It's now or never! – and it never is as expected

When it's time to talk about social engineering it's difficult for me to decide from where to start, because it is everywhere around us. The definition of social engineering is "the psychological manipulation of people into performing actions that they wouldn't normally do". And this happens over and over again, every day.

Words: Simona Venuti, GARR

Consortium GARR

Every mum tries to convince her children that broccoli is much tastier than Nutella, by hiding the green suspect stuff under layers of more appetising food. And they (almost) always win! That young lady at the supermarket said that I could have a huge 5% discount if I bought 20 kilos of pasta, "Hurry, it's now or never!!" – Then I bought it, and now I need a bigger cupboard!

And what about the boy in line at the ticket machine, who is missing his train and needs to jump the queue? It would be very mean of me to let him be late home. And then he buys a ticket for the following day…

My granny used to skip the line at the doctor's by saying she had to cook for me, but I used to live with my parents in an entirely different location… And so I've been an unintentional accomplice in her little mischiefs!

Historical scams

If these are only a few examples of harmless social engineering, now let's have a look at some historical big, risky scams.

Probably the oldest evidence of social engineering attack is in the Bible, Genesis 27, where Rebecca deceives her husband Isaac into blessing the second-born Jacob, making him his successor, instead of Esau, the eldest. Later, in 1211 AC, let's move to the Chinese Empire: it seems that the Mongol emperor Genghis Khan was able to pass the Great Wall of China by simply tricking the enemy soldiers: unable to directly attack the impregnable passage, he decided to lure the Jin soldiers out for an open field battle. After several small attacks, the Mongol soldiers threw down their weapons, left their horses and fled (pretending to be afraid). As expected, the Jin soldiers on guard left the passage to chase them. Suddenly numerous Mongol soldiers, who were hiding nearby, easily conquered the (now unmanned) passage.

But the most famous social engineering attack in history is in Virgilio's Aeneid, when Ulysses was able to take the city of Troy by tricking its inhabitants into allowing in the city walls a beautiful and incredibly large wooden horse. As everybody knows, the horse was packed with Greek soldiers. The trick of the trojan horse is so exemplary that we call "trojan horse" the kind of malware that persuades the victim to be harmless and bona fide, while it plans to destroy or steal data from a device.

Picture
The Procession of the Trojan Horse in Troy by Giovanni Domenico Tiepolo. © Copyright The National Gallery, London

Cyber security context

In the cyber security context things are not so different, and this kind of attack can be very dangerous or harmful to our organisation, and to ourselves too.

One of the latest big social engineering attacks was carried out against Twitter, in July, where 130 VIP personal profiles were hacked (Barack Obama, Bill Gates, Elon Musk, Jeff Bezos and many others). In all of these profiles the following post appeared: "All bitcoin sent to our address below will be sent back to you doubled!". Of course, none of the involved celebrities posted this message. It was a group of teenage hackers, who were able to manage all of the 130 accounts at one time: they contacted by phone selected Twitter IT staff who were using a custom application to manage Twitter accounts pretending to be the application helpdesk and induced them to give their own passwords. And, unbelievable but true, some of Twitter IT employees actually gave the hackers their passwords.

The damage was double: Twitter users lost $140.000 donating bitcoins to hackers, while the celebrities' accounts were breached, their contact list stolen, and probably their personal data was 'nicked' too.

There are so many examples of social engineering in cyber security that it is not possible to list them all: every day a new technique is used to steal data, money and to cause harm inside an

organisation, as ransomware does. But they all obey some rules, based on the emotional nature of human behaviour, and this knowledge can help us to recognise and mitigate them.

