

Understanding Human Vulnerabilities

Trust Me

by Ian Mann

A social engineer's primary goal is to develop the trust to enable them to carry out their attack. Therefore, it is essential that we thoroughly understand the processes that make up the development of trust.

For an organization to function effectively, it needs to store information between people in a variety of situations. However, in understanding and protecting ourselves from social engineering attacks, it is important that we understand where the limits of trust should lie. We shall also be showing just how flaky the foundations of trust can be and how easily it can be established with the target of a social engineering attack.

Trust is important to us, yet can also be very risky in certain situations.

The following example shows just how trusting people can be, even when the consequences are dangerous. It is an interesting example of how well-educated professionals can be made to undertake specific actions, against all their training and better judgement, if they accept the authority of the person who is telling them to do so.

Incident: Nurses Killing Patients

One well-known experiment was that conducted by Stanley Milgram in the 1960s and presented in *Obedience to Authority*, 1974. Milgram led the participants to believe that they were a part of a memory experiment; testing recall and that they, as the teacher, should punish the learner with electric shocks. The intensity of the shocks were increased as the learner (unseen, yet heard) got an increasing number of questions wrong. As the experiment proceeded the teacher continued to administer shocks, even when the apparent feedback (and latterly lack of feedback) indicated the learner was possibly dead.

It showed how the majority of a given population can be quickly manipulated into performing deadly actions on fellow human beings. It has been well documented, so I will not analyse it in depth here. However, it is still interesting, especially to challenge any mistaken beliefs that groups of people who commit atrocities are somehow different to the rest of us.

There is another interesting experiment that is worthy of examination. During the 1960s a group of researchers in the US were investigating cases where skilled nurses had not questioned doctors' judgement, even when the doctors were clearly making mistakes. The researchers conducted the following experiment:

A number of on-duty nurses were contacted by phone, by a man identifying himself as a doctor. In 22 cases the man instructed the nurse to give a drug to a specific patient on the ward. There were a number of good reasons why the nurses should have questioned the instruction:

- the drug was not authorized, nor on the stock list;
- the dosage instructed was twice the safe dose which was clearly stated on the container;
- a policy existed that stated prescriptions could not be authorized over the phone;
- the instruction came from someone the nurses had never met or spoken to previously.

Worryingly, only one nurse out of 22 refused to follow the instruction. You will be pleased to know that, as this was an experiment, the nurses who attempted to give the drug were intercepted.

Vulnerability analysis

These examples clearly show how people respond to authority. However, there are some interesting features. The 'success' rate is very high considering a) the professional status of the targets and their related training in patient care; and b) the single call.

In our experience, to get a hit rate this high you usually need to establish a relationship of some trust through a series of contacts.

So why did the nurses behave in this way?

Firstly, the notion that a nurse's role involves acting as a check and balance to the doctor is a complete fallacy. Nurses are trained from day one to follow doctors' instructions. In addition, questioning the doctor is not viewed as a good career move.

Secondly, is it likely that the nurse had ever encountered or been warned against this type of scenario? Almost certainly not.

Possible countermeasures

1. You should always be wary of any situation where authority figures can and do bypass procedure. It creates obvious vulnerabilities for the attacker to exploit.
2. Elements of peer review and segregation of duties can help here. If one nurse had to issue the drug, and another administer it, then you have two opportunities to question the instruction. Also, two people are more likely to challenge a request as they do not feel as isolated in the face of an authority figure.

However, given the mindset of the nurses demonstrated in this example, I believe that even this double check would not have guaranteed a refusal to comply. After all, both nurses would presumably have the same conditioned response to a doctor's request. Numerous previous instances of having to respond in an emergency, under pressure, will have effectively trained the nurses to follow instruction.

Trusting the Attacker

SENIOR MANAGERS WORKING AGAINST SECURITY

The above example illustrates the difficulty in developing an effective security culture where individuals are required to challenge authority figures. This is an important element to consider when building your social engineering protection. There are numerous cases of senior staff routinely bypassing security rules and procedures and expecting others to also do the same on their instruction.

You need strong backing from the people at the top of organizations to support security. This requires consistent activities to help senior managers understand the threats and potential impacts of information security breaches.

This task is getting easier as cases generate more publicity. A current example is the security breach involving the loss of millions of records of personal data by the Inland Revenue and Customs (the UK tax authority) which led to the head of that department resigning.

Events like this do help get the attention of senior managers. In general, the media attention is helpful in strengthening the case for increasing the effectiveness of information security countermeasures. However, in this case I wonder whether the immediate resignation of the head of the department was appropriate. In many cases there are two possibilities for the person at the top:

1. The incident was a genuine mistake, or intentional breach of policy/procedure. In these instances disciplinary measures, or extra training, is required at the level of the actual incident within the organization. It is not appropriate for the person at the top to resign.
2. The incident is associated with known weaknesses in information security that have previously been communicated to management, with no action taken. Or management had been made aware of the widespread weaknesses in information security and taken no action. In these instances it is appropriate for senior people to take responsibility.

