Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Social Engineering: Hacking the Human

What is Social Engineering?

Audience: General **Reading Time: 20 Mins**

We live in a digital age where the technolgy is continually improving. Whilst cyber security is constantly evolving to combat cyber criminals, human psychology remains realtively unchanged. Social engineering is threat we must always consider. This article looks to inform you what it is, and how to stay ahead of it.

Key Points

- Social engineering is defined in the context of information security as *"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."*
- Social engineering (or human hacking) is becoming a more common threat in the world of cyber security. Whilst the technology side of security is constantly improving, cyber criminals are realising that the easiest way through a firewall is to manipulate a person already behind it.
- Social engineering is one of the most dangerous threats to go against companies and IT systems alike as many people are not aware of the damage that can be done due to the information gained by a talented social engineer.
- Social engineering techniques rely heavily on the ability to manipulate information freely from humans. If you were to ask ask any con-man, magician, or psychologist then they will inevitably tell you that humans are very easily manipulated.
- Due to the way we communicate digitally, via email in the modern world, Phishing has become the most common type of social engineering attack. Phishing itself comes in many forms and employs numerous methods which we should look out for.
- Social engineering is largely preventable through good awareness, regular training, and knowledge of the techniques and methods used to extract sensitive information.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

Human Hacking

In the context of information security *social engineering* is defined as **"The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes."** *["social engineering, n." OED Online. Oxford University Press, December 2019].* Social engineering, also called *human hacking*, is becoming a more common threat in the world of cyber security but can be prevented simply through increasing awareness. As computer antiviruses and firewalls become stronger, malicious actors are realising that the weakest link in cyber security is actually the person behind the computer. Therefore, the easiest way through a firewall is to manipulate a person already behind it.

The social engineer lives by the motto *Knowledge is Power* and will attempt to extract any and all information they can. This information could be leveraged against a company for monetary gain, or perhaps simply used to cause reputational damage. While private and sensitive data is often protected through measures such as a firewall, social engineers specialise in extracting information by manipulation. If you ask any con-man, magician, or psychologist, they will inevitably tell you that humans are very easily manipulated.

Common Social Engineering Techniques

There are many methods which social engineers employ to extract sensitive information, let us explore some of the most common techniques in the social engineer's toolbox according to the infamous social engineer Kevin Mitnick.[1]

There are four classifications of problems which are exploited. For each explanation we present three sections, the first outlining the problem, the second providing an example scenario, and the third explaining how to protect or prevent the type of attack.

The problem classes covered in this article are:

- **Innocuous Information** - Information that seems harmless, but in combination with other factors can be used maliciously.
- **Causing and Fixing the Issue** - Using empathy and "owing a favour" to get potentially sensitive data from someone.
- **Just Asking for It** - Using authority, empathy, fear, and panic to extract sensitive information from someone.
- **Phishing** - Gaining personal information through the use of fake emails and websites.

Innocuous Information: Problem

In any company or organisation specific articles of paperwork and phrases or terms get passed around from employee to employee, so much so that the employees see this information as common place and unimportant. Whilst it is unlikely, a malicious actor can use some of this information to take down a company with one call. The more skilled social engineer treats their attack like a large puzzle, slowly gaining all the right pieces to give them a fuller picture. A simple and innocent sounding piece of information could be used as a stepping stone for a larger scam. A harmless question such as: *`When you phone in to CreditChex, what do you call the number you give them is it a `Merchant ID'?'* could later be used to pretend that the caller was from the bank. Often a social engineer will learn some phrases or words that are only really used in the target job, e.g. acronyms of a particular retail business if they plan to attack a retail business, or acronyms related to the IT sector if that was the target. By saying these phrases casually, the person the social engineer is conversing with will tend to think that they also work in the field. Thus, making a request for some innocuous information seems normal and is not questioned.

