

The Origins of Social Engineering

By Hiep Dang



One would be hard pressed today to read a news article or book about computer security without coming across the term *social engineering* more than once.

Popularized by Kevin Mitnick (arguably the most infamous social engineer in the modern computing era), social engineering is in essence the art of persuasion—convincing individuals to disclose confidential data or perform some action. Although social engineering is a contemporary term, the techniques and philosophies behind it have been around as long as humanity itself. We find stories of deception and manipulation in the pages of history, folklore, mythology, religion, and literature.

Prometheus: The God of Social Engineering?

According to Greek mythology, humanity's proficiency in social engineering today is probably a direct result of its greatest mentor: Prometheus, who was so skilled in this craft that he could trick Zeus, the king of gods. In *Theogony* and *Works and Days*, the epic poet Hesiod tells the story of Prometheus, a Titan known for his wily ways and cunning tricks. He is credited for the creation of man by molding him out of clay. In what became known as the "Trick at Mecone," Prometheus offered Zeus two choices to settle a dispute between the gods and mortals. One offering was ox meat stuffed inside an ox's stomach, the other was an ox bone covered with shining fat. One was nourishment wrapped in a vile covering while the other was an inedible choice, though visually tantalizing. Zeus chose the latter and, as a result, humankind would henceforth need to make sacrifices only of bones and fat to the gods, while keeping the flesh for themselves. Angered at being tricked by Prometheus, Zeus

punished mortals by withholding fire. However, in yet another act of social engineering against Zeus, Prometheus stole "the far-seen gleam of unwearying fire in a hollow fennel stalk" from Mount Olympus and bequeathed it to man. As punishment for his acts, Prometheus was chained to a rock, where every day an eagle would come and eat his liver, which would grow back again at night. As a punishment for man, Zeus created the first woman, Pandora, who brought with her a jar that she opened out of curiosity, releasing countless plagues.

Jacob and Rebekah's Phishing Attack

From the Old Testament comes the story of Jacob and his mother, Rebekah, who used a social engineering technique that is the foundation of today's phishing attacks—making the victim believe that the phisher is someone else. Jacob's father and Rebekah's husband, Isaac, had gone blind in the last years of his life. As he prepared for death, he instructed his oldest son, Esau, to "hunt game for me, and prepare for me savory food, such as I love, and bring it to me that I may eat; that I may bless you before I die." (Genesis 27:2–4.) Wanting Jacob instead of Esau to receive Isaac's blessings, Rebekah devised a plan. Jacob was reluctant at first, saying "Behold, my brother Esau is a hairy man, and I am a smooth man. Perhaps my father will feel me, and I shall seem to be mocking him, and bring a curse upon myself and not a blessing." (Genesis 27:11–12.) In order to fool Isaac into believing he was with Esau, Rebekah prepared Isaac's meal, dressed Jacob in Esau's best garments, and attached a goat skin to the smooth parts of Jacob's hands and neck. Jacob delivered the meal to Isaac, passed the authentication test, and successfully gained the blessings that had been intended for Esau.

Samson and Delilah: Espionage for Hire

Samson was a biblical figure with tremendous strength who battled the Philistines. The secret of his power was his long hair. While in Gaza, Samson fell in love with Delilah. The Philistines were able to convince her to uncover the secret of Samson's strength by offering her 1,100 pieces of silver. "Coax him, and find out what makes his strength so great, and how we may overpower him, so that we may bind him in order to subdue him; and we will each give you eleven hundred pieces of silver." (Judges 16:5.) Samson resisted disclosing his secret before succumbing to her persuasiveness. "How can you say, 'I love you,' when your heart is not with me?" she said. "You have mocked me three times now and have not told me what makes your strength so great." Finally, after she had nagged and pestered him day after day, he gave in. So he said to her, "A razor has never come upon my head; for I have been a Nazirite to God from my mother's womb. If my head were shaved, then my strength would leave me; I would become weak, and be like anyone else." (Judges 16:15–17.) Soon after Samson fell asleep, Delilah exploited his vulnerability by shaving off his hair. In his weakened state, the Philistines seized Samson, gouged out his eyes, bound him in shackles, and imprisoned him for life.

