Please (Don't) Lie to Me!

Who doesn't love a good magic show? Magic performances give us the opportunity to let down our guard, suspend our disbelief, and be deceived for entertainment's sake. When a magician successfully pulls off a trick, we do not criticize ourselves for being *dumb* or *unobservant* – our egos smooth things over and convince us that the magician was "*simply amazing*!"
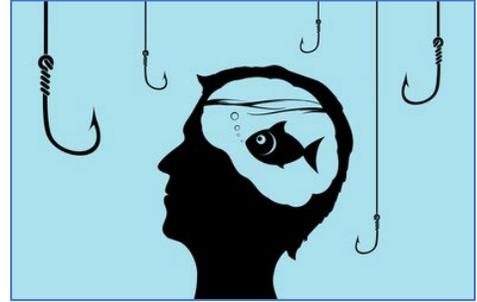
Outside of magic shows, we may believe that we are shrewd detectors of others' fraudulent intentions. Individuals with training in critical thinking, or those whose job it is to analyze misinformation may feel immune to deception. However, humans are surprisingly susceptible to deception due to limitations of our sensory organs and gaps in the way we process information.

It can be uncomfortable to admit that we often prefer lies over the truth. For example, "white lies" are useful social lubricants that get us out of sticky situations. We say, *"You look amazing in that (awful) dress!"* because we are sure that the social consequences of telling the truth would be worse than getting caught in a lie. We say, *"Give me honest feedback"* when we really mean "*Be gentle*"; we laugh at jokes that we don't understand because we fear social isolation or exclusion – a fake laugh is a survival tactic.

In the course of their duties, intelligence and cyber professionals expose misinformation to render it inert or to nullify its intended operational effects. However, these individuals' training could lead them to erroneously conclude that they are immune to deception in their personal lives. Do we conduct our private lives as though we're attending a magic show – allowing and even inviting deception into our personal lives? Online we may unwittingly (or knowingly) propagate falsehood in ways we would never dream of in our professional lives.

Social engineers with malign intentions use psychologically sophisticated methods to evoke emotions (e.g. greed, fear, urgency, curiosity) designed to ensnare us and elicit information and behaviors that can be weaponized. We may tell ourselves that we would never fall for a "stupid" urban legend or forward a chain letter or hoax/scare email, but maintaining this belief may make us more vulnerable to attacks, especially those that appeal to our need to think of ourselves as intelligent beings. Unfortunately, once ensnared, the fear of future embarrassment is often enough to coerce our compliance with further solicitations.

It is safer to acknowledge that no one is completely immune to deception, and to approach our communications with healthy doses of humility, skepticism, and restraint. The next time you feel attempts to influence your thinking or behavior, ask:

- Why would someone like *me* receive this kind of communication?
- Is the communication sender appealing to my emotions and leading up to an offer/opportunity?
- Are there gaps in the sender's story that apparently only I can help fill?
- Am I being pressured to act quickly, either to capitalize or to avoid negative consequences?
- Is what's being asked of me reasonable, plausible, or legal? Why is it being asked of *me*?
- What pitfalls could occur if I comply with the communication sender's request?
- Is the communication sender offering favors, engaging in so-called "love-bombing", appealing to authority, or making suggestions that imply time constraints, or scarcity? If so, why?

Like magicians, malicious social engineers disguise their intentions, use misdirection, and exploit our perceptual limitations in their efforts to deceive. In the same way we protect our networks, we can make ourselves harder targets by acknowledging our fallibility and refreshing our OPSEC/COMSEC practices.

Questions/Comments? Contact us at 363ISRW.ART.363ISRW@us.af.mil