Innocent Data

Innocuous Information: Scenario

Assistant: *Acme Products, this is Madison, how can I help you?*

Malicious Actor: *Hi Madison, this is Jesse, I'm a new hire down in Budgets trying to update some contact lists. Do you have Mr. Charles Foster Offdenson's email address for our records?*

Assistant: *I do, but that's not often given out, you can just use my address for most things it is madison@ac.me*

Malicious Actor: *I know that, but I'm being put through the ringer down here and I was supposed to have this on my manager's desk an hour ago and now he keeps checking up on me and I just started this job and I've ...*

Assistant: *All right, I understand, you can calm down. The email address is CFO@ac.me*

Image: Hannah Wei on Unsplash

Innocuous Information: Solution

The important prevention measure that should be taken in this case is to keep up-to-date with what information, even if seemingly innocuous, could still be a risk. The most direct measure would be to class all information as classified, unless explicitly stated otherwise.

Often in the situation of a social engineer calling a company, they use insider words and language which helps to make the targeted people feel that the engineer is a part of the company. Just because someone knows the terminology it does not mean they are entitled to have the information.

A *Merchant ID* may be used in the bank every day, but such an identifier can be equated to a password and should be protected as such. Another common request is direct phone numbers of department and work groups. While the direct numbers of the CEO or members of the board are generally not given to outsiders, they are often shared with employees (or those who pose as employees).

A suggestion to counter this is to implement a policy forbidding the exchange of phone numbers to outsiders, and to implement a procedure to be sure the caller is actually a member of the company.

> *Just because someone knows the terminology, it does not mean they are entitled to information*

As will become apparent in all the prevention techniques the best way to stop a social engineer is to have strong verification procedures. The most common and effective way of implementing this would be to include Two Factor Authentication (2FA), this way even if the social engineer got an employee number that would not be enough to be considered a member of the company. In the scenario above, the assistant could simply have offered to email the malicious

user the information. That way, she can verify that the email address is associated with the company and the member of staff is real.

The hardest part of preventing social engineering attacks is overcoming the human instinct to be helpful, If someone asks for a favour, decline until you can verify the request is legitimate. Social engineers use and abuse human psychology and the easiest way to not be a target is to be knowledgeable of different approaches.

> *The hardest part of preventing social engineering is overcoming the human instinct to be helpful*

Causing and Fixing an Issue: Problem

If you are experiencing a technical problem with a computer system and someone claiming to be from IT called and said they would fix the issue, then gratitude is typically the emotion that would be felt, not distrust. This is one very useful method in the social engineer's toolkit. A couple of convincing phone calls could result in a scammer being both the source and saviour of an issue.

The target of the con can be lured into a false sense of security seeing the social engineer as a very helpful member of the company. Once the social engineer has built up this false trust of themselves, they would then often ask for a favour in return for helping them out. This favour may come in the form of asking the target to install a piece of software on the grounds that *"this will stop the error causing a downed network in the future"*. However, the software would actually be malware and not perform as claimed. In fact, it would install a key logger and a piece of malicious software that would provide the social engineer with virtual access to the computer.

Causing and Fixing a Issue: Scenario

Staff Member: *"Accounts, how can I help?"*

Malicious Actor: *"Hi there, it's Sam from the IT helpdesk. We're trying to troubleshoot a computer network problem. Do you know if anyone in your team has been having trouble online?"*

Staff Member: *"Uh, not that I know of"*

Malicious Actor: *"Okay, that's good. Listen, we're calling people who might be affected because we have been having reports of people losing their connection, and we are trying to be proactive in solving this before it escalates. It sounds like having your network connection go down would be a problem for you and your team..."*

Staff Member: *"Yeah, it certainly would!"*

Malicious Actor: *"...so while we're working on this, let me give you my work mobile phone number. Then you can reach me directly if you need to in case you need"*

Staff Member: *"Thanks, that's great"*

Malicious Actor: *"It's 07123456789"*

Staff Member: *"Very useful, thanks again"*

Malicious Actor: *"Listen, one more thing before I go. I need to check your port number. Take a look on your computer and see if there's a sticker that says port number"*