The First Trojan Horse

The story of the Trojan horse, made famous by the Greek epic poet Homer in *The Odyssey* and the Roman epic poet Virgil in *The Aeneid*, was one of the most ingenious social engineering tricks in the history of humankind. During the Trojan War, the Greeks could not break down the walls surrounding the city of Troy. The crafty Greek warrior Odysseus devised a ruse to fool the Trojans into believing the Greeks had given up their assault on the city. The Greeks sailed their fleet of ships away and left only a large wooden horse on the beach with a lone Greek soldier named Sinon. After being captured by the Trojans, Sinon told them that the Greeks had left the large wooden horse as an offering to the Gods to ensure their safety as they traveled home and that they made it large enough so that the Trojans could not move it into the city—as this would bring the Greeks ill luck. The story was so tantalizing to the Trojans that they moved the wooden horse within the city walls—despite the warnings of Cassandra, who was cursed with the ability to foresee the future without anyone ever believing her, and of Laocoön, a Trojan priest, who said in *The Aeneid*:

O wretched countrymen! What fury reigns?
What more than madness has possess'd your brains?
Think you the Grecians from your coasts are gone?
And are Ulysses' arts no better known?
This hollow fabric either must inclose,
Within its blind recess, our secret foes;
Or 't is an engine rais'd above the town,
T' o'erlook the walls, and then to batter down.
Somewhat is sure design'd, by fraud or force:
Trust not their presents, nor admit the horse.

The Trojans' poor judgment became their downfall. That night, led by Odysseus, the Greek soldiers hidden within the horse killed the guards and opened the gates to the rest of the army. Thanks to the ingenious social engineering tactic devised by Odysseus, the Greeks defeated the Trojans to win the war.

Today's Trojan Horse

When Odysseus devised his scheme to infiltrate Troy, little did he know that he would set a precedent for millennia to come. The most prevalent type of malware found in the wild today, the silicon "Trojan horse" was coined by Daniel Edwards of the U.S. Government's National Security Agency in the 1970s. Edwards named it after the social engineering technique used by the Greeks. Before the days of the Internet, personal computer users who wanted to share software files did so through physical media (such as floppy disks or tape drives) or by connecting to bulletin board systems (BBS's). Hackers with malicious intent soon realized that they could entice users into executing malicious code simply by disguising it as a game or utility. Due to the simplicity and amazing effectiveness of Trojans, malware authors still use this social engineering technique decades later. Today, PC users are tricked into infecting themselves with Trojans at an alarming rate. They are drawn by the allure of free music, videos, software, and endearing ecards from anonymous "loved ones."



