

Test. Educate. Protect.

**SOCIAL-ENGINEER**



2023

STATE OF  
VISHING REPORT

# INTRODUCTION

Over the last decade, our lives have been radically transformed by technology, from social media and online shopping to digital pay slips and tax documents. What's more, following the COVID-19 pandemic, the number of organizations conducting business electronically has increased exponentially.

But it is not just the corporate world that has embraced this new normal, digital transformation in healthcare and forensic investigation is also increasing. Although this transformation supports the convenience and operational efficiencies across sectors, it also opens the doors to an increased level of information security threat.

It does not come as a surprise that, especially during the global pandemic, we saw a massive increase in human based attacks in the form of social engineering. Increases in all forms of phishing, vishing, SMiShing, and impersonation, attacks have become daily news. And although we focus on phishing as the number one vector used by these attackers, vishing is quickly taking its place in the ranks of the most devastating attacks. So much so, that in 2015, the word 'vishing' entered the Oxford dictionary as an official word to describe phone-based phishing attacks.



Yet, despite vishing being a dangerous and pervasive social engineering attack vector, very little is empirically, or operationally, known about vulnerability factors based on first-hand data. Unlike phishing, where emails used for attacks can be collected, it is very rare for phone calls to be collected, recorded, and analyzed. This very problem is addressed in this inaugural State of Vishing Report.

## Report Overview



In the **2023 State of Vishing Report**, we first examine the threat landscape and analyze data from 83,053 vishing calls, carried out first-hand by the team at Social-Engineer, LLC, to identify vulnerability factors and data compromise rates. Finally, we address the lack of operational and academic understanding regarding vishing and discuss ways to improve data security. This is the first industry report solely focused on human-to-human vishing data to date.

### What is Vishing?

#### DEFINITIONS

Vishing, also known as voice phishing, is the practice of eliciting information or attempting to influence action via the telephone.

The goal of vishing is to obtain valuable information, contributing to the direct compromise of a target. Attackers may “spoof,” or fake, their outgoing phone number to add authenticity to their attack. Additionally, some bad actors may use voice changers to conceal their identity or even use artificial intelligence-based software to mimic authentic voices. High profile examples of such vishing attacks will be detailed in section one of this report.

Vishing may also be carried out by professional social engineers, but for different reasons. A professional social engineer is an individual who has been hired by an organization to run simulated attacks on their human network, as a means to uncover vulnerabilities.

## Related Terms Explained

### OSINT

Open-source intelligence (OSINT) is the practice of collecting information from publicly available sources.

### Spear Vishing

When information obtained during OSINT is used to tailor an attack specific to the chosen individual(s)

### Penetration Testing

Penetration testing (also called pen testing) is the practice of testing a computer system, network, web application or onsite perimeter to find vulnerabilities that a malicious attacker could exploit. At Social-Engineer, we call this Adversarial Simulation and that is how it will be referred to in this report.

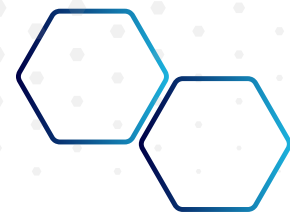
### Pretext

As defined by Merriam-Webster's, pretexting is the practice of presenting oneself as someone else in order to obtain private information.

### Flag

The data or access the attacker is seeking to compromise from the target.

# CONTENTS



<b>Introduction</b>	<b>1</b>
<b>SECTION I</b>	
<b>Threat Landscape</b>	<b>5</b>
<b>Impersonation</b>	<b>7</b>
<b>A Closer Look at Vishing Topics</b>	<b>9</b>
<b>High-Profile Examples</b>	<b>14</b>
<b>SECTION II</b>	
<b>Compromise Rates &amp; Vulnerability</b>	<b>16</b>
<b>Vulnerability Factors</b>	<b>19</b>
<b>Time of Day</b>	<b>20</b>
<b>Sex of Target</b>	<b>24</b>
<b>Sex of Caller</b>	<b>25</b>
<b>Interaction Data</b>	<b>26</b>
<b>SECTION III</b>	
<b>Current Understanding &amp; Education</b>	<b>28</b>
<b>A Lack of Lessons from Academia</b>	<b>29</b>
<b>The Problem of Ethics</b>	<b>30</b>
<b>Future Directions</b>	<b>33</b>
<b>Conclusions</b>	<b>34</b>
<b>Contact Us</b>	<b>35</b>



# 1

# THREAT LANDSCAPE

There is a dangerous mindset lurking among the general population that “I’m not important enough for a hacker to target me” or “hackers only go after big businesses.” But that is simply not true. One of the largest scale attacks we have seen in the vishing world in 2022 was against grandparents. The caller makes believe they are a grandchild and convinces the grandparent to send bail money or support the grandchild for another financial loss.

Often times these attacks cost the grandparent, or even the parent, thousands of dollars at once. Regardless of whether you are a big business, small business, start up, non-profit, charity, or even a grandparent or consumer, you are a potential target. If there is money coming in, scammers make it a goal to find a way to get it out.



According to a report from the Federal Trade Commission (FTC), the phone (inclusive of vishing and smishing) is the most common attack vector used by scammers when trying to reach a target. Phone based attacks are typically more successful than other attack vectors such as phishing, which uses email to reach a target.

## Threat Landscape



### What Information Can Be Obtained?

Attackers usually obtain phone numbers from an organization's website, in addition to any specific routing emails used for customer support. Criminals can also collect company information from social media platforms and other open-source intelligence gathering (OSINT). Attackers may call from a spoofed or private phone number. The data that malicious attackers may target is potentially limitless, but the most common information that attackers may try to obtain are:

- Email addresses
- Manager names/contact information
- Company organizational information
- Direct phone numbers
- Addresses
- Social Security numbers
- User credentials
- Multi-factor authentication tokens or codes
- Technology used (hardware, software, security, etc.)
- Banking/Financial data
- Credit Card Information
- Vendor Information
- Processes in place or Intellectual Property Details



---

**\$1.2  
Billion**

**Lost to  
Imposter Phone  
Scams**

---

## Impersonation

The FTC also reported that nearly 500,000 phone scam reports were related to imposter scams, leading to a total loss of \$1.2 billion USD.


Imposter scams, or impersonation, can be defined as the *“practice of pretexting as another person with the goal of obtaining information or access to a person, company, or computer system.”*

For example, in their attacks, malicious attackers may attempt to impersonate individuals or organizational representatives that are typically perceived as trustworthy, such as government agency representatives.

### Some of the Most Commonly Used Vishing Pretexts are:

#### **The IRS (Internal Revenue Service)**

In the IRS’ 2021 dirty dozen list, which represents the worst of the worst tax scams, the IRS reported that vishing scams relating to federal tax liens are on the increase. These scams involve malicious actors typically using phone spoofing and fake IRS badge numbers to make their calls seem legitimate.