Staff Member: *"Yeah, it says Port 6 dash 47"*

Malicious Actor: *"Great, that's what we had you down as, just making sure"*

Get What You Ask For

Causing and Fixing a Issue: Solution

The simplest solution is to not fulfil the requests made by a stranger, even commands or applications that seemingly do nothing on the surface could lead to bad consequences for the company. A significant part of preventing these types of requests is to designate a single employee in each department to handle all requests for information to be sent outside of the work group. These designated employees must then go through an advanced security training program so that they become fully aware of the procedures they should follow.

An important thing to be noted is that everyone from receptionists to high-level managers need to have adequate security training so that they are aware of the ways people will attempt to get information. The heads of security should establish a single point of contact so that if employees are not sure if they have been targeted by a social engineering ruse, they can bring it forward to someone who would better understand what next steps to take.

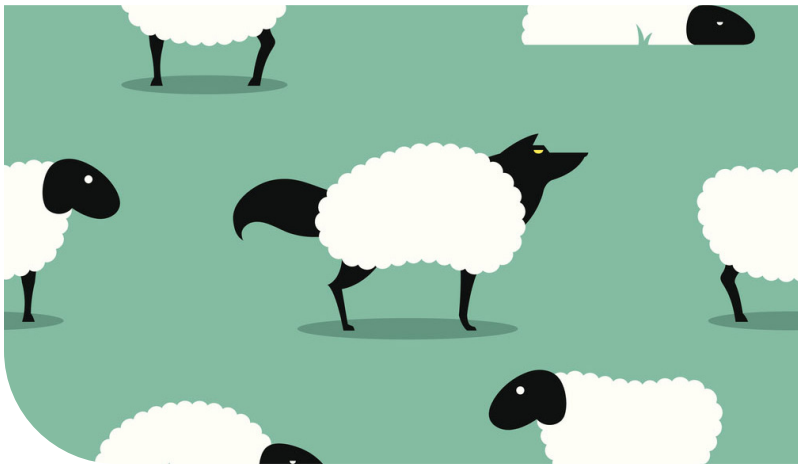
If someone calls claiming to be a person in the company an easy way of verifying if it is them would be to put the caller on hold and actually call the person from the staff directory that the caller claims to be. If you call their company phone and they respond, you can speak to them about the attack. If instead you reach voice mail you can listen to the voice of the person and compare it to that of the caller.

Companies should teach their employees about the practice of accepting people as legitimate employees just because they know what to say or know about the company. If someone knows this information it does not mean that they belong to the company, they must still be verified. Yet again, employees must be verified and no information, even if it is considered innocuous should be given to outsiders.

Just Asking for It: Problem

As group animals, thanks in part to how society functions, people are always looking out for each other and this instinct to help increases if the person requesting help is from the same company. This means a social engineer who has an aura of confidence may sometimes just straight up ask for what they want and worryingly they often get it.

To make this request seem more reasonable often the social engineer would use language that is specific to the field or the company. If the social engineer is entering the premises, they may also wear clothing that would fit in with the people legitimately working there.



Just Asking for It: Scenario

Alice works at a company where key cards are required to get through security doors. One day, as she had just scanned herself in and opened the door she looked behind her and saw a man she did not recognise, both hands full of coffee cups. *"Oh!"* he asked *"Please, can you hold that for me?"* as he started to move towards the door faster so she did not have to wait as long. Once he reached the door and Alice had made sure that he could get through she turned and went about her normal work routine. It now may be obvious, that the man in the brief example above is not someone who works at the company. Yet he has been given access

simply because he asked for it, this is such a common risk that almost everyone has done at some point.

If your company or building has a key card door just sit and watch it how many times will people just hold it open for others? Or ask yourself how many times have you held a secured door open for someone that you did not recognise? In the scenario above, the malicious actor entered the premises but often social engineers will avoid that as it increases the risk of discovery unless they are very sure in themselves.

