A DANCE OF DECEIT

A REPORT ON TECHNIQUES USED BY VISHING FRAUDSTERS TO ESTABLISH PATTERNS OF TRUST

TAKE FIVE

Report by Doctor Paul Breen, The University of Westminster

Introduction and contextualisation

Human beings have evolved with the instinctive "willingness to accept someone at his or her word" and this "leaves many of us vulnerable to attack" (Granger, 2001). That is particularly true in the online context, where the cost of fraud committed in the UK in 2016 "topped £1bn for the first time since 2011" (Treanor, 2017). Today's fraudsters are operating with increasing sophistication at the intersection of our physical and online lives, taking advantage of trust and data readily accessible in the public domain. They ensnare their victims by engaging in a carefully plotted masquerade in which they engineer a suspension of belief on the part of victims akin to the way we suppress our sense of reality when watching actors play the part of characters in a TV show.

Such "clever manipulation of the natural human tendency to trust" (Granger, 2001) is referred to as social engineering; "a euphemism for non-technical or low-technology means – such as lies, impersonation, tricks, bribes, blackmail, and threat – used to attack information systems" (McDowell, 2007). Increasingly, bank customers have been a favoured target of fraudsters and human beings represent "the weak spot" in the security of our financial institutions (Keyworth, 2016). This is because our innate tendency is to trust others, especially those in authority, and to view ourselves as being "too clever to be caught out" (ibid). After all, if human beings did not evolve with a natural disposition to trust, then everyday relationships, such as those in the workplace or the selection of a marriage partner would prove difficult.

The meaning of trust

Though the meaning of *trust* is a "complex multidimensional construct" (Jones & George, 1998) encompassing "moral, cognitive, and emotional elements" (Barber, 1983), the basic signification remains entrenched in the origins of the word. Coming from the Old Norse word *treysta*, the core definition is one of 'confident expectation' and 'fidelity' in the course of interaction with others. By the late 15th century, 'trust' had found its way into legal parlance, meaning "confidence placed in one who holds or enjoys the use of property entrusted to him by its legal owner" (Etymology Online). Such a definition is particularly apt for the banking context, where institutions are expected and legally obliged to safeguard their customers' financial interests.

However, there is also a responsibility on the part of customers and this has become an Achilles Heel through which fraudsters can attack customers' security, using the affordances of the digital age. Today's digital technologies are characterised by their "protean", "unstable" and "opaque" nature (Koehler & Mishra, 2009, p. 61); making them hard to trace, and capable of constant adaptation. This leaves the authorities engaged in a constant battle to guard their customers from compromising situations, and has stimulated debate about the best ways to address this growing challenge. Several theorists including Song, Kim & Gkelias argue that "for the time being, the best option is to try to educate users about these attacks and the associated risks" (2014, p. 865), even though "many security researchers" have also "warned that the effectiveness of such education is inherently limited" (ibid).

Other theorists such as Hasan et al acknowledge that even though technology serves as the vehicle for fraud, "user education is the first and most powerful defence against social engineering" (2010, p. 21). This is because technological resources alone cannot facilitate a fraud, any more than fishing rods and reels guarantee a catch, on their own. The human element is essential, and it all boils down to the basic human predisposition towards trust. Hasan et al (ibid, p. 18) suggest that such a basic manipulation of trust has been going on since ancient times, charting the example of the Trojan horse which was "one of the most ingenious social engineering tricks in the history of humankind."

In that story, it was not just the design of an unsuspected weapon that gave the enemy entrance to the gates of Troy, but also the fact that the Trojans failed to heed warnings about Greeks bearing gifts (ibid). If the Trojans had heeded the signs, the horse outside the city walls would have proven useless, just as malware is useless without the human curiosity of being seduced by clickbait. Had they been fully aware of the dangers, the Trojans would have fortified their city, rather than making guests of their enemies. It is such awareness that is crucial to people's self-protection.

Education over technological solutions

This report thus favours education of banking customers rather than solutions that are purely "technocentric" (Papert, 1987), and will focus on the phenomenon of *Vishing* to provide a rationale for this. Song et al (2014, p. 865) outline how vishing is a combination of 'voice' and 'phishing', specifically referring to phishing scams enacted over the phone, with fraudsters "masquerading as a trusted authority." The purpose of this masquerade is "to trick people into divulging financial data or transferring money to a scammer" (ibid), who disappears as soon as the dance of deceit has come to an end. Such a vanishing act is possible because vishing attacks are mostly based on VoIP *(Voice over Internet Protocol)* through which fraudsters "start and end a call on a computer that can be located anywhere in the world" (Nadeem, 2017). Hasan et al (2010, p. 20) further add that "vishing actually emulates a typical bank protocol in which banks encourage clients to call and authenticate information." As such, a sense of trust is engineered by the fraudsters wearing masks of authority and authenticity.

Actual techniques used by fraudsters

Hasan et al (2010, pp. 18-19) suggest that there are four phases to a social engineering attack, which they list as information gathering, relationship development, exploitation, and execution. Yeboah-Boateng and Amanor (2014, p. 305) further argue that these stages are facilitated by incorporating a specific taxonomy of language, with "alluring" and "decoying" words used throughout the vishing process. Added to this, they cite Tétard and Collan's (2009) Lazy User Theory, in which "end users do not necessarily pay attention to risk mitigation measures" or "take any security actions, unless there's an experience or an incidence" (2014, p. 301). An essential part of vishing is to create a sense of urgency from the outset, and to establish the "perfect psychological environment" (Granger, 2001) for an attack; as achieved by the Greeks in Hasan et al's (2010) example of the Trojan horse.

This was a feature of almost every example that I listened to, with some of the most reprehensible being those that specifically target the elderly. The vishing process is carefully scripted from beginning to end. Often the opening line of attack involves involves impersonating staff and "inventing scenarios" that simultaneously involve "hoaxing" and "creating confusion" on the part of customers (Hasan et al, 2010, p. 19). This entails a twin-track approach of creating a sense of urgency at the same time as establishing "the appearance of a comfortable relationship" (Granger, 2001). Enacting such scenarios help to create the illusion of an emergency which is under control, and in the safe hands of the fraudster on the other end of the phone. This is why the masquerade requires sophisticated levels of impersonation – "creating some sort of character and playing out the role" (ibid).

Gradually this builds towards a point of "sudden decisions being taken due to fear of an untoward incident" (Hasan et al, 2010, p. 19). Deliberately, the build-up is a slow process involving "impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness" giving rise to a "main objective" of convincing victims that the social engineer is somebody they can trust with "sensitive information" (Granger, 2001). In the most extreme cases this can lead to the fraudsters setting up actual face-to-face meetings with their victims or as happened in one case, persuading an elderly lady to withdraw money from the bank, to then be physically passed to the fraudsters. Generally, the criminals assume the identity of somebody in authority, often involving impersonation of staff from an outside organisation there to protect customers (Hasan et al, 2010, p. 19). Nowadays they work in highly organised teams, far beyond those once associated with "the infamous fax from a 'Nigerian prince' you've never heard of asking you for money" (Keyworth, 2016). Today's vishing operations use elaborate techniques of modification, including "Caller ID spoofing" which is "a technique that modifies the displayed number of an incoming call" to replicate or resemble "the number of a trusted institution" (Song et al, 2014, p. 866). This can be enacted in several ways including "using an online service" such as "spoofcard.com" (ibid).

However, as argued herein, without the human dimension most of these attacks could get no further than initiation of contact. This then gives rise to several key questions. Firstly, how do fraudsters get past the initial stage of "masquerading as a trusted authority" (Song et al, 2014, p. 865)? Secondly, in an environment where people see themselves as too clever to be caught out (Keyworth, 2016), how do these vishers lure their victims into a dance of deceit, designed to strip them of their finances, and disappear at the speed of a pickpocket? In the next sections of this report, I will try to answer these questions by looking at the language used in authentic cases of fraud, and seeing what patterns emerge in terms of dialogue and techniques.

Methodology

Some of what has been discussed in the contextualisation and review of literature could be described as everyday knowledge that supports people's common view that they are "too clever to be caught out" by such scams (Keyworth, 2016). Yet, as illustrated by Treanor (2017), this type of fraud appears to be on the rise, rather than in decline. Therefore to find out how people fall victim to such scams, it was essential to access instances of vishing where ordinary people have been duped. This has been done through an ethically-sound process of listening to a range of phone calls and reading transcripts, ranging from a few minutes to whole scenarios broken up over a total of several hours, into different episodes. The ways in which ethical issues were addressed included supervised sessions where all recordings were listened to in the company of banking or security professionals, anonymisation of individuals involved, and the storage of all data in a safe space.

Having accessed this series of transcripts and recordings under supervision and made anonymised notes, the language was then analysed using a system of "thematic analysis" as defined by Braun & Clarke (2006). This involved six stages, beginning with familiarisation of data and context to the point of saturation, so as to search for "repeated patterns of meaning" (ibid, p. 15). Once initial patterns had been established preliminary themes were separated from the transcripts of text (p. 19), listed out as codes and then reviewed on a second reading (p. 20) to generate a primary set of results. These initial codes then acted as a foundation for the fifth stage of "defining and naming themes" (p. 22), so as to feed into the final stage of *"producing the report"* (p. 23). The goal of that report is to find patterns of language and techniques used by the fraudsters in authentic cases of vishing. On a final note, the rationale for listening to calls rather than simply reading the transcripts was to get a sense not just of what was said, but how it was said. This is because the literature on vishing suggests that "atmosphere" (Keyworth, 2016) and "masquerading" (Song et al, 2014) are as important as language. Finally, in producing the report, I have also taken out names of individual banks so as to further protect the identities of the victims.

Findings and discussion – More than language

Through accessing and analysing a series of discussions between vishers and their victims, it became evident that fraudsters neither rely on technology, nor language alone to lure in their targets. This is indeed a sophisticated process of seduction where individuals seem to be specifically targeted, almost to the extent of being staked out, even stalked beforehand. This can be done either physically or in the ever popular domain of social media, wherein so much private information is now readily made public. An example of this could be a fictitious scenario where someone posts holiday snaps from Prague or Rome and comments that they are going to be there for a couple of weeks. Fraudsters could latch onto this information very easily and contact the bank pretending to be that customer - overseas, in a panic, without access to passwords back home, and needing to transfer money in a hurry. Since the banks are there to help and expect us not to be so loose in our provision of personal information, this creates a real security risk. Indeed in such a situation the bank is caught in a Catch 22 scenario wherein with a genuine case it needs to help the customer, but at the same time protect against potential fraud.

Whether contacting an individual or a bank, the fraudsters build up patterns of trust in a process of reeling in their victims, by adding layer upon layer of seeming authenticity to their masquerade, up to the point of catchment. The visher acts like a fisherman: patient, determined, willing to put in the required effort to get a bite because with the vast sums of money available they can profit considerably from a single catch. Like fishermen too, they will cast their nets even further afield if they think that they will be rewarded for their efforts. Some cases have involved attempts not just to trick customers over the phone but also to impersonate them physically, whether by going into banks in person or by contacting call centres, fishing for information from staff. In another incident they went so far as to arrange an appointment at an elderly woman's home, promising to go through the withdrawal process with her, and make any required calls to her local bank branch on her behalf. Luckily, in this case, her son intervened and saved the woman from being scammed.

To achieve this type of scam they take on a persona: observing the techniques used by banking professionals and adopting these to convince people to go against their instinctive suspicion, and to bolster their natural disposition to trusting others, especially those in authority. One example included a visher posing as "Charlie ... calling from Money Laundering Operations" who contacted a small business with an accusation of somebody trying to launder money in their accounts; again using reverse psychology by placing suspicion and guilt on the victim rather than the fraudster. Through doing this, "Charlie" managed to convince the company's financial officer to hand over the name of the client relationship manager, and use this information to eventually engineer details about the company's accounts, wherein they gave him their bank access details so as to prevent money being laundered via their account.

As in the case of "Charlie" it is more than just language that lulls victims into a false sense of security, or urgency in securing their accounts. Words are just one part of an elaborate masquerade, involving a series of techniques that replicate many of the strategies outlined in the earlier sections. Ultimately this is a very clever act using diverse layers of entrapment. In the calls studied here, the range of personas included worried customers, fraud detection officers, and even police officers who in one case managed to convince a former policeman of their authenticity. From this, it is possible to say that nobody is too clever to get caught out at some level, though the ratio of calls far outweighs the number of actual victims who get snared in this masquerade.

Overcoming doubts on the part of victims

To sceptics it might seem as if victims have to be naïve from the outset. However, the reality is that vishers appear to address and welcome scepticism because everyone in the calls that I accessed expressed some form of cynicism or questioning. As stated in Keyworth (2016), most people see themselves as too smart to get caught in this trap. In order to overcome this, the vishers build up familiarisation slowly, fishing for the details one at a time, rather than casting the whole net in one go. This is why "the smart hacker knows when to stop pulling out information" (Granger, 2001), and also when to stop and start talking. It appears that an essential part of this scam involves giving the victims time, at the start, to express their doubts about the authenticity of this contact from a stranger.

Thus, from early on in their calls, the vishers acknowledge that their targets need to be security conscious and protective of their personal information. Recurringly, there is an emphasis on not seeking private details and on providing new layers of security to systems that have been breached – effectively engineering the role of a

Trojan horse coming inside the city walls for protection rather than attack. Through a combination of patience, trust, and familiarisation, the attackers gradually use a form of reverse social engineering to get additional required information such as passwords and account details from victims.

This is done largely through incorporating a specific taxonomy of language, with "alluring" and "decoying" words used throughout the vishing process (Yeboah-Boateng & Amanor, 2014, p. 305). Again that is facilitated through creation of atmosphere, and a delicate balancing act of urgency alongside drip-feed solutions. The language of fishing could be applied too, with customers baited, over time, and reeled in gradually, hooked past the point of escape. Constantly, the vishers create a sense of being in control but demonstrate ability to switch tempo and turn up the pressure when needed, such as in moments of heightened suspicion.

As if working to a script, they appear to have answers to everything, often featuring a lexicon of *understanding* – incorporating such phrases as "I know", "okay", "of course", "I understand" – and of *being there to help* – "going to sort this out for you" or "going to set up a new account for you." Generally, at the start, there is no immediate rush on this but as the victims are lured in a sense of haste and urgency is introduced to catch the targets off guard.

Detailed example of techniques in action

One of the most polished examples that I accessed of vishers succeeding in their efforts came from a telephone fraud scenario, in which the fraudsters synthesised many of the techniques witnessed in other scenarios. Here a woman found herself conned out of £12,000 in savings. The enactment of this fraud took place over the course of an entire day, during which time the victim spoke to a number of people purporting to be from a respected institution's "Payments' Verification team." The first stage of the fraud began with the shock tactics outlined in Hasan et al (2010), where the cold caller who named himself as Mark, invented a scenario that created fear of an "untoward incident" wherein payments had been taken from the customer's account "in the last ten to fifteen minutes."

'Mark' then enacted a masquerade of assuring the target that he was there to help, by "going through procedures." Pre-empting, and perhaps even sensing the primary fears of his prey, he assured her that he was not going to ask for "any personal information" about her accounts. Subsequently, he bombarded her with a series of straightforward yes-no questions, repeatedly using the word “okay” as a source of psychological reassurance whilst continuously averting her initial suspicions and inherent distrust with the constant mantra that “I’m not asking you for any information.” This was the crucial first stage as outlined in Hasan et al (2010) where the fraudster has to seem unhurried, helpful, authentic, and systematic in adhering to procedures. If trust is not attained, and the victim becomes suspicious or uncooperative, as happened in several recordings, then the fraudster terminates the call.

In this case of the “Payments’ Verification team” fraud, the tempo of the call played a crucial part in establishing trust, and fossilising the masquerade in the mind of the victim. The fraudsters demonstrated great ability to adapt and react to circumstances, responding with the alacrity of fishermen to each suspicion on the part of their target. Gradually, as the victim eased her suspicions, and became interested in how much had been taken from her account, rather than questioning their authenticity, the fraudsters switched tempo. Having lured his target to the bait, and begun teeing up access to her online banking facility, ‘Mark’ set up a second call. Such a call arrived some hours later, with the pronouncement of it being “James calling from the company’s “Fraud Operations team” making “a quick security call” – again employing language of *security* and *authority* to establish trust.

‘James’ then sought to authenticate the call in the victim’s mind by the provision of a password, and the outlining of a bank’s generic security script, which included such phrases as “all calls are recorded for training purposes.” Here, he was using language to create the atmosphere of a professional environment, and playing on the fact that people’s natural tendency is to switch off mentally when given information with which they believe themselves to be already familiar; with a prime example being pre-flight safety demonstrations on aircraft. Having enacted this stage of the masquerade, the fraudster then persuaded the victim to impart information about her password by feigning concern over “payments attempted to buy luxury goods.” In spite of this attempt to establish a “perfect psychological environment” (Granger, 2001) for a vishing attack, ‘James’ then roused the woman’s suspicions by asking her for a mobile number. However when she said that “I think the bank knows about my mobile”, he assured her that he needed the number for her good rather than his, “to send her a text later on.” This was again presented as being for the victim’s own benefit so that ‘James’ could call her again later in the day.

When 'James' made that third and final call, he repeated the security script, wearing down his victim's defences with the constant masquerade of authenticity. This time he asked his target for a password of her choice, which she willingly gave to him – creating the illusion of her being the one in control, being allowed to "take your time." Having given his victim this sense of control, the fraudster proceeded to ask her questions about her accounts, until such times as he could announce "that's you past security." Then suddenly, he switched tempo from patiently going through the motions to creating a sense of alarm and urgency, making reference to "a police investigation" and "somebody trying to buy luxury watches in your name", through "a different IP address."

This creation of disturbance in the mind of the victim allowed him then to recommend "a replacement account" and his help "to set up a new payment", which roused suspicions at first. However, again he told the victim that he was "not asking you for any passwords or PIN numbers", and that she was in charge of the process of setting up her own payment. In order to facilitate this, he then moved to a stage outlined in Hasan et al (2010), where there is the introduction of a senior manager and more intimidatory tactics used to stimulate closure with greater urgency.

Thus, 'James' passed her on to 'Neil', who once again read from a script, outlining protocol, but in a more affirmative voice. Now, instead of a patient approach, he was more instructional from the outset, giving orders as to what needed to be done, moving the process on in the manner of salesmen switching from front-of-house advertising to back-room signing of the actual papers. Once again, he reiterated the word "security" several times, especially within such lexical chunks as "for your own security." This stage also included the "Caller ID spoofing" process outlined in Song et al (2014, p. 866), with the sending of a text message, purporting to come from the bank, and adding authority to the process.

Once that text message came through, 'Neil' pushed for closure of the money transfer at a speed which made it difficult for the target to think rationally; getting access to the online account and then using a subsequent genuine text message from the bank as a further means of triangulating his masquerade of authenticity. By the end, having conned his victim into transferring twelve thousand pounds into a new account, he closed the discussion with a statement that "the system is down at the moment" and a promise to call at eight o'clock in the morning. By then, the victim had started to become suspicious but almost instantly the call ended with a declaration of “thank you for your help.”

As always, the dance of deceit ended with the victim seeing the fraudsters fade into thin air. This instance of fraud though serves as an exemplar of the approaches used by organised vishing crime gangs, combining standard patter with language almost identical to that used by banking professionals. Other cases that featured in the research include constant references to “safeguarding”, “suspicious activity” in accounts, “protection from fraud” and apologies for the fact of systems having been breached. Much like film and television scriptwriters, the fraudsters use our human sense of empathy with others to step out of a fictional universe into a realm of believability akin to Kevin Spacey coming into our living rooms as Frank Underwood in the TV show *House of Cards*.

Deep down, our instincts tell us that this is not real but the fraudsters know which mental buttons they need to touch in order to have us suspend our disbelief for long enough to be reeled in. Certainly our natural disposition towards trust plays its part, but so does a desire for intrigue and excitement. There appears to be something about the moment of being contacted by authorities and helping to resolve a suspicious situation that echoes our attraction to fictional stories such as the aforementioned *House of Cards*. In suspending our disbelief, we let our guard down and become vulnerable to attack, creating that ‘weak spot’ in bank security.

Conclusion and recommendations

This study, and particularly the case highlighted in greatest detail, has shown that there is much more to vishing scams than simply a reliance on technologies and choice of language. There is a huge psychological element as well, and it is perhaps from this angle that educational approaches to the problem should be shaped. As the literature suggests, vishers make use of very sophisticated systems, scripts, and scenarios, but all these would be redundant if they could not exploit the weak spots in human nature. Perhaps the greatest weakness of all is the feeling of being invulnerable to such a situation because when viewed from a distance it appears foolish to transfer money from our accounts into someone else’s.

Yet, as shown in the specifically detailed example of telephone fraud and witnessed in other cases analysed, these scammers operate through a system of convincing victims that they are engaging in a watertight activity of safeguarding their own money. It is indeed then a masquerade or dance of deceit of the highest order. By using language and processes of security and safeguarding almost identical to those of financial institutions, victims are encouraged to let their guard slip, sweet talked by criminals who seem to have the answers to every question. Again, something about the masquerade seems attractive to begin with, and the fictive scenario is part of a patient and cunning process of fishing in the waters of everyday life.

Perhaps then the way to educate people in protecting themselves from getting ensnared in such situations is to make them aware that these fraudsters are creators of fictions every bit as powerful as *House of Cards, Mad Men,* and the various other box sets that we bring into our living rooms on a nightly basis. Of course we know these are not real, but most of us have very little experience of dealing with a fiction that is presented as reality, and no idea how we would react when drawn into the midst of a sophisticated fiction. Those who are drawn into such a scenario are real people, and could be any one of us. One of the police officers that I spoke to during the stage of accessing transcripts and recordings used the excellent example of another popular TV show to illustrate why people fall for this masquerade – *Big Brother*. None of us can know how we would react in such an environment until we are caught up in it, even though we watch the TV and insist that in such a situation, we would still be able to behave normally. Unfortunately, this study has shown that none of us can know how we would react until we are in such extreme situations, and our greatest weakness is believing these scenarios can never happen.

REFERENCES

Barber, B. (1983). *The logic and limits of trust*. New Brunswick, New Jersey: Rutgers University Press.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), pp.77-101.

Etymology.org (2017) - www.etymologyonline.org

Granger, S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics.' *SecurityFocus* - Accessed at http://www.securityfocus.com/infocus/1527

Hasan, M., Prajapati, N. and Vohara, S. (2010). Case study on social engineering techniques for persuasion. *arXiv preprint arXiv:1006.3848*.

Jones, G.R. and George, J.M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of management review*, *23*(3), pp.531-546.

Keyworth, M. (2016). *Vishing and smishing: The rise of social engineering fraud*. BBC World Service report 01-01-2016. Accessed at http://www.bbc.co.uk/news/business-35201188

Koehler, M., & Mishra, P. (2009). What is technological pedagogical content knowledge (TPACK)?. *Contemporary Issues in Technology and Teacher Education*, *9*(1), 60-70.

McDowell, M. (2007). White paper: Avoiding Social Engineering and Phishing Attacks. *Cyber Security Tip ST04-014* – in Hasan et al (2010).

Nadeem, M.S. (2017). *Social Engineering: What is Vishing*. Blog post from 05-05-2017 – accessed at https://blog.mailfence.com/vishing/

Papert, S. (1987). Computer criticism vs. technocentric thinking. *Educational Researcher*, 22-30.

Song, J., Kim, H. and Gkelias, A. (2014). iVisher: real-time detection of caller ID spoofing. *ETRI Journal*, *36*(5), pp.865-875.

Tétard, F. and Collan, M. (2009). Lazy user theory: A dynamic model to understand user selection of products and services. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1-9). IEEE.

Treanor, J. (2017). *UK fraud hits record 1.1bn as cybercrime soars*. Article in The Guardian Newspaper 24-01-2017. Accessed at - https://www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg

Yeboah-Boateng, E.O. and Amanor, P.M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), pp.297-307.