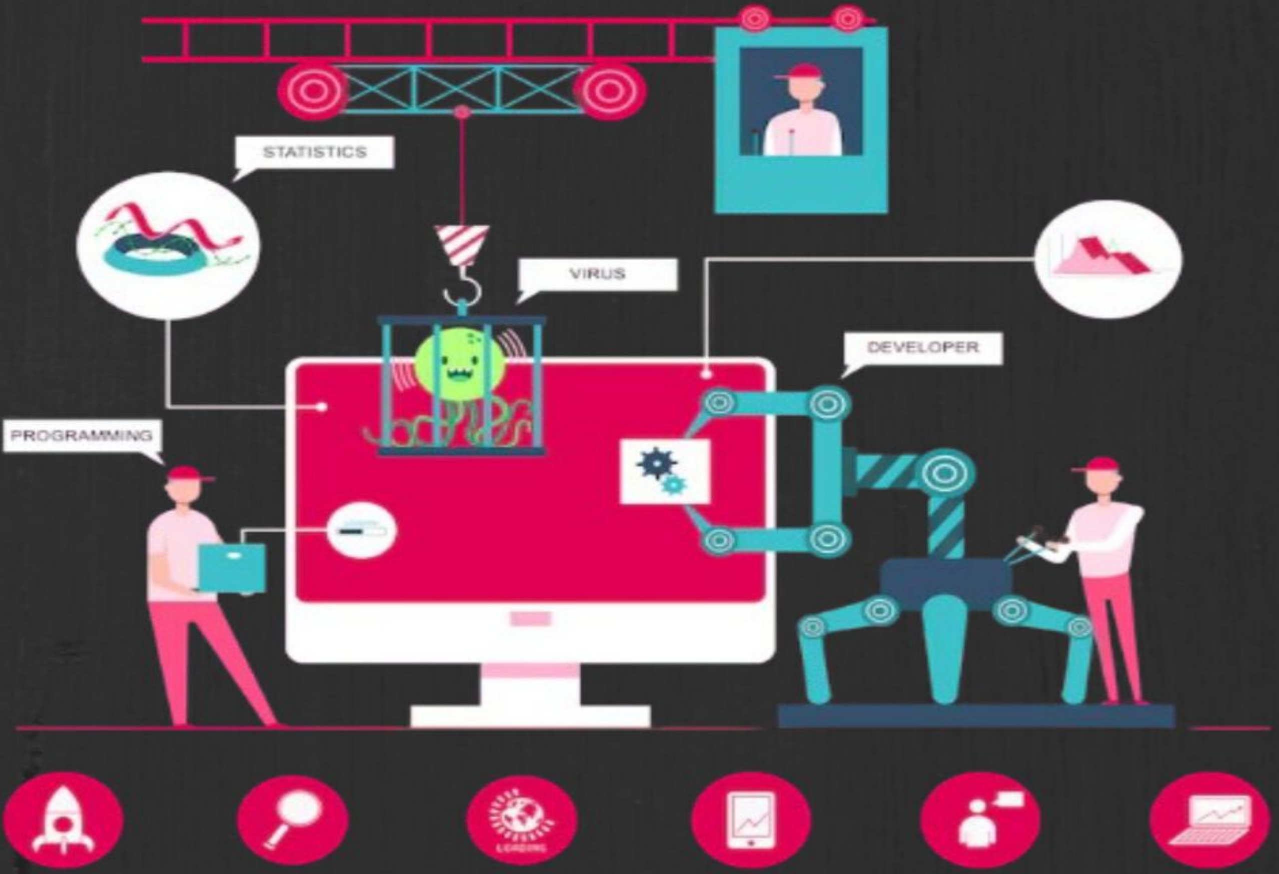

Cyber Security Social Engineering Hacking Human Firewalls

WRITTEN BY

BHARAT BHUVAL NISHAD

Cyber Security Social Engineering - Hacking Human Firewalls

Bharat Bhuval Nishad

Published by Bharat Bhuval Nishad, 2024.

Copyright

Cyber Security Social Engineering - Hacking Human Firewalls

Cover design by Bharat Bhuval Nishad

Interior design by Bharat Bhuval Nishad

First published in 2024 by

Bharat Bhuval Nishad

Table Of Contents

About

Hacking people is the most effective hacking technique, has the highest success rate and is very difficult to detect and prevent against. Learn how to hack the human firewall and how to protect yourself and your organisation against so called social engineering attacks where people get manipulated to do things they usually would not do and companies get way too easily hacked with the support of their own employees without them noticing.

This course is for non-IT people/absolute beginners up to cyber security professionals that want to get into social engineering.

Your teacher has over 3 years experience including a bachelor and master in Cyber Security and was within various expert and head of positions in the security government area, large international consulting and the banking industry.

Introduction

Let's leave our cards aside for a while and talk about the whole other story. The whole other faces of modern ethical hacking and hiking are like so let's discuss social engineering. So in the beginning I shouldn't worry that this topic deserves a whole separate training to be only partially covered in order for you to grasp the amount of risk and the amplitude of threats that social engineering poses to modern cyberspace. So everyone most probably already knows this.