> *How often have you held a secured door open for someone you did not recognise?*

Often important information is asked for over the phone and again it is often given. Here is another example scenario:

Ben works for a company where they keep a phonebook of all of the employees' phone extensions, names and job titles. At the end of each business year they update the information to account for changes in staff, and replace the book and shred the old copy. On the day of the new phonebook delivery Ben receives a call from a woman who says they have the new phonebook. She tells him that they are running late, and need to pick up and dispose of the old one - so she asks that he puts his old copy outside for it can be quickly be picked up. Wanting to be helpful, Ben complies and then a few minutes later a car pulls up. The woman walks out and picks up the phonebook that has *classified* written all over it.

Just Asking for It: Solution

Why does this bold approach work? Psychologically there is a lot going on and many papers and blogs have been written investigating the psychology of helping others.[5] To summarise and paraphrase these happenings it all comes down to the instinct humans have to be part of a bigger group, or pack.

The person who holds the door is also subconsciously thinking *"if this person sees me struggling in the future, they would help me as they will feel indebted"* this is how the norm of reciprocity motivator works. The second example triggers the kin selection model and the norm of social responsibility response, both of these revolved around benefiting the wider company or society. The thought process behind leaving a classified phonebook outside for a stranger is *"if I help this person do their job faster, the company as a whole will do better"*, yet it can be a major flaw in security.

image: Dima Pechurin on Unsplash

This is the boldest of cons and often the most successful, yet preventing this con still comes down to making sure that the person is who they say they are. These cons often use sympathy, guilt, and intimidation as a psychological trigger to get what they want. To prevent this the company and the employees needs to protect data; implement solid instructions about passwords; have a

central reporting point; and understand how to protect the company network.

Many of these attacks have data being sent to someone unknown to the user, even if it appears to be sent internally. The company needs to have a security policy that is very specific about sending valued data to anyone not known by the sender. When a request is made, there must be a strong procedure to verify the requesting party. Other ways to limit the impact of such attacks is to keep a departmental log of requests made. Meaning, that if one has been compromised the company know specifically what the social engineer knows.

The company could also train specific people to be trusted to authorise the sending out of sensitive information. By making only these people able to send sensitive information out of the company, the risk will be mitigated.

Image: CeruleanSon from Pixabay

Passwords are a common target of social engineers, and even changing a password for a few moments can lead to a security breach. Due to the modern use of passwords people have many accounts secured by password, yet because of the large number of different accounts for various things, people tend to use a single password for most of them. If this single password is compromised, then so is every other account they have. Training needs to cover the topic of passwords, when and how to change them; and what a strong password is. Users should be instantly suspicious of any request involving their passwords. This may seem like a very obvious message to get across, but users should also be told *why* it is bad to have a simple password, or the same password for all personal items, otherwise it comes across as following a rule in blind obedience. Often, rules requiring blind obedience are forgotten or ignored.

The name of a computer server or network must be considered sensitive data, a social engineer can use this information to gain trust or find the location of the information they require. It could also be used to bring the network down (and lead to *Causing and Fixing Problems*). People who provide computer help need to be well versed in what requests should bring up red flags. This links back to creating a central reporting point of specially trained staff who focus on deciphering whether a request is an attack or legitimate. By making this central point easy to contact, employees could ask a specifically trained member of staff to assist them if they suspected something amiss.

Phishing: Problem

One of the most well-known approaches to social engineering is a method called *phishing* where an email is sent, often to a large group of people, that hosts a malicious link or attachment which will infect any computer where a user clicks the link.

It was once the case that the typical phishing email contained poor English with spelling and grammatical errors - which made them easier to spot for those with an eye for detail. These emails were sent en-mass with the intention of only getting a small amount of return on the email, this is obviously an inefficient method of get information. However, these phishing emails are becoming more and more sophisticated. They may often have imagery which represents a service that you subscribe to,

such as a bank, or email provider, indicating your account is locked or compromised. They will often contain a link for you to *'Reset your password'* on a fake website made to look like your bank, or email provider etc. These can look very convincing, and prey on the fear that your account has been locked. Unfortunately, as you enter your details in the webform, you are unsuspectingly giving your login/password credentials to the social engineer.