## Threat Landscape

### COVID-19

During 2020 to 2022, the global COVID-19 pandemic supplied the perfect cover for vishing scams, with attackers impersonating contact tracing and testing representatives. Additionally, attackers were also reported to have commonly impersonated health care providers under the false pretense of booking a COVID vaccination.

### Tech Support

Each year, tech support scams continue to be a common pretext for malicious attackers. During these scams, the attacker will typically call a company employee, lead them into believing their computer is compromised, and then offer to help fix the problem. The 'fix' will allow the attacker access to the desktop, credentials, or other secure information.

### Crypto Scams

In mid-2020 Bitcoin had an over 200% spike in its price. Quickly scammers started fake crypto scams that attracted many to part with their very valuable crypto currency for the promises of massive returns on their investment.

## A Closer Look at Vishing Topics

When looking to examine, what the general public understands about vishing, or if vishing is being discussed in social spaces, the data is limited. As such, Social-Engineer, LLC worked with PhD researcher Aneese Baquir, of Ca’Foscari University of Venice, Italy to identify how frequently people talked about vishing on social media and what the context of these discussions were centered around.

To achieve this, Twitter was used as the source of data. This is because Twitter is a popular platform with many active users where individuals and organizations tweet their views and ideas, share news, and amplify other perspectives.




---

### Data Collection and Processing

Data was collected from Twitter using a search query (#vishing OR #vished OR ‘voice phishing’ OR ‘fraudulent phone call’ OR ‘scammer call’ OR ‘scam call’). The process of data collection was performed by using the Twitter API for academic research.

## Threat Landscape

The data gathered was publicly available and no data from private accounts was included in our dataset. It includes all the tweets published with any of the hashtags in our search query during the period from 01 January 2019 to 27 October 2022, resulting in 1.34+ Million Tweets. Table 1 provides a breakdown of the data.

	2018	2019	2020	2021	2022	Total
All TWEETS	216,234	253,910	294,693	310,730	267,458	1,343,055
TWEETS After Removing Duplicates (ReTWEETS)	89,131	111,426	135,770	148,099	133,626	618,052

Table 1: Overview of Twitter data from 2018 to 2022

The sheer quantity of individuals discussing this topic provides an insight into the scale of the issue. As can be seen in Table 1, 2021 had the highest contribution of Tweets with any of the hashtags of our search query, with 310,730 tweets, including retweets, in that year being related to vishing.



## Threat Landscape

### Themes

To determine the most prevalent themes in the public discourse surrounding phone scams or vishing calls, we utilized BERTopic (Grootendorst, 2022)<sup>1</sup>, a cutting-edge topic modeling tool.

BERTopic is a tool that helps us understand the main topics that are being discussed in a large number of documents. It does this by using advanced language technology that was already developed and trained by experts. It can analyze the text in the documents and identify patterns in the words used, so that it can group similar documents together. This process is called "clustering", and it helps us to see which documents are talking about similar things (Sammut and Webb, 2010)<sup>2</sup>. To do this, BERTopic uses something called "TF-IDF", which is a way of understanding how important certain words are in a document. By looking at the frequency of words in each document, it can identify which words are most important for that particular document. By applying this technique across all the documents in our dataset, BERTopic can then cluster similar documents together and create topic representations.

Overall, BERTopic is a powerful tool that helps us make sense of large amounts of text. It can identify key topics and themes across multiple documents, which can be useful for analyzing data and gaining insights into important trends.

The five most talked-about topics for each year are shown in the following graphs.

<sup>1</sup>Grootendorst, M., 2022. *BERTopic: Neural topic modeling with a class-based TF-IDF procedure*.

<sup>2</sup>Sammut, C., Webb, G.I. (Eds.), 2010. *TF-IDF*, in: *Encyclopedia of Machine Learning*. Springer US, Boston, MA, pp. 986–987. [https://doi.org/10.1007/978-0-387-30164-8\\_832](https://doi.org/10.1007/978-0-387-30164-8_832)

# Threat Landscape

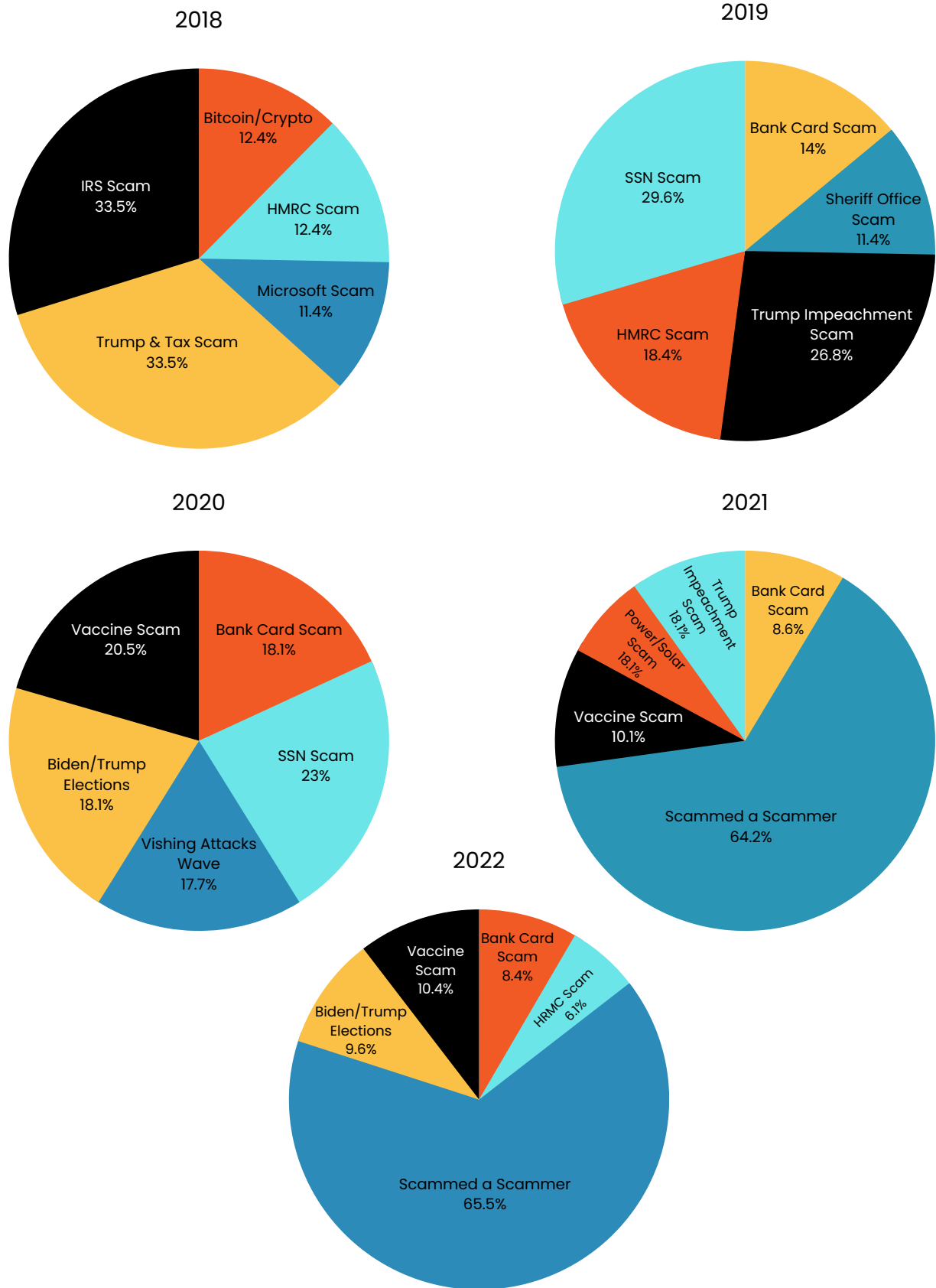


Figure 1: Twitter data detailing the five most prevalent topics tweeted about for each year from 2018 to 2022