In this particular incident, involving a government department, it is likely that someone had to do the 'honourable' thing. Pressure from the media will have played a big part in the response.

So senior managers have much responsibility, not only in leading the development of an information security programme, but also in demonstrating their commitment on a day-to-day basis by complying with policy and procedure.

THE POWER OF TRUST

The example of the nurses' compliance was partly due to the authority position of the doctor and also the natural tendency of the nurses to trust the identity of the person calling. This tendency to trust what people tell us is exploited time and time again by social engineers.

There are occasions when you cannot rely automatically on trust. Trust needs to be built up over time and there are gradations in the trust required depending upon the situation and risks. I suggest that you require one level of trust to lend someone £5 and rather more trust to let someone inject you with a drug (especially having read the example above).

Therefore, a social engineer needs to acquire the skills needed to develop trust with their target in proportion to the task they are going to request from that target. One attack could be easily accomplished in a single telephone call whilst another may take many weeks of developing trust, both off-site and on-site, to totally convince the target of the attacker's identity before the attack is effective.

Tricks to Building Rapport

If we want to develop trust with someone in order to deceive them into giving us information or performing an action, then developing rapid rapport can be key to our success.

Many observers have pointed to the fact that people in a high state of rapport will mirror each other's body language. You can see this when observing people in public, where couples who are attracted to each other will tend to be mirroring (that is, copying) each other's posture and movements. It is at times as if they are deliberately doing this and concentrating on it, however it is usually a completely subconscious activity.

This has been translated by some into the simple instruction to mirror someone's body language if you want to develop instant rapport. This can easily be detected. In logical terms the mistake is to observe that rapport leads to mirroring and therefore conclude that mirroring leads to rapport. This is not necessarily the case.

Rapport is actually developed following a complex mix of attributes which can convince us into feeling confidence and trust in someone, including:

- Dress – we tend to dress to project a certain image and to try and reflect something of our perceived personality. Therefore, someone dressing in a similar style to us is likely to be similar to us, and therefore more likeable.

- Looks – this is more than just being ‘good looking’, although that helps. When judging you for the first time, someone will tend to allow you to inherit the characteristics of the person/people that you remind them of. Our natural prejudice is a genetically inherited process, important to judge whether people we meet are a threat.
- Voice – especially the tone, and speed of speech. This is often an indication of the current state of mind, and a reflection of the communication mode the person is in at the time. This will be explored later when we look at Neuro-Linguistic Programming (NLP).
- What we actually say. After all, would you develop instant rapport with someone stating views that were the complete opposite to yours, even if they were sat in front of you mirroring your body language?

When teaching rapport building during one of my social engineering masterclasses, I often point people to a number of different techniques to develop rapport with ease.

Without these other factors, simple body language mirroring does not come across as genuine. It is in these situations that someone is more likely to detect that they are being manipulated in some way.

MIRRORING BREATHING

This technique can be powerful. Since a person’s state of mind is reflected in their breathing rate, you can quite quickly begin to match them by mirroring this attribute. It is also difficult to detect, partly because the technique is not as well known as simple mirroring. Nevertheless, be careful not to stare intently at the person’s chest as this can cause offence. Subtle movements of the shoulders are usually sufficient to pick up on the rate.

This approach to developing rapport has some added benefits. Firstly it helps you forget the body language mirroring, although you may naturally do this as you mirror their breathing. (‘Natural’ mirroring is generally a good thing, as it is unlikely to be misinterpreted as forced and artificial.) Secondly, it means you are likely to talk less, and follow the second point:

TRUE LISTENING

True listening is the sort of listening that people rarely do; an intense concentration on the content of what the person is saying. This will tend to have a powerful effect, particularly since it is quite a rare experience for most people. In conversation, most people are spending their time formulating what they want to say next; whilst not actually listening. The other person quickly picks up on this. The reason we don't object is that we are so used to this in many conversations. When the opposite happens, it can have a powerful effect upon us.

One great aid to listening intently is to try and repeat back portions of what the person is saying. Salespeople use this technique to encourage you to say 'yes'.

Say, for example, someone says to you, 'If we are really to establish a comprehensive information security management system, then we must give the appropriate attention to our human vulnerabilities'.

You can say, 'So if we are to really establish a comprehensive information security management system, then we must give the appropriate attention to our human vulnerabilities'.

They will then look at you as if you are rather strange. If you keep on just repeating back to them their words, they will either get bored with the conversation (or lack of), or think you are going slightly mad.

Remember, we are trying to show that we really are listening, and understanding, what they are saying to us. So let's rerun the example, and use a little more intelligence in our response.

The reply to, 'If we are to really establish to comprehensive information security management system, then we must give the appropriate attention to our human vulnerabilities,' could well be, 'I see, so we mustn't put all our efforts into just technical countermeasures?' 'Exactly!' could be their reply.

The 'I see' is expressing understanding. By saying that, you have not only listened, but also translated the idea into an internal picture. This is extremely powerful if the other person is primarily visual in their internal processing. More of this in the next chapter when we explore reading people in more depth.

The rest of your reply shows you have listened and understood. Rather than simple mimicking, you have restated their idea, paraphrasing what they have said, using different words.

