4

Pretexting: Recognizing the Mitnick Mythology

> The goal of the social engineer is to get you to make a decision without thinking. . . . I need to state one very important point: social engineering is not politically correct. . . . [social engineering] takes advantage of the fact that gender bias, racial bias, age bias, and status bias (as well as combinations of those biases) exist.
>
> —Chris Hadnagy[1]

> We all have stereotypes which minimize not only our thinking habits but also the ordinary routine of life.
>
> —Edward Bernays[2]

For several years, the *Social-Engineer.org Podcast*, a flagship podcast in the field of hacker social engineering, used a song called "Trust Me" as its theme song. Written by the nerdcore hip-hop duo Dual Core, "Trust Me" includes a boast about the social engineer's ability to take on any role:

> I can be anyone, anywhere I aim
> I just need the mindset, a story, and a name.[3]

Dual Core's lyrics bring to mind the clichés of spy movies, where spies quickly don disguises that get them into the most secure areas. The song's subsequent lyrics continue this theme, with rapper Int80 exploring a host of roles he could play: clipboard-carrying foreman, customer service worker, corporate executive, tech support.

Hacker social engineers have a word for this: pretexting. Put simply, a pretext is the role a hacker social engineer will play when they are engaging with the target. Obviously, a hacker can't call up an organization and say, "Hello! I am a hacker. May I please have a password to your network?" Instead, the hacker social engineer practices deception by playing a role with a seemingly legitimate need for sensitive information. Logically, pretexting follows trashing quite nicely: trashing provides a wealth of information that can inform the roles a social engineer can play.

Here, we take up this hacker social engineer term with several goals. We'll explore the interpersonal dynamics of hacker social engineering, and then we'll use the concept as a lens to look backward at similar mass social engineering practices. Just as in Dual Core's "Trust Me," we'll see a range of pretexts: construction workers, representatives of charitable organizations, citizens' councils, and medical professionals. This basic analysis will appear to reinforce Dual Core's observation that social engineers can be anyone, anywhere they aim.

However, the heart of our analysis is not about the social engineer's wild abilities to take on any role they please. Instead, we focus on the social structures that constrain as well as inform social engineering pretexts. To explore such social structures, the bulk of our chapter engages with perhaps the most famous social engineer of all, Kevin Mitnick. Mitnick started as a phone phreak, became a felon after being convicted for hacking crimes, then later evolved to be the respected security consultant he is to this day. Stories about Mitnick's exploits abound, giving us the impression of a man with

mythical pretexting abilities. If anyone can be anyone, anywhere he aims, it might be Mitnick.

And yet, as we argue, Mitnick's individual genius is grossly overstated. Mitnick's pretexts were reliant on social structures. The lesson we learn from Mitnick's case is that it's not the virtuoso abilities of the social engineer that enables a pretext to succeed. Ultimately, pretexts succeed thanks in large part to the pernicious persistence of reductive stereotypes. We will see the power of reductive stereotypes not only in hacker social engineering, but also in mass social engineering and later in masspersonal social engineering.

Hacker Pretexting

The pretext is an exceptionally important aspect of a hacker social engineer's attack; it is not to be left to chance. It must be methodically planned out in advance, and the literature from professional social engineers reinforces this idea. The social engineer needs what security consultant Sharon Conheady's book *Social Engineering in IT Security* refers to as "the backstory that explains who you are and why you need the information you are requesting." The pretext "even influences your attitude while executing the test."[4] Conheady's colleague, Chris Hadnagy, invokes a pseudo-method acting description of the process:

> Pretexting involves not just coming up with the storyline but also developing the way your persona would look, act, talk, walk; deciding what tools and knowledge they would have; and then mastering the entire package so when you approach the target, you are that person, and not simply playing a character.[5]

Such attention to the pretext is needed because hacker social engineers directly engage with their targets in interpersonal communication: on the phone, over email or text, or even in person. The

role, then, must be carefully prepared before it is put to trial during an engagement.

These roles can vary based on what the social engineer learns during the trashing phase. Does the target donate to charities? Perhaps I should email a malicious PDF of a charitable society's flier. Does the target contract with a particular cafeteria vendor? I can mimic their uniforms and get into the organization that way. Does the target use a particular type of computer? Perhaps calling up and saying that I'm with tech support and I need to update their operating system can work.

During these pretexts, social engineers use the "stuff of authenticity": material artifacts that align them with the organization they seek to infiltrate.[6] Common artifacts are uniforms, ID badges, lanyards, business cards, hardhats, lunchboxes, toolboxes, business attire, phones, or (if one is trying to tailgate through a door) several to-go cups of coffee.[7] Consider this social engineer's guide to visual (and, to a lesser extent, olfactory) authenticity during a pretext as a construction worker:

> A common mistake is to purchase brand-new high visibility vests and hardhats, which stand out as somewhat unusual. How many workmen [sic] are seen with a pristine outfit? When the [social engineers] eventually built up the wardrobe . . . , they swapped brand-new high visibility vests and hats for used ones. Unfortunately, the used items stank of diesel, but at least they looked authentic, because they were.[8]

Here, used and thrown-out clothing can help with playing the role.

