Social Engineering – How strong is your human security?

Haider M. al-Khateeb and Mitul Shukla

Rationale
The idea of this section is to let the reader get an idea of what is meant by social engineering and what can be done about this type of ‘attack’. In essence, social engineering is an umbrella term which here encompasses those acts perpetrated through lying, manipulation, persuasion, impersonation, misdirection and deceitfulness in order to gain the social engineer’s objective. If you think of how a con-artist works, then you have a good idea of a form of social engineering.

Those who employ these techniques are often skilled in their use and have a good understanding of how certain psychological traits can be leveraged against other people. Social engineers know what to look for and they are usually trained (or train themselves) to deceive people in order to collect valuable information. Being aware of how these types of attack can be used and what can be done to defend against them will enable you to form the basis of a robust defence. You should keep in mind that social engineering attacks may target those around you who may also have shared knowledge that you may want to keep private, such as your mobile phone number or where you are on a given evening.

For the purpose of this text we will assume the goal of the social engineer is to gather information about you and/or steal something of yours.

Why would social engineering be used by a cyberstalker?
Social engineering is simply a name given to a set of persuasion techniques and is often used as the most straightforward way to gain a given objective. From a general security perspective it is often said that people can be the weakest point in a system, after all exploiting human psychology has been effective and proven through history. Books such as ‘The Art of Deception’ or ‘The Art of Intrusion’ both by Kevin Mitnick demonstrate how social engineering can be used.

Even tech-savvy and well trained people can be susceptible to this form of attack, humans are not always alert to the consequences of what they share. Sometimes we are simply not mindful when answering a call or clicking on a link to a website from an email.

How might social engineering be used?
We should keep in mind that social engineering need not be only physical in nature - that is to say the social engineer may not be present in person. Take for example an office worker finding a lost USB memory stick found in a communal area of their building. This diligent individual may well take the memory stick to their office computer and plug it in to try and ascertain to whom it belongs. In this particular instance the memory stick may have been left in the communal area as that is
relatively easy area to gain access to. The memory stick being one that is loaded with all manner of stealthy software that will give the Social Engineer access to that particular computer or the network it is on from a remote computer at a safe distance.

A social engineer may also take a more direct attack, let us say in the same office environment. One technique used is called ‘tailgating’, which is essentially following a group of people. In this example the social engineer may have studied the office staff for a while, possibly even creating a false identity badge for themselves if necessary. They would dress in a similar manner to other workers and then simply follow a group of people returning from their lunch break. Once in, they are less likely to be challenged and can then go about gathering further information. Or they may then wish to leave surveillance devices in your office, for example by adding a keylogger* to the back of your computer. Another approach would be to disguise themselves as a printer repair technician, gain access to the workplace, make their way to the printer used by you and steal or copy the hard-drive from that printer. Most modern printers use hard-drives in order to store documents about to be printed and is likely to contain all of the most recent documents sent to that device irrespective of if you have deleted the document from your computer.

Above examples might be somewhat extreme which are possibly more suited to corporate espionage but keep in mind that these attacks have and continue to happen. We should also keep in mind that the better someone already knows you, or is thought to know you, the easier it becomes for them to gain further access or information.

* A keylogger can be software or hardware. Essentially they record your keystrokes as a minimum capability. For the software variety, someone would need to be able to install it on your computer. For the hardware keyloggers, someone would need to have access to the wiring around your computer. Further information on these can be found in the section on ‘How you can protect your computer and mobile devices from malware and data theft’.

**What information is a social engineer interested in gaining from you?**

Mainly confidential information such as passwords, location, contact and personal details but also less questionable information they can use to conduct a well-planned social engineering attack. For instance, a social engineer could find it useful to learn your browser or PDF viewer version over the phone in order to find technical vulnerabilities, or to identify/verify your insurance company to create a personalised phishing email.

**What methods might social engineers use? And how can you resist social engineering?**

Typically social engineers will have a number of approaches that they rely upon to meet their objectives, some of these have already been discussed but more are highlighted here. Information gathering is usually the first step. This might be done entirely online using search engines like Google or more directly using ‘elicitation’ to gather information from you directly or from those who know you. Elicitation is basically a means of finding out information based on the response to a line of questioning and is often used with the drawing logical conclusions.