Yeah this is really an arguable statement that the weakest link of any security system is always a human being. So yeah this is quite a popular phrase and it can be heard from many different people with different experiences and levels of personality. However there are ways to mitigate human threat. And here we will discuss how. First of all we should be able to exploit it and to what extent in order to stay within ethical boundaries. And second we will certainly discuss how to possibly mitigate the amount of risk that is associated with human and related threats. So you know, let's start from some definitions and just shape the content concepts. So yeah. I will not ask you to be empty jars right as many trainers do because human humans are social creatures.

Right so until this point in your life you had already had a lot of social interaction so you have experience. And most of you probably already know all these things related to psychology: how brains work is the basic structure and how different parts of it are responsible for different actions and classes of actions and how reflexes are different from things and how higher brain activity is different from everything now. So that's just something we consume from our education process. But we are not always able to employ all this snow which would be in cyberspace. OK so the main problem with social engineering is that people who are normally very good with dealing with threats with physical threats with environmental threats with health issues and so on just because they have been told yeah even evolutionary theory or through education to do with it to do with all these risks are really bad when it comes to treating similar threats and similar risks in cyberspace for one reason.

Sabertooth tigers we're living on the earth with us for a really long time. And we have practically by trial and error have learned how to avoid them or how to fight them or whatever. Yeah. So how to be more or less safe from them. And computers are with us for I mean massively for a little more than 40 years. Networks are prominent even for the last time. So practically there was no time sufficient to learn all these things. For older people it's a big problem for younger people. It's less of a problem just because they are growing up in this environment and they already have all this knowledge and they're more technical savvy and so on. And there were very few cases of formal education especially on most of these concepts and tools and tricks and the possible attack vectors. So people are not aware.

Knowledge is not important. People just aren't aware of what can happen. And if you go out there and talk to some non-security people you will understand what I'm talking about. Yes. Or C or fraud for example is a thing and 3 3 3 billion dollars are lost on the reported incidents since 2000 and 15. Yeah but the business people are still not aware that this is possible. They still believe that internal controls and external audits could save you from that. Let's discuss this in more detail later but for now I have to make you admit to yourself that this is the thing and we are not.

We are a security community and security in this we are not doing enough for educating and promoting awareness through the masses. So what we do instead is focus on separating the responsibility of security related issues here and in the user. So we are trying to put the user aside from the responsibility for his or her actions. So this is what is the main meaning to me at least of this phrase by Bruce Schneier Amateurs hack systems professionals hack people because your systems are They're quite quickly developed and they're developed by different people and they combine different technologies and always win against different technologies when there is some intersection there inevitably will be security problems. And the main point that huge problems arise is this intersection between a human being and the technology that he or she uses. OK so there's a difference between the internals of these two things: a human being and the machine they result in all sorts of security issues. So what is social engineering and security meaning and security playing. So in my opinion and believe me I do a lot of information related to social engineering in my life.

The best definition and the most constructive definition was given by a joint effort of the FBI and DHS. A few years ago they issued a joint report and they have shaped the definition as social engineering is the threat of a motivated insider. OK so what a motivated insider we all are. All right so someone is just committing internal fraud or is paid for giving out some information from inside that some actions. Yes. This is a malicious insider here and he is motivated. He or she is motivated to some extent by groups or by threatening and or whatever. So he or she is performing deliberately what social engineering is , it's operating within these limits. So we are not motivated and so we Tricom would influence him somehow to perform actions or disclose information. What do we do for that?

Of course we have to operate over some data and for that we use reconnaissance techniques and all these open source intelligence things that we have already discussed. The videos here. So in order to proceed with social engineering or technical doing we have to collect a lot of information. First of all we have to identify all those people then we have to know more about those people about their interactions with or close relatives and friends and family and so on their hobbies, their desires and passions, interests , who they play golf with and so on. So this is the basis we have to do that with weight. So we have to collect a lot of information that psychologists have to some extent. So most people think they know some psychology just because they operate within social environments. But in fact when you touch even a basic 101 course on psychology which I recommend to every security person you. You understand that that is simply not correct.

People have a lot of misunderstanding of what psychology is, what psychoanalysis is, what clinical psychology is , social psychology, behavioural psychology and so on. And moreover these concepts are always changing social psychology and behaviour is behavioural psychology are the thing right now. However, the very popular books that were sold on Amazon for many years are suddenly becoming bestsellers because there is a lot of public interest. So you go there and read a book you know and then we will discuss them. They called me just kidding. That's not only the basic concepts to operate over social engineer engagements. But in order to master them all you definitely will need some basic training. And I hope you'll find a source that will be credible enough like a well-respected university or professional author. OK so this leaves us in a little bit of ambiguity. So is social engineering science or is it the beat of art. I would say it's a little bit of both. I wouldn't say it is art explicitly and is limited to this concept. So I do not believe that this requires any talent.

This is a skill it could and should be trained in and it is not a science yet too because it employs a little grey area that is not yet covered with the scientific psychology approach. So there was no formal scientific research that covered all these things. So there is some observational research that there is some surveying but that's not enough. Yeah that's what I was talking about when I'm trying to round up the people who think they know psychology when they really don't. That's the science. The real science method there. And you know it's a state where half of the population can't conduct a lot of research. But social engineering is just a thing. It's there for some time but it's still an emergent threat. And there is not much scientific research conducted over the population that is facing social engineering or threatening the Internet. So we have statistics about the incidence but we have not conducted scientific experimentation and programs yet.