Even in the case of pretexting over the phone or over digital channels, all the right details need to be in place. If a hacker social engineer is making a telephone call and playing the role of an office worker, they'll probably want to play office sounds in the background; a phone center employee pretext may call for a different soundscape (both easily available via YouTube videos).[9] If they're using email, a company logo or spoofed website may be in order.

And all of this is not to mention using the proper tone during the phone call or in written correspondence.

Mass Social Engineering Pretexts

While the interpersonal hacker social engineers have spent a great deal of time focusing on constructing roles and scenarios, they weren't the first social engineers to do so. As pioneering public relations practitioners in the 1920s, mass social engineers Edward Bernays and Doris Fleischman regularly created "circumstances which will modify" the habits and customs of targeted groups.[10] To do so, these mass social engineers used pretexts just as hacker social engineers would do. However, unlike hacker social engineers, mass social engineers did not adopt the roles themselves. Instead, their created circumstances were populated with surrogates who played the roles. Bernays wrote about this explicitly:

> the public relations counsel . . . may enlist the interest of an individual or an organization in his client's point of view. . . . That individual organization may then propagandize [the client's issue] through its own channels because it is interested in it. In such a case, *the point of origin then becomes that individual or organization*. The public relations counsel, having made the link between the interest of his client and the interest of the third party, no longer need figure in the resulting expression to the public.[11]

If there were no existing groups or individuals willing to propagandize on behalf of Bernays and Fleischman's clients, they would simply borrow from the playbook of the social reformers of their time and create

> seemingly independent organisations which profess to support concerns of the common good: the Committee for the Study and Promotion of the Sanitary Dispensing of Foods and Drink; the Radio Institute of the Audible Arts; the Temperature Research Foundation; [and] the Middle America Information Bureau.[12]

While these organizations imitated the early twentieth-century progressive social reformers' use of citizen committees, their purpose was not for self-governance. Instead, they were always tied to a specific public relations campaign Bernays and Fleischman were hired to conduct. For example, the American Council for Wider Reading was formed while they were doing public relations for a book publisher.[13] The Committee for the Study and Promotion of the Sanitary Dispensing of Foods and Drink was reportedly created to promote Dixie's disposable paper cups as more sanitary than reusable, washable cups.[14]

One of their efforts, a wildly successful idea Bernays and Fleischman pitched to Proctor & Gamble in the early 1920s, deserves more mention: soap carving competitions. These were created to support P&G's goal of selling more bar soap.[15] Starting in 1925, P&G began sponsoring contests for Americans to create art carved out of Ivory soap. But rather than appear to be a "string-pulling mastermind," P&G established a "National Soap Sculpture Committee" as a pretext:

> This sounded very official, indeed, and its New York City address only punctuated the authenticity of the committee's art world credibility. All aspects of the contest were handled publicly under this name. The committee published every contest announcement and exhibition catalog, and it was responsible for an informative series of books by soap carvers on the how-tos and wherefores of their chosen art form.[16]

P&G was never mentioned as the "contest's sole originator and coordinator (thus 'donating' money only to its own PR programs)."[17] As Jennifer Jane Marshall writes in her article "Procter & Gamble's Depression-Era Soap-Carving Contests," "This way P&G was able to avoid the appearance of impropriety, an important measure of decorum in an era when advertising gimmicks—and exasperation with them—ran high."[18] Indeed, even the name of the contest was a front: "The National Soap Sculpture Competition in White Soap"

didn't mention Ivory by name, but Ivory was the only white soap on the market at the time of the contests.[19]

In other words, the National Soap Sculpture Committee was a pretext, playing the role of sponsors of wholesome art contests but designed by the mass social engineers Bernays and Fleischman to help P&G sell soap. Sales of Ivory did indeed rise—even during the Great Depression.

But perhaps the most infamous pretexts concocted by Bernays and Fleischman came from their late 1920s work for American Tobacco, a company seeking to increase the number of women smokers. This work relied heavily on pretexting. They linked smoking to thinness and health by enlisting experts to condemn sugar and praise cigarette smoking. Bernays and Fleischman solicited a physician who obliged them with this medical advice: instead of having a sugary dessert,

> the correct way to finish a meal is with fruit, coffee and a cigarette. The fruit hardens the gums and cleans the teeth; the coffee stimulates the flow of saliva in the mouth and acts as a mouth wash; while finally the cigarette disinfects the mouth and soothes the nerves.[20]

Bernays and Fleischman shared this quote with journalists in order to get news coverage of the physician's recommendation. To bolster the claim that cigarettes are healthier than sundaes, Bernays and Fleischman recruited dance school instructors, photographers, and dance troupes to praise being thin, cutting out sweets, and smoking cigarettes.[21] Again, they shared these sentiments with reporters, creating the appearance of a nationwide consensus against sugar (and, incidentally, in favor of cigarettes). This way, their client, American Tobacco, never had to make direct claims; these proxies did.

