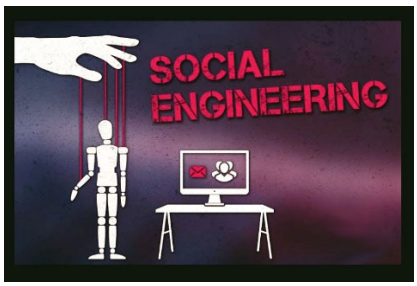
520.743.7554
info@computerdimensions.net
www.computerdimensions.net

5 Ways Human Beings Fall Victim To Social Engineers



These common human traits are the basic ingredients in the con-man's recipe for trickery.

1. Humans Are Trusting

"Social Engineers use specific strategies for establishing trust and familiarity, often referred to as 'pretexting,'" says Margaret Cunningham, principal research scientist for human behavior with Forcepoint X-Labs. "Once they've established rapport and a positive first impression with their target, it is much easier to successfully request information or access to sensitive personal or organizational assets."

Once trust is established, Social Engineers manage to pull information out of their target they might not otherwise disclose. Why does exploiting trust work on us?

Chris Hadnagy, founder and CEO of Social-Engineer, references a book called The Moral Molecule by Dr. Paul Zak, which examines how trust impacts a "feel good" chemical called oxytocin in the brain.

"Dr. Zak found that when you make someone you feel trusted it releases this chemical and the brain attaches that feeling to the object that helped release it. It is not controllable unless trust is broken."

Example:
Victor Lustwig is one of the world's most notorious conmen. He "sold" the Eiffel tower a number of times, said Hadnagy. "He shared a 'top secret' message with some very wealthy people," said Hadnagy. The ruse worked by claiming the monument was being scrapped and the metal would be worth millions. Lustig "made them feel a rapport and trust with him and they parted with their money," says Hadnagy.

2. Humans Want to Be Helpful

"We all have a desire to be helpful and viewed as friendly," says Hadnagy. "It is built into us. Mix that with the world we live in now; people are isolated, alone, depressed. Now even a little kindness can go a long way to making a human connection."

Cunningham says Social Engineers make the target feel as if they are doing something altruistic.

"Sympathy can be a powerful behavioral motivator for highly agreeable people, and bad actors know that their storylines can be powerful tools for garnering sympathy." They often deploy emotional tactics to build intense sympathetic responses in their targets, including tactics like playing recordings of babies crying.

Example:
"We are seeing a lot of this on LinkedIn impersonation attacks," says Hadnagy. "The type of attack where someone is asking for help with a report, as a reporter or as a student. We also see people asking for help with getting a job. Often these are attackers using this to gather intel on target companies so they know how to further attacks."

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

3. Humans Fear Authority
"Fear is one of the largest motivators in Social Engineering," says Hadnagy. "Fear is handled and processed by the amygdala, as are all emotions before the rest of the brain takes over. When the amygdala is hijacked there is no other processing in the brain - which means decisions will be made with emotion and not logic. Many a bad decision in human history has been made in this state."

Example:
"Recent phishing tactics have capitalized on COVID-19," says Cunningham. "These attacks use official-sounding subject lines, reference the government, and vaccine manufacturer names. Knowing that people are worried and emotional about COVID-19, and in many cases very willing or agreeable to signing up for a vaccination appointment, these authoritative phishing emails can be highly effective."

4. Humans are Optimistic
Cunningham says research shows that optimistic bias can make people believe that they are less vulnerable than others to online risks associated with privacy. Social Engineers understand and capitalize on the fact that people are typically not in a defensive mindset; they aren't expecting to be taken advantage of or manipulated.

Example:
One particular example of this came not at the hands of a criminal, but an employer in 2020. The employer at the center of it, a web company, told their employees there would be no bonuses in 2020 since money was tight due to COVID.

"Then near the end of the year they phished their entire organization with a $600 bonus offer," he says. "To dangle the carrot of hope in front of parents struggling during the holidays is an abuse of the basic optimistic emotions that drive us all forward." The company later apologized.

5. Humans are Honest
Hadnagy says humans will naturally correct false statements and this is often how bad actors exploit honesty.

"If we are driven enough, we will verbally correct a complete stranger, that is how powerful it is," he says. "This principle I mentioned is used by expert human hackers to exploit information from targets."

Example:
Hadnagy says he employs this strategy himself in pen tests and engagements. "I get birth dates and Social Security numbers from strangers by using this. Simply stating something like:

'I see you are so organized. You must be born in September, right?'
'Um, no, I was born on October.'
'Oh, wait not the 31st on Halloween?'
'No, the 13th.'
'Ok, cool.'

"Now in a matter of a few seconds I obtained their DOB. People want to be honest and they want to also have truthful information out there."

Social Engineering and scam emails are rampant and take only a few clicks to work. Your best defense is to simply pay attention to the details in front of you and always error on the side of caution. Remember to slow down and think before you act.