## Threat Landscape



As can be seen, in 2018, discussions centered around Donald Trump and the Tax scam allegations against him, followed by the IRS scam. The following year, 2019, saw the SSN scam take center stage, followed by the Trump impeachment scam. It is worth noting that "Bank card scam" has remained a consistent topic of discussion from 2018 to 2022. Likewise, the "Vaccine scam" has been a recurring theme since 2020.

However, the topic that has dominated the discussions in the past two years has been "scammed a scammer".

The concept of "scammed a scammer" refers to instances where individuals have successfully outsmarted or deceived individuals who were attempting to scam them. This can involve individuals taking proactive measures to thwart the efforts of scammers, such as by providing false information or manipulating the situation to their advantage. The prevalence of this topic in recent years highlights the ongoing issue of scams and fraud in society, as well as the ingenuity of some individuals in finding ways to protect themselves from such schemes.

Furthermore, results suggest that the prominence of bank card scams is not impacted by external factors, whereas the rise of vaccine scams may be related to the coronavirus pandemic.

## High Profile Examples

Vishing attacks have taken center stage in many news reports over the last few years. Let's look at some high-profile examples you may recognize.

### **TWITTER**

In the summer of 2020, Twitter became the target of a coordinated vishing attack. By impersonating internal Twitter employees, attackers made vishing calls to Twitter's tech support and consumer services employees. The attackers' instructions were simple, "we need you to reset your password." As a result, attackers gained valuable credentials such as usernames, passwords, and multi-factor authentication codes. This vishing attack led to the hijacking of high-profile Twitter accounts.

### **APPLE**

In 2019, this vishing scam targeting iPhone users started making the rounds, with the caller stating that they are a representative of Apple, Inc and are calling due to suspicious activity associated with the user's iCloud account or compromised Apple ID information. Additionally, the automated call displayed Apple's real customer support phone number and logo.



## Threat Landscape

### MICROSOFT

In the beginning of 2020, Microsoft announced the end of support for Windows 7. Seizing this opportunity, attackers began running scams known as the “Expiring License” scam, supposedly calling to suggest upgrading to Windows 10 or simply to let them know that the license is expiring. The true motivation for calling was to gain remote access to victims’ computers and thereby accessing their banking information and login credentials.

### FORTELUS CAPITAL MANAGEMENT, LLS

In July 2015, the CFO (Chief Financial Officer) of Fortelus Capital Management LLP, a London-based hedge fund, received a phone call from an attacker impersonating a financial representative from Coutts, the hedge fund’s bank. The caller stated there had been suspicious charges on the company’s account that needed to be cancelled. The CFO agreed to generate codes from the bank’s smart card security system to help the caller with the removal of the “fraudulent” charges. This resulted in £742,668 (\$1.2 million USD) being withdrawn from the organization’s account.

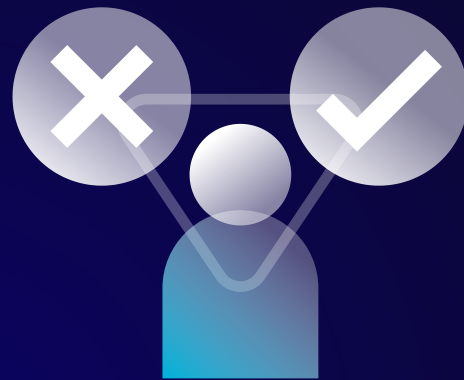
**In each of these examples, a high-profile person or company was targeted to gain maximum benefit for the attacker in the least amount of time. Many high-profile attacks lead to not only millions of dollars in loss, but thousands or millions of people affected by the attack.**



# 2

## COMPROMISE RATES & VULNERABILITIES

As stated before, it is very hard to find actual vishing data to use for analysis. Fortunately, Social-Engineer, LLC has conducted 83,053 human-to-human vishing calls through 2022 and coded them for analysis to help us understand the problem and what can be done.



With this data we look for a few points:

- **Shutdown:** The person called does not give over information but shuts down the attacker.
- **Compromise:** The person called gives over information that could have led to a breach for the company involved.
- **Voicemail Compromise:** The person called does not answer but has a voicemail message that gives out information that could lead to a breach of data.



Please note, what is deemed as a compromise is determined by the client, such that in some cases a “compromise” may refer to a single data type (i.e. User ID, Password, etc.), or flag, obtained while in other cases it refers to multiple flags obtained. The data was also cleaned so that calls which were interrupted due to technological errors were removed.

Let’s first look at overall compromise rates, that is calls which collected data that would be considered a compromise for the companies called. We broke this down into two graphs, 01 January 2020 – 31 December 2021 and then all of 2022:

## Compromise Rates

2020 – 2022

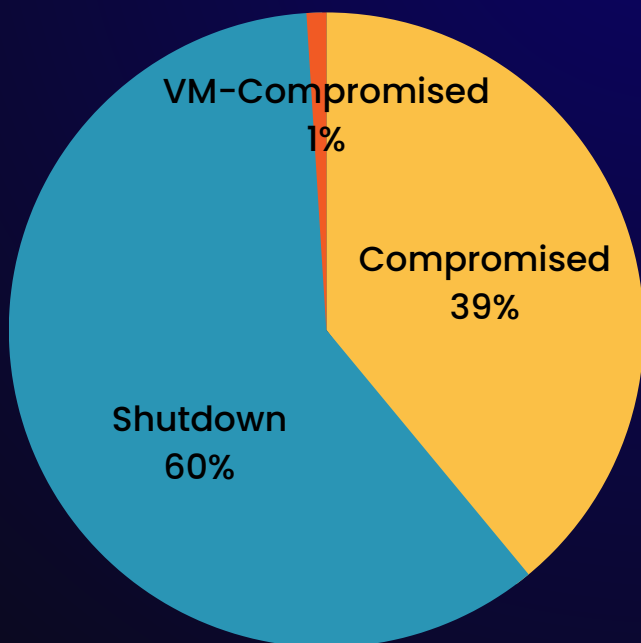


Figure 2: Compromise data for 2020 through to 2022

2022

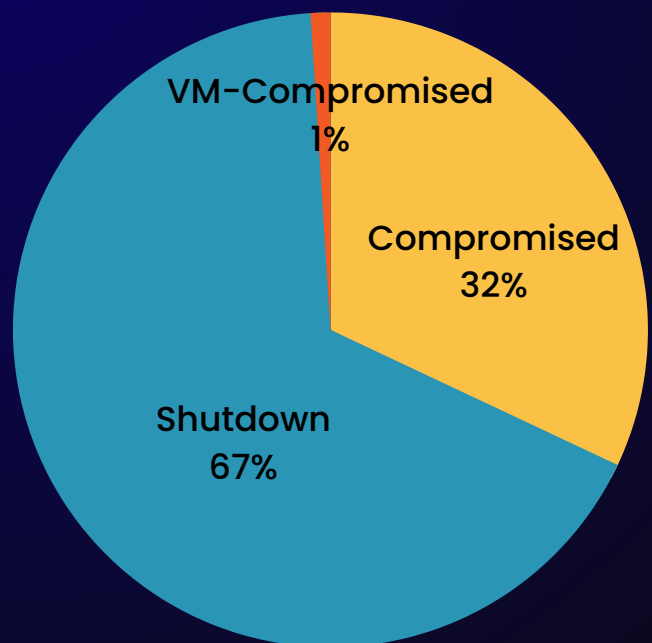


Figure 3: Compromise data for 2022

As can be seen in figure 2, between 2020–2022, the percentage of vishing calls which led to a data compromise was 39%. This percentage is concerning, to say the least. Additionally, in 1% of cases, a compromise was possible simply through the target’s voicemail message. That may seem like a small number, but think about how many employees you have at your company, 1,000? 10,000? 100,000? That’s 10, 100, or 1,000 of those employees, respectively, sharing compromising data via their voicemail.

This clearly points to the fact that there is a desperate need for employee education as well as internal corporate policy and change as to the warning signs and dangers of vishing.

---

However, although the trend is moving in the right direction, a 32% compromise rate is still largely concerning. What’s more, the percentage of voicemail compromises remained the same, suggesting a lack of awareness that recorded voicemail messages may pose a threat to data security.

When comparing compromise rates from 2020–2022 against 2022 alone, the percentage of vishing calls which were considered a shutdown by the target increases by 7% in 2022. It should also be noted that the data obtained from Social-Engineer, LLC consists of vishing calls made to their client base, rather than from malicious attacks on the general public. Hence, many of the calls made in 2022 were employees of clients tested and trained in previous years. As such, the data not only suggests that awareness may be increasing, with employees exercising greater skepticism when answering phone calls than in previous years, but also highlights the importance of consistent training for improved data security.

**Let's now take a look at some of the factors that may increase, or decrease, an individual's vulnerability to a data compromise during vishing attacks.**

## Vulnerability Factors

When it comes to general cognitive awareness and productivity, some people consider themselves a 'morning person' while others claim that they function best as a 'night owl.' While there is much empirical research to debate the topic of cognitive function and time of day at length, there is no research on how it may affect vishing vulnerability. As such, we examined compromise rates broken down by the time of day in which the call was made.

However, it is important to remember that calls are often made across states, and even internationally, meaning that the time zone of the target may be different to the time zone of the caller. The different time zones are not taken into consideration, it is problematic for two main reasons.

Firstly, when designing effective security awareness training it is vital to understand the varying vulnerability levels across the day. If compromise rates are not adjusted to reflect the local time zone of the target, periods of heightened awareness may be emphasized for the incorrect time.

Secondly, if professional social engineers do not consider the target's local time zone, it may lead to ineffective pretexts and greater target shutdown, and thus inaccurate perception of client vulnerabilities in subsequent report writing.

As such, we first carried out our analysis from the time zone of the caller (Eastern Time (ET)) and then inverted the time zones of each client to reflect a standard time for when the call was answered by the target (not centralized to a specific time zone).

**Please note, analysis of data was only possible for times of the day in which calls connected to the target and the target picked up the phone, thus calls that suffered carrier error or not answered were not included in the following analysis.**

## Compromise Rates & Vulnerabilities

### Time of Day According to Caller Time Zone (ET)

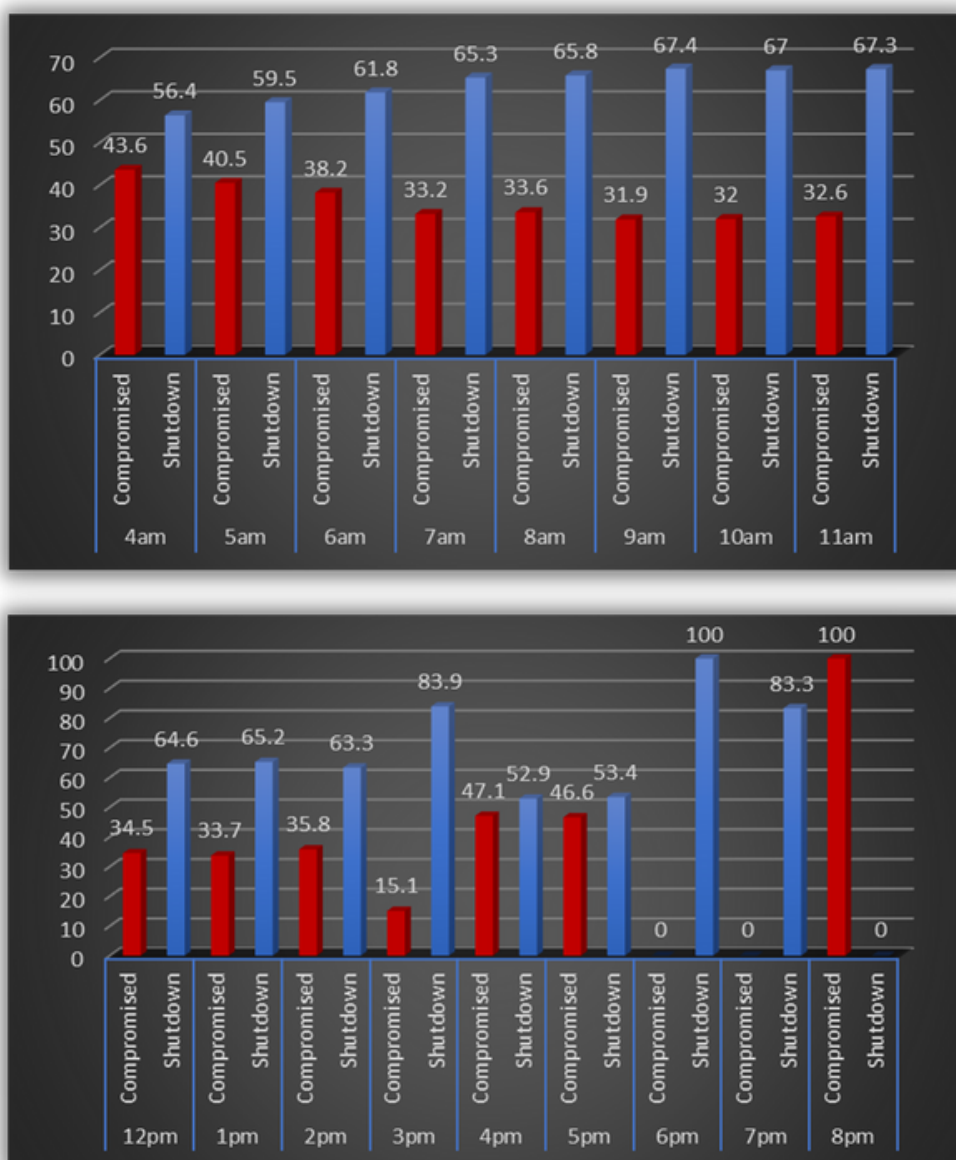


Figure 4: Compromise data according to time of day (Caller time zone)