In addition, Fleischman and Bernays linked cigarette smoking to feminist emancipation, recruiting women to march in the 1929

Easter Parade, carrying lit cigarettes as "torches of freedom" to protest a taboo against women smoking in public.[22] The goal was to have this seemingly subversive act covered in the news. The women did not reveal that they were recruited to march by a PR firm hired by American Tobacco.[23]

Finally, in order to encourage more women to smoke American Tobacco's Lucky Strike cigarettes—which came in distinctive green and red packaging—Bernays and Fleischman concocted a "Green Ball" at the Waldorf Astoria hotel in New York City. While American Tobacco sponsored the ball, Bernays and Fleischman hid that fact behind a front of New York socialites who took credit. The ball required everyone to wear green, and it was so successful in its "propaganda efforts," recalls Fleischman, "that the country was swept by a demand for green costumes and accessories."[24] And again, American Tobacco was never openly named.

These practices were not atypical for mass social engineers—indeed, histories of public relations are rife with documentation of "front groups" who stood in for powerful organizations—but Bernays and Fleischman perfected the form.[25] The use of pretexts is now a common public relations tactic.[26] Today, while multiple professional public relations groups urge their members not to use this "third party technique," a wide range of interests, from pharmaceutical companies to governments, employ mass social engineers who create these pretexts with few to no consequences for such deceptions.[27]

To work, such pretexts had to be believable, and such belief had to start with the mass social engineers themselves. "Whatever cause they serve or goods they sell, effective propagandists must believe in it—or at least momentarily believe they believe in it."[28] Like the recommendation that the hacker social engineer must totally inhabit the pretext they create, the mass social engineer must believe that their work is important, that the cause they champion is beneficial to all of humanity.

The "World's Most Famous Hacker"

This accounting of hacker and mass social engineering pretexts might give the impression that social engineers can take on just about any pretext imaginable. The pretexts used by Bernays and Fleischman are particularly legendary—many commentators present their work on behalf of American Tobacco as being the key reason women increasingly smoked cigarettes in the twentieth century. And our contemporary vision of hacker social engineers is of devious geniuses who can take on a wide range of roles.

But there is one figure in social engineering history who appears to be the master pretexter: Kevin Mitnick, the self-proclaimed "world's most famous hacker."

More than just about anyone in the past century, the most common name associated with social engineering—mass, interpersonal, or otherwise—is Kevin Mitnick. Almost every time we mentioned this social engineering book project to people, they would say, "Oh, you mean like Kevin Mitnick." The FBI manhunt in the mid-1990s, his arrest in 1995 for computer hacking, his conviction, and his subsequent writing, speaking, and security consulting careers have all contributed to Mitnick's self-proclaimed status as the world's most famous hacker. And his hacking technique of choice is not to break into networks through computer-aided techniques, but instead to use a pretext and simply call people up on the phone and ask for access. Mitnick is not just the most famous hacker; he's the most famous social engineer.

Media coverage of Mitnick's criminal career and subsequent reformation and legitimation have not challenged Mitnick's self-mythology.[29] Recent headlines about Mitnick refer to him as "legendary," a "master hacker" who can "access your system in less than an hour."[30] Mitnick himself does little to discourage such praise, bragging to journalists that he is a "rock star in the hacker community" and that "I'm very good at what I want to do."[31] And he

reinforces his legendary status with his books, especially *The Art of Deception* and *Ghost in the Wires*. In those books, he relives his social engineering pretexts: on one telephone call, he's a customer. The next, he's a police officer. Next, he's the CEO. And in the end, businesses are infiltrated, information purloined, and Mitnick's status grows. Above all, reading through the news coverage and his books, we learn that the rest of us, we hapless humans, are the "weak link" of computer security, to repeat one of Mitnick's favorite phrases.[32]

We could easily contribute to the Mitnick mythology by repeating stories of his exploits, using them to illustrate hacker social engineering pretexts in action, but ours is a different approach. Emphasizing Mitnick's exploits obscures more than it reveals. Instead of focusing on the virtuoso social engineering skills of Mitnick, we want to focus on the structures that enabled him to succeed. We will focus on how his use of pretexts is aided and abetted by social structures of recognition.

Theories of Identity Play

Social engineers' ability to inhabit roles invites us to explore postmodern theories that hold that identity is entirely malleable. Such ideas were especially powerful in the 1990s as the internet gained popularity and people performed a range of identities in online chats, games, and early social media. Recently, however, an increasing number of scholars across a range of fields are starting to shift their analysis away from the individual-focused performance of identity to the larger social structures that both enable and constrain such performances.