So the tools and the methods that are to be used in doing social engineering penetration tests could be split into two categories. Yeah. So there is some high tech human hacking that's used this wording and shoeman ethical hacking of course. Yeah. And there is some low tech human ethical hacking. So we'll discuss those in more detail. And I'm leaving you in the slide with more ambiguity regarding social engineering. So the cool game social engineers have when they gather in quantities more than two here is asking each other questions and arguing about whether social engineering always employs lightning, providing incorrect or truthful information to the target.

OK so there are different positions. Some people say that it is possible not to lie and still be successful in social engagements. And some people are completely sure that that is not possible at some point you will just have to lie. And this is basically the point where you will have to use some verbal communication skills and nonverbal communication skills that will prevent your targets from uncovering your or your pretext and actually figuring out that you are trying to social engineer them. So yeah this is the problem and basic counter current concepts that you discuss in this section. So yeah it started out.

Social Engineering Methods

Let's go through the methodology and the possible ways to approach a target. When you were using social engineering after social change I also think so. There are different ways to conduct social engineering attacks and they're split. As I said the two categories are high tech and low tech hacking so on the high tech side we have these things that are done over the electronic means of communication. So phishing, spearfishing , reshaping and all Wi-Fi. Bees are all really really high tech. I would say Vishay and somehow related to life and direction because it's basically using voice. Yeah. And the waiting is to some extent physical but still then I.T. space So let's go buy one.

Let's go through them one by one. Phishing is. There is no typo here You already know that hackers are using some sort of modifications to the words the users dirhams. Yes of phishing is basically sending a lot of malicious or fraudulent e-mails to many email addresses in hope that even with a small success rate someone will take the bait and respond back or click the link that is within the mail or open attachment there on the application or open malicious Deshmukh in a vulnerable program such as Adobe Acrobat or Microsoft Office Word or something. So this is phishing. This is just spreading your threat and large amounts without actually focusing on a certain target. Metaphorically it's really close to fishing, I mean fish in the real world. Yeah. In a sense that you're just throwing it out and waiting until someone takes the bait. So it was spearfishing.

The techniques are actually the same. Yeah. So in fact it's absolutely the same and from a technical standpoint. But in this situation you are much more narrow on choosing targets and much more broad collecting information so you will collect as much information about the person you are species spearfishing as possible. And you will limit the target list to very specific, very concrete individuals. OK so unlike normal fishing yet normal spearfishing is taking this rifle and putting the mask on and going down and finding that big fish. Yeah that big fish. That is a high profile target. And then shooting at it. This is the thing that is really simple. You are firing CEOs or CFOs or any people in the socially important points and loads of organisational structure and positions of trust and so on. And then organise attacks on them again. So this is how different it is technically it looks the same way. But yeah remember that we are doing all this stuff to the people who do not understand a bit of hacking.

Everything we do talks real do the same Yeah we're just sitting and staring at a computer screen for money. And then wishing. What is phishing sometimes is just voice phishing and sometimes this term is used which is not really popular. Hackers try to avoid that. So this is approaching at Target on the phone and through impersonation of pretexting or whatever method you use it is getting some information. OK so is basically just trying to do this thing but using different media you could even try to manipulate surrogates to open a link or open attachments if you know it's there and it's in the spam folder and it's your calling and impersonating a fellow employee or a boss or a boss in a rival department or whatever. So this is really dependent on what information you already have about the initial structural traditional culture and cultural constraints and so on.

But still this is voice vision and what is waiting is basically using physical tokens to do fishing or a game or spear fishing like. So you're taking a used B thumb drive for example. Yeah. And putting some to keep the poison tab for example by semicon cards is a very popular concept nowadays. Yeah. So you're just arranging a surrogate original situation where your target finds it somewhere in a parking lot or in an office building or wherever. Yes so you just put it there and just start your senses service hour and wait for incoming connections. So that's what waiting is. It could take forms other than you can use beef from Rove. Of course it could be a poster with a QR code. Why not? It could be just a short and you all go on your windshield on the windshield of your car. Yeah. So it's just people leaving this information somewhere and other people for some mystical reasons saying that they have no information they obtain in the physical world deserve some more trust than something they collect over e-mail or follow. Yeah there is an explanation for that because when we are dealing with physical objects we just have more of our senses involved in this communication. And that's why physical contact is more trustworthy just subconsciously.

This thing also works and what is wrong. AP Wi-Fi and why it's not in a separate section it will have a lifetime because it's purely social engineering. There is no high tech hiking here actually so it's just raising an access point that looks like the target's one. Yes. So it either has the same name or it has a popular name like default to IDs of vendor access points used by the client or something like Mendon us or Lifton's lobby or whatever. So it's just something that most devices will automatically connect to once they have it in range. Yeah. So that is like just just luring the clients to your access point and then sniffing the information that they pass out from the Internet. So without high tech methods that run others but these are the most prevalent. So let's focus on them in this video.

