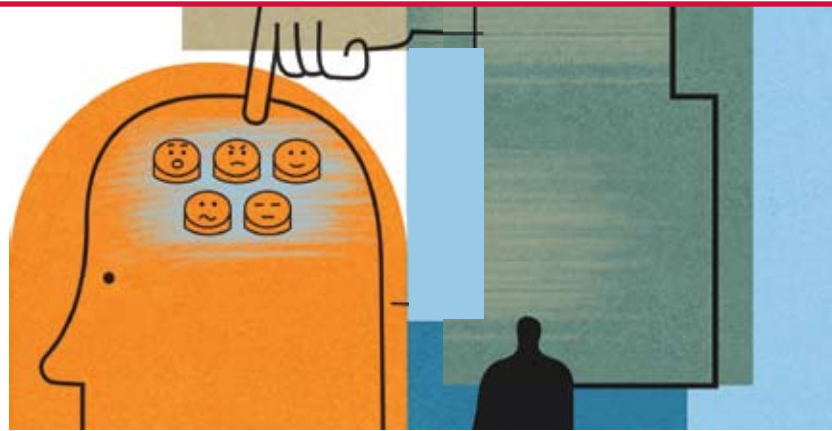


Ask and You Will Receive

By Karthik Raman



In January 2007, cybercriminals used social engineering tactics to carry out the world’s biggest online theft on record, stealing US \$1.1 million from customers of the Swedish Nordea Bank.

Customers received an email that appeared to have originated from Nordea Bank, and 250 of them downloaded and installed the “anti-spam” software that the email asked them to set up. The anti-spam software was in fact a Trojan that collected customer information, which the criminals used to log into the bank’s web site and steal money.¹

A well-known information security principle is that in any security system, people are the weakest link. Although security attacks and the defenses developed to respond to those attacks continue to evolve, human nature remains unchanged. To an attacker, social engineering is more efficient and brings quicker returns than a brute-force assault on encryption algorithms, fuzzing to find new software vulnerabilities, or adding complexity to malware. In the Nordea Bank fraud, it was easier for criminals to ask the bank’s customers to install a Trojan than to break into a vault to steal cash.

We are gullible, greedy, and curious, which means social engineers can manipulate our feelings and thoughts. They ask us for something, and very often they receive it. But why do we behave this way?

In pioneering work on the psychology of security, renowned security expert Bruce Schneier identified four research areas—behavioral economics, psychology of decision-making, psychology of risk, and neuroscience—that can help explain why our feeling of security deviates from reality.² This edition of the *McAfee Security Journal* and this article in particular focus on one aspect of security: social engineering. In this discussion, we shall draw from neuroscience, the psychology of decision making, and elementary social psychology to analyze why people fall for social engineering without perceiving the deception.

A Tale of Two Brains

The human brain is arguably the most complex system in the universe. Part of its complexity lies in its complicated layout and convoluted interaction of subsystems.

In the brain, emotions seem to arise from the older, inner parts, such as the amygdala, and reasoning from newer, outer parts, such as the neocortex.³ But the seats of emotion and reason are not mutually exclusive, as Isaac Asimov observed in his book *The Human Brain*:⁴

Emotions do not arise from any one small part of the brain, it would appear. Rather, many parts, including the frontal and temporal lobes of the cortex, are involved—in a complex interplay.

The parts of the brain responsible for emotion and reason can sometimes work with or against one another. That is why it is hard for us to keep reason and emotion separate, and why it is easy for emotion to override reason when the two contradict one another.

Let’s look at how we deal with fear, for example. Examining how we react to imminent danger, science writer Steven Johnson points out that the fear response is “an orchestral mix of physiological instruments launching with masterful speed and precision”:⁵

We talk about it colloquially as the fight-or-flight response. Feeling it kick in is one of the best ways to experience your brain and body as an autonomous system, operating independently of your conscious will.