Queer theorists considering trans identities are a good guide here. Synthesizing the postmodern, identity-play theories of identity with sociology's interest in social structures and power relations, Raewyn Connell and Carla Pfeffer have argued that "passing,"

where, for example, a transgender woman is deemed "successful" insofar as she passes as a cisgender woman, places far too much emphasis on the particulars of the woman's performance.[33] Instead, both argue for the concept of "recognition," focusing on how such performances are accepted or denied by those with the privilege to do so. For Connell, recognition is a relational perspective. While a focus on passing may help us to understand the performative aspects of social categories (such as male/female, queer/straight, or Black/white), recognition helps us understand the structures in which such performances are legible.[34] Building on this, Pfeffer argues that,

> rather than focusing on transgender social actors' accomplishment of normative gender through "passing," sociologists might focus, instead, on the interactional processes whereby all social actors serve as arbiters of the gender order as they recognize or reject others as "belonging" to (or rightful members of) particular gender and sexual identity categories and groups.[35]

Such a relational, interactionist conception of how identities are enmeshed in social relations can be seen in the enigmatic philosophy of Michel Serres, whose book *The Parasite* puts forward a triangulating theory of three-part relations and communication.[36] For Serres, communication is not simply a matter of one entity sending messages to another. There has to be a third term, a channel between the two entities. One special type of a third term is the "blank" or "joker," a concept Serres draws from card and domino games:

> The joker is a card in a game that serves to alter the direction of play. It interrupts the game and makes a new set of moves possible. Likewise, the white or blank domino can change the fortunes of a player because it can be played to link sequences of dominoes that are otherwise incommensurable.[37]

Hence, while it is wild, the joker or blank takes on value only in relation to other elements in the game. Its presence is part of the game. Though its special capacity to change its role depending on

its context allows for a more dynamic game, it must be played in relation to existing cards.

Bringing these perspectives together, a joker or blank domino can only function within a game if the players both agree upon the rules of the game and recognize its relationship to other cards or dominoes. Likewise, identity performances—including pretexts—work insofar as they are recognized and legitimated by other members of a community who operate under often unspoken social norms and rules. To focus solely on passing ignores the legitimating processes of the other social arbiters who implicitly or explicitly judge the performance and subsequently include and support or exclude and diminish the person attempting to pass. Likewise, focusing solely on the wildness of the wild card, joker, or blank domino is to overstate its capacity to change the game. The joker or blank "certainly adds disruption to social order, but we should not lose sight of the fact that it can also save rather than destroy order."[38]

Thus, role-playing is not simply a matter of taking on a role; it requires others to recognize and accept the role-player. Social structures can constrain, but they allow for creative identity performances within those constraints. As organizational studies scholars argue, "'identity' is a matter of claims, not character; persona, not personality; and presentation, not self. . . . 'Identity' is discursively fashioned by *both* the observers and the observed."[39]

Turning back to Kevin Mitnick, one way to tell his history of social engineering is to focus on his virtuoso pretexts, and indeed many commentators do precisely this. They imply that his interpersonal communication skills are such that he could take on any pretext. This mythology arguably aids Mitnick today, since he claims the title "the world's most famous hacker" and owns a security consultancy boasting of having a "100% success rate" in penetration testing.[40]

However, another way of understanding Mitnick—and by extension, social engineering pretexts as a whole—is to consider his capacity to act as a social joker, a blank that is capable of taking on

roles thanks not just to his own pretexting skills but also to a wide range of social structures of recognition. Within these metaphorical rules of the game, Mitnick's varying roles offer a chance to preserve existing orders as much as they disrupt them. This approach draws attention to the social webs that make pretexting possible, showing how pretexting can help maintain—rather than subvert—those social webs. When we read the reporting on Mitnick, as well as his own writings, from this perspective, we start to consider how social structures of social capital, transnational corporate organizational dynamics, and racial stereotypes (particularly, juxtapositions of Asianness against whiteness) help create the conditions that allow Mitnick's pretexts to become recognizable.

Recognizing Mitnick's Pretexting Successes: Structural Factors

Social Capital

Perhaps the most commonly told story of how Kevin Mitnick awakened to the promises of social engineering is his figuring out how to ride public buses for free throughout the San Fernando Valley of California as a child in the 1970s. He noticed that the bus system used paper transfer slips validated with a special paper punch, and he surmised he could ride the buses for free if he could punch his own transfers. In Mitnick's memoir, he tells of what may have been his first pretext, playing the role of a student in need of supplies:

> I walked to the front of the bus and sat down in the closest seat to the driver. When he stopped at a light, I said, "I'm working on a school project and I need to punch interesting shapes on pieces of cardboard. The punch you use on the transfers would be great for me. Is there someplace I can buy one?"[41]

The pretext worked: the bus driver told Mitnick where the paper punches were sold. Later, Mitnick did some trashing to get books

of unused transfers from a dumpster behind a bus depot. From that point on, he rode for free "everywhere the bus system covered—Los Angeles County, Riverside County, San Bernardino County."[42]

Thus, Mitnick's career starts with transit fraud. This is a crime that many researchers have noted gets prosecuted quite unevenly, with disparities playing out along racial lines: Black and brown citizens bear the brunt of transit cop attention.[43] But, as the white Mitnick recalls,