As can be seen in figure 4, compromise and shutdown rates stay relatively consistent between 4am-11am, with compromise rates being slightly greater in the earlier part of the morning from 4am-5am. In contrast, from 12pm-8pm compromise rates fluctuate, with clear peaks in shutdown rates being 6pm followed by 3pm and 7pm. The most concerning finding was that 100% of vishing calls made at 8pm led to a compromise.



## Compromise Rates & Vulnerabilities

### Time of Day (Standardized Across Targets)

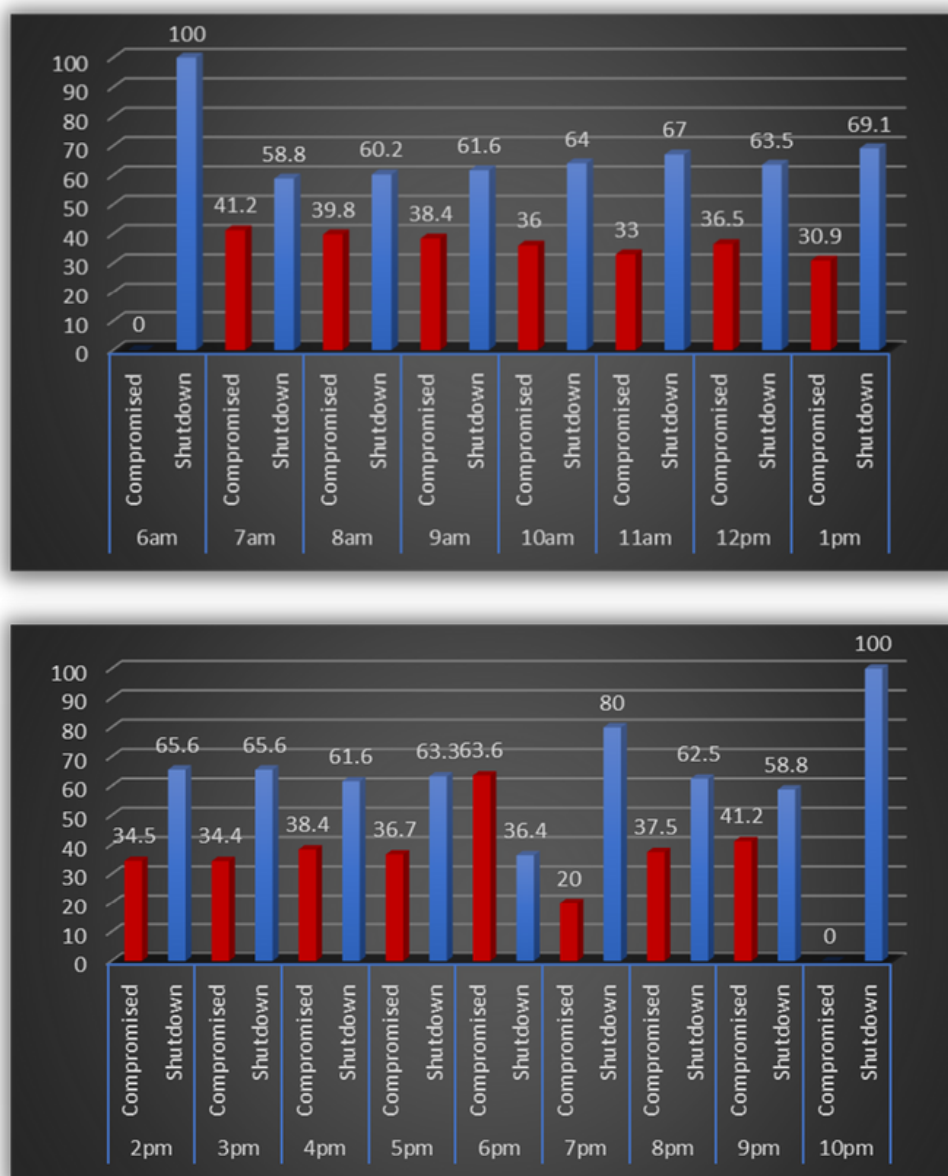


Figure 5: Compromise data according to time of day

As can be seen in figure 5, when the differing time zone of targets is taken into consideration, the fluctuation of vulnerability is significantly altered across the day. This highlights the importance of professional social engineers considering the regional time zone of the target and adapting accordingly.



## Compromise Rates & Vulnerabilities

Additionally, although our findings clearly evidence the fluctuating nature of susceptibility across the day, the compromise rates are much more closely related across time, compared to the prior analysis.

As can be seen, there is a sudden increase in compromise rates to 63.6% at 6pm, followed by a significant drop to 20% at 7pm. Although it is not possible to say with certainty why this pattern has emerged, it can be speculated that the increase observed at 6pm may be due to people being rushed and busy finishing work and traveling home, thus not engaging in as much critical thinking when being asked for information over the phone. In contrast, at 7pm most people are likely to be preparing for dinner and spending time with friends or family, and thus may be reluctant to engaging in conversation over the phone.



---

Following this, the times in which target's show increased susceptibility to influence attempts by attackers are 7am and 9pm. This may reflect the average sleep/wake cycle of most people making them less 'on guard' and more vulnerable to vishing attacks as they wake up and 'wind down' in the morning and evening.

---

## Compromise Rates & Vulnerabilities

These are not trivial findings. The awareness that at certain times in the day we may be more susceptible to influence than other times can support us in our information security efforts by acting as a reminder to exercise greater skepticism at these times. Additionally, armed with this information, organizations can make greater efforts to keep employees alert during these times by providing breaks, reminders, or internal messages.

With this in mind, we urge employers to work with security professionals to identify the times of day at which your employees may be most susceptible to phishing attempts. Additionally, given that the times of heightened vulnerability are outside of work hours, it demonstrates the importance of employers teaching that security awareness should be employed both inside and outside of the office. Making security awareness personal can have a much larger impact on security culture creating an environment of security awareness.



However, given the complex nature of human factors in security, adjusting training based on time relevant susceptibility is a start, but it is not the full picture. To be able to implement more effective training procedures, additional vulnerability factors need to be taken into consideration, such as sex difference in employees' information security behaviors.

## Sex of Target

### Male Targets

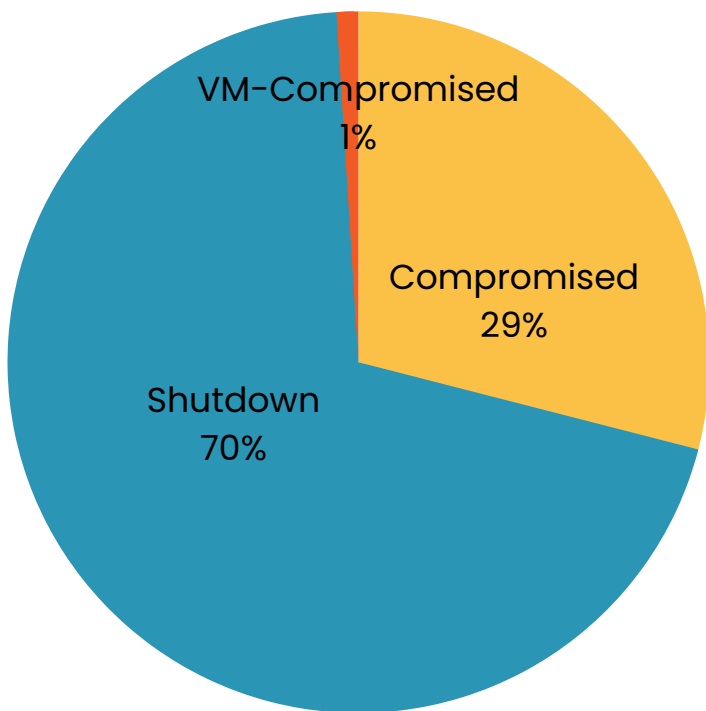


Figure 6: Compromise data for male targets

### Female Targets

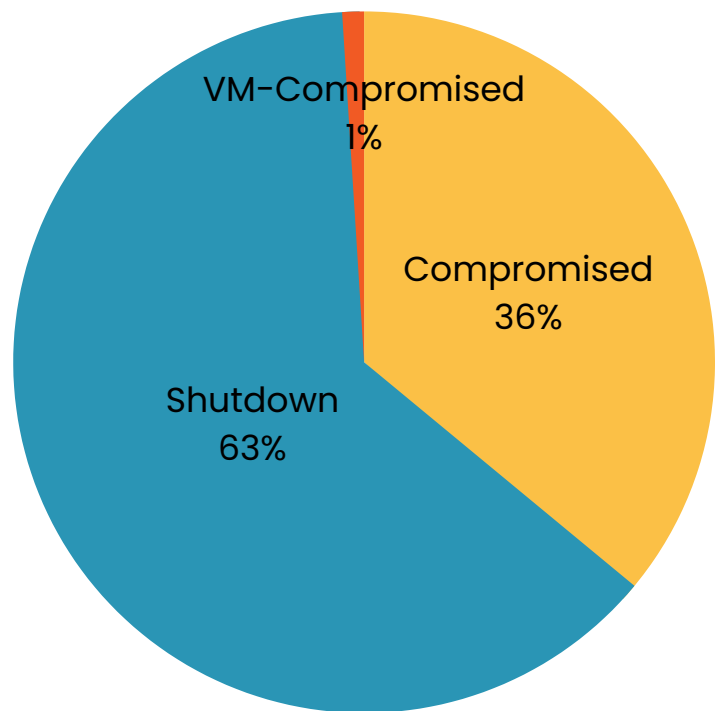


Figure 7: Compromise data for female targets

Figure 6 shows that when the target was male, there was a data compromise 29% of the time. As concerning as this statistic is, the percentage for female targets was even higher, with a compromise occurring 36% of the time, as shown in Figure 7. Based on the available data, it is not possible to make assumptions as to why this difference in susceptibility was recorded, however these findings demonstrate the necessity for information security and cybersecurity education across sectors, particularly for females.

## Sex of Caller

Next, we further examined compromise rates according to the sex of the caller (attacker).

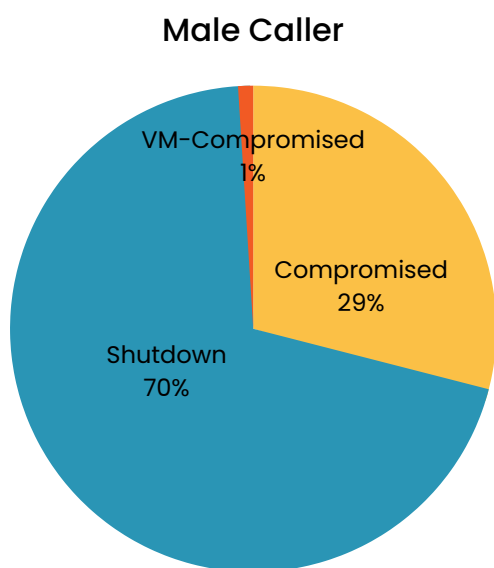


Figure 8: Compromise data for male callers

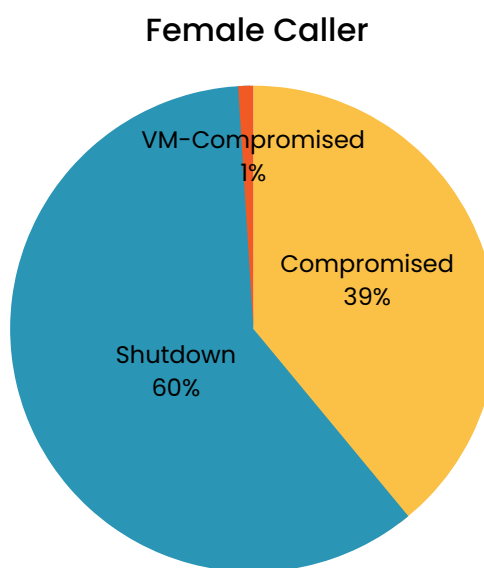


Figure 9: Compromise data for female callers

Findings from our analysis, as shown in Figure 8 and 9, demonstrate that a compromise occurred more often when the caller was female, by a 10% difference, compared to when the caller was male. Given that a sex difference was found for targets when looking at compromise rates, we subsequently expected to find a sex difference for callers. However, the difference between the two conditions was much greater than expected, with a compromise occurring 10% more often if the caller was a female than if the caller was male.

Nevertheless, it is not yet known whether there is an interaction effect between the sex of the caller and the sex of target, effecting the likelihood of a compromise. This is what we examined next.

## Interaction Data

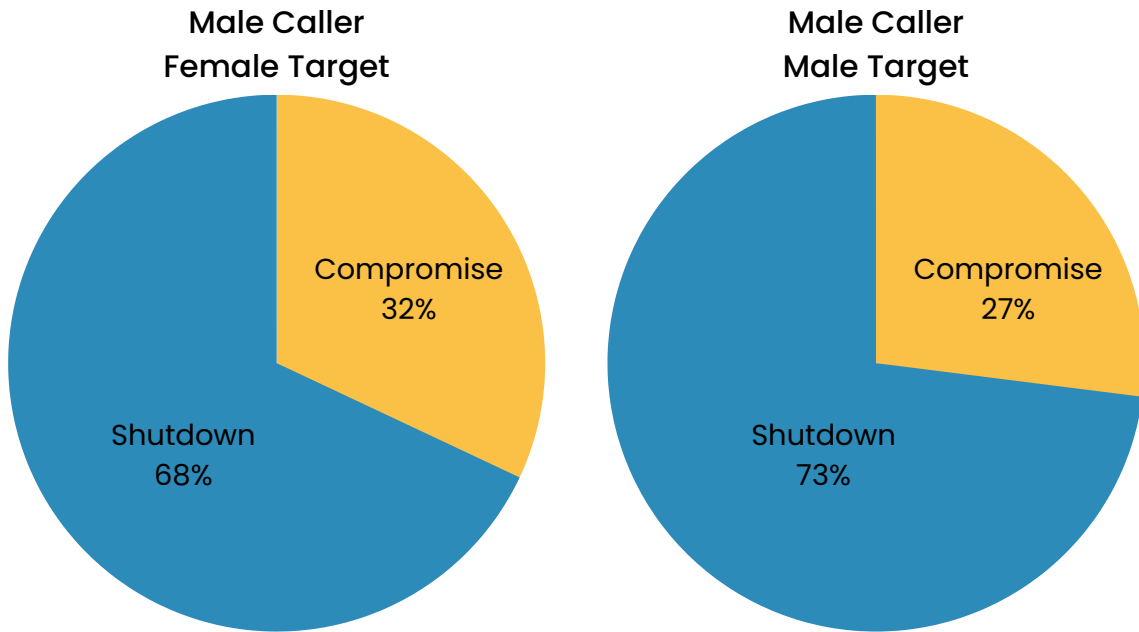


Figure 10: Interaction data for compromise rates for male callers

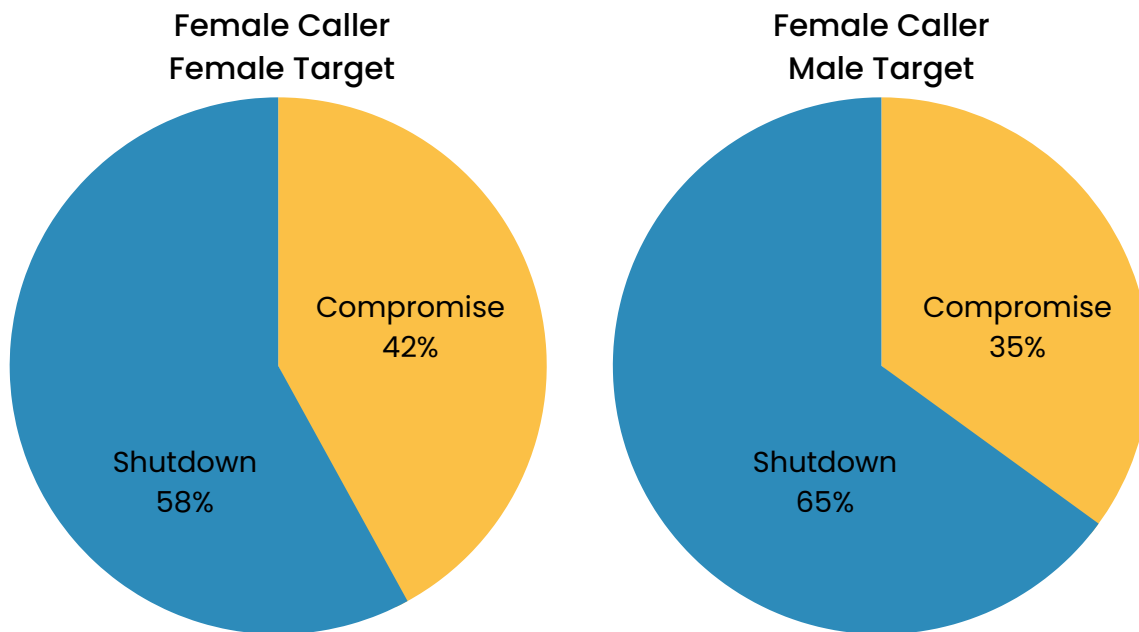


Figure 11: Interaction data for compromise rates for female callers

## Compromise Rates & Vulnerabilities

These findings demonstrate that the interaction between caller and target sex does play a role in the likelihood of a compromise, and as can be seen in figure 9 and 10, the interaction effect is not a subtle one. Male callers were able to achieve a compromise 5% more often if the target was a female, compared to if the target was male. Similarly, female callers were able to achieve a compromise 7% more often if the target was a female, compared to if the target was male.

The interaction group of male callers and male targets showed the lowest compromise rates, at 27%, which is a stark contrast to the interaction group of female callers and female targets, at 42%. These findings may suggest a higher degree of skepticism in males than in females during vishing calls. Additionally, given that females were more successful at achieving a compromise as a caller but were also more likely to be compromised as a target, this may suggest that females are more likely to be trusting of unknown callers and are perceived as more trustworthy.

---

Although the effects of sex on trust have been inconsistent and mixed in the empirical literature,<sup>3 4 5</sup> the present findings clearly evidence a sex difference when responding to vishing calls, as well as evidence an interaction effect of sex and compromise likelihood.

---



<sup>3</sup>Croson, R., and Buchan, N. (1999). *Gender and culture: international experimental evidence from trust games*. *Am. Econ. Rev.* 89,386–391. doi: 10.1257/aer.89.2.386

<sup>4</sup>Chaudhuri, A., and Gangadharan, L. (2003). *Gender Differences in Trust and Reciprocity*. Melbourne, VIC: University of Melbourne.

<sup>5</sup>Buchan, N. R., Croson, R. T., and Solnick, S. (2008). *Trust and gender: an examination of behavior and beliefs in the investment game*. *J. Econ. Behav. Organ.* 68, 466–476. doi: 10.1016/j.jebo.2007.10.006

# 3

## CURRENT UNDERSTANDINGS & EDUCATION

The teaching of good cyber hygiene typically simplifies the risk of data security threats being purely digital, focusing heavily on the technological factors such as digital firewalls, strong passwords, and network security.



As a result, the human element, which is a major threat to data security, often gets overlooked or oversimplified. Additionally, this is not just a problem within the private sector, but the human element of cybersecurity is also often overlooked by scholars.



## A Lack of Lessons From Academia

When looking to educate clients on how they can protect themselves against malicious attacks, experts often turn to the scientific literature for empirically supported methods. In turn, practitioners provide academics with industry data that would not have otherwise been possible to obtain. This collaboration between fields allows for continued growth in the knowledge base and enables practitioners to continue running effective training for clients.