What is low tech low tech hacking easy or worse the intrusion. So it's passing a physico perimeter. First of all, this is the most effective because if you show the evidence that you were there successfully and to the data centre and were able to work with the server that the critical server likes physically standing in front of it in the server room that would be impressive. And this is much more than this is much easier than it may look like. So once you start doing that and once you have proper permission you will be surprised to what extent people around you are actually willing to help you with zero trust established beforehand.

Especially in Western cultures, impersonation of identity theft is just masquerading as someone else. As long as we collect all this open source information we may at some point find ourselves capable of impersonating a trustworthy figure in the target company. And then just pursue that, pretend to be them and do the social engineering stuff. Yeah. There is a whole new class of malicious attacks that are called sea of fraud. This is a situation where presumably they see or that is on vacation or on a business trip somewhere or somewhere far away in a different time zone sending out this email. I'm not asking but ordering. Yeah. So bending the wire transfer to a specific account and then has a pretext and a form of like urgent investment opportunity or something else.

So yeah this is a direct use of authority principle, the one to discuss a little bit later in the business environment and this is a really big issue. It generated lawsuits and billions of dollars over the last two and a half years. And this is just within the range of incidents reported we are aware of. This is just the portion of incidents that had been reported by the victim companies to the FBI. So the other thing is tailgating piggybacking, which is a specific type of intrusion that employs people's willingness to help. Yes, so is luggage going in and reaching the critical point is just performing this exercise of circumventing physical boundaries. So it's just following authorised personnel through the checkpoints with or without asking for their help. So it is just that it is ordered a lot more than the complete intrusion exercise. So this is why I'm just putting it as a separate matter. So this sort of thing of course is just to figure out what people are typing on the keyboard by observing what they type, observing their hands or just seeing what's going on on their screens. So this is easily avoided but it's really prevalent in public areas such as airport lobbies.

So you have to be really cautious about that yourself because there is no effective way to prevent that other than just sitting your back to nontransparent or something. So it's OK to stare at the person that is trying to tell her you're scared. Yeah. And showing that. Come on. It's not OK to do that when I'm typing in my passport and Dumpster diving . It's here mostly for historical reasons. I tried to view these notions. I tried to do that before and this is the case like that just to show you that this thing evolves and there are new methods every year. And the old ones become irrelevant. So dumpster diving is this thing that you might have seen in hacker and hacking different ways about hackers when they are taking these shoes on with really large bottoms.

Yes, in order not to hurt themselves in just containers and then get in those containers at night with flashlights and try to find some important data on the brains out printouts that have been just trashed out of the offices. That those days are gone. Not because this is not effective but because that is a much easier and cleaner way to obtain the same information. So in the last successful pretext they can give you that just comes to my mind is pretending to be this go green company that just arrives at your office and free of charge releases you from all this stash of paper you have at your printer Arius So yeah there were organisational departments that were really willing to increase their company's karma by employing such external parties.

But yeah this is too risky to be allowed in your company and you have to check out whether the clients are paying attention to what they pass through their physical perimeter and whether they shred that first the wall or whether they allow others access to the open air as if it contains confidential information. But again just remember that everything that's left the client's offices in this form of printouts in most jurisdictions is open information. So this should be checked no matter what if. If it's not strictly excluded from the scope.

Tools And Techniques

What are the tools and techniques that could be used in order to executor's those decks? Yeah. Conduct these craft methods you have to apply those methods in order to gain advantage of human factors and social engineering. So there are those psychological things that Cogeco techniques I would say are all based on very fundamental psychological grounds so I'm not saying and I do not certify that all these results are true but this is the state of the science at the moment. So there is no a.p or hypnosis here So this all is scientific truth as we know it. And there are technical means of harvesting information required to conduct the tests and the research. Even this really handy social engineering tool. There is a way behind any other tools said that could be used in order to arrange those kinds of attacks. Yeah. And there are some tricks and advice that I will share.

In the end Londa gives you direction on how to sharpen your social engineering skills and technical perspective. So let's first look around what the psychology behind all this is. Yeah. So I will try to make it really quick because there is a lot of information to cover but let's go one by one through those methods. So these are what they are called. Yeah. So these literally are psychological principles that lead one person to influence other people. They are based on our similarities. So people try to maintain their individual individuality but in the end we share a tremendous portion of our DNA. From culture to culture there are differences.

The other Reymond structural differences but socially we are more or less the same. And so we do not really differ in terms of psychological reactions to different events or actions of others. So yeah there are some deviations there are psychological disorders that make people irrelevant you make people ambivalent to certain stimuli to certain events and those people are most probably not your best social engineering target. Yeah. And that there are like Statistically the one sociopath per 100 people. Yeah. So there is a 1 percent chance that you will fail in your social engineering game engagement just because you have chosen the wrong target. But the good thing is that sociopath's are detected with a good success rate so yeah let's go. So first of all there is the scarcity principle. This is the high value it is that is the result of a limited amount. So everything that's not really large an amount is valued higher in price. This is purely psychological.