> Did I get into trouble for Dumpster-diving for those bus transfers and riding for free? . . . [N]o. My mom thought it was clever, my dad thought it showed initiative, and bus drivers who knew I was punching my own transfers thought it was a big laugh. It was as though everyone who knew what I was up to was giving me attaboys.[44]

In other words, rather than having what Black and brown parents call "the talk"—that is, the warning that American society will viciously prosecute or execute young Black and brown men for even minor transgressions—the Mitnick family either turned a blind eye to young Kevin's pretexts and transit fraud, or they praised him for beating the system.[45]

From this moment on, a pattern emerges: Mitnick goes forth and revels in the identity-play possibilities of telecommunications, using a range of pretexts to gain access to restricted information and software, and, when he is caught, retreats to his family, particularly the loving women in his life. His mother, for example, allows him to use a pretext as an apartment building manager to con GTE out of phone service after the phone company shut down their connection; later, she laughs off a visit from the FBI. "What harm could a boy come to just from playing with a computer at home?" his mother asked. As Mitnick admits, "she had no concept of what I was up to."[46] His mother, grandmother, and aunt provide money for suits, tuition, attorney's fees, and bail. Later, Mitnick's wife Bonnie also supports him (although she does eventually divorce him

because he continues hacking). All of them drive him around, including to work, from work, and from various jails and police stations. He moves from social engineering free rides on the bus to bumming free rides from his family.

As professional social engineer Sharon Conheady notes in her book, *Social Engineering in IT Security*, pretexting can be draining. "Your adrenaline pumps so hard that afterward you are completely exhausted." Likewise, on the *Social-Engineer.org Podcast*, episode 120, the panelists, including former FBI behavioralist Robin Dreeke and social engineers Chris Hadnagy and Perry Carpenter, all cautioned would-be social engineers about the emotionally draining aspects of pretexting.[47] These professionals strongly recommend setting aside time to recover from pretexts, whether they be in-person, online, or over the phone (the channel Mitnick preferred). For Mitnick, having social support from his relatives may have allowed him to engage in pretexts knowing that he had some safe space to retreat to and recover from his adrenaline-pumping engagements. He had a support structure allowing him to go forth, "be anyone, anywhere he aims," and yet have somewhere to return to and recover in.

Indeed, the necessity of social support structures for pretexters is highlighted further when we consider the period in the mid-1990s when Mitnick was on the run from the FBI. He cut ties with his family, changed his identity, and moved to new cities. His account of this period in *Ghost in the Wires*, as well as journalist Jonathan Littman's book *The Fugitive Game*, are marked by exhaustion, paranoia, and uncertainty, as Mitnick flees helicopters, is suspicious of anyone sitting in a parked car, and refuses to get close to anyone lest they betray him.

Communication, Organizational Structures, and Transnational Capitalism

Mitnick's pretexts often exploited a simple fact: many organizations are so far-flung that employees don't know each other personally.

Many of Mitnick's targets—NEC, Bank of America, Digital, Pacific Bell, Oakwood Corporate Housing, and TRW, to name a few—were, in the 1990s, regional, national, or even transnational-spanning organizations with branches in many locations. Often, Mitnick would infiltrate these distributed organizational structures with the relative anonymity of telephone calls to slowly but surely gather small pieces of information. As he describes the process, he would gather

> information about the company, including how that department or business unit operates, what its function is, what information the employees have access to, the standard procedure for making requests, whom they routinely get requests from, under what conditions they release the desired information, and the lingo and terminology used in the company.[48]

What Mitnick learns is how communication constitutes these transnational organizations. As communication scholars argue, communication helps define reality, and thus structures interaction, enacts power, and animates hierarchies within organizations.[49] This is especially true in the cases of geographically distributed organizations, where communication across distance facilitates the very existence of organizational units, such as teams.[50] Mitnick demonstrated an intuitive understanding of how communication structures an organization, and much like a manager, he wanted a larger picture of who speaks to whom in organizations, under what conditions, what terms and language they use, and how organizational power is expressed in those communications.

An example from Mitnick's social engineering of Pacific Bell illustrates this further. Based on his previous reconnaissance (whether through trashing, trading for documents, or phone-based inquiries), Mitnick learns the rituals of communication that members of the target corporations engage in. This knowledge includes familiarity with insider lingo. Using this and

> posing as a technician in the field, I called Pacific Bell's Mechanized Loop Assignment Center, or MLAC, also known simply as the Line

> Assignment Office. A lady answered and I said, "Hi. This is Terry out in the field. I need the F1 and the F2 on 310 837–5412 . . ."
>
> "Terry, what's your tech code?" she asked.
>
> I knew she wasn't going to look it up—they never did. Any three-digit number would satisfy, so long as I sounded confident and didn't hesitate.
>
> "Six three seven," I said, picking a number at random . . .[51]

In order for his pretext as a technician to work, the ritual of asking for information (Mitnick's tech code) and giving it must be satisfied, and the rest of the lingo and technical elements are in place. Thanks to this, Mitnick is able to get the information he seeks—an address for a rival hacker—while the Pacific Bell employee believes that she successfully reconstitutes the organization through her interaction with him.