Principles of Social Engineering

Cyber criminals know that social engineering works best when focusing on human emotions and risk. Taking advantage of human emotion is much easier than hacking a network or looking for security vulnerabilities. These examples of social engineering emphasise how emotion is used to commit cyber-attacks:

- Authority: people will tend to obey authority figures, even if they are asked to do strange things. "I'm the President of XXX Bank (or Police Office Chief or President of the own working organisation) and ask you to do YYYY"
- Urgency/Panic/Fear of getting into trouble: "You have a virus (both digital and biological)! Before losing all your data (or dying) click HERE!"
- Scarcity: "there are only 2 places left… It's now or never!"
- Greed: "Give me 10 euros and I'll give you back 100" or "You won the lottery!" or "I have this big wooden horse as a gift for you"
- Sense of guilt: "I know what you downloaded on your PC. Send money and nobody will know it"
- And, on the other side, the "secret desires": "Do you want to see your favourite celeb half-naked? Click HERE"

Human vulnerabilities

The underlying principle of social engineering is to exploit the human factor, which is to put people in situations where they will rely on the most common forms of social interactions:

- The desire to be helpful and polite, especially in a public environment
- The tendency to trust people
- When people are praised, they are likely to talk and divulge more information
- Professionals desire to exude intelligence and superiority in a field
- Most people respond as pleasantly as possible to people who appear to have concern about them
- Conflict avoidance

Tactics: Elicitation

In the context of social engineering, elicitation is used to draw targets out through a set of questions that stimulate them, leading them to the behaviour that the social engineers want. Elicitation is quite low risk and extremely difficult to detect. More often than not, targets never know where the information leak about them comes from, and, even if a request does seem suspicious, targets usually put it down just as a question that they should or should not answer. Nobody cares or even remembers the content of the withdrawn information.

Just ask the target the right question at the right moment and all doors will open.

Types of Social Engineering

Now let's see the most common type of social engineering vectors used in our digital scenario.

Pretexting: it is the art of creating a fake but realistic world. It is where the attacker becomes anyone in a position to influence the target into making some decisions. The attacker chooses a certain personality that befits the character he or she opts to become during the social engineering attempt. With the advent of the internet, it is easy to become anyone, for example on Facebook or Twitter. Pretexting can also be used to impersonate co-workers, police, bank, tax authorities —or any other individual who could be perceived as wielding authority or right-to-know in the target victim's mind.

Phishing: It is a systemic-based attack that utilises a fraudulent email in order to get people to execute malicious code or reveal pertinent information. The email is crafted in a way that makes it appear from a legitimate company. Or this can just be a really cool advertisement for a product that no one would want to live without.

Phishing can be targeted to a specific organisation (spear-phishing) or to the CEO of one organisation (whale-phishing).

Baiting: baiting takes advantage of the most basic of human traits, curiosity. In baiting, a social engineer will leave a media such as a CD, DVD, USB Stick, or floppy drive in a conspicuous location relying on the curiosity factor of a passer-by to pick up the media and try to take a look at what it contains. Which is mostly keylogger and malware.

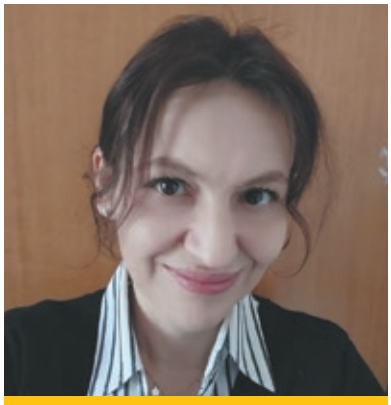
Physical: social engineering can also take on a physical form where the cyber criminal will try to gain access to a facility or sensitive/restricted area in a facility.

Mitigation

Advice could be infinite, and the space for this article is almost up!

Don't trust anyone, any mail, don't reveal your personal or working information, don't click on links in suspicious emails, don't download and open any attachment. If an object you won is too good to be a prize, probably it is not the real prize. Report any suspicious case to your local IT department.

And finally, the golden rule: Remember the National Cyber Security Alliance tag line: **STOP, THINK, CONNECT™**



About the author

Simona Venuti is security manager at GARR, the Italian research and education network. Since 2007 she has been working at the GARR-CERT (Computer Emergency Response Team) of the Consortium GARR. Her task is to develop automation systems in the reporting and management of cyber incidents and to carry out research in the field of new cyber threats, cyber security, monitoring, defence and containment systems. A fundamental part of her work is to establish a network of relationships with national CERTs of the European and non-European Union, security experts, company CERTs and Italian and foreign providers, to share experiences, studies, solutions, and above all to establish relationships of mutual trust in the eventuality of joint management of IT incidents involving several CERTs.

Simona also deals with the dissemination of information and training for systems engineers and security officers.

Twitter: **@Simo_GARRCERT**