This is why platinum has more value than gold and gold has more wealth than silver and silver has more value than steel . Only steel from all these has some material. Well you know yeah. Yeah. So this is something based on the small amounts and our willingness to have more of something that others don't. And this is really working out in terms of time because the resources are limited. Normally the time is the only resource that is in no way recoverable. So we can not get more time in time just by using it and we can just spend it effectively. Yes, the most critical resource limited in amount looks like this situation: mostly artificial you're in a business environment where you really have to hurry. So if someone is trying to speed you up so someone is pushing you to do something really fast these already may mean that you are being social engineer in a way maybe with a good intention but still this is a direct use of scarcity principle. So maybe this is in many places. Just look around and see what happens.

Authority also this is basically I think the most important and the strongest psychological principle in our culture. We are social creatures and we are for the sake of our social survival our delegate authority to limit the number of people so there are others that true the rest. So there are some people who just are entitled to be of higher authority and we will raise our children basically and the environment that makes this authority plausible. Yes, so we teach them to respect the people in uniform, to respect the elderly and so on. So being an authority or successfully pretending to be of authority or even being associated with an authority figure like an assistant or C or something is a really successful point of issuing the social engineering and Demps of attack. So you have to know that people value authority, people comply with authority and this is the strong influence of social engineers to good liking. So people normally like people who look or behave like them. So this likeness between people if you successfully demonstrate that you were similar to a person this person is more likely to say yes to you. This is natural. And there are ways to make people like you more.

Yeah artificial wasted earnings and skills that could be employed in order to raise the success rate. Also, You see there is some reality here. So first of all we like someone who is like us and we are more willing to help people who we like. So this work has too many meanings. Yeah and maybe that's why we understand we behave like that or I'm just missing the cause and effect in this relationship. So maybe it's the other way around but whatever. This is how things are. This is how social engineering attacks could be performed like consistency. A really important thing to understand here is that people once they permit something in their life except something embrace something and start acting in a certain way. They have this inertia and so on.

Once you said yes to a person if they are continuing if you are if they go on asking you for a little bit more. Most probably will be tending to say yes to them more and more. Again and again. So yeah we can see that in different fraudulent activities in the streets. And so just starting from a simple favour that is impolite to be rejected and to have been denied certain fraudsters or trying to involve the victims into a more and more high stakes communication. And you just leave them without money and maybe even close here. So let's not forget about that. Just raising the stakes between the conversation so through or throughout the single conversation based on this consistent psychological principle we can conduct a social engineering attack so always start from something small and then go on with extending your demand and just raising the value of the favour you are requesting from the Dartmouth social proof.

This is basically just acting in a way that acts in a way as everyone else acts in a situation of incomplete information. So every time you see something happening and demand your reaction, look around to see what the others do and behave in the same manner. So you see that a lot of people are writing from somewhere else or they're just trying to tell you why you are not going to the source of all of this behaviour. Yeah. Who you're starting to run with them with the crowd. This is not an instinct. This is a social ability that we have developed throughout our history and this can be really damaging. So for example this bystander effect is thinking that someone else will take responsibility for what's going on right now. Yeah when someone is a victim of a crime or someone is suffering a health issue or health crisis and no one helps them just because they think that other people will help them.

This is also the manifestation of the social proof principle. And this is really scary so every time you find yourself in a situation like this and then you require immediate help. Please do not just show it. You have to address your request for help to a specific individual because that is that explicitly identifies the person you are requesting to help. And this might resolve the issue. But just asking for help asking for her help from someone or a group of people is not efficient. It is as inefficient as the number of those people. So there were cases in history when people just did not react thinking that somehow someone other than them would do the job. Reciprocation.

What it is is just giving back. OK so if someone is approaching it with a compliment or with a small gift or something this might not be a sign of attack already but this certainly is a sign of applying these reciprocation psychological principles so you know to get something you have to create this impression that the person owes you something. Yes, so give a smile to complement the good look. In extreme cases but not on the first engagement of course give an unintentional presence a gift. So this all is reciprocation. Inaction and you don't like holding the door that is not controlled by the press. KURTZ Yes. And then when you're holding the door to a person and letting them into the building and then going with them side by side and the next door that requires that pass that you enter. You may find yourself in a situation and this person that is having this bash in his best will let you in.

Tools And Techniques Part 1

Beyond influencing my thoughts the race of a set of cognitive wise is I will just highlight some of them for example anchoring and priming is just using Not even the psychological ability or specifics of the brain. They use some really hard wire things within our brain, our tendency to use the neurons that were just highlighted by some activity. OK so if we are starting in negotiation about the price for example and the person who is entering these negotiations first has upper hands basically because they have an ability to have a chance to shape the further discussion and get both sides to a specific fear. So they just say It will be $100,000. And the other side could not possibly just split this amount in half. So it's not culturally acceptable.

It will either just break it. OK so you guys This is not what we expect and initiations will end. But if the other side will decide to proceed it most probably will hang around this figure for the rest of negotiations and this might be far higher than is acceptable for the first site for the one who declared this an issue of price. Priming is basically the same. We are trying to make people think about something about the concept or effect or just or just remember the figures in their hands here and we can expect them to use this information in their further decisions. OK so for example again priming with the number when you're trying to present something to a price you might start from OK and now we are talking about the price of course it won't cost you a million dollars. Yeah. And then you just narrow it down to those $100000 which is more pleasant to hear for the other side.