Malware and PUP growth

Unique families from years 1997 to 2007 *in thousands*

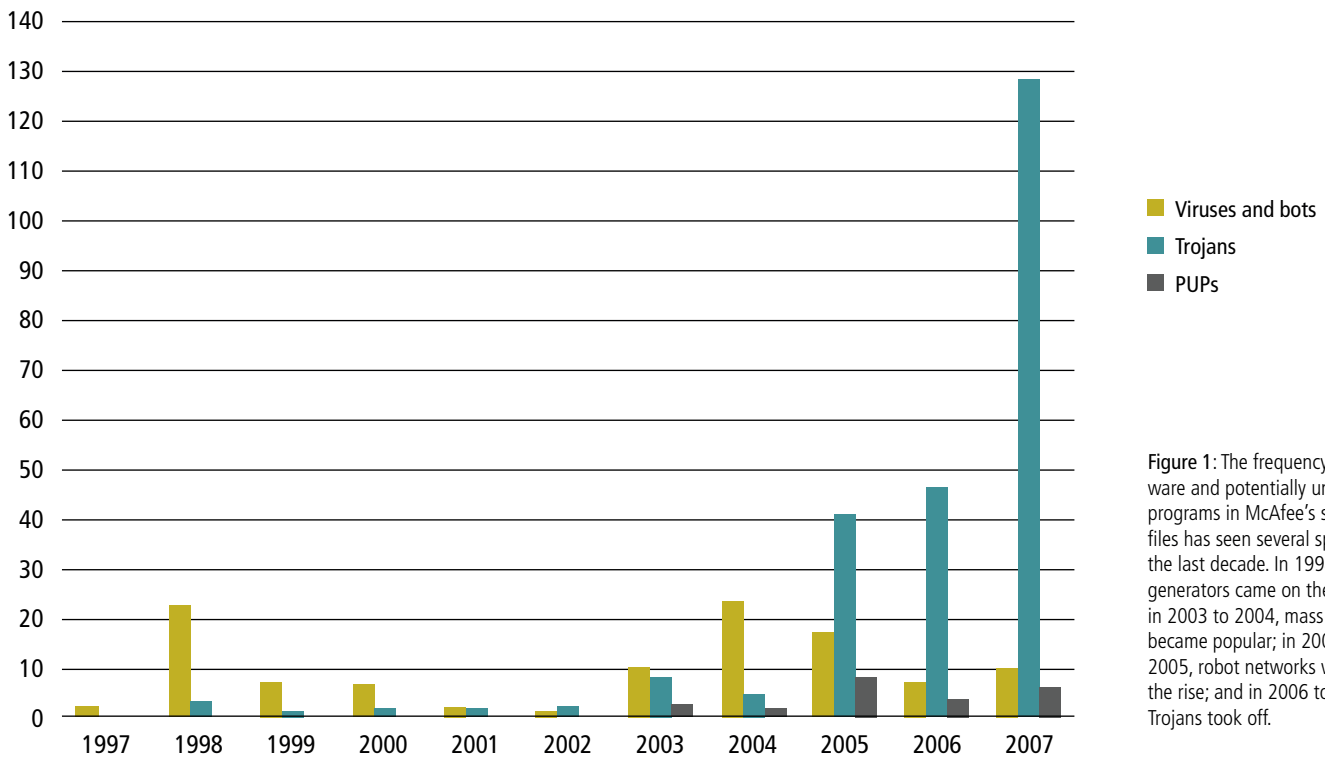


Figure 1: The frequency of malware and potentially unwanted programs in McAfee's signature files has seen several spikes in the last decade. In 1998, virus generators came on the scene; in 2003 to 2004, mass mailers became popular; in 2004 to 2005, robot networks were on the rise; and in 2006 to 2007 Trojans took off.

An Updated Con

Advanced Fee Fraud, better known as the Nigerian Email Scam (419 Fraud), has been around for decades and is still one of the most prolific types of spam. The numeral "419" refers to the section of the Nigerian Criminal Code that outlaws this scam. This "get rich quick" social engineering tactic arrived in the form of a letter and was first delivered to postal mailboxes in the 1970s. The con evolved into unsolicited faxes through the 1980s, and it is almost exclusively sent via email today. Its origins date back to the sixteenth century, when it was known as the Spanish Prisoner Con. The scheme is straightforward: A naïve victim is told about

an extremely wealthy Spanish prisoner who needs someone's help in getting free. This so-called prisoner relied on the con artist to raise enough money to free him. The con artist approached the victim with the story and "allowed" him or her to help with a portion of the fundraising—with the promise of great financial gain. We see numerous variations of the letter today, but the concept remains the same. The Nigerian Email Scam lures its victims with the tantalizing promise of a multimillion-dollar payout with an "investment" of only a few thousand. Even though most recipients realize the offer is too good to be true, an estimated 1 percent of recipients still reply. According to the U.S. Secret Service, the scammers successfully social engineer their victims out of an average of \$100 million per year.