When revisited by the conditions that led to a fight-or-flight response in the past, we allow the emotional response to take over even though we can reason objectively that the response is without merit.

Dishonest politicians, spies, and con men know that appealing to emotion—fear especially—to elicit an emotional response is a very effective means to their ends. Social engineers continue that tradition.

Theories of Social Engineering

Manipulating emotions

Many social engineers zero in on the emotions of fear, curiosity, greed, and sympathy. It is well-established that these are universal emotions; from time to time everyone feels afraid or curious or greedy or sympathetic.

Fear and curiosity are useful in many situations. Escaping a burning building is a good thing. Curiosity can help us challenge ourselves and learn something new. Still, acting out of fear or curiosity can cause us to do dangerous or undesirable things.⁶

Some attacks can be carried out even without the presence of the social engineer by manipulating a victim's curiosity. In April 2007, a banking Trojan planted in USB drives was left in a London parking lot. People who were curious to see what these drives contained and likely glad to become owners of a free storage device, plugged the drives into their computers only to infect them with malware.⁷

Attackers who threaten or blackmail victims manipulate their fear. The GPCoder.i Trojan, which appeared in June 2008, is an example of malware that manipulated fear: it encrypted users' files and demanded a ransom for their decryption.⁸ Likewise, attackers who bribe victims manipulate their greed, and attackers who pose as needing help manipulate their sympathy.

Misdirected mental shortcuts

Sometimes social engineers will appeal to something outside of our emotions. They'll try to trip up our mental rules for processing information. We call these rules heuristics, or rules of thumb.

Dishonest politicians, spies, and con men know that appealing to emotion—fear especially—to elicit an emotional response is a very effective means to their ends. Social engineers continue this tradition.

Although we must recognize that our heuristics are fallible, we cannot function without them. Our lives would be too difficult if we had to think through everything we perceived, said, and did. We desperately need our mental shortcuts. Psychologist Robert Cialdini explains this need:⁹

We can't be expected to recognize and analyze all the aspects in each person, event, and situation we encounter in even one day. We haven't the time, energy, or capacity for it. Instead, we must very often use our stereotypes, our rules of thumb, to classify things according to a few key features and then to respond mindlessly when one or another of these trigger features is present.

Let's see how social engineers can elicit automatic responses in us that work for them.

Triggering cognitive biases

A cognitive bias is a mental error caused by a simplified information-processing strategy.¹⁰ When a heuristic goes wrong, it becomes a bias. Social engineers nudge our heuristics into "severe and systematic" errors.¹¹

Here are a few cognitive biases that can explain social engineering:

- **Choice-supportive bias** People will remember an option of their choosing in the past as having more positive than negative aspects.¹² An online shopper could get used to purchasing discounted items on the Internet using referrals from friends. An occasional spam email could seem like another referral and lead the shopper into disclosing credit card information to a fraudulent web site.
- **Confirmation bias** People will collect and interpret evidence in a way that confirms their views.¹³ Let's take a hypothetical example. Suppose Acme Corporation contracts with Best Printers to maintain its printers, and all Best Printer service people wear gray, full-sleeved shirts with name badges. Over time, Acme's employees will get used to seeing Best Printers

service people in their uniforms and will identify anyone with gray, full-sleeved shirt with a badge as a custodian. A social engineer could fabricate or steal a Best Printers uniform to pose as a service person. The social engineer may not be challenged to identify himself because of the Acme employees' confirmation bias.