Mitnick's success here hinges far less on his putative skills than on simple, organizational communication routines. As he explains,

> Why was the lady in Line Assignment so willing to answer my questions? Simply because I gave her one right answer and asked the right questions, using the right lingo. So don't go thinking that the Pacific Bell clerk who gave me [the] address was foolish or slow-witted. People in offices ordinarily give others the benefit of the doubt when the request appears to be authentic.[52]

In other words, Mitnick's performance as "Terry out in the field" was not some virtuoso acting, nor was it reliant upon some sort of hypnosis. Simply put, it was recognized by the operator he called as a seemingly normal part of day-to-day communicative structure that constituted the large, regional organization that is Pacific Bell.

After having mapped the organization via its communication network, Mitnick could use the relative anonymity of the phone to insert himself into the organization and capture information as it flowed across the network. He would use a variety of pretexts, ranging from claiming to be a specific member of the organization to claiming to be an outsider, such as a contractor or business

partner. But he always had to do so *in relation to others*, making sure his communicative practices aligned with those of his target organization.

"My Hero Is Japboy": Mitnick's Yellowface Minstrelsy

Mitnick also took advantage of existing cultural structures, particularly racial stereotyping. Mitnick's—and by extension, American culture's—peculiar relationship with Japanese people in the 1990s informed one of Mitnick's most notorious pretexts.

As several newspapers and books reported, a key person who helped the FBI catch Mitnick during his fugitive period in the mid-1990s was the Japanese-born American computational physicist and security expert Tsutomu Shimomura. At one point, Mitnick broke into Shimomura's computer. In response, Shimomura aided the FBI in hunting down Mitnick. Thanks to Shimomura's help, the FBI caught Mitnick in his apartment in Raleigh, North Carolina, in 1995.[53]

As a Japanese-born American who gained fame in the 1990s for tracking and catching "the world's most wanted hacker," it is not surprising that the American journalistic coverage of Shimomura played up his ethnic background. Also not surprising—but nonetheless deeply disturbing—was the racism of the coverage. The coverage of Shimomura versus Mitnick took on valences of what American studies scholar Joseph Won calls "yellowface minstrelsy," "the use of Asian martial arts, artists and artifacts by non-ethnic Asians for fun and profit."[54] As Won argues, yellowface minstrelsy parallels older white American appropriative practices of blackface minstrel shows

> in the same way that black dance, music and verbal play summarized black culture in the 19th century, Asian martial arts images today comprise in large part what contemporary consumers of television, film, newspapers and magazines know as "Asian (and Asian American) culture."[55]

A *New York Times* profile of Shimomura was one of the first articles on the security researcher, and it subtly invoked visions of martial arts. Discussing Mitnick's hacking of Shimomura's computer,

> It was as if the thieves, to prove their prowess, had burglarized the locksmith. Which is why Tsutomu Shimomura, the keeper of the keys in this case, is taking the break-in as a personal affront—and why he considers solving the crime a matter of honor.[56]

A "matter of honor" invokes a peculiar American fascination with Asian martial arts movies and, through them, the uneasy relationship between American and Asian cultures—particularly Japan—in the 1980s and 1990s.[57] Framing Shimomura's pursuit of Mitnick in such terms gets amplified in subsequent coverage. A *Rolling Stone* article, for example, presented the contest between Shimomura and Mitnick as a battle of "the samurai and the cyberthief."[58] Such coverage is part of the larger anxiety about the mysterious, technologically adept and wealthy Japanese in 1990s America.[59] Shimomura's abilities with computers and digital networks—two things that many people find inscrutable and difficult to fathom—likely intensified the mystery, resulting in the use of familiar and yet exotic popular culture tropes of martial arts.

Perhaps the most egregious examples of the yellowface minstrelsy framing of Shimomura appears when Mitnick comments on his erstwhile foe, especially in the book *The Fugitive Game*, where journalist Jonathan Littman includes transcripts of his phone calls with then-fugitive Mitnick. Several of their conversations were about Shimomura, who by then was tracking Mitnick. Littman describes Shimomura as a "touted samurai."[60] He discusses a picture of Shimomura in *Newsweek* with Mitnick: "Next to the keyboard," Littman tells Mitnick, "I swear it looks like there is a samurai sword."[61] Mitnick replies, "I'm sure he'd like to chop some people's heads off. . . ."[62] Then, according to Littman, "Mitnick does his best kung fu master imitation. 'You dishonored my family. You

will die! I'll meet you . . . and we will fight to the death!'"[63] Here, Mitnick's accent is an instance of yellowface minstrelsy, using martial arts clichés to discuss the "matter of honor." To further fuel the antagonism, Mitnick also mocks Shimomura in an online chat, saying, "my hero is japboy."[64]