After you mentioned this million dollars fee. So this is Bryony or just making people think of large numbers before you are starving, persuading them to think about the price is also really promising in terms of negotiations. This was what Brian anchoring is OK: a risk appetite is the whole different story. So people are willing to accept risks if they have something to lose. So this is our innate ability to deal with different risks in critical situations and all the time we see that something can be taken away from us. We are more willing to race. So if you shape your proposition as a potential loss in the result of taking action that is not in your interest here you will most probably elicit this risky behaviour from the target. And on the other hand if you shape this as a gain. So if you phrase it in a manner that if the person takes the actions you are proposing they will gain something. This will decrease the risk appetite.

So the decision will be less risky from people who are less risky. From what you propose. OK so if you use two variants and they think that one is risky and one is not and you want a person to take a risky decision in this situation you have to shape it as a possible loss. And if you want the person to take the second decision and not a risky one you have to phrase it as a game. So this is quite tricky but it really works and the relation between these two is really large. OK stereotypes. This is basically my favourite thing. So we have these templates in our hands. Yeah. So we cannot think through all the things that happen around us in full capacity. We have two shortcuts. So we build these stereotypes based on some portion of things we know of an overclass of things and then about every other thing in this class we just apply this stereotype.

This is really tricky because the types of things are really fragile and volatile so people are really really different in some situations. So there was a really strong experiment about that. When most people know that there are strong stereotypes first that girls are not as good at maths as the boys are. And second is that Asians are really more capable at maths than the rest of the world. So believe it or not they had to focus groups of Asian girls who were before the test taking the standard maths test were primed by the stereotypes. So the first group was asked if they live in Germany for only four girls or if you combine it once. Yeah. And the second group was asked what language they use at home. Yeah. So like covertly they were prime and should think about their nationality or their gender before the test and the results of these tests differ dramatically. OK so of course the ones who remembered their nationality right before the test they performed outperformed the first group. The other group dramatically. So this is not only the effect of stereotypes on people.

This is the effect of stereotypes on the objects of those stereotypes. This is a really strong thing so employing stereotypes is really ethically tricky because. Yeah to and not to harm the feeling so to target and not to miss the target. First of all by playing war stereotypes you have to be careful. And that non-verbal communication is also a really really broad topic. But here I will just highlight that. Yeah there is some notion of lying or not lying on the social engineering measurements. So let's start from emotions and microexpression so you might really know from popular culture emotions are quite universal so human beings independent of their nationality or culture express emotions more or less universally. So it's ok to find out for yourself. I know. But you know here and you will be able to read emotions of the people there although they may not always share the same cultural values or even seen a European person before for example. So they express the same emotions that microexpression is when you're trying to limit the extent of your emotions showing up on your face or on your body. So this control of emotion microexpression is really important when you are under stress and when you are performing a social engineering attack you are normally under stress.

Yet at least for the first 10 years of practice. So this is really interesting to be able and really important to be able to control that and to read that on the target as well because sometimes early reactions and early and they lose the real emotions and text that you're being actually detected or there are some signs that the target is not willing to proceed. This engagement, this communication with you will help you to withdraw with the least harm on you both. And what about gestures and positions? These two are also universal to some extent but gestures especially are very cultured about different gestures and different cultures make the same gestures and different cultures may signify may be read by your target very differently.

So it's a good idea if you are trying to work within different culture to get familiar with what's the traditions about that in order not to you know not to draw a Dessau Densham to what you do in positions of your body are actually able to to make a person more willing to communicate with you to it can allow you to achieve this stage for a border between the two. In this stage of reporting that is way over used in popular culture. So but but this is the thing. It exists and synchronising your behaviour with your target is really important when one is trying to get situational trust. So this thing that lasts only for a few minutes can help you achieve your goals and then leave without any harm to you both and present the evidence to the management and point out what cultural organisational changes should be introduced in order for this to never happen again. So this is what psychological techniques are. Some of them are even in the anthropological area. But this is the human side of our operation and when we are exacting social engineer x.

Tools And Techniques Part 2

The technical side of the toolkit of course we will use the same old same tools we have already discussed. Yes so starting with the multi-grain the Harvester and then recalling G and Folco and others we will automatically and manually collect as much information as possible about the people within the scope or sample and then we will use our hands and our abilities to cross different content for different messages and our communication skills and most importantly this really handy thing. Social engineering is a tool kit that will have them all.

But for now I will tell you that it's quite tricky to install in certain environments but once you install it's really easy to use. It's much easier even then we Collinge you or let us put it framework really it's just the multiple choice menu and you're typing your parameters in just selecting different paths of the text so you can clone the Web so you can arrange credential harvesting and this way you can make mass fishing or Spearfish an index you can use different templates for email messages or for the Web sites that harvest credentials or whatever you can to use different payloads to be sent. Is it dangerous or used for Brize browser exploitation. You can just type in the or else for a website that you want to clone. Yeah that when Google Facebook or linked in or your client's VPN gateway. So this all is really thought through there.

This is a living organism that is developed as we speak. And you could not rely on its stability once the changes are introduced because it's open source. That's what it is. And I do not recommend it as the same strength of recommendation of not updating Keller next during a penetration test. Yeah. Applies to social engineering toolkits. And by the way it's included in Galileans so you can start using it right now trying to call some sites, try to craft even some email templates and create those you're all on your own. And yeah let's give some time to discuss how actually you can do that. So content creation in the form of websites offering messages or some other communication styles here. It's really a deep topic. And in this case and for the sake of this training let's focus on seven different types of messages.