Phishing reports

In thousands

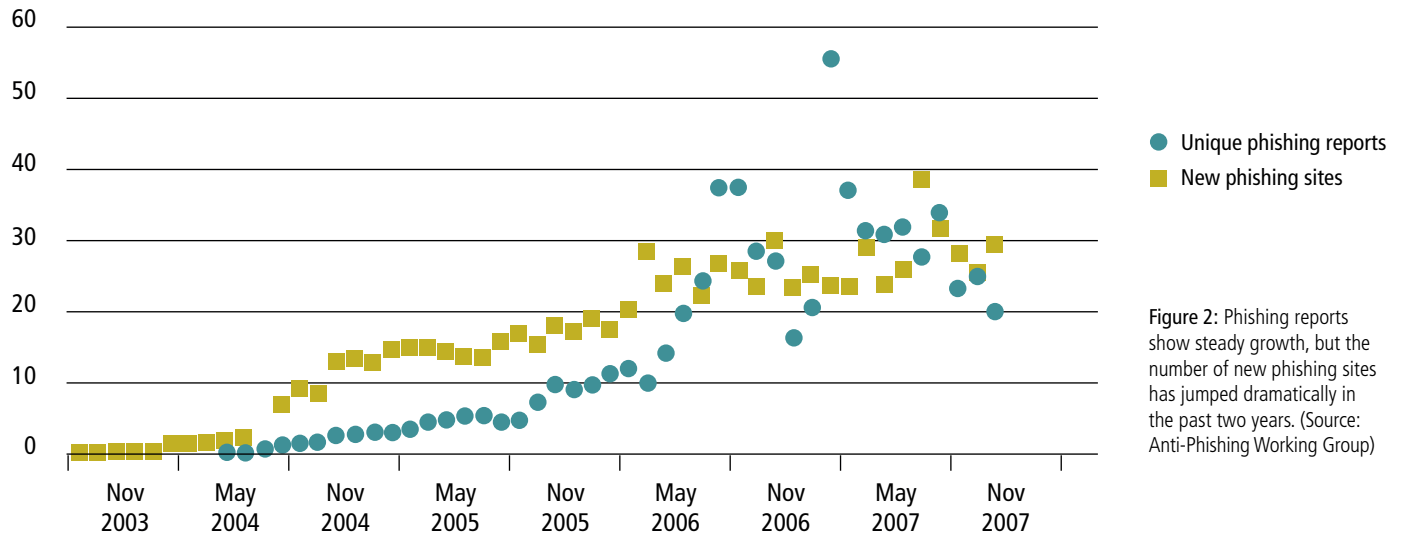


Figure 2: Phishing reports show steady growth, but the number of new phishing sites has jumped dramatically in the past two years. (Source: Anti-Phishing Working Group)

Phishing

The term phishing was coined by hackers. It derives from fishing because this social engineering technique lures its victims (phish) into disclosing their user names, passwords, credit card numbers, and other personal information. In the 1990s, many hackers exploited America Online's (AOL) free trial offers of Internet service by using fake, autogenerated credit card numbers that didn't actually correspond to existing accounts. After AOL improved its security and credit card validation tests to ensure that credit card numbers were indeed legitimate, the bad guys started going after real user names and passwords to get onto AOL's networks.

They started sending fake emails and instant messages that appeared to come from AOL support. Many unsuspecting victims gave away their information and were subsequently billed for the activities and purchases that the hackers made on their compromised accounts. Malicious hackers soon realized the potential profit margin and success rate of such an attack and started targeting companies (banks, eBay, Amazon, and others) that conducted transactions and commerce online.