Recently, a new type of phishing has become more prevalent, this is known as *spear phishing*, which focuses more on making the email more personal and directed at specific people. For this attack, the social engineer does a lot of research and employs various techniques to obtain personal data about the target, so that their crafted phishing email appears to be far more legitimate, and therefore more likely to succeed. A common source for such personal data is actually publicly available. Consider how much could someone find about you simply by looking at your social media, or searching for your name online?

> *a new type of phishing has become more prevalent, this is known as spear phishing*

Phishing: Scenario

The subject and body of these emails often contains urgent reasons to act:

- Account had been suspended
- Confirm account ownership
- Your card will be disabled etc.

This is designed to panic the person reading the email. Once the reader feels rushed, they may click on a link provided and while this may look legitimate in the email, the software allow for the renaming of hyperlinks to display safe looking site while directing you to another. e.g: https://www.google.com/update could actually link to the malicious site: http://I.AmStealing.Your/Information

image: Melinda Gimpel on Unsplash

In other cases, if the social engineer does not want to spend extra time and effort to disguise a link, they may use one that looks very similar to the website the email claims to be from, i.e. www.paypa1.com at a quick glimpse this says *Paypal* but in reality the final 'l' has been replaced by a '1'. Looking more specifically at the psychology behind this method, the urgent subject line or body content initiates the human *fight or flight instinct* where logic and rational thinking is put to one side and replaced by the instinct or a need to act, quickly. This often will mean that the recipient of the phishing email will be paying less attention to the detail, and be focusing on the need to fix a bad situation. They click on the malicious link and put their system at risk. Instinct is easier to predict, which makes people easier to manipulate and thus leads to more successful cons. In the Paypal example above, if you feel the urgent need to act you are less likely to notice the l/1 swap.

Phishing: Solution

Phishing is the most common form of attack in the modern era of computing, due to the sheer amount of email communication that people do daily. However, there is also a wealth of information available to help guide you and your organisation. We would recommend starting with the NCSCs resources on the subject of phishing: https://www.ncsc.gov.uk/guidance/phishing

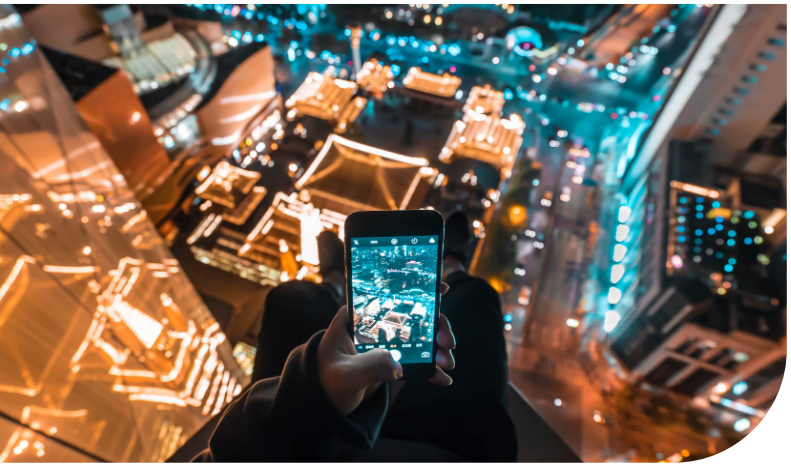


Image: Yiran Ding / Unsplash

The key things to keep in mind while looking at emails; protect your personal information, do not click links unless you have checked where they lead, look for common phishing language, and any mistakes in spelling or grammar.