So using it even for email using this old school connection to see the word 25 and feeling some text file it can maybe base 64 encoded dash and multipart messages and see that this is really old. And also everyone is using the API right now. So for example there is mail on the service that is dedicated to mailing lists. Yes so you can use that for free with the limitation of $10000 per domain a month. Yes. So you have to go through some business validation from your accountant for the main register but this works almost all the time. So if you just tell the truth that you're going to fish to legally fish your client they most probably will let you do that and that that's how it's working right now. Sending phishing email campaigns through your Gmail account is not practical anymore.

First of all because Google Apps and Google Mail are progressing really fast on detecting those kinds of attacks, even originating from legitimate accounts and using open S.M. Tippy gateways are also not really practical because they have Khurram us nowadays. So if it's a new host it has not been operating for some time. It will have a really low rating in this MTA to MTA communication. So they have to wait , they have a reputation and your recreated MTA will have really the legality of it so API is for the win and social networks are there as well. Yeah. As well as email so you will have to employ an API. So Facebook called Twitter and others in order to first of all collect data because some things are not available through official Hughey of Facebook or LinkedIn. So with the letter that's a really interesting story every time you do a search length then you actually get all the results from the first try. But depending on your account status whether it's premium or a share or just the regular account and based on your social network so whether you are able to reach those people in their search results through some of your connections you will be showing different results. OK but taking advantage of the fact that the data is already there in some of the client side.

You can just expert that to some adjacent structures to circumvent the limitations that the web application gooey applies on the client side. That is quite a tricky and really serious flaw from LinkedIn at least for the moment. But yeah you can use that in order to make your work easier for less money. Okay so yeah and when I'm talking about content creation that's at least four emails. You will have to get familiar with the MIME types that are used. It is really similar to HDMI also there are a lot of headers in the email body. And then there is a plenum to line the data. The body starts out and there are different content types. It can be split into two parts and they can be alternative to one another.

For example you can create a separate section for plain text viewing of Urim and they should you know being a wearying voice can be encoded somehow in order to fit into the window with. Yeah and in shreds so yeah and attachments are also base 46 and call it most probably and poods into the single file with all the rest of the email body. So it's worth just maybe saving some emails from your mailbox. You have already moved to the file and the file system and then just going through them and seeing what they are or what they consist of and so on. So you can start doing that right now and later in this section in the demonstration part will actually send out some non-malicious phishing emails.

Physical Security Considerations

Social engineering is the area when you get the closest to the real people who work for your clients. So does this imply some physical security considerations of course. And this implies some ethical boundaries we have to stay within in order not to harm certain individuals and the company as a whole. So first I want you to remember all the time you are performing this kind of assessment. Is that your main goal is not showing that people are silly. Yeah. So showing that the person clicked the link and pointing it out at that person and blaming them on their stupidity is not what your client expects from you.

You have to highlight the results of the processes or the lack of the processes. You know the absence of training or organisational controls or awareness programs or whatever but has been chosen by the client to prevent social engineering threats. So focus more on processes not people even more from my experience. Good penetration testers always try to obfuscate to obscure the actual individuals that have been used as paths to successfully attack things for structure. So some are even surprising to some clients. Poods this clause of demand of not firing people who figuratively clicked the link. Yeah. After the penetration test. So from one point this is highly ethical. OK so putting a person under the pressure just because you were skillful enough to trick them to do something is not to go off course. And the second thing is that they are no longer around the people who have suffered from the attacks.

Actually the most valuable assets to the client in this regard. So they know that now they know where they were mistaking where they were tricked basically. Yes. So they have learned from the incident. And you cannot do better, you know. So learning from experience is the best way of obtaining procedural memory so you can try to make people imagine in those situations. And this is always less effective but still more effective than just sending them a newsletter as a Mafia and pretending that is your security or wellness program. But go into training. Yeah it's strong but going through an incident is an extreme version of training. So it's like a real world battle you are going through. And after that that person that target will spread this knowledge throughout the company. Believe me they won't limit that to themselves. They will tell everyone they know and they will spread it even further in a matter. You see this is possible even though I was trained to do that to open that attachment or click that link or go to this link and then enter my login and password into the page. So this is a highly positive side of the penetration test and term in terms of increasing personnel awareness about those threats.

Second thing I want to point your attention to is to rush certain things that are out of scope. So in the same way there are some ethical boundaries to psychological experimentation. For example psychologists could not put a subject in a situation where the subject could hurt themselves or hurt someone else. Yeah. So there are certain considerations about ethical conduct in social engineering. So lying is not in this list because it's still questionable whether we could or could not lie all the time when the penetration tests through social gen's but certainly do no harm to individuals. Focus on the company. So if we are talking about taking people we are taking them in the business context. So breaking into someone's Facebook account is really private.