THE MAGIC PAUSE

Try combining this technique with counting to three whenever they stop talking before you start to speak. If they don't start again, then it really is your turn to speak. This is especially important if you are about to put new ideas (yours) into the conversation, because you may well have been constructing what you are about to say at the expense of listening. This will be quite evident if you interrupt them before they have finished. This is really like saying, 'Shut up now, what I have to say is more important than what you are saying.' Not a good way of developing rapport.

In social engineering terms simple listening can be a very powerful tool for the attacker. As many people have not experienced someone taking this level of interest in what they say the effect can be profound. They can feel as though they have just met a true friend, in a very short space of time. In addition, an attack strategy based on making friends is difficult to counter. 'Be suspicious of anyone who appears nice to you' is not a realistic training approach.

MIND SCRIPT

An alternative to forced mirroring is to use a mind script – a simple technique that you can use to direct your thinking with some powerful results. You may remember it was used earlier to gain access to a bank's drinks reception. In this application we want the other person to feel that we like them. So a simple answer is to really believe you do like them – your body language and other subconscious signals will naturally follow. However skilled and knowledgeable we are in human communication, it is very difficult to consciously construct each aspect of our behaviour. This is especially the case if you want to maintain the performance for more than a few minutes. Your conscious brain just cannot keep control over all the aspects of our communication (verbal and non-verbal) for any length of time before the subconscious naturally takes over.

As we shall explore in Chapter 7, although the subconscious is very powerful, it is relatively easy to manipulate. If you tell yourself something in the right way, your subconscious will believe it and begin to act in new ways commensurate with the new belief. You then don't have to consciously control your every movement.

I once attended an extremely effective 'train the trainer' course, during which the trainer managed to captivate, entertain and inform approximately 200 people for the day without any visual aids. The trainer effectively supplemented the materials with great examples. He gave us a great tip for establishing the right 'atmosphere' at the start of the training.

As we all assembled in the room, he stood at the front, watching us taking our places, and making small comments and greetings, avoiding any lengthy conversations. He later told us he was making an effort to find something to like about every single person, even if it was only their choice of shoes. Notice he didn't concentrate on the shoes being nice, rather on thinking that the person was good for making such a wise choice. He was in fact running his own mind script to like the people he was going to train. He was setting himself up for a good day whilst his subconscious would be giving out all the right non-verbal signals to the audience that he really liked them.

On talking with him later I discovered that he was a trained courtroom lawyer who had been part of the support team for one of the top US defence lawyers. I wonder whether this technique was taught to him with respect to establishing rapport with jury members. If it wasn't, then it should be.

I AGREE

Simply agreeing with what the other person is saying helps to develop rapport. Obviously this can have its challenges if the other person is saying something very silly or in complete contrast to your deeply-felt beliefs. However, you can develop your skills in finding areas of common interest that you can agree on. In terms of conducting a social engineering attack, personal opinions can be instantly suspended. An attacker may wish to use a mind script to help develop the same beliefs and interests as the target.

It is fascinating how quickly people develop rapport when they discover that they come from the same town or region. The size of the area of significance appears to be proportional to the distance they are from home. If you are in the next county, then your home town is significant. If you are on the other side of the world then home is a bigger area.

This tendency links back to our genetic need to belong to tribal groups. We tend to pick groups on a short-term basis. For example, where I grew up in the heart of Yorkshire, England, there was significant local inter-village rivalry, sometimes friendly, and sometimes not (particularly with young men after an evening of alcohol). However, these rivalries were quickly forgotten in, for

example, a Yorkshire versus Lancashire cricket match. This northern rivalry was also put to one side when a North versus South event occurred. This in turn would be replaced by national allegiances if we were against another country, whether in something as simple as a sporting event or more serious such as military conflict.

Looking for areas of common interest and associations is a good tactic to build rapport. Skilled social engineers will build up profiles of individuals, where hobbies and outside interests can be a powerful knowledge base. Sales people (often skilled in social engineering techniques) will use this information in order to develop effective relationships with their customers.

DRESS

When conducting face-to-face attacks, making your appearance similar to that of your target, or to fit with your adopted attack role is an important part of an attacker's armoury of techniques. Dress may be a simple, yet effective, change of appearance as it is relatively easy and generally inexpensive.

The dress strategy can be as simple as enabling an attacker to blend naturally into a given environment. A design agency or e-commerce company is unlikely to share the same dress code as a bank or law firm. A little target reconnaissance can go a long way in deciding what may be an appropriate dress for a given attack.

HAIR

Changing hair, either through restyling or with a wig, is another technique for the social engineer. Using this tactic allows an attacker to disguise their appearance during reconnaissance activities; particularly when surveying sites for future physical security breaches.

PUTTING IT ALL TOGETHER

By combining techniques, especially if the attacker can really believe that they are like the other person, an attack will be convincing. By not explicitly using conscious body language, yet adopting other techniques that develop deeper rapport, the attacker will find that any body language will automatically fall into place in a very realistic way.

Taken from *Hacking the Human* by Ian Mann