- **Exposure effect** People like things (and other people) according to how familiar they are with them.¹⁴ News of natural and man-made disasters often spawn phishing web sites that exploit this sentiment.¹⁵ People exposed to such news could be enticed easily into visiting phishing web sites that claim to have a connection with the news. Finally, people's exposure to the news might have lowered their guard with respect to the malicious nature of the web site they are visiting.
- **Anchoring** People focus on an identifying trait that is first apparent when they make decisions about something.¹⁶ A spoofed bank web site that prominently displays the actual bank's logo might deceive users even if other security indicators scream out the deception.¹⁷

Causing errors in schemas

Social psychologists define a "schema" as the picture of reality we refer to, so that we can draw conclusions about our environment. As children, we learn that being nice to others is a good thing. The notorious social engineer Kevin Mitnick has remarked that attackers know this and craft a request to victims to "sound so reasonable that it raises no suspicion, all the while exploiting the victim's trust."¹⁸ Thus, social engineers abuse the design of our social schema.

Here's a list of common social errors or judgments that people make, with illustrations of how social engineers exploit them:

- **Fundamental attribution error** People will assume that the behaviors of others reflect their stable, internal characteristics.¹⁹ This is the error of mistaken first impressions. A social engineer will train diligently to make a favorable first impression. Attackers could act personable when making requests or

act domineering when coercing victims into doing something. Victims may not realize that their interlocutors are actors and that their behavior is situational—a means to an end.

- **Salience effect** Given a group of individuals, people will guess that the most or least influential person is the one who stands out the most.²⁰ Social engineers are expert at fitting into their surroundings and blending in. They strive to flip the salience effect to their favor. They might pose as a client in a business suit or a custodian in overalls, but not as a juggler on stilts. Blending in is not limited to clothing and appearance—it can extend to knowledge of company lingo, events, employees, and even regional accents. A social engineer from California trying to breach a company in Boston may know about "Jill's" new baby and "Josh's" leaving the company for a competitor and may exchange this with the receptionist in a Boston accent to be allowed into the office for "IT repairs."
- **Conformity, compliance, and obedience** People respond to the pressures of conformity, compliance, and obedience by changing their behavior. Many social engineering attacks can be explained by victims' predictable responses to these pressures. A social engineer might pretend to be a visiting executive and prevail upon a young security guard to let her enter the premises in spite of the fact that she is not wearing a badge. (The attacker's promise of reward or threat of punishment may further pressure the guard). The guard may feel overwhelmed and will obey. Group social engineering attacks have not been observed, but they are conceivable. A number of social engineers might pose as legitimate employees and nag a receptionist to gain entry into an office by repeating "Don't waste our time" or "Let us get back to our work." The receptionist might just let them in to avoid being unpopular. A different technique that spies are known to use is to socialize with a victim for a while. The attacker at first requests innocent information from the victim and then moves onto sensitive information. The victim is trapped; he is pressured to comply with the next request, given his history of compliance, or risks a form of blackmail.



Conclusion

Our susceptibility to social engineering is rooted in the design of the human brain, in the complex interplay between the centers of emotion and reason. Social engineering is the manipulation of a victim's fear, curiosity, greed, or sympathy. Cognitive biases and errors in our social schemas help explain social engineering's success. So why is this knowledge so valuable to us?

In the 2007 CSI Computer Crime and Security Survey, only 13 percent of respondents said they had checked how effective their employees' training was against social engineering attacks.²¹ Although 13 percent is a low figure, the survey did not include those respondents who did not have any training program for social engineering attacks.

One obvious step is to create and improve security policies and user education programs about social engineering. Any policy on social engineering will be more persuasive if it uses scientific research to justify itself. User education materials will also be more effective if they list the cognitive biases that social engineers generally exploit, and training videos will be more effective if they demonstrate attacks that exploit each of our cognitive biases.

We can't change human nature. We are born with a split between our emotions and reason, and are prone to committing mental errors. This is normal, but such behavior is dangerous when exploited by social engineers. By understanding the psychology of social engineering and training users about its effects, we can defend against these attacks with greater success.



Karthik Raman, CISSP, is a Research Scientist at McAfee Avert Labs. His research interests in security include vulnerability analysis, network security, and software security. Beyond security, his interests include the cognitive and social sciences and computer programming. For fun, Raman plays cricket and the guitar and learns languages. Raman graduated with B.S. degrees in computer science and computer security from Norwich University (Vermont) in 2006.