However, Mitnick did not limit his use of yellowface accents to his private conversations with Littman. The same yellowface minstrelsy stereotyping that informed coverage of Shimomura also aided Mitnick with one of his pretexts, bringing us to another structural context that social engineers might exploit: racial stereotypes. As he writes in *Ghost in the Wires*, Mitnick wanted to "break into NEC's network and download the source code for all the NEC cell phones used in the United States."[65] To do so, he first used the pretext "Rob in the IT department" to gain access to one computer.[66] But he wanted to get more data, so he called the same NEC employee back, this time with a different pretext altogether. With this second pretext, Mitnick gets, as he claims, "gutsy":

> I was no Rich Little when it came to doing accents, but I was going to try to pass myself off as Takada-san, from NEC Japan's Mobile Radio Division.
>
> I called [NEC USA employee Jeff Lankford] at his desk. When he picked up the phone, I launched into my act:
>
> "Misterrrr, ahh, Lahngfor, I Takada-san . . . from Japan." He knew the name and asked how he could help.
>
> "Misterrr Lahng . . . for—we no find, ahhh, vers'n three ohh five for hotdog uhh project"—using the codename I'd picked up for the NEC P7 source code. "Can you, ahhh, put on mrdbolt [an NEC server]?"
>
> He assured me that he had Version 3.05 on floppy and could upload it.
>
> "Ahhh, thank . . . ahhh, thank you, Mr. Jeff . . . I check mrdbolt soon. Bye."[67]

Because this works, Mitnick gives himself a pat on the back: it was an "apparently not-too-pathetic accent."

In invoking a yellowface accent, Mitnick played to the same 1990s American visions of Japan that fueled the journalistic coverage of Shimomura. This was not a nuanced understanding of the many ways the Japanese speak, live, and act, but rather a mode of speaking that satisfied American perceptions of the Japanese. In this framing, Shimomura, who had lived in America since he was six, was no ski bum, but rather a sort of samurai sword-wielding cyber-kung fu warrior on a quest to regain his honor. And Mitnick becomes a rival kung fu master who ultimately fails to best him.[68] Likewise, Mitnick's yellowface accent as Takada-san is a pretext readily recognizable in 1990s America.

In terms of the relational aspects of pretexting, such yellowface minstrelsy benefited Mitnick because it satisfied the recipient of his call, who may himself have drawn on prejudices to judge the legitimacy of Mitnick's call. The accent was apparently "not-too-pathetic," a passing accent, for Lankford. This is a specific case of how stereotypes function during an identity performance:

> Because these structures are so ingrained and because taking advantage of them can offer such concrete advantages, the reproduction of these stereotypes (through passing and to pass) may in the abstract present a challenge to social hierarchies, but in the literal sense also reinforces them.[69]

Whereas we may view a social engineer like Mitnick as subversive and his victims as hapless rubes, taking up the relational aspects of pretexting, we have to question how Takada-san or "Shimomora the Samurai" *reinforce* social hierarchies in the context of the American anxieties about Japan during the 1990s. Who is more recognizably "Japanese"—the staid, long-haired ski bum from Princeton, New Jersey, or the white man fast-talking in a Kwai Chang Caine-esque or Mr. Yunioshi-esque accent? Which accent is more believable: a flat Ohio Valley radio voice or speech punctuated by "ahhs" and dropped consonants? Both accents—the presumably white "Rob in IT" and the faux-Japanese "Takada-san" were ready to hand

for Mitnick for his pretexts, and both worked on the same NEC employee, who is invested in helping the corporation function by supporting—and not questioning—his colleagues, the organizational hierarchy, or the dominant racial order.

Social Engineering and Stereotyping

The myth of Kevin Mitnick held that he could do any pretext over the phone and bullshit his way into any information system. Such a myth focuses solely on Mitnick's performances, making it seem as if his abilities are those of a singular genius. We may then extend such mythologies to social engineering more broadly. A social engineer—mass, interpersonal, or masspersonal—can play any role they please and manipulate us. The wild stories of hacker social engineers like Mitnick, the stories from mass social engineers like Edward Bernays and Doris Fleischman, or the specter of Russians manipulating online communication, create the perception of extremely skilled, elite manipulators of targets.

As we have shown, this is not entirely the case. In practice, Mitnick's social engineering pretexts rely heavily on the recognition of others, especially their targets. He operated within webs of relationships and benefited from the recognition of others to pass in the roles he chose to play. In doing so, he was able to be a joker or blank and "[engineer] a kind of difference by intercepting relations."[70] Mitnick on the phone, in the midst of a pretext, *must* be understood in relation to the larger social, organizational, and cultural contexts he was operating in, not independent of them. We've examined the case of Mitnick to show some specific dimensions of this relationality: social capital, organizational structure, and social stereotyping. Here, we want to use the last category, social stereotyping, and return to the broader pretexting practices of mass and interpersonal social engineers we began this chapter with.

One lesson is clear: some bodies and subjectivities enjoy more flexibility than others when it comes to pretexting. The range of options open to white, cisgender males who have a great deal of social capital and speak the dominant language of a region is likely larger than those available to a non-binary person of color who does not have a stable home and speaks with a non-normative accent.[71]

But no matter the embodied existence of the social engineer, their pretexts must be relationally recognized.