It is good to be suspicious of all emails sent from entities that require sensitive data. If an email is received informing you that there is something wrong with an account, the safest thing to do would be to not follow the link in the email. Instead, open a browser and navigate to the trusted home page of the entity and log in there. If there is something wrong with an account then it may be legitimate and the actual website would say so, or phone up the company using their official company phone number. Here, enquires could be made about your account and if it is actually in need of action.

As a general rule of thumb never click links from emails, it is very easy to disguise a malicious website as a trusted one. In most email readers if you hover over a link, at the bottom of the screen will be the directed address which may be contrary to the website the link claims to be.

Another thing to look out for is typical phishing language. Most emails intended to scam will try and convey a sense of urgency so that the receiving party rushes to act not fully paying attention to the links or the message of the email. A key give-away for phishing emails is if they aren't addressed to a person directly rather, `Dear Customer' or similar. Also in phishing emails, less so in spear-phishing emails, there are commonly spelling mistakes and formatting errors, where legitimate businesses would not have such errors.

> *Phishing is the most common form of attack in the modern era of computing.*

It used to be the belief that if a website has a padlock next to its name in the browser it is secure, but this is no longer the case if you are suspicious of a website but it has a padlock click on the icon, it will tell you the name of the organisation that applied for it. If these do not match, leave that website and remain very suspicious of the email or site.

Summary

The social engineer makes use of many psychological triggers and methods of attack to gain access to information or credentials. Social engineering attacks are actually quite preventable, all that is required is to have an

Wrapping it All Up

understanding of the methods they use and knowledge of what to look out for.

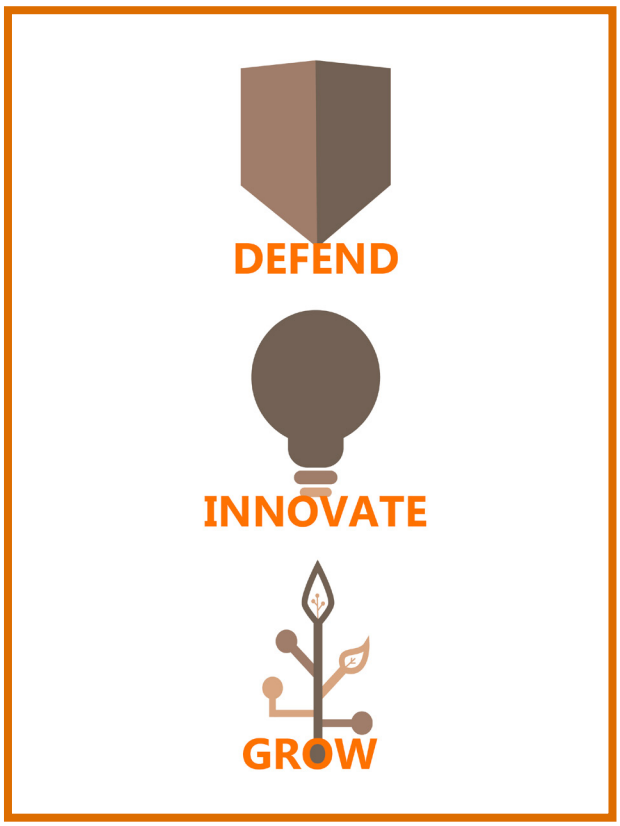
The social engineer has a lot of techniques at their disposal, this article has covered a few of their methods for attack as well as some ways which you can prevent these. It is important to bear-in-mind that while the social engineers will use combinations of all the above methods, and more, to achieve their goal.

Most readers of this article would have themselves believe that they would not fall for such simple tricks, yet studies[7] have been done to show the majority of people will fall for these methods even if they have been warned about them in advance!

This article concludes with four ways to improve security against these types of threat:

- **Increase Awareness** - Show people how to recognise the tactics used and how to react
- **Repeat Training Regularly** - Repeat the training using different approaches and materials.
- **Tackle and Reduce Optimism Bias** - Stop people from thinking "I am less likely to be targeted" or "I am better at resisting these attacks"
- **Focus on Vulnerable Groups** - Often young and recent hires are the most at risk provide training during job induction.

