tr>
<td>TSS webmasters</td>
<td>9444</td>
<td>2826</td>
<td>815</td>
</tr>
<tr>
<td>Toll-free number providers</td>
<td>3104</td>
<td>511</td>
<td>226</td>
</tr>
<tr>
<td>Victim data sales</td>
<td>2757</td>
<td>519</td>
<td>204</td>
</tr>
</tbody>
</table>
**TSS web developers: Call prices**

<table>
<thead>
<tr>
<th>Brand name</th>
<th>min</th>
<th>median</th>
<th>max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>$2.52</td>
<td>$4.90</td>
<td>$8.05</td>
</tr>
<tr>
<td>iOS</td>
<td>$3.15</td>
<td>$4.20</td>
<td>$9.10</td>
</tr>
<tr>
<td>PayPal</td>
<td>$5.11</td>
<td>$6.37</td>
<td>$7.70</td>
</tr>
<tr>
<td>Cash App</td>
<td>$7.70</td>
<td>$10.50</td>
<td>$11.90</td>
</tr>
<tr>
<td>Norton</td>
<td>$2.52</td>
<td>$4.90</td>
<td>$8.05</td>
</tr>
<tr>
<td>Roku</td>
<td>$5.46</td>
<td>$6.02</td>
<td>$10.50</td>
</tr>
<tr>
<td>EBay</td>
<td>$5.88</td>
<td>$8.40</td>
<td>$8.40</td>
</tr>
<tr>
<td>Windows</td>
<td>$5.60</td>
<td>$5.60</td>
<td>$5.60</td>
</tr>
<tr>
<td>Delta</td>
<td>$13.30</td>
<td>$13.30</td>
<td>$13.30</td>
</tr>
</tbody>
</table>

Median cost of each call is US $6

=> The average revenue for each victim call should be more than US $6!
TSS Data collection

- Elaborate pipeline beginning with a volunteer scam baiting community website
- 806 confirmed TSS websites
- Used LDA to derive 44 scam topics!
Insights for Detection (1/3)

• Explicit age-based targeting of seniors.
  • **RQ**: Are there any discernible visual traits in the TSS websites?
TSS Site measurements: Visual indicators

• Median phone number text area:
  • TSS: 2856 pixels
  • Benign 3rd party TS: 1380 pixels
  • Benign official sites: 1100 pixels

• 50% of TSS web pages has phone number repetitions vs. only 3% of official Benign site pages
Insights for Detection (2/3)

• Explicit age-based targeting of seniors.
  • \textbf{RQ}: Are there any discernible visual traits in the TSS websites?

• Blackhat promotion of TSS websites.
  • \textbf{RQ}: Can this be utilized to detect TSS websites?
TSS Site measurements: Blackhat SEO

- Many TSS Backlinks appear on spam-infested pages.
- Sub-sites of microsoft.com, ibm.com, hp.com, gnu.org are allowing followable links in profile pages that get abused!

Likely due to inorganic link-farming Blackhat techniques used by TSS site developers.
Insights for Detection (3/3)

• Explicit Age-Targeting.
  • RQ: Will this imply any visual characteristics in the TSS websites useful for detecting TSS sites?

• Blackhat promotion of TSS websites.
  • RQ: Can this be utilized to detect TSS websites?

• Effects of TSS Compartmentalization.
  • RQ: Are same phone numbers being re-used across campaigns?
  • RQ: Is there discernible *dynamism* (temporally) in phone number of a given TSS site?
TSS Site measurements: Website Records

• 65% of TSS sites share phone numbers with another TSS site!
• Only 0.58% benign 3rd party TS sites do so

• 45% of TSS sites changed phone numbers.
• Only 1.5% of benign 3rd party TS sites did so!

• 81.6% TSS sites use toll-free phone numbers.
• Only 9.5% benign 3rd party TS sites do so!
Topic-Agnostic TSS Detection: TASR

(a) Cross-Validation RoC

(b) Topic generalization RoC
Conclusion

• First publicly available labelled TSS datasets and an effective detection method.
  
  Code/data available at: https://github.com/NISLabUGA/TSS_ESP23

• Several insights into TSS marketplaces for future research.

• Immediate impact: Detailed disclosure reports to Google, Meta and law enforcement authorities.