History of computer security

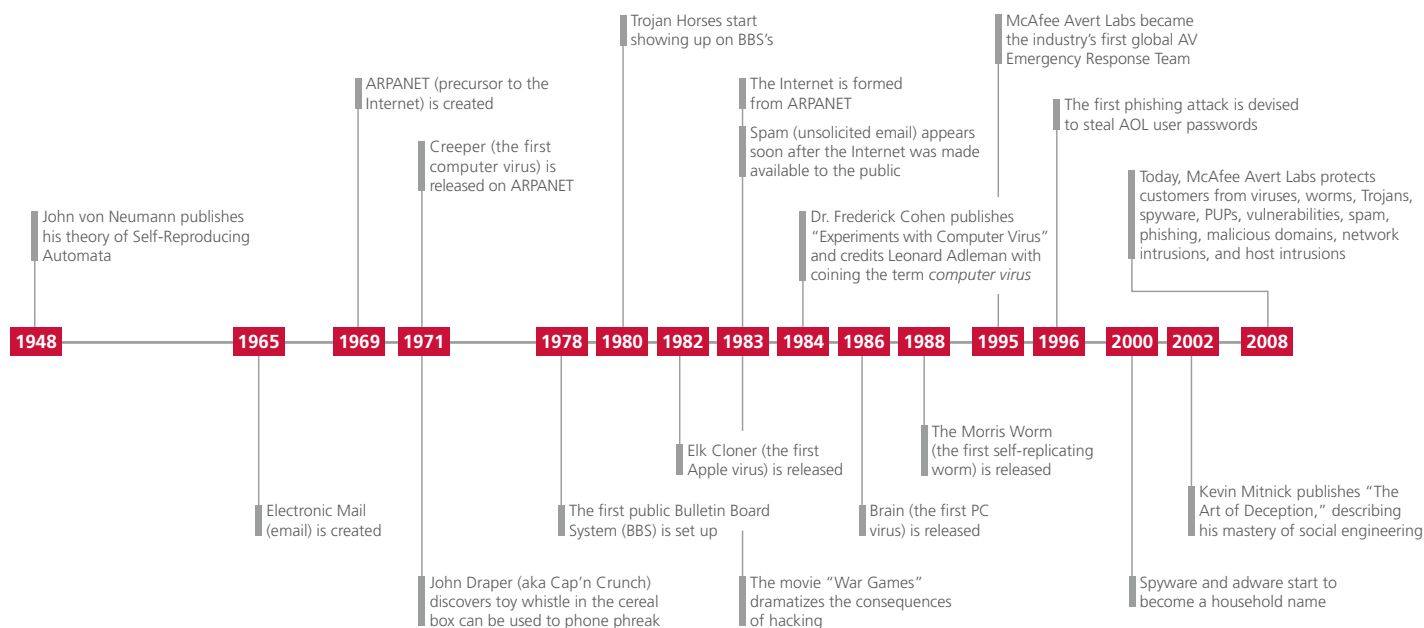


Figure 3: Timeline of significant social engineering events.

History Repeats Itself

Whether it's called social engineering, trickery, confidence tricks, cognitive biases, or scams, the concept of exploiting a person's naivety and trust is as prevalent today as it has been since the dawn of time. Ask security experts, and they will agree that people are the weakest link in the security chain. We can develop the most secure software to protect our computers, implement the most restrictive security policies, and strive for utopian user education. However, as long as we continue to be driven by curiosity and greed without concern for the consequences, we could face our own version of a Trojan tragedy.

Progress, far from consisting in change, depends on retentiveness. When change is absolute, there remains no being to improve and no direction is set for possible improvement: and when experience is not retained, as among savages, infancy is perpetual. Those who cannot remember the past are condemned to repeat it.—George Santayana, in "Reason in Common Sense," from The Life of Reason.

WORKS CITED

- Anderson, J. P. (1972). *Computer Security Technology Planning Study vol. II*. U.S. Air Force.
- Farquhar, M. (2005). *A Treasury of Deception*. New York: The Penguin Group.
- Hesiod (1914). *Theogony*. (Translated by H. G. Evelyn-White)
- Hesiod (1914). *Works and Days*. (Translated by H. G. Evelyn-White)



Hiep Dang is the Director of Anti-malware Research for McAfee Avert Labs. He is responsible for the coordination of McAfee's global team of malware researchers dedicated to the research, analysis, and response to malware outbreaks, including viruses, worms, Trojans, bots, and spyware. Dang is a regular contributor to Avert Labs blogs and white papers and writes for the *McAfee Security Journal*. He has been interviewed by the *Wall Street Journal*, MSNBC, *PC Magazine*, and many other publications and media outlets about new threats and malware trends. Dang is also a devoted practitioner of Wah Lum Tam Tui Northern Praying Mantis Kung Fu and Tai Chi. He is currently on a hiatus from his lifetime of training to concentrate on the computer security industry.

- Homer. *The Iliad*. (Translated by S. Butler)
- Mitnick, K. (2002). *The Art of Deception*. Indianapolis, Indiana: Wiley Publishing.
- Myers, M. J. (2007). *Phishing and Countermeasures*. John Wiley & Sons, Inc.
- Santayana, G. (1905). *The Life of Reason*.
- Virgil (19 B.C.E.). *The Aeneid*. (Translated by J. Dryden)