The easiest way to prevent any kind of social engineering attack is to verify the caller. If a company has a strong identification procedure or uses multi-factor verification, attacks become much harder to carry out. The addition of a trained team or specific individuals who are in charge of whether information is sent outside of the company would also add another layer of security. Additionally, constant reminders about methods of attack to employees will aim to make sure that the workforce are always aware of possible threats.



Further Support Available

The Greater Manchester Cyber Foundry runs a Secure Digitisation Programme designed to support businesses facing cyber challenges in the Greater Manchester. The programme consists of two full-day workshops, alongside some online open learning elements, to better defend, innovate and grow your business. The support is free due to being part funded by the European Regional Development Fund, and is in partnership with Lancaster University, the University of Manchester, Manchester Metropolitan University, and Salford University.

To find out more contact us:

gmcyberfoundry@lancaster.ac.uk

Further Reading

About the Author

Alexander Lee is an analyst developer on the Greater Manchester Cyber Foundry project. Having recently graduated from Lancaster University with a master's in Physics, Alexander has always enjoyed software development building multiple physics based simulations. Alexander is also a part time magician, which sparked an interest in human psychology and how to use it to influence others

Lancaster University

READ MORE

1. **The Art of Deception - K. Mitnick** *[Mitnick, Kevin D., and William L. Simon. The art of deception: Controlling the human element of security. John Wiley & Sons, 2003.]* – Written by one of the most infamous social engineers of modern time this book covers over 10 different approaches of the social engineer with entire sections dedicated to security procedures that business could adopt to prevent future attacks.
2. **Advanced Social Engineering Attacks** - *K. Krombholz, H. Hobel, E. Weippl [Krombholz, Katharina, et al. "Advanced social engineering attacks." Journal of Information Security and applications 22 (2015): 113-122.]* - A short digestible article describing common attack scenarios, as well as real-world examples. Aiming to classify the different types of attacks.
3. **Steps to Avoid Phishing Scams** - *Comodo Security Solutions [Comodo Security Solutions, "What is a Phishing Scam?" COMODO, 26 February 2020, https://www.comodo.com/resources/home/how-to-avoid-phishing.php]* - A short but comprehensive list of steps to take to avoid the most common type of scam.
4. **Social Engineering: The Art of Human Hacking** - *C. Hadnagy [Hadnagy, Christopher. Social engineering: The art of human hacking. John Wiley & Sons, 2010.]* - A book aiming to reveal and dissect the technical aspect of social engineering attacks as well as providing examples and detailed accounts of methods used by the social engineer.
5. **Social-influence processes of control and change: Conformity, obedience to authority and innovation** *[Martin, Robin, and Miles Hewstone. Social-influence processes of control and change: Conformity, obedience to authority and innovation. London: Sage, 2003.]*
6. **Introductory Guide: Phishing** *[Joinson, Adam. "Introductory Guide: Why Do People Click On Phishing Links?" CREST, 26 February 2020, https://crestresearch.ac.uk/resources/introductory-guide-phishing/.]*
7. **Social Engineering From Thoughts To Awareness.** *[Bullée, Jan-Willem. "Social Engineering: From Thoughts to Awareness" CREST, 26 February 2020, https://www.crestsecurityreview.com/article/social-engineering-from-thoughts-to-awareness]*
8. **A study of social engineering in online frauds.** *[Atkins, Brandon, and Wilson Huang. "A study of social engineering in online frauds." Open Journal of Social Sciences 1.03 (2013): 23.]*

Copyright: This guide is made available under a Creative Commons (CC BY-NC-SA 4.0) licence.

For more info about GM Cyber Foundry: https://www.lancaster.ac.uk/security-lancaster/cyber-foundry/

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University

MANCHESTER 1824
The University of Manchester

Manchester Metropolitan University

University of Salford MANCHESTER