A number of widely used social engineering methods are summarised below followed by practical countermeasures and advice for your reference.
Phone phishing

Let’s say Mr. Smith gets a phone call, “Hello, is that Mr. Smith?” is asked by the person on the other end. This question plays a dual role, on the face of it the question allows a kind of pretext for the rest of the conversation. But equally it has also confirmed for the caller that this number belongs to Mr. Smith which may be valuable for them to know for a number of reasons. Cold callers for marketing purposes will often employ this technique in order to confirm that their database is correct and current – this is often sold on to others. Further, simply the act of answering that call allows the other party to know the line is live and used, this approach is often used when it comes to mobile phones.

If you do answer a call like the one described, you can take the following approach to assess and possibly authenticate the call. Rather than answering their question, simply ask one of your own – such as “May I ask who is calling?” This neither confirms nor denies your identity and put you in a better position to assess whether or not you wish to continue the call. You would have however, as mentioned, confirmed the line is in use.

Nevertheless, the number that appears to be calling you (also known as Caller ID) can be easily forged. This does not require advanced skills and can be handled with minimal cost and effort via many internet calling services (also known as VoIP providers), mainly because they provide their customers with an option to customise what should appear as their Caller ID.

Key points to remember:
- Take the phone number of suspected calls and offer to call them back.
- Check that the number is actually owned by that party using a phone book or their formal website
- An online search (e.g. using Google) can help you to verify the number and check whether it has been reported earlier as spoof.
- It is a good practice to consider what questions are being asked. For example, why would a salesman ask you to share which technology you use? Perhaps, it is fair that they pass on their offer as is.

Trojan horses

Are you familiar with the ‘Trojan Horse’ trick used by the Greek to enter the city of Troy? They built a big wooden horse with selected number of soldiers hiding inside, the army then faked a pull back from the war. The people of the city took the wooden horse as a victory trophy inside their well-protected city and celebrated. At night, the Greek soldiers made their way out of the wooden horse and opened the gates for the army to enter the city and win the war.

In computing, trojans horses are very similar. They are malicious malware contained within a safe-looking item such as an email attachment sent to you seemingly from someone you might know, this attachment can look like an image or a Word document. To make his further complicated, it can indeed be an image you can view, but the malicious code is nevertheless inside. A Trojan often creates a backdoor to enable unauthorised access to the system.
Protection against Trojan horses as a type of malware requires an anti-malware software and you to follow safe-use guidelines, these are disused in the chapter titled ‘How you can protect your computer and mobile devices from malware and data theft’.

**Phishing**

Phishing, is a known –quite technical- social engineering technique where web technologies are utilised to illegally obtain sensitive information. In a typical phishing attack, users are sent an email guiding and convincing them to click and follow a hyperlink pointing to a login page, an online form or to reply the email and share certain detail. A phishing page is designed with the look-and-feel of a genuine service while it is -in reality- a ‘clone of the original’ hosted on the attacker’s server.

Phishing emails and pages can be very believable and continuously becoming more difficult to identify, research surveys shows millions of adults losing money due to Phishing attacks each year. Similarly, a cyberstalker could utilise this technique to effectively recover information about you, unless of course, you develop the necessary awareness about this challenge.

A phishing email could be written to clone a message coming from known services you use such as Facebook, your bank, Paypal or your insurance company. Many phishing scam captured in the wild are written to target as many people as possible, they are therefore not personalised to an individual. This could be one of many signs to suspect a malicious email. However, in the case of a cyberstalker, attacker’s effort is focused on an individual and such emails can be written carefully and addressed to the recipient as expected from a genuine service.

In a very sophisticated attack, when the attacker has excellent technical knowledge, clicking a phishing URL (even if you do not interact with that new page) is enough for the social engineer to collect technical information about your browser and get your IP address and location. Similarly, the same details can be acquired if the email sent to you includes images loaded from the attacker’s server. For this reason, email providers usually give you an option to configure your email client to ask before displaying external images. However, a service such as Gmail, protects you from this, they automatically save these images on their own servers before showing them to you instead of letting them load directly from an external link.

*Key points to remember:*

- Avoid clicking hyperlinks from within emails or on popup windows

Instead of clicking hyperlinks, direct your browser to the main website manually or use bookmarks to open websites you use frontally, if you suspect someone has altered your system, examine the URL very carefully.

Similarly, do not to click hyperlinks on popