Computers in Human Behavior 124 (2021) 106930

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

# Performing social engineering: A qualitative study of information security deceptions

Kevin F. Steinmetz *, Alexandra Pimentel, W. Richard Goe

*Department of Sociology, Anthropology and Social Work, Kansas State University, 1603 Old Claflin Place, 204 Waters Hall, Manhattan, KS, 66506, USA*

ARTICLE INFO

*Keywords:*
Cybercrime
Social engineering
Symbolic interactionism
Practice theory
Qualitative analysis

ABSTRACT

Contemporary computer and networking technologies have expanded the scope and scale of deceptions worldwide. Among hackers, security practitioners, and other technologists, ruses designed to gain access to otherwise secure information or computer systems are often referred to as "social engineering." To date, little research has explored the creation of fabrications from the perspective of social engineers. The current study addresses this gap by examining the attributes that social engineers ascribe to successful and effective social engineering deceptions through a grounded theory analysis of interviews with social engineers (n = 37). Results reveal twelve characteristics of effective social engineers according to participants–findings which indicate that perpetrators consider social context, assumptions about human nature, the complexities of social networks, the role of social conventions, and the limitations of human processing and reasoning in the execution of their deceptions. The study concludes by considering the theoretical implications of the results and advancing propositions to guide future criminological research on social engineering, fraud, and deception more generally.

Among hackers and information security practitioners, the manipulation of people through deceit to gain access to sensitive information or secure systems is often referred to as "social engineering" (Hadnagy, 2018; Mitnick & Simon, 2002).[1] The term describes a constellation of deceptions used to compromise information security systems like "phishing" (email-based frauds), "smishing" (text-message-based frauds), "spear-phishing" (targeted email-based frauds), "vishing" (phone-based frauds), and in-person ruses.[2] Estimates place losses from such frauds in the billions of dollars per annum (IC3, 2019, p. 20).[3] Yet not all harms are economic as individual victims of social engineering and related frauds may experience significant emotional, psychological, physiological, and lifestyle damages (Cross, Dragiewicz, & Richards; Cross, Richards, & Smith, 2016; Whitty & Buchanan, 2016).

Such deceptions are a considerable source of worry for information and systems assurance providers. A recent Verizon (2019, p. 5) report claims that 32 percent of data breaches in their study involved phishing emails and the Internet Crime Complaint Center (2020, p. 20) reports that personal data breaches, phishing/vishing/smishing/pharming scams, and business email/email account compromises were among the most frequently reported online crimes in 2019. It is thus not unreasonable to say that many security incidents involve at least some measure of deception.

Considerable attention has been given by scholars and information security practitioners to detailing the various tactics used by social engineers and related perpetrators (e.g. Cross, Dragiewicz, & Richards, 2018; Holt & Graves, 2007; Huang & Brockman, 2011; King & Thomas, 2009; Leukfeldt, 2014a; Whitty, 2013). Little research, however, has explored social engineering from the perspectives of social engineers (e.g. Hutchings, 2013; Lusthaus, 2018). The current study addresses this gap by examining the attributes social engineers ascribe to successful and effective social engineering deceptions through a grounded theory analysis of interviews with social engineers.

Results reveal twelve characteristics of effective social engineers according to participants–findings which indicate that perpetrators

* Corresponding author.
*E-mail addresses:* kfsteinmetz@ksu.edu (K.F. Steinmetz), pimentel@ksu.edu (A. Pimentel), goe@ksu.edu (W.R. Goe).

[1] Historically, social engineering has referred to the use of social science and policy to increase the efficiency and effectiveness of organizations and institutions in an optimistic attempt to reform society but the term has since been appropriated to apply to information security related deceptions (Hatfield, 2018).

[2] Because social engineering tactics do not exclusively rely upon telecommunications technologies, they constitute what Cross (2019, p. 129) terms a "cyber-enabled offense"—one which includes both on-line and off-line dimensions.

[3] Damage estimates should be observed with some caution as problems have been noted concerning estimates for losses from technology-enabled or assisted crimes (Yar, 2008a, 2008b).

https://doi.org/10.1016/j.chb.2021.106930
Received 11 September 2020; Received in revised form 30 April 2021; Accepted 21 June 2021
Available online 25 June 2021

consider social context, assumptions about human nature, the complexities of social networks, the role of social conventions, and the limitations of human processing and reasoning. These themes are organized into four categories corresponding to different stages of a social engineering deception: *planning, proximity, activation,* and *concealment.* In this manner, the results organize themselves into a kind of crime script, a sequence of actions taken by perpetrators to commit an offense (Cornish, 1994; Cornish & Clarke, 2002; Leukfeldt, 2014a). Further, participant responses indicate that social engineering deceptions are intractably intertwined in situational, cultural, and structural circumstances.

After the presentation of results, this study turns to various social theories useful for tracing the connections between social engineering deceptions and their broader social circumstances, namely the theories of Erving Goffman, Pierre Bourdieu, and Anthony Giddens. The study ends by drawing from the results and relevant theories to offer propositions to guide future social engineering and deception research. Before describing and discussing the results in detail, however, a review of the relevant literature is provided with an eye toward the different methodological approaches taken by prior studies. The methodological approach used in the current study is then detailed.

## 1. Social engineering and information security fraud research

A robust criminological and sociological literature exists that has examined various forms of deception and fraud, including mortgage fraud (e.g. Baumer, Ranson, Arnio, Fulmer, & De Zilwa, 2017), insurance fraud (Tracy & Fox, 1989), stock brokerage fraud (e.g. Yenkey, 2018), con-artistry (e.g. Goffman, 1952; Maurer, 1940; Williams & Milton, 2015), professional thievery (e.g. Sutherland, 1937), long-firm frauds (e.g. Levi, 1981), credit card fraud (e.g. Jackson, 1994), intermediate fraud (Baker & Faulkner, 2006), identity theft (Copes & Vieraitis, 2012), and telemarketing fraud (e.g. Doocy, Shichor, Sechrest, & Geis, 2008; Shover, Coffey, & Hobbs, 2003). To date, only a handful of studies have empirically analyzed the strategies used in social engineering and related forms of computer- or network security-oriented frauds (Atkins & Huang, 2013; Bullée, Montoya, Pieters, Junger, & Hartel, 2017; Cross et al., 2018; Holt & Graves, 2007; Huang & Brockman, 2011; King & Thomas, 2009; Leukfeldt, 2014a; Leukfeldt, Kleemans, & Stol, 2017a, 2017b; Rauti & Leppänen, 2017; Whitty, 2013; Whitty & Buchanan, 2016). Several approaches have been used to conduct these studies including analyses of fraudulent emails, interviews with victims, interviews with law enforcement officials, court documents, books written by social engineers, and observations of scams in progress. To our knowledge, only two studies have examined social engineering and related deceptions through interviews with perpetrators (Hutchings, 2013; Lusthaus, 2018). It is toward a consideration of these different methodological approaches this analysis now turns.

One approach used by scholars to understand the strategies used by social engineers are content analyses of phishing emails (Atkins & Huang, 2013; Holt & Graves, 2007; Huang & Brockman, 2011; King & Thomas, 2009). These studies have argued that such emails attempt to elicit emotional responses such as trust, urgency/fear, empathy, and greed under the guise of official business, religion-laden pleas for help, and promises of great reward. A related approach has involved the observation of online scams in progress. In their study of technical support scams, Rauti and Leppänen (2017) allowed fraudsters to access their own computer system under the guise of providing technical support services. The authors found that the fraudsters would diagnose and pretend to fix non-existent computer issues, then charge a fee and require payment in such a manner that the victim's credit card information could be captured.

Victim narratives have also provided a robust source of data for understanding offender strategies (e.g. Cross et al., 2018; Whitty, 2013; Whitty & Buchanan, 2016). For instance, Whitty (2013) used interviews with the victims of romance frauds to create the Scammers Persuasive Technique Model. Involved is a process whereby a target for the fraud is selected, a ruse is constructed, and the target is slowly "groomed" to accumulate trust with the perpetrator. Once sufficient trust is developed, the offender solicits money and gifts from the victim—usually starting small and working toward larger sums—often under the guise of needing assistance from the victim. Sexual extortion of the victim may occur and victims may be revictimized after the conclusion of the original scam.

Some scholars have turned to analyses of court documents and interviews with law enforcement officials to understand phishing and related forms of online deception (Leukfeldt, 2014a,b; Leukfeldt, Kleemans, & Stol, 2017a, 2017b). In one study, for instance, Leukfeldt (2014a) detailed the strategies, division of labor, and operations of the fraud group, focusing specifically on how social engineering efforts can emerge from relatively sophisticated and coordinated group efforts. He presented a crime script detailing the steps involved in these frauds including (1) sending phishing emails containing a link to redirect recipients to a falsified bank webpage designed to harvest information from the target, (2) calling the target under the guise of bank employees to elicit a transfer code allowing an illicit transfer of funds to accounts held by the fraudsters, and (3) the use of "money mules" to withdraw funds from these accounts to prevent tracing and interception (Leukfeldt, 2014a, pp. 243–235). The scammer group played to the strengths of each member to maximize the potential of payoff and to reduce the likelihood of being caught.

Another source of insights regarding the strategies employed by social engineers are instruction books authored by social engineers. These books are often filled with descriptions of scenarios of social engineering deceptions, typically by security auditors. Bullée et al. (2017) analyzed 74 scenarios provided in four such books and found that these scenarios often featured deceptions conducted over telephone that exploited the persuasion principles described by Cialdini (2009) (*authority*, *scarcity*, *likeability*, *reciprocity*, *consistency*, and *social proof*), with appeals to authority being the most frequently used.

Only two studies, to our knowledge, have directly interviewed computer-oriented deception and fraud perpetrators to understand their activities from their point of view. Hutchings (2013) examined court documents, interviews with law enforcement officers, and interviews with active and former fraud and hacking offenders. She concluded that fraudsters were generally motivated by financial gain (in terms of both "need" and "greed") and engaged in cost-benefit decision making regarding perceived risks and rewards of their activities when selecting targets. Further, both hackers and fraudsters engaged in various strategies to reduce risk such as focusing on "systems that are easily accessible and well known to them" and taking "steps to conceal their activities" (Hutchings, 2013, p. 109). Her study also described the various rationalizations used by offenders to justify their activities and target selection (ibid). In what is likely the most robust analysis of online cybercrime organizations to date, Lusthaus (2018) examined the rise of the "cybercrime industry" by drawing from multiple sources of data including over 200 interviews with law enforcement officials, cybersecurity professionals, journalists, and others with twenty interviews involving former offenders. In his analysis, he demonstrated how cybercriminals—which may include fraud perpetrators—form worldwide networks where offenders participate in a division of labor, specialize in specific roles, engage in professionalized business operations, create marketplaces, curate trust and develop mechanisms of assurance, and conduct their activities both on- and off-line. He also explores how cybercriminals create online identities, cooperate with one another, and create mechanisms of governance.

## 2. The current study

Though both the studies by Hutchings (2013) and Lusthaus (2018) are commendable, they do little to examine the execution of social engineering. In other words, neither study examines the elements involved

in constructing and performing such deceptions. The current study addresses this gap through an inductive analysis of qualitative semi-structured interviews with individuals who engage in social engineering to understand the attributes social engineers ascribe to effective deceptions. In some ways, the current study is an extension of criminological decision-making research (e.g. Clark & Cornish, 1985; Cornish & Clarke, 1986). This literature has historically focused on elements of crime like target selection, onset, persistence, frequency, and desistance from criminal activity, motivations, and evaluations of punishment. This study differs in that it does not explicitly examine in-the-moment decision making of perpetrators. It instead asks perpetrators to reflect upon the knowledge they have accumulated over time to describe what makes for effective deceptions from their perspective. Relatedly, the focus of this study is defined narrowly, confined to the elements of successful social engineering performances or deceptions. It does not consider other important elements of social engineering like target selection. Such decision-making processes are sufficiently complicated to warrant their own analyses (e.g. Hutchings, 2013). In addition, this study breaks from prior research on social engineering which largely emphasizes the psychological elements supposedly exploited by social engineers such as cognitive biases and Cialdini's (2009) principles of persuasion (e.g. Atkins & Huang, 2013; Chantler & Broadhurst 2006; Huang & Brockman, 2011; Norris, Brookes, & Dowell, 2019; Vishwanath, Herath, Chen, Wang, & Rao, 2011). This study contends that deceptions cannot be reduced to individual psychology.

By relying on themes inductively derived from participant responses, this analysis finds that social engineering deceptions are inseparable from situational context, culture, and structural circumstance. In other words, these deceptions are not created and implemented in a void but instead draw from, or at least must account for, the situational rules that govern social interactions, cultural expectations and values, structural elements like race, class, and gender, and other factors. To develop these points, this study incorporates insights from symbolic interactionism, specifically the work of Erving Goffman who considered interpersonal deception or "fabrications" in depth as matters of situational performance and relational negotiation. We also borrow Goffman's (1952) term "mark" to refer to the target of social engineering.[4] To connect situational performance with their structural and cultural contexts, this analysis incorporates Pierre Bourdieu's (1980/1990) work on *habitus* and Anthony Giddens's (1990) structuration theory. Both Bourdieu and Giddens are theorists in the tradition of "practice theory" which examines "the practices of social actors 'on the ground' and the big 'structures' and 'systems' that both constrain those practices and yet are ultimately susceptible to being transformed by them" (Ortner, 2006, p. 2). As will be demonstrated in the discussion section of this analysis, these theories are useful to consider how social engineering deceptions are enmeshed in complex arrangements of situational, cultural, and structural factors that may directly or indirectly shape such fabrications and their likelihood of success.

## 3. Methods

Building from prior research on technology-oriented fabrications, the current study examines qualitative semi-structured interviews drawn from a National Science Foundation-funded research project of social engineers and information technology professionals tasked with securing organizations against social engineering frauds (n = 54). This analysis draws from a subsample of 37 interviews with social engineers including both non-professionals (n = 7) and professionals (n = 30). Professional security auditors use social engineering techniques to test organizational information security systems (Caldwell, 2011). While these participants may not have illicit or illegal motivations underlying a large proportion of their activities, they do often use the techniques of fraudsters to great effect to compromise organizational security for testing purposes. It is also not uncommon for criminal hackers to matriculate into legitimate security positions later in life (Taylor, 1999).[5] Further, considering that their livelihoods hinge on their ability to conduct effective deceptions, such participants are a valuable source of insights regarding the elements of effective and successful frauds in the information age. Seventeen interviews with IT security professionals (e.g. CIOs and CISOs) were excluded from the analysis because these individuals do not engage in social engineering but, rather, protect their organizations against information security threats (including social engineering).

**Table 1**
Descriptive statistics of study sample.

| Variable | n (percent) |
|---|---|
| Age | Range: 25–57, $\bar{x}$ = 36.8 |
| Race | |
| White | 33 (89.19%) |
| Asian | 1 (2.70%) |
| African American | 2 (5.41%) |
| Bi-Racial | 1 (2.70%) |
| Gender | |
| Male | 28 (75.68%) |
| Female | 9 (24.32%) |
| Education | |
| High School Diploma/GED | 2 (5.41%) |
| Some College | 4 (10.81%) |
| Associate's Degree | 4 (10.81%) |
| Bachelor's Degree | 17 (45.95%) |
| Graduate Education | 10 (27.03%) |
| Self-Described Socio-Economic Status | |
| Lower/Working Class | 2 (5.41%) |
| Lower-Middle Class | 2 (5.41%) |
| Middle Class | 14 (37.84%) |
| Upper-Middle or Above | 19 (51.35%) |
| Illegal Social Engineering Participation | 40.5% (15) |
| Harmful Social Engineering Participation | 35.14% (13) |

Participants were recruited through both purposive and snowball sampling strategies. Researchers traveled to hacking conventions (in-person events for hackers and other technology enthusiasts) and corporate security conferences to network and solicit participation, a strategy used in previous studies of hackers (Bachmann, 2010; Holt, 2009; Holt, 2010; Schell & Holt, 2010, pp. 190–213;Schell & Melnychuck, 2010; Steinmetz, 2016). The researchers also cold-called information security contractors identified through Internet search engines. Finally, we relied on interviewees to provide references to others possible participants. Individuals were considered viable for recruitment if they espoused or demonstrated participation in social engineering activities. Only those who actually claimed to have performed social engineering in some capacity were included in the study. The 37 interviews totaled 73 h ranging from 43 min to 4 h and 4 min in length ($\bar{x}$ = 1 h and 59 min). Table 1 presents descriptive statistics for the participants. The sample is predominantly male, white, and relatively educated. These demographics roughly mirror other studies on hacking and related populations (Bachmann, 2010; Holt, 2009; Holt 2010; Schell & Holt, 2010, pp. 190–213; Steinmetz, 2016). For reasons of human subjects ethics, we avoided recruiting minors meaning that adults of

[4] Goffman (1952, p. 451) defines a "mark" as "any individual who is a victim or prospective victim of certain forms of planned illegal exploitation." This term was derived from the argot adopted by fraudsters in his studies.

[5] To this end, 40.5 percent our participants report engaging in criminal social engineering in some capacity at some point in their lives. Percent engaged in prior criminal social engineering is derived from self-report questions. In total, fifteen participants admitted to or described engaging in some form of illegal social engineering (3 non-professional social engineers and 12 security auditors). Additionally, this percentage does not count two security auditors who reported finding out in retrospect that their activities were illegal while conducting a security audit.

**Table 2**
Major themes present in interviews with social engineers.

| Theme | *f* (n = 37) |
|---|---|
| Planning | |
| 1. Research | 36 |
| 2. Asset and Liability Assessment | 23 |
| 3. Timing | 8 |
| Proximity | |
| 4. Rapport Building | 35 |
| 5. Network Integration | 31 |
| Activation | |
| 6. Call for Help | 27 |
| 7. Incentivize | 18 |
| Concealment | |
| 8. Authenticity | 31 |
| 9. Ordinary | 22 |
| 10. Spectacle | 17 |
| 11. Efficiency | 12 |
| 12. Accommodation | 17 |

Note: Frequencies refer to the number of participants who described the theme in their interviews.

various ages ($\bar{x}$ = 36.8) comprise our sample.

The research was approved by our institution's review board.[6] Informed consent was gathered, and each participant was assigned a pseudonym to protect their identity. Interviews were conducted through encrypted voice over Internet protocol (VoIP) programs and were audio-recorded and transcribed. Personal information has been scrubbed from transcripts to ensure confidentiality. Electronic data was stored on hardware encrypted external media. Participants were not compensated for their involvement in the study.

The current analysis focuses on interview descriptions of social engineering ruses. During the interviews, participants were asked to describe their first social engineering experiences, favorite or most successful social engineering deceptions, as well as deceptions that may have been illegal or harmful to others. They also often provided examples of social engineering scenarios in response to an assortment of other questions presented in the interviews. The responses were analyzed by the first author for common themes using a grounded theory-based approach which involves the transformation of data into concepts which are then summarized into broader analytic categories through open, axial, and selective coding strategies (Charmaz, 2002; Corbin & Strauss, 1990; Glaser & Strauss, 1967). Open coding involves comparisons between units of data and the assignment of conceptual labels. Axial coding means that concepts are compared to each other and categories are developed to organize the concepts. Finally, open coding involves the process of comparing and refining the data, concepts, and categories identified in prior stages of analysis and developing one or more core categories to organize the totality of the data is *selective* coding (Corbin & Strauss, 1990, p. 14). The Atlas. ti qualitative data analysis software was used to organize the data and facilitate the grounded theory analysis.

## 4. Results

Twelve themes emerged from participants' descriptions that correspond to characteristics associated with successful and effective social engineering deceptions (Table 2). These themes are organized into four categories commensurate to stages of the social engineering process: *planning, proximity, activation,* and *concealment.* It bears repeating that these themes concern the performance of social engineering deceptions. Other processes involved in social engineering, such as target selection, are beyond the scope of this analysis.

Before describing the results, it is worth considering two points regarding the role of technology in social engineering. The first is that participants reported engaging in social engineering through three vectors—email, phone, and in-person. Though they highlighted various advantages and disadvantages associated with each vector, the themes described in this analysis are applicable across the three vectors, with few exceptions. Participants focused more on in-person social engineering deceptions in their narratives, likely because such instances were often more emotionally intense and memorable. Additionally, some of these vectors allow for automation or "scripting" of social engineering deceptions such as the automated mass distribution of phishing emails. The distribution of such ruses may be automated but their format and messaging involve human input and intent. As such, even scripted deceptions will likely employ at least some of the thematic elements described in this analysis.

The second point to consider is that technology plays an additional role in the execution of social engineering deceptions beyond mediating communication. Information technology can provide a means through which information is gathered to facilitate a social engineering deception as well as comprise the end objective of such fabrications like convincing a mark to click on a malicious link or download a malicious email attachment.[7] Importantly, the themes described throughout this analysis pertain specifically to interactional elements of the ruses which may be facilitated by, but exist independent of, the technology used.

### 4.1. Planning

Many participants described planning their deceptions prior to execution by considering circumstances that may influence delivery, presentation, and the likelihood of success. The first theme described in this section concerns research conducted by the social engineer as a preliminary step in deception creation. The second entails the demographic characteristics, experiences, and skillsets of the social engineer that may be assessed as assets or liabilities for social engineering. It then explores the temporal circumstances surrounding the mark (time of day, time of year, and current events) that can be considered when formulating a social engineering deception.

#### 4.1.1. Research

Like other forms of deception (Williams & Milton, 2015, p. 172), participants indicated that social engineering may involve significant research on the part of the social engineer (n = 36). The approach taken in a social engineering deception often hinges on the details uncovered during investigation—it is "entirely based on the information gathering" (David). Research helps the social engineer plan their deceptions. The consensus among participants is that the more time is invested in research, the more likely a deception is to be successful. As Gerald explained, "if I know enough about you ahead of time, I can manipulate you to do anything I want because I'm going to know, you know, sort of where your mind is." One participant, however, argued that research—while potentially useful—is not a necessity. Edward explained that he may make use of research (or have a team member do it for him) but he also claimed that "I literally have had the client drive me to a location blind, to break into their branch. It's like without knowing anything about it, and I succeeded, and I broke in."

Research and preparation, according to study participants, are useful for crafting the social engineer's "pretext," a fictional identity or

[6] The IRB protocol number for this study is 8194.

[7] Goffman (1974) describes two general types of fabrications: benign and exploitive. While participants provided many examples of exploitive fabrications (where "one partying containing others in a construction that is clearly inimical to their private interests" (Goffman, 1974, p. 103)) many of our participants engaged in benign fabrications in the name of testing organizational security and raising security awareness among members, namely "training hoaxes" (Goffman, 1974, p. 96). Importantly, while the motivations underlying the deceptions may vary as well as the situations in which they are employed, the elements of deception remain consistent.

scenario employed by the social engineer to influence a mark. Pretexts can be boilerplate deceptions used against a broad pool of potential marks (this is at the heart of most phishing scams, for example). Participants generally argued, however, that the odds of success increase the more tailored a pretext is to a particular mark and such customization requires research.[8] Many of the subsequent themes presented in this analysis concern the development and execution of pretexts.

#### 4.1.2. Asset and liability assessment

For participants, creating effective pretexts involved taking inventory of the social engineer's pre-existing traits, experiences, and skillsets to assess for potential assets and liabilities such characteristics might pose for the social engineer and their deception (n = 23). For instance, a social engineer without experience working in the information technology (IT) sector may have a more difficult time pretexting as an IT service provider. But if one has such experience then it can be an asset: "I almost always pretend to be an IT guy, where a lot of other people will not. That's easier for me partly because I did IT" (Bernard).

Responses suggest that social engineers may need to account for their physical attributes like age, race, gender, physical size, and appearance.[9] Such features can be a disadvantage. Gerald, for instance, described the limitations his age imposes on social engineering, "I'm not non-descript anymore, you know. I have a very recognizable look. So I can't lie to you twice 'cause you'll see me comin' the second time." Appearance can provide advantages to the social engineer as well. Claire remarked that a social engineer's sexual attractiveness can be exploited against a mark, "I don't do this as much, but I know some other female social engineers who do, who flirt a lot when it's a guy because that's really successful, especially if you're attractive." In Brian's words, "sex works."

Of course, it stands to reason that the physical characteristics of the social engineer matter less for engaging in frauds through mediated communications than in-person frauds, as identity markers can be more easily fabricated. Brian explained that one of his female colleagues has an impressive vocal range and, as a result, she can "go from the 50-year old HR Nazi to a 25-year old, blonde college girl on the phone." In person, however, she would be more limited by her physical appearance. In phishing or other digital text and image-based frauds, the limitations imposed by bodily characteristics are absent. This does not mean, however, that physical appearances cannot still be exploited. Social engineers can develop a fabricated online persona to become a person with whom the mark is likely to interact. Victor, for instance, described creating a false online identity of a sexually attractive woman specifically with the intent of enticing men online to surrender sensitive information (a strategy commonly associated with "catfishing" scams).

Part of making use of personal characteristics is being aware of and exploiting social stereotypes. "Social engineering," Anna explained, "isn't politically correct." Some participants recounted conforming to stereotypes surrounding their age, race, and accents to play on the biases of a mark. Stereotypes surrounding gender, however, were most frequently cited—specifically the stereotype that women are less threatening than men. For instance, women who are social engineers may draw from stereotypes like the "damsel in distress" (Tara) or the "dumb blonde" (Lucy) to appear vulnerable and to a mark. Stereotypes may also restrict the kinds of roles a social engineer can adopt, according to participants. Here too, gender was cited as a particularly potent source of stereotypes for social engineers to consider. Some participants, for example, claimed that marks may be less willing to accept women in stereotypically masculine roles. Stereotypes may also be exploited in phishing emails through fabricated personas.

#### 4.1.3. Timing

When formulating a plan, some participants describe timing as an important element to consider in creating a successful deception (n = 8). Time of the year, for instance, may impact the type of deception utilized. Lucy claimed that scams enacted during the holidays may take advantage of the generosity people feel with the "spirit of the season." Similarly, the time of day may matter. When plotting a phishing campaign against an organization, Zeke explained, "Like usually I don't want to send things at lunch or first thing in the morning 'cause most people will check their emails and things like that from their mobile devices and then forget about it."[10] The social engineer may also consider taking advantage of current events according to participants (see also: Holt & Graves, 2007). Edna described such an approach,

> So, so for an example, the phishing campaign that I launched on Friday, I was actually supposed to launch a completely different campaign but the whole Equifax thing blew up and I actually used that pretext, and this is actually, so far we're on day three, the highest click rate that I've ever done in the five years of doing this.

For her, drawing from a current event, particularly one that potentially impacted so many, gave her scam not only a sense of urgency, but realism as well.

### 4.2. Proximity

After taking stock of the circumstances, assets, and limitations confronting the social engineer, they must then execute their ruse. Participants indicated that successful social engineering deceptions may depend on developing a kind of social proximity to the mark. This process may involve forming a trusting relationship—or *rapport building*—with the target. The social engineer may also pretext in such a manner as to appear as an expected (or at least not unexpected) actor in their social landscape, which this analysis terms *network integration*. These two methods for creating social proximity are described in turn.

#### 4.2.1. Rapport building

According to many participants, aggressive or intimidating pretexts can be effective— "almost anything fear based works" (Arlo). They also cautioned, however, that such heavy-handed approaches may "put people on the defensive" and make "people shut down" (Anna). Bernard explained that "being a bully is usually ineffective. That's one of those things that would get you in quickly but also get you kicked out quickly." Some participants also claimed to avoid such methods on ethical grounds: "I never use intimidation as a tactic. I don't believe in it, ethically. Also, I've never needed to. So just by being a friendly person, I usually get what I'm looking for" (Lucy).

Instead, a preferred strategy was building rapport with marks (n = 35). Such rapport building reflects what some researchers have described as "love, liking and similarity" (Lea, Fisher, & Evans, 2009; Whitty, 2013) or what Cialdini (2009) terms "likeability." Rapport concerns getting the mark to like and, more importantly, trust the social engineer:

> I like to call it like the art of the conversation because if, it doesn't matter how great your pretext is, it doesn't matter, you know, how fancy your fake website is, but if you can't get someone to trust you then none of that matters. (Marilyn)

[8] Of note, while many frauds are boilerplate deceptions, custom-tailored pretexts are not unusual. For instance, Verizon's (2018, p. 32) *2017 Data Breach Investigations Report* found that 28% of the data breaches in their study conducted through phishing attacks were targeted.

[9] In his classic study of professional thievery, Sutherland (1937, pp. 23–24) similarly acknowledged the limitations placed on thieves and fraudsters by factors like age, gender, and race.

[10] Ellipses added into quotes indicate that text was removed for the purposes of clarity or concision.

While aggression may be "a total crapshoot" (Gerald), building positive rapport was generally considered to produce more predictable reactions from a mark.

Participants articulated various methods for building rapport. The first is simple: be nice, friendly, and polite to the mark. "You'll be surprised," Herbert explained, "how many times just, just bein' nice to people and understanding their day or things of that nature, how many other doors or avenues open up." August cautioned, however, against appearing inauthentically friendly as the social engineer may risk being viewed like a salesperson and thus "completely full of shit." Rapport can also be developed, according to participants, through "reciprocity" (see also: Whitty, 2013, p. 672; Lea, Fisher, & Evans, 2009). The idea is simple: the social engineer will do a favor for the mark and this, in turn, should encourage the mark to reciprocate the gesture. For instance, Brian explained that "I just opened the door for somebody before me and actually they want to show the same respect and open the second door for me." This may allow the social engineer entrée into an otherwise secure facility.

Some participants asserted that building rapport may involve creating the impression that the social engineer is like the mark in some manner through communicating shared interests and experiences. For instance, Zeb described conducting a deception in a rural area and relating to his marks by talking "about trucks and doin' four-wheeling and stuff like that." Participants also described achieving likeability using "mirroring techniques" like mimicking breathing rate, body language, and mannerisms.

#### 4.2.2. Network integration

People tend to be embedded in networks of relations with both individuals and organizations with which they are familiar to varying degrees. Further, they have expectations for interactions with these actors and organizations in their day-to-day life (Granovetter, 1985). Participant responses indicate that if a social engineer can trace a connection between themselves and persons and institutions familiar to the mark, then the mark may find the social engineer credible and trustworthy (n = 31). One of the reasons given by participants for conducting prior research is to better situating themselves within the mark's network and gain a more immediate level of trust (the exploitation of trust in social networks has previously been noted in Ponzi scheme frauds, see: Comet, 2011). The closer the social engineer can successfully situate themselves within this network, the more trust they may be conferred. Friends seen on a regular basis may be more trusted than an acquaintance not seen in years, for example. Importantly, the social engineer may want to situate themselves close enough to the mark in their network of familiarity to gain trust and achieve their objective but not so close that their ruse falls apart upon inspection. As Patrick explained, "I try not to impersonate a real person if I think there's a chance that the other person might know them personally, right?" In other words, while posing as an organizational insider may be useful, it also is risky if the mark is familiar with the person the social engineer is impersonating.

Creating a direct or indirect relationship to the mark in this manner, according to participants, allows the social engineer to appropriate the trust the mark has in various roles, organizations, and institutions. Trust, in this sense, has a "transitive property" (Jeremiah). For instance, Lucy described posing as third-party vendors or contractors because she can appropriate the trust a mark has in those actors: "I want somebody who's removed enough that they, that whatever I'm asking or saying makes sense to them but, and they're probably heard of it, so I'm getting the benefit of the legitimacy, inheriting the legitimacy of whatever I'm pretending to be." Other sources of transitive trust described by participants include organizational insiders, organizational management or leadership, experts, technicians, and government agents (including law enforcement).

Participants described other ways to become embedded in a trusted network beyond appropriating trust from other people, organizations, or institutions. For instance, if a mark believes a social engineer has been properly vetted through a security system, then they may assume that the social engineer belongs in a setting. Robert described creating a counterfeit badge to gain access to a utility company's campus and was waved through a checkpoint by security. He explained that he had unobstructed access as that point because "once you're on the campus, you know, it's just kind of assumed that you belong there." In addition, participants indicated that social media is also a boon for social engineers looking to place themselves within the relational networks of a mark, usually by fabricating a social media profile and connecting with the mark.

### 4.3. Activation

In addition to establishing social proximity with the mark, participants argued that social engineering ruses involve explicit nudges by the perpetrator to encourage the mark to act in a desired manner. While they acknowledged that social engineers can make explicit demands and threats to secure their objectives, the participants in this study, as previously noted, generally balked at such heavy-handed methods. Instead they focused on two approaches to *activate* the mark or motivate them toward action: request their help and offer an incentive. These approaches are discussed in turn.

#### 4.3.1. Call for help

For many participants, a good pretext involves a request for help from the mark (n = 27) (see also: Atkins & Huang, 2013; Holt & Graves, 2007; Huang & Brockman, 2011; King & Thomas, 2009; Whitty, 2013). Participants tended to view people as inherently helpful which presents a vital point of exploitation. As Brian stated, "In the end, people want to be good. They want to be helpful. They want to be, they want to be nice. So how do I abuse the natural trusting nature of people?" Edward similarly explained that the best approach is "helping. It's always gonna be helping. Humans, no matter what country, no matter what regions, humans naturally will tend to help someone in a person [*sic*], one-on-one position, when that person's in distress." There are limitations on the level of assistance that can be reasonably requested, however. Therefore, according to Edward, the pretext should be framed such that the social engineer will "just need a little bit of help."

#### 4.3.2. Incentivize

Study participants also explained that offering an incentive to the mark could be effective (n = 18). Such an incentive may be in the form of a service. For instance, John described approaching a mark disguised as a telecommunications employee and saying, "I'm Evan with AT&T. I need to get into your server closet because we're doin' some work down the street and we need to make sure we don't cut your lines so you lose all your Internet connectivity." Such a pretext may be successful because the work appears to provide a valuable service by preventing a work-halting Internet outage. Incentives may also be more direct—like the promise of a monetary reward for cooperation. Zeke claimed that the most successful frauds are those "that you can tie a reward or incentive to it, like a ten-dollar Amazon gift card." For him, "people will click it no matter what. Like guaranteed." This tactic mirrors incentive strategies adopted by social scientists to increase survey response rates (Dillman, 2007). And like these survey response strategies, Zeke warned that "you do a hundred-dollar gift card, people will not click it because it's not believable." Thus, the incentive should be enough to convince the

person to click on a link and perhaps surrender sensitive information, but not enough to raise suspicion.[11]

### 4.4. Concealment

Once the mark realizes the situation is not what it appears to be, the ruse will be unsuccessful. Participants described several general tactics that can be used to avoid raising a mark's suspicion. These approaches generally involved giving the deception a sense of realism and ordinariness. It may also entail specific conversational rules-of-thumb and tricks to prevent the mark from thinking too deeply about their interaction with the social engineer. Finally, avoiding detection to maintain a ruse may require situational flexibility and improvisation on the part of the social engineer. Importantly, planning may be a way to develop these mechanisms of concealment. These strategies are considered in detail below.

#### 4.4.1. Authenticity

For most participants, generating and maintaining trust with social engineering targets required curating situational authenticity; the appearance of truth or realism (n = 31). Williams and Milton (2015, p. 81) similarly claim in their own study that, "every con game is predicated on believability. Without it, the actors (con artists) would not be able to hold the mark in their grip." To achieve authenticity, some participants claimed that a person must embody the role—engage in "method acting" where, as Donnie explained, "you have to actually be the part … there's a huge distance between being the part and acting the part." Fleshing out a role in this manner for participants involved adopting strategies such as curating a back story, learning relevant skills, becoming fluent in professional jargon, and avoiding breaking pretext or character when challenged. Participants explained that these performances require control over presentation-of-self, including facial expressions and body language, specifically in vishing and in-person deceptions. Most significantly, this meant avoiding expressing anxiety. "If your anxiety level is up," John explained, "that transfers to people. People can detect all those things and all those count against you in social engineering." Acting appropriate for a given setting may also involve performing everyday activities like striking up casual conversation or entering a break room and making a cup of coffee (Dorian).

Achieving authenticity also involves understanding and adhering to the social conventions (norms, customs, and scripts) that govern a mark's expectations for interactions within the context of their everyday life or, as Arlo explained, one becomes "whatever the other person wants to hear." According to some study participants, marks are less likely to question a pretext which adheres to social convention. A key reason given is that violations of interactional expectations may be jarring for a mark which may, in turn, cause them to question the interaction. The more the mark questions the interaction, according to participants, the more likely the social engineer will be resisted, challenged, shut-out, exposed, or apprehended. Additionally, participants indicated that understanding the social conventions that dictate interactional conduct for the mark can be vital for finding points of vulnerability to social engineering.

Another way to achieve authenticity, as explained by participants, is to change appearances. For in-person deceptions, this may involve the use of costumes and props including wearing uniforms, creating counterfeit credentials, carrying a clipboard, displaying relevant branding on clothes and props, among other strategies. As Brian stated, "If you're physically doing social engineering, dress up the part." Yet, there are ways to change appearances across other vectors of communication as well. For vishing calls, participants explained that social engineers may "spoof" their phone numbers to appear as if they are coming from a number or location familiar to the mark. Phishing emails may similarly be made to replicate the visual design of legitimate emails like those coming from banks, government agencies, and other organizations. Similarly, participants indicated that email addresses may be used which approximate a legitimate email address to fool the mark into thinking the email is from a credible source. Webpages maybe spoofed or otherwise designed to appeal to the target using carefully selected imagery to increase credibility. As previously mentioned, the social engineer can also create a fabricated persona to be presented through these communications according to participants.

#### 4.4.2. Ordinary

Related to achieving authenticity, another common feature of many of the pretexts described by participants is that they are often ordinary or mundane in appearance (n = 22). Such pretexts should draw "the least amount of attention" and require "the least amount of thought on the person who is tasked with making the decision with whether to allow you or not" (John). It means blending into the surroundings and engaging in interactions that appear to be business-as-usual (see also: Atkins & Huang, 2013; Holt & Graves, 2007; Huang & Brockman, 2011; King & Thomas, 2009). An ordinary pretext, based on participant responses, is non-threatening, normal for the situational context, and often boring to avoid drawing scrutiny from the mark. For example, Daniel explained, "I like maintenance pretext better because people ignore the garbage man, they ignore maintenance folks." Other examples given by participants include fire extinguisher inspectors, electrical inspectors, pest-control personnel, IT personnel, and telecommunications technicians. As Lucy explained, "they're people you ignore. They're around the environment, they're doing stuff, but you ignore them."

In a phishing example, Zeke described sending fraudulent emails to two persons working in the financial arm of an organization. The email claimed to need some information to comply with a new law designed to "ensure confidentiality around HIPPA requirements" and that "you may not receive health benefits next year if you don't complete it." Many employees are regularly asked to complete forms for liability, compliance, or other bureaucratic reasons. As a result, according to Zeke, the mark thinks "yes, that seems acceptable in my mind. It's something I can do. It's only gonna take a few seconds."

#### 4.4.3. Spectacle

On the other end, participants also indicated one method of ensuring their ruse goes undetected is to be spectacular (n = 17)—to overwhelm the mark or engage in what Whitty (2013) describes as "visceral influences." As discussed previously, this may involve invoking intense emotions, like fear, which can be effective but also can have significant drawbacks if not applied appropriately (e.g. mark resists or even becomes combative) (see also: Williams & Milton, 2015, p. 89). One popular approach for overwhelming a mark, according to participants, is to create a sense of urgency or crisis (see also: Whitty, 2013, p. 672; Huang & Brockman, 2011). Urgency is the desire to resolve a matter as quickly as possible to avoid negative consequences or losing out on a valued goal—outcomes that may coincide with fear. John explained, for instance, that a social engineer can "send an email that says, 'hey, your credit card charge to Amazon.com for two-thousand dollars has been approved.'" In this manner, "you might click on that link before your logical brain tells you, 'hey, I need to wait a minute. This doesn't make any sense. That's not even from Amazon!"

Stirring up intense emotions or creating urgency is not the only way to overwhelm the mark, however. Participants indicated that a mark can be overwhelmed through a deluge of stimuli or information—so much that the mark may have difficulty processing the situation (see also: Chantler & Broadhurst, 2006; Sutherland, 1937, p. 74; Vishwanath

[11] The provision of material or monetary incentives is similar to the strategy of con-artists who take advantage of the greed or "larceny" of a mark (Maurer, 1940, pp. 117–118; Sutherland, 1937, p. 56; Williams & Milton, 2015, p. 2). The distinction is that social engineers may not require that the mark believe they are "making money by dishonest methods" (Sutherland, 1937, p. 56), only that they are making money.

et al., 2011). According to August,

> You know, if I'm talking to people, the overload technique is always great. Really trying to either hit 'em with a bunch of stuff all at once or having, you know, like kind of loud noises or screaming babies in the background or, you know, stuff like that. People tend to get really antsy and want to get off the phone with you when they hear a screaming baby that won't stop.

In this sense, the social engineer confuses and distracts the mark through intense stimulation to undermine their ability process to deception properly.

This study posits that ordinary and spectacular represent two ends of a stimulation continuum which are related to deception success in a curvilinear fashion. As Forrest explains this stimulation continuum through an insect analogy,

> You can either be an insect that tries to blend into his or her surroundings and not become prey, or you want to be so ostentatious in your adornment and coloration that you catch the eye of a bunch of other living creatures for whatever reason, either to intimidate them as a potential predator or to throw them off their guard.

In this sense, while ordinary pretexts try to "blend into the landscape," a social engineer may disrupt the target "in a way that spins people's head and throws them off their regular cognitive processes."

#### 4.4.4. *Efficiency*

Participants indicated that successful social engineering deceptions involve interactions which are quick in execution and avoid unnecessary complexities (n = 12). Victor, for example, explained that he tends to think about building "big plans" and has to stop himself from "overthinking it," especially when a simpler approach may be effective. Similarly, in phishing emails Herbert advised that "when you're writing an email – short, short but using something that will elicit a response." A simple approach may be all that is necessary to achieve significant results according to John: "it can be the most innocuous, small thing could lead to some pretty dire consequences." He added that, conversely, complexity can undermine a fraud: "Complexity makes it less successful … the more somebody [the mark] has to think about something or the more somebody is uncomfortable or doesn't understand, the less successful you're going to be." Similarly, quick deceptions may also be most effective. As Walter explained, "don't give them time to think about it." He also cautioned, however, that "you don't want to sticker shock 'em either. I mean, there's a happy medium." In other words, the interactions should be quick but not unnaturally so—social interactions tend to have a certain rhythm and flow to them. If the social engineer rushes, the mark may notice and become suspicious. The mark, however, should also not be given enough time to fully consider the fraudulent nature of the interaction.

#### 4.4.5. *Accommodation*

To remain undetected, participants claimed that social engineers may need to "read" a mark's emotions, body language, and other signs to determine if and how the social engineer should adjust their approach to account or accommodate for the mark's perceived interpretation of the situation (n = 17). The ability to do this successfully is not unlike a con-artist's "grift's sense" or the professional thief's "larceny sense" (Sutherland, 1937, p. 32; Williams & Milton, 2015, p. 76). For instance, in phone interactions, "within the first minute or two of the phone call, I can kind of tell how it's gonna go because it, I mean, it's just, you know, the people's tone, their tone of voice and how short their answers" (Robert). Even in phishing emails, the social engineer may need to interpret reactions from the mark to determine how to proceed according to participants. If a mark replies, then their textual responses may give the social engineer insight into the next steps to be taken. If they do not, then the social engineer can interpret non-response as a failure of the initial pretext and can recalibrate or approach through a different method.

Participants described various methods for dealing with resistance or rejection. One method is to be persistent. During a physical trespass into a facility, Zeke despaired upon getting caught by a security guard. His partner on the scene, however, insisted that they continue the deception and attempt to lie their way out of the situation. They were successful and Zeke attributes that to their persistence. Another strategy is to learn to overcome what Brian termed "conversation stoppers" or utterances, facial expressions, and body language expressed by a mark which are intended to halt a social interaction or shut down a request by the social engineer. Additionally, the social engineer may want to back off and allow a situation to cool before proceeding (see also: Goffman, 1952; Maurer, 1940, p. 48). Zeb, for example, described hiding in a bathroom for a few hours when he garnered too much attention during a physical penetration test of an organization.

## 5. Discussion

The results of this study indicate that effective social engineering deceptions (1) are well researched, (2) take into account the demographic characteristics, prior experiences, and skillsets of the social engineer, (3) consider the routine activities of the mark and current events, (4) foster a positive relationship with the mark, (5) embed the social engineer within the mark's network of familiarity, (6) appeal to the mark for help, (7) provide an incentive for the mark to act, (8) possess authenticity, (9) appear business-as-usual, (10) overwhelm the mark, (11) are quick and simple in design and execution, and (12) consider the mark's reactions to the ruse and adjusts accordingly to maintain the deception. Any single social engineering deception does not require all these elements for success. The data from this study, however, suggest that successful and effective deceptions require at least some and the more that are involved, the greater the likelihood of success against a given target.

The themes uncovered in this analysis show that social engineering is a complicated and nuanced endeavor. It takes advantage of the norms of social interaction, status and power, the malleability of perception, and cultural values and expectations. It also accounts for the role of social structure in the patterning of everyday life, relationships, and interpersonal exchange. At this juncture, this study turns to social theories which facilitate a deeper consideration of the implications of this study. In particular, the symbolic interactionism of Erving Goffman is employed to consider how participants exploit foundational elements of human interaction. Also considered are the theories of Pierre Bourdieu and Anthony Giddens whose work considers the role of social structure and culture in shaping the rules and expectations of social encounters. Use of these theories is not to imply that these are the only theories appropriate for understanding social engineering—only that they are useful in the context of this study which considers social engineering as a performative enterprise.

To begin, what is noteworthy about these traits that underpin social engineering deceptions is how unnoteworthy they are. There is a tendency to treat contemporary information security and technology crimes as something relatively novel and unique—that that addition of computer and network technologies is an important factor in determining the nature and causality of the offense (for an overview, see McGuire, 2020). Yet, the results indicate that social engineering deceptions are often rather banal. In many ways they parallel other forms of social deceptions or fabrications—parallels perhaps most evident in Erving Goffman's foundational analyses of social interactions. For instance, social engineering may involve prelude activities like research or what Goffman (1959, p. 13) terms "preventative practices" to make effective pretexts and avoid "incidents" or adverse events in the field. Social engineering is also a performative endeavor whereby the perpetrator must execute their ruse in a manner that appears true-to-life, is sensitive to social conventions, and typically—but not always—avoids disruptions

to the routine patterns of everyday life for the mark. They may deploy costumes, props, and backstories to create a fraudulent social identity that will appeal to the sensibilities of the target (Goffman, 1969, pp. 22–24). Social engineers may build rapport or engage in what Goffman (1969, p. 37) terms "seduction" where they "maneuver a definition of the situation such that the subject is led to believe that the observer is to be treated as something of a teammate, to whom strategic information (among other things) can be voluntarily entrusted" (Goffman, 1969, p. 37; see also: Williams & Milton, 2015, p. 78).[12] They must exhibit "emotional self-control" or "poise" to avoid appearing nervous or uneasy during a social engineering encounter and thus giving up the ruse (Goffman, 1969, p. 31; 1967, p. 9). Should anything go awry, they may need to engage in "corrective practices" to recover from possible disruptions to their ruse (Goffman, 1959, p. 13). In other words, the roots of effective social engineering are buried in the foundations of social interaction and exist independently of their technological context—though technology certainly plays a role in mediating, shaping, and facilitating such interactions.

In addition to revealing how banality of social engineering deceptions, the results of the study also highlight dimensions of deception that have hitherto been underexplored in the area. The analysis underscores the role of social context and social stratification in deceptive encounters—that social engineers may consider, for instance, the role of factors like gender, race, age, and socioeconomic status. Goffman (1961, p. 33) refers to such considerations as "transformation rules" that dictate social standing in any given social encounter. Bourdieu (1980/1990, p. 56) elaborates on such interlinkages between individual performance and these situational rules through his concept of *habitus* or "embodied history" that simultaneously structures current actions within a social setting (or "field") and is structured by social circumstances. To use a sports metaphor, *Habitus* is the playing field and rules of the game that influence the actions of players on the field. The playing field and rules structure player actions yet players also reinforce the rules and the legitimacy of game through participation.

From the perspective of Bourdieu, social engineers need to understand a mark's *habitus* to appeal to their sensibilities and appear to belong in each field—to generate a sense of authenticity. The perpetrator can also deploy fraudulent forms of capital (economic, social, and cultural) to situate themselves within a mark's field, both horizontally and vertically (Bourdieu, 1980/1990, p. 66).[13] In other words, there exist rules within a social setting that determine social standing and these rules can be gamed (within reason) to maneuver one's position. For instance, bringing to bear forms of capital (monetary assets, social connections, tastes, etc.) can allow a person to elevate their standing within that setting. Presenting real or fabricated forms of capital may afford the social engineer varying degrees of visibility (or invisibility) and status. Such *habitus* may be communicated through the physical characteristics of the social engineer as well as their mannerisms, language, clothing, use of props, and other elements endemic to a pretext. For instance, when a social engineer attempts to appropriate the trust or fear a mark has in an authority figure, they are cultivating a particular kind of social capital that will elevate them enough within the hierarchy of the field to provide clearance for otherwise prohibited information or systems access. Or, when considering the varying stereotypes that social engineers account for, it seems that a perpetrator should be mindful of the degraded *habitus* that certain characteristics bring to their encounters. In this manner, a pretext can be understood as an attempt to curate a "false" *habitus*.

Beyond understanding the rules of social interaction and station, the way participants described borrowing the trust placed in various roles and institutions reflects an attunement to the mechanisms of trust within modernity as described by Anthony Giddens. Giddens (1990, p. 80) contends that trust in the context of modernity is linked to "abstracted systems," notably "expert systems." Because the layperson often lacks the knowledge of experts, they must trust that the expert knows what they are doing. He likens this placement of trust to "faith" but not faith in the individual expert *per se* but "in the authenticity of the expert knowledge which they apply" (Giddens, 1990, p. 28). From a Giddensian perspective, the appropriation of trust in IT professionals, administrators, and third-party contractors by social engineers exploits modern mechanisms of trust in social networks. The social engineer can gain trust by developing a credible link between themselves and an expert system—which can be accomplished through the judicious use of professional jargon, trade-knowledge, costumes, props, and other methods. Once this perceived link is established, the fraudster can take advantage of the privileges afforded to them by a mark's faith in those expert systems and related institutions. In this sense, the high level of trust placed in expert systems by a mark may be exploited by the social engineer to overcome the lower level of interpersonal trust accorded to the social engineer as a result of having a "weak tie" in the mark's social network (Granovetter, 1973).