However, to date, a limited number of empirical research articles are focused specifically on vishing attacks. Thus, practitioners' ability to provide scientific-based education is limited by a lack of empirical research into vishing vulnerability and protective factors.

At the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), scholar Sumitra Biswal discussed the findings from a preliminary experiment on a Real-Time Vishing Prediction and Awareness Model (RIVPAM) and highlighted current issues with the progress of this research endeavor and vishing research more generally. As such, Biswal states that:

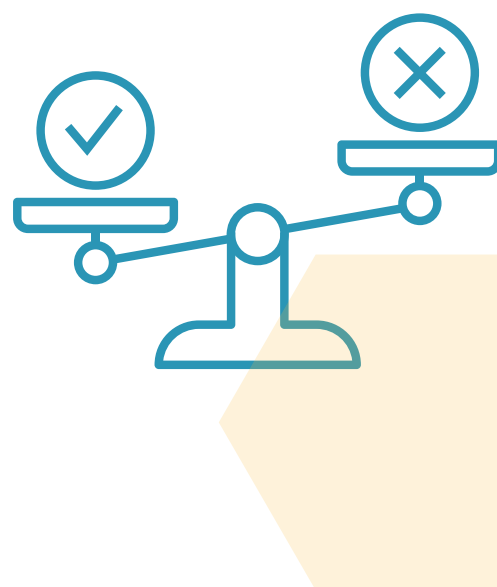
“  
...on using larger dataset, classifiers,  
and features involving psychological  
attributes

Sumitra Biswal

The current report, which utilized the largest known dataset on vishing ever recorded to date, demonstrates an important step forward in this understanding.

## The Problem with Ethics

A key reason there is a lack of research in this field is due to ethical restrictions for academics. The nature of social engineering is sensitive, with ‘attackers’ obtaining sensitive and personal information from ‘targets’ being the main objective. As such, simulating this in a laboratory or field setting is highly unethical and could lead to psychological harm of targets if the experimenters do not have sufficient procedures in place.



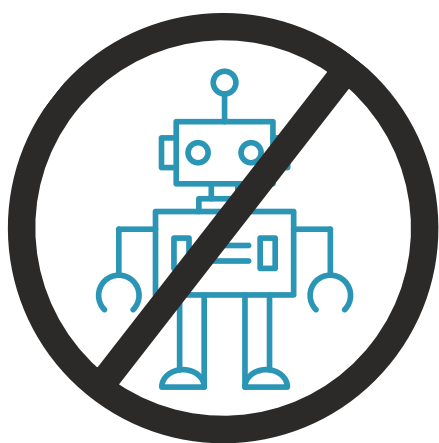
In a paper published in the journal of Computers & Security, lead author Francois Mouton and colleagues describe how:

“Several ethical concerns and requirements need to be taken into account when social engineering research is conducted to ensure that no harm comes to the participants.” They then go on to add that, “The problem is that these requirements have not yet been formalized and most researchers are unaware of the ethical concerns related to social engineering research.”<sup>7</sup>

Francois Mouton & Colleagues

<sup>7</sup>Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114-127.

## Current Understandings & Educations



Consider this, for scholars to obtain ethically collected data, data would need to be provided by industry professionals, following a thorough sanitization process to remove any personally identifiable information.

But herein lies another problem, simply put, the use of ROBOCALLS. What we have found in our research is that the majority of operational security (OPSEC) companies test client's security using robocalls rather than human-to-human vishing tests, which overlooks the vastly dynamic interactions that take place during genuine real-world attacks.

According to Patrick Laverty, Expert Social Engineer and Senior Team Lead at Social-Engineer, LLC, *"using robocallers is not an effective way to test for vulnerabilities because real malicious attackers don't use them. Our team uses certified, professional social engineers to make the calls because the human voice is more believable. Our agents are trained to be empathetic and flexible to achieve a goal, which is impossible with robocalls"*.

As for the companies that do use human-to-human tests, there is often the question of ethics left unanswered, with little enforcement of strict ethical policies or regulations during data collection.



*We are, all of us, susceptible to social engineering attacks given the right emotional and environmental triggers. Because of this, we need to test our employees in the most realistic way possible. That means real callers, and real conversations.*

**Shelby Dacko, Human Risk Analyst  
Social-Engineer, LLC**



To avoid the problems and challenges of ineffective training, it is important to take a few steps for any company interested in real world training:

- Use human-to-human attacks, as the real attackers do.
- Ensure your vendor adheres to a strong moral code, so they do not harm your employee base.
- Have an internal POC that works with the vendor to ensure realistic pretexts are being used.
- Adapt the attacks each month to match the skills of the employee.



*Robocallers and untrained auditors cannot simulate a real attack and will make your security training ineffective and a waste of money.*

**Christopher Hadnagy, CEO & Chief Human Hacker  
Social-Engineer, LLC**



## Future Directions

Social-Engineer, LLC have begun to bridge the gap between academia and industry, through the initiation of several social-engineering focused research collaborations and the continued development of science-based practical courses.

However, with the scale of increasing vishing attacks, there is pressing need for greater research efforts to be carried out.

As such, Social-Engineer, LLC is releasing an official call for collaboration with scholars and academic researchers looking to advance current understanding of vishing vulnerability and protective factors.

Additionally, each year a new “State of Vishing” report will be issued by Social-Engineer, LLC. Future reports will include more detailed analysis of vulnerability factors, such as what types of information are most vulnerable and under what conditions, as well as detailed analysis of psychological principles and influence tactics being employed by attackers.

# CONCLUSION

Although vishing attacks are on the rise, public awareness of such attacks is also increasing, with businesses and individuals alike beginning to recognize the consequences of poor security awareness training. However, the lack of first-hand vishing data available for examination, prior to this report, has meant that very little is empirically nor operationally known about vulnerability factors.

The findings from the inaugural State of Vishing report evidence a concerning rate of success for data compromise via vishing, including data compromise via voicemail. Although, there appears to be a slight improvement in 'shutdown' rates in 2022 compared to previous years, suggesting improvements in awareness, a data compromise is still being achieved 32% of the time. Additionally, it is evident that factors such as time of day, sex of caller, and sex of target, as well as the interaction of these factors play a role in an individual's vulnerability. This report highlights an important step forward in understanding the complexities of vishing vulnerabilities as well as, more generally, the threat landscape.

But, before you go, we want to leave you with one final message. Although the increasing threat of vishing may seem daunting, attackers can only get through the door if a person opens that door for them. Thus, when we focus on tailored training programs, we can turn the human security vulnerability into awareness and protection.

---

**The difference between  
your employees being  
your weakest link or your  
secret weapon is  
effective security  
awareness training.**

---

Threats to information security consistently focus their attacks on company employees.

Our managed services programs are designed to test, educate, and protect your human network. We apply scientifically proven methodologies to uncover vulnerabilities, define risk, and provide remediation.



## We're Hear To Help

Learn more about today's most serious vishing and other social engineering trends and threats — and how the team at Social-Engineer, LLC can help keep your organization safe.



[Learn More](#)