It's most probably out of scope in most jurisdictions. So it's something really private pertaining to an individual, not the company who hired you. So always think about that even with limited access to the sites you clone and the sites you prepare beforehand before social engineering engagement starts. Yeah. Limiting access to the IP addresses of business use to the IP addresses that are used by offices and VPN gateways to connect to the Internet is sometimes said to be a device. They certainly do not threaten because that's going beyond social engineering really. Case of physical threat or moral threat or threats to significant others or children or close relatives or friends whatever it is. Aimed at something way below the level of social engineering. So it's like going really deep into our nature and this is absolutely out of scope of organisational structure and through the initial processes and something a person could learn from training or an incident. So this is a physical or mental threat that triggers a natural response. And this is totally acceptable and gauge gauge end overall you know you will. So remember you were there to cause good not bad consequences. So there is no there is no sparing a particular interest of an individual for the greater good in these situations. OK so you should not harm anyone and do no evil.

So once you see yourself as a potential source of any type of negative effect you have to stop right there.

You should not take that path even if you think on the larger scale it will cause some positive change. That's just not acceptable. You should think about other ways to get there. And then for your own safety always have an engagement letter before starting any activities of course. Yes or just for legal reasons. You have to have an authorization from your client at all times but especially when you are going in when you are on site on the client's premises. Remember that in case you are caught and identified as a potentially malicious Asian threat agent you will have to present something. So always have a copy or a second original copy of engagement's letter with you on site. That's a must. You don't have to try your luck to the extent that you find yourself somewhere waiting for police officers to figure out you or your faith. Yes, so that's not a good thing. You will have to present something to security guys or some others you will fail and most probably engage. But this is a positive result as well. So something went. Absolutely Yes. So not wrong but So something triggered the expected response, positive result and contrition. This is also a result.

You have to highlight that and the report that something called here and you were prevented from successfully mounting the attack. But this is the result as well. Intrusion in certain jurisdictions is strictly forbidden. So no matter what your client writes down into the engagement's letter This could be just not permitted by law. So I could not encourage you more to just go and consult your lawyer whether in a specific jurisdiction or when your client wants to consume your consulting services. It is theoretically allowed to attempt intrusion into a private or corporate property by the owner's consent. So this is really important and even especially in the countries with the cold law of a British type of law. But the codes that explicitly contain all the rules that might be the case. Yeah. And the majority of the countries out there are like this. OK it won't look because we didn't touch this throughout the video but just to mention that first of all this is really interesting as a sport.

So picking locks is really similar to all other offensive security activities. So if you have time and you can get a hold of a set of lockpicks and some training locks do that. This is really cool. This is really Zen. Yes. Picking locks and trying to compete with someone else. That's what's really interesting. And it trains your technical skills as well. So just putting effort into a sort of time and concentrating on a task that's really useful in the career. But again lock picking is really old. Locksmith's were really strong in lobbying. Certain rules are in some jurisdictions it could be also just explicitly for business. Yeah. Also all the time you will have some physical channels for attack and you will be asked to use lock picking skills. Consult your lawyers first and see what they say about whether it is theoretically possible to do on client's consent on a client's premises.

Conclusion

First of all, why are you trying out this social agency with two kids right now? It's available to get help and this is the website with the description trusted SEC is the company founded by Dave Kennedy, a really well-established person and social engineer, to go hiking. And another one another guy Chris had naggy. Yeah. So they co-host actually christens or co-founded the social engineering podcast and the social engineering or web site. And Chris has written a couple of books about social engineering and we're committing the first one because it's simply better. It's not because it's artistically better but it contains much more bootstrapping information. So you know a lot if you are very close to that topic and it's much better than a memoir. So for Kevin Mitnick for example because.

Given this is a nice guy he had a very difficult life. But in the end he has written a really interesting book but it's based on cases on a case by case basis. He describes what could be done, what's been done and what were the results and how to prevent that. Social engineering the art of human Heckel is more of a method or method methodology I guess. So it's not scientific but still it's like more of a trade manual than the memoirs of the half fictional book. Yeah. And as for years this time I have to share just to see what you can do by observing by only solid shoulder surfing the environments around you or at the airport Claudie for example. Yeah. Or in the street you can see this U-joint talk and be really surprised about the amount of information you can collect without actually giving any effort just by paying attention.

A journey of course is the author of Google hacking database and the book on the topic so you can google more about them. And the key is she says she's also a really nice guy and he has established this discourse for helping children in Africa by collecting money and other resources throughout the hacking community. So it's a good feeling to even be a role model in the industry. And this is a demonstration of some really basic social engineering. The text is really not technical hiking there and it's recorded I guess on Defcon along with social engineering CGF can petition that. Again Christian nature has arranged a long time ago and it's recurring every time the con is held in Las Vegas. So it's also really interesting to show yourself to your family and the public.

What are the threats of social engineering attacks and what would be their consequences. So yeah that was stuff of information a lot of direction for getting for the information that's now rip up the presentation and get to the visuals. First of all I'll show you a recent example of phishing attempts that really impressed me and believe me I'm not easily impressed and this social engineering world here. So it's really a little slice. And of course most of us wouldn't be triggered by that bike.

But compared with the way social engineers operate normally this is like the genius level of conducting an attack. So it's circumventing the content filtering of Google mail without actually interfering with content filtering so that the Complicite through the environment to do whatever you like. And then I will demonstrate how to mount a modern social engineering deck using some tools and specifically social engineering to it. So see you there.