Participant responses also indicated that social engineers may purposely endeavor to avoid scrutiny from a mark by appearing to be an expected and unremarkable presence in a social setting. In this manner, social engineers appear sensitive to what Goffman (1971) terms "civil inattention." Civil inattention involves two parties in a social setting—like two people passing each other on the street—showing awareness of one another without further engagement. Giddens (1990, p. 81) argues that civil inattention is a quintessential type of encounter with strangers in public places within modernity. For him, "civil inattention is trust as 'background noise'—not as a random collection of sounds, but as carefully restrained and controlled social rhythms" (Giddens, 1990, p. 82). Mundane pretexts, particularly ones reliant on adopting ignorable roles within an organization (like maintenance and custodial staff) exploit such civil inattention. Marks are likely aware that such workers are present but know that these people generally belong in such settings and do not need to be "dealt with." In other words, they are people who are integral for the maintenance of organizational operations but who other members generally ignore or do otherwise give considerable attention to—they constitute organizational "background noise."

Finally, while it was a relatively minor theme in this analysis, it is worth considering the theoretical implications of the role of timing in social engineering deceptions. Participants indicated that social engineers may account for current events, cultural traditions (like holidays), and the mark's schedule when formulating pretexts or deciding when to execute a deception. Routine Activities Theory posits that crimes are likely to occur when suitable targets and motivated offenders come together in time and place in the absence of capable guardians (Cohen & Felson, 1979). In this manner, macro-structural and cultural contexts shape the activities and expectations of the mark (see also: Ferrell, Hayward, & Young, 2015). The results of this study thus suggest that social engineers can take advantage of the routine activities of the mark to target marks when they might be least vigilant and, therefore, most vulnerable.

## 6. Conclusion

Synthesizing the results of this study indicate that social engineering deceptions are best understood as a performative, situational endeavors structured by interactional norms dictating social congress across hierarchically and vertically situated actors, the abstraction of trust under

[12] The "definition of the situation" is a term developed by from Thomas and Thomas (1929) to mean that "people act in social situations toward objects and other people on the basis of their interpretations and definitions" (Ulmer, 2017, p. 108).

[13] By "horizontally" we mean the level of familiarity established between the mark and the social engineer. In another sense, it is the proximity the social engineer situates themselves within a mark's social network. By "vertically" we refer to the hierarchical positioning between the social engineer and the mark.

**Table 3**
Propositions to guide future research on social engineering deceptions.

| # | Proposition |
|---|---|
| $P_1$: | As level of preparation by the perpetrator increases, so too does likelihood of successful perpetration. |
| $P_2$: | Deception success increases with rapport building efforts (both in quantity of efforts and quality). |
| $P_3$: | Deceptions which borrow trust from other sources rather than attempt to cultivate trust purely through rapport building will be more successful. Sources of transitive trust may include familiar actors within a mark's social network as well as representatives of expert systems. |
| $P_4$: | Horizontal social distance between the perpetrator and the mark (the familiarity between the two or the proximity within a social network) influences fraud success in a curvilinear fashion. Pretexting with too much familiarity (e.g. close friend or co-worker) is likely to fail as is pretexting with too little (complete stranger). |
| $P_5$: | Vertical social distance between the perpetrator and the mark (the hierarchical positioning between the two actors) has a curvilinear relationship with deception success. For example, social engineers can attempt to position themselves hierarchically above the mark to establish authoritative dominance or below to elicit help and sympathy. |
| $P_6$: | Pushes to action that appeal to fear, help, or through an incentive will increase success. In other words, perpetrators should energize action on the part of the mark. |
| $P_7$: | Deceptions which incorporate signs of authenticity (both in quantity and quality) are more likely to deceive a mark. |
| $P_8$: | Deceptions which build upon social stereotypes increase likelihood of deception success. This proposition could also be considered a subproposition to $P_7$. |
| $P_9$: | There is a curvilinear relationship between pretext sensationalism and success. At one end, ordinary pretexts may allow the social engineer to take advantage of civil inattention or otherwise enter unnoticed into a mark's *Umwelt* or "the region around shim from within which signs for alarm can come" (Goffman, 1971, p. 252). On the other, deceptions that over-stimulate a mark may defuse their ability to pick up on the situational deception cues, effectively disabling their *Umwelt*. |
| $P_{10}$: | As duration of contact between the mark increases, the likelihood of deception success decreases. |
| $P_{11}$: | As the complexity of the ruse increases, the likelihood of success decreases. |
| $P_{12}$: | Proper timing of a ruse will increase success. This proposition can be subdivided into two subpropositions: |
| | $P_{12a}$: Deceptions which take advantage of current events or the holidays may play to the emotions of the mark and thus increase success likelihood. |
| | $P_{12b}$: Deceptions which account for the routine activities of the mark to make them more suitable targets or less capable guardians will increase likelihood of success, a proposition consistent with Cohen and Felson's Routine Activities Theory (1979). |

the expert systems of modernity, and proximity within social networks. In other words, deceptions are situations where the micro-interactional and the macro-structural interplay and co-mingle (Ferrell et al., 2015). Yet this is only one study of social engineering. Other studies may, of course, draw different conclusions. For this reason, this analysis advances testable propositions concerning factors that influence social engineering success drawing from the previously described themes and social theories. These propositions may be useful for criminologists and other social scientists interested in social engineering and related forms of deception (Table 3).

In addition to the aforementioned propositions, research should further investigate the role of perpetrator traits in deception and fraud execution, including the race, gender, age, physical appearance, skills, and prior experience of the perpetrator. Further, though evidence is mixed concerning the effects of victim sociodemographic characteristics on fraud susceptibility (e.g. Button & Cross, 2017; Titus, Heinzelmann, & Boyle, 1995; Whitty, 2019), these factors may be more evident when considered in interactions when both the victim and the perpetrator are able to detect or infer these characteristics, like in-person or over the phone. Future research should also consider the potential independent or dependent relationships between the dynamics described in the proposed propositions. For instance, while vertical social distance (relative position within hierarchy) may impact deception success, it may be unnecessary if sufficient horizontal distance (familiarity) is established to garner trust. Thus, a social engineer may be able to occupy a flat hierarchical position relative to the mark if they can garner the appropriate level of horizontal proximity.

Scholars should also consider the subject of social engineering from a deception detection perspective. Involved is the consideration of the psychological and social mechanisms through which individuals attempt to discern authentic from deceptive social exchanges (e.g. Eckman & Friesen, 1969; Jacobs, 1993). Goffman (1969, pp. 14–19) refers to such deception detection strategies as the "uncovering moves" employed by potential marks to discern the intent of the perpetrator and the authenticity of their performance. Though this analysis does consider strategies used by social engineers to avoid deception detection ("counter-uncovering moves"), it does not focus on deception detection outright as this would require data gathered from potential marks. This is a gap that deserves further consideration to develop a more holistic view of deceptive or fraudulent encounters. Analyses may also consider how motivation impacts the deployment of social engineering deceptions. For instance, it is possible that perpetrators motivated by purely instrumental ends (like pecuniary gain) might be more likely to rely on certain characteristics of effective deceptions described here rather than others. Those who rely do social engineering for expressive purposes (e.g. for the challenge) may focus on others. It is thus worth considering how motivation may shape the performance of social engineering deceptions.

## Funding

This work was supported by the National Science Foundation (SES #1616804).

## Credit author statement

This work is a co-authored paper. The work is 100% by the authors.

## Acknowledgements

We would like to thank Travis Pratt, Trevor Durbin, and Jurg Gerber for their comments on prior versions of this manuscript. Thanks are also extended to Gerad Middendorf for his insights. We also appreciate the support and constructive feedback of the *Computers and Human Behavior* reviewers.

## References

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23–32.

Bachmann, M. (2010). Deciphering the hacker underground. In T. J. Holt, & B. Schell (Eds.), *Corporate hacking and technology-driven crime* (pp. 105–126). Hershey, PA: IGI Global.

Baker, W. E., & Faulkner, R. R. (2006). Diffusion of fraud: Intermediate economic crime and investor dynamics. *Criminology, 41*(4), 1173–1206.

Baumer, E. P., Ranson, J. W. A., Arnio, A. N., Fulmer, A., & De Zilwa, S. (2017). Illuminating a dark side of the American Dream: Assessing the prevalence and predictors of mortgage fraud across U.S. counties. *American Journal of Sociology, 123*(2), 549–603.

Bourdieu, P. (1980/1990). The logic of practice. Stanford, CA: Stanford University Press.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling, 15*(1), 20–45.

Button, M., & Cross, C. (2017). *Cyberfrauds, scams and their victims*. New York, NY: Routledge.

Caldwell, T. (2011). Ethical hackers: Putting on the white hat. *Network Security, 2011*(7), 10–13.

Chantler, A., & Broadhurst, R. (2006). *Social engineering and crime prevention in cyberspace*. Brisbane, Queensland, Australia: Queensland University of Technology. Technical report retrieved from http://eprints.qut.edu.au/7526/1/7526.pdf.

Charmaz, K. (2002). Qualitative interviewing and grounded theory analysis. In J. F. Gubrium, & J. A. Holstein (Eds.), *The handbook of interview research* (pp. 675–769). Thousand Oaks, CA: Sage.

Cialdini, R. B. (2009). *Influence*. New York, NY: HarperCollins.

Clark, R. B., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime & Justice, 2*, 147–185.
Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588–608.
Comet, C. (2011). Anatomy of a fraud: Trust and social networks. *Bulletin de Méthodologie Sociologique, 110*, 45–57.
Copes, H., & Vieraitis, L. M. (2012). *Identity thieves: Motives and methods*. Boston, MA: Northeastern University Press.
Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3–21.
Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 151–196.
Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. Berlin, Germany: Springer-Verlag.
Cornish, D. B., & Clarke, R. B. (2002). Analyzing organized crimes. In A. Piquero, & S. Tibbetts (Eds.), *Rational choice and criminal behavior* (pp. 41–64). London: Routledge.
Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice, 5*(2), 120–131.
Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology, 58*, 1303–1322.
Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice, 518*, 1–14.
Dillman, D. A. (2007). *Mail and Internet surveys: The tailored design method*. Hoboken, NJ: John Wiley & Sons.
Doocy, J. H., Shichor, D., Sechrest, D. K., & Geis, G. (2008). Telemarketing fraud: Who are the tricksters and what makes them trick? *Security Journal, 14*(3), 7–26.
Eckman, P., & Friesen, W. (1969). Nonverbal leakage and clues to deception. *Psychiatry, 32*, 88–106.
Ferrell, J., Hayward, K., & Young, J. (2015). *Cultural criminology: An invitation* (2nd ed.). Thousand Oaks, CA: Sage.
Giddens, A. (1990). *The consequences of modernity*. Stanford, CA: Stanford University Press.
Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory*. Chicago, IL: Aldine Publishing Company.
Goffman, E. (1952). On cooling the mark out. *Psychiatry: Interpersonal and Biological Processes, 15*(4), 451–463.
Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Anchor Books.
Goffman, E. (1961). Encounters: Two studies in the sociology of interaction. In *Indianapolis*. Bobbs-Merrill.
Goffman, E. (1969). *Strategic interaction*. Philadelphia, PA: University of Pennsylvania Press.
Goffman, E. (1971). *Relations in public: Microstudies of the public order*. New York, NY: Basic Books.
Goffman, E. (1974). *Frame analysis: An essay on the organization of experience*. Cambridge, MA: Harvard University Press.
Granovetter, M. (1973). The strength of weak ties. *American Journal of Sociology, 78*(6), 1360–1380.
Granovetter, Mark (1985). Economic action and social structure: The problem of embeddedness. *American Journal of Sociology, 91*(3), 481–510.
Hadnagy, C. (2018). Social engineering: The science of human hacking. In *Indianapolis*. Wiley.
Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*, 102–113.
Holt, T. J. (2009). Lone hacks or group cracks. In F. Schmalleger, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 336–355). Upper Saddle River, NJ: Pearson Education.
Holt, T. J. (2010). Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review, 28*, 466–481.
Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology, 1*(1), 137–154.
Huang, W., & Brockman, A. (2011). Social engineering exploitations in online communications: Examining persuasions used in fraudulent emails. In T. J. Holt (Ed.), *Crime online: Correlates, causes, and context* (pp. 87–111). Durham, N.C.: Carolina Academic Press.
Hutchings, A. (2013). Hacking and fraud: Qualitative analysis of online offending and victimization. In K. Jaishankar, & N. Ronel (Eds.), *Global criminology: Crime and victimization in a globalized era* (pp. 93–114). Boca Raton, FL: CRC Press.
Internet Crime Complaint Center. (2020). *2019 Internet crime report*. Washington, D.C: Federal Bureau of Investigation. Retrieved February 19, 2020 at https://pdf.ic3.gov/2019_IC3Report.pdf.
IC3 (Internet Crime Complaint Center). (2019). *2018 Internet Crime Report*. Retrieved July 15, 2019 at https://pdf.ic3.gov/2018_IC3Report.pdf.
Jackson, J. E. (1994). Fraud masters: Professional credit card offenders and crime. *Criminal Justice Review, 19*(1), 24–55.
Jacobs, B. A. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology, 31*(2), 281–299.
King, A., & Thomas, J. (2009). You can't cheat an honest man: Making ($$$s and) sense of the Nigerian e-mail scams. In F. Schmalleger, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 206–224). Upper Saddle River, NJ: Prentice Hall.
Lea, S., Fischer, P., & Evans, K. (2009). *The economic psychology of scams*. Nova Scotia, Canada: International Association for Research in Economic Psychology and the Society for the Advancement of Behavioral Economics.
Leukfeldt, E. R. (2014a). Cybercrime and social ties: Phishing in amsterdam. *Trends in Organized Crime, 17*(4), 231–249.
Leukfeldt, E. R. (2014b). Phishing for suitable targets in The Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551–555.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017a). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*, 704–722.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017b). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change, 67*(1), 39–53.
Levi, M. (1981). *The phantom capitalists: The organisation and control of long-firm fraud*. London, England: Heinemann.
Lusthaus, J. (2018). *Industry of anonymity: Inside the business of cybercrime*. Cambridge, MA: Harvard University Press.
Maurer, D. W. (1940). *The big con: The story of the confidence man*. New York, NY: Anchor Books.
McGuire, M. (2020). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In R. Leukfeldt, & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 3–28). New York, NY: Routledge.
Mitnick, K., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. In *Indianapolis*. Wiley.
Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of Internet fraud victimization: A systematic review. *Journal of Police and Criminal Psychology, 34*(3), 231–245.
Ortner, S. B. (2006). *Anthropology and social theory: Culture, power, and the acting subject*. Durham, NC: Duke University Press.
Rauti, S., & Leppänen, V. (2017). "You have a potential hacker's infection": A study on technical support scams. *2017 IEEE International Conference on Computer and Information Technology*. https://doi.org/10.1109/CIT.2017.32
Schell, B. H., & Holt, T. J. (2010). A profile of the demographics, psychological predispositions, and social/behavioral patterns of computer hacker insiders and outsiders. In T. J. Holt, & B. H. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications*. Hershey, PA: IGI Global.
Schell, B. H., & Melnychuck, J. (2010). In T. J. Holt, & B. H. Schell (Eds.), *Female and male hacker conference attendees: The autism-spectrum quotient (AQ) scores and self-reported adulthood experiences* (pp. 144–168). Hershey, PA: IGI Global: Corporate hacking and technology-driven crime: Social dynamics and implications.
Shover, N., Coffey, G. S., & Hobbs, D. (2003). Crime on the line: Telemarketing and the changing nature of professional crime. *British Journal of Criminology, 43*, 489–505.
Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. New York, NY: NYU Press.
Sutherland, E. H. (1937). *The professional thief*. Chicago, IL: University of Chicago Press.
Taylor, P. A. (1999). *Hackers: Crime and the digital sublime*. New York, NY: Routledge.
Thomas, W. I., & Thomas, D. S. (1929). *The child in America*. New York, NY: Knopf.
Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency, 41*(1), 54–72.
Tracy, P. E., & Fox, J. A. (1989). A field experiment on insurance fraud in auto body repair. *Criminology, 27*(3), 589–603.
Ulmer, J. T. (2017). The extensive legacy of symbolic interactionism in criminology. In R. A. Triplett (Ed.), *The Wiley handbook of the history and philosophy of criminology* (pp. 103–122). Indianapolis: Wiley.
Verizon. (2018). 2017 Data breach investigations report. *Retrieved*. at https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2017.pdf . (Accessed 21 February 2020).
Verizon. (2019). 2018 Data breach investigations report. *Retrieved*. at https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf . (Accessed 20 August 2019).
Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586.
Whitty, M. T. (2013). The scammers persuasive techniques model. *British Journal of Criminology, 53*, 665–684.
Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292.
Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice, 16*(2), 176–194.
Williams, T., & Milton, T. B. (2015). *The con men: Hustling in New York City*. New York, NY: Columbia University Press.
Yar, M. (2008a). Computer crime control as industry: Virtual insecurity and the market for private policing. In K. F. Aas, H. O. Gundhus, & H. M. Lomell (Eds.), *Technologies of insecurity: The surveillance of everyday life* (pp. 189–204). New York, NY: Routledge-Cavendish.
Yar, M. (2008b). The rhetorics and myths of anti-piracy campaigns: Criminalization, moral pedagogy and capitalist property relations in the classroom. *New Media & Society, 10*, 605–623.
Yenkey, C. B. (2018). The outsider's advantage: Distrust as a deterrent to exploitation. *American Journal of Sociology, 124*(3), 613–663.