ENDNOTES

- 1 "Bank loses \$1.1M to online fraud," BBC (2007). <http://news.bbc.co.uk/2/hi/business/6279561.stm>
- 2 Schneier, B., "The Psychology of Security," Essays and Op Eds (2007). <http://www.schneier.com/essay-155.html>
- 3 Ibid.
- 4 Asimov, I. "The Human Brain: Its Capacities and Functions." New York: Mentor Books, 1965.
- 5 Johnson, S. "Mind Wide Open: Your Brain and the Neuroscience of Everyday Life." New York: Scribner, 2004.
- 6 Svoboda, E. "Cultivating curiosity; how to explore the world: Developing a sense of wonder can be its own reward," *Psychology Today* (2006). <http://psychology-today.com/articles/index.php?term=pto-4148.html>
- 7 Leyden, J. "Hackers debut malware loaded USB ruse," The Register (2007). http://www.theregister.co.uk/2007/04/25/usb_malware/
- 8 McAfee VIL: GPCoder.i, June 9, 2008. http://vil.nai.com/vil/content/v_145334.htm
- 9 Cialdini, R. "Influence: The Psychology of Persuasion." New York: HarperCollins, 1998.
- 10 Heuer, Richard J., Jr. "The Psychology of Intelligence Analysis," Center for the Study of Intelligence, CIA (2002). <http://www.au.af.mil/au/awc/awcgate/psych-intel/art12.html>
- 11 Tversky, A. and Kahneman, D. "Judgment under uncertainty: Heuristics and biases," *Science*, 185, 1124-1130 (1974). http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf
- 12 Mather, M., Shafir, E., and Johnson, M. K. "Misrememberance of options past: Source monitoring and choice," *Psychological Science*, 11, 132-138 (2000). <http://www.usc.edu/projects/matherlab/pdfs/Matheretal2000.pdf>
- 13 Nickerson, R. S. "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology*, Vol. 2, No. 2, 175-220 (1998). <http://psy.ucsd.edu/~mckenzie/nickersonConfirmationBias.pdf>
- 14 Zajonc, R. B. "Attitudinal Effects of Mere Exposure," *Journal of Personality and Social Psychology*, 9, 2, 1-27 (1968).
- 15 Kaplan, D. "Virginia Tech massacre may spawn phishing scams," *SC Magazine* (2007). <http://www.scmagazineuk.com/Virginia-Tech-massacre-may-spawn-phishing-scams/article/105989/>
- 16 Tversky, A. & Kahneman, D. "Judgment under uncertainty: Heuristics and biases," *Science*, 185, 1124-1130 (1974). Available at <http://psiexp.ss.uci.edu/research/teaching/Tversky_Kahneman_1974.pdf>.
- 17 Dhamija, R., Ozment, A., Schecter, S. "The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies" (2008). <http://www.usablesecurity.org/emperor/>
- 18 Mitnick, Kevin D., Simon, William L. "The Art of Deception." Indianapolis: Wiley Publishing, Inc., 2002.
- 19 Gilbert, D. T., & Malone, P. S. "The correspondence bias," *Psychological Bulletin*, 117, 21-38 (1995). [http://www.wjh.harvard.edu/~dtg/Gilbert%20&%20Malone%20\(CORRESPONDENCE%20BIAS\).pdf](http://www.wjh.harvard.edu/~dtg/Gilbert%20&%20Malone%20(CORRESPONDENCE%20BIAS).pdf)
- 20 Taylor, S.E. and Fiske, S.T. "Point of view and perception so causality," *Journal of Personality and Social Psychology*, 32, 439-445 (1975).
- 21 Computer Security Institute, CSI Computer Crime and Security Survey (2007). http://www.gocsi.com/forms/csi_survey.jhtml (registration required)