For example, in a presentation at a security conference, hacker social engineer and security professional Sharon Conheady takes her audience through a thought experiment: "which . . . pretexts are the most likely to work for me?" She notes she's short and "doesn't look like a hacker"; she presents as female, and her accent is Irish. She then goes through scenarios, asking the audience to judge her likelihood of success. IT department? No, she says, it's awkward; people ask her if she's lost. Teacher? Yes. Cleaner? "Yeah, totally," she says. Waitress? Yes. Construction worker? No. Telecoms engineer? No. CEO? At that point, she states her point: "We play to stereotypes. As much as I hate it, we play to stereotypes."[72] As she notes, her pretext as a CEO over email in a phishing attack might work, but doing so in person would be "pretty brazen." And indeed, given her embodiment and ways of performing her identity, Conheady would have advantages in some of these roles that other people may not enjoy. But she cannot be just anybody. She must be recognized.

That a social engineer has to "play to stereotypes" is not limited to contemporary hacker social engineers. As an analysis of the work of Edward Bernays argues, Bernays

> regards stereotypes as "a great aid to the public relations counsel in his work" because they can be grasped by "the average mind," even though, he acknowledges, they are "not necessarily truthful pictures of what they are supposed to portray." No matter, according to Bernays, [public relations] practitioners can use stereotypes to reach

> a public and then add their own ideas to fortify their position and give it "greater carrying power."[73]

For Bernays (and Fleischman), a stereotype is conformity to a particular worldview, consonant with communication theorist Walter Lippmann's formulation of stereotypes as a reductive shorthand.[74] But unlike Lippmann, who is critical of the use of stereotypes, Bernays and Fleischman see in them resources to leverage for mass social engineering. To leverage stereotypes, Bernays suggests paying attention to the "tendency the group has to standardize the habits of individuals and to assign logical reasons for them."[75] Bernays vehemently denies that just any appeal will work for the group being targeted:

> The cause [the public relations counsel] represents must have some group reaction and tradition in common with the public he [sic] is trying to reach. This must exist before they can react sympathetically upon one another.[76]

"Public opinion is the resultant of the interaction between" the public relations counsel and the group mind.[77] And stereotypes help mediate that interaction. As mental shortcuts people use to conform to their groups, stereotypes become powerful tools for social engineering—they are easily recognized. So, returning to Bernays and Fleischman's use of front groups as pretexts, their groups had to be recognized—they had to fit the stereotype—in order to successfully manage the targeted crowds.

Overall, playing to stereotypes is possible, as we suggest, due to the preconceptions of those the social engineer is seeking to engage with. In Conheady's experience, being a petite Irish woman working on servers broke the expectations of others, who asked if she was lost. But being a waitress is easy for them to recognize and fits their notions quite well. For Mitnick, his male voice on the phone was a supple instrument that could play the role of technician, police officer, or manager—or even a cartoonish version of a Japanese

engineer, so long as the roles could be recognized. For Bernays and Fleischman, social stereotypes become convenient shorthand in public relations campaigns directed at various groups. These moves just have to be recognizable.

In other words, as Hadnagy and Bernays put it in the epigraphs to this chapter, the social engineer uses stereotypes in order to avoid having the target think. The goal is *recognition*, not cognition.

Conclusion

Pretexting is a staple part of the social engineering approach. While we have largely focused on Mitnick's career in the 1990s, as well as his recollection of it in the 2000s, the dynamics that made Mitnick's pretexts work are reflected across the social engineering literature. Here, we've touched on how the mass social engineers Bernays and Fleischman theorized stereotypes in mass social engineering, and later, we will return to this focus on stereotypes in pretexts in what we're calling masspersonal social engineering. We encourage others to analyze pretexting in terms of relationality, rather than the ostensible skills of the social engineer, to better understand how these deceptions work.

While the social engineer works hard to develop a recognizable pretext, there comes a moment when the pretext has to be put into action. This is the moment of engagement with the wily target. This is a moment for bullshit. We turn to this next.

Social Engineering

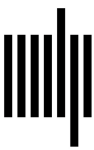
How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication

By: Robert W. Gehl, Sean T Lawson

Citation:

Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication
By: Robert W. Gehl, Sean T Lawson
DOI: 10.7551/mitpress/12984.001.0001
ISBN (electronic): 9780262368926
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Gehl, Robert W., author. | Lawson, Sean T., 1977–author.
Title: Social engineering : how crowdmasters, phreaks, hackers, and trolls created a new form of manipulative communication / Robert W. Gehl and Sean T. Lawson.
Description: Cambridge : The MIT Press, 2022. | Includes bibliographical references and index.
Identifiers: LCCN 2021016750 | ISBN 9780262543453 (paperback)
Subjects: LCSH: Social media—Security measures. | Computer networks—Security measures. | Internet fraud. | Social engineering.
Classification: LCC HM742 .G45 2022 | DDC 364.16/3—dc23
LC record available at https://lccn.loc.gov/2021016750

10 9 8 7 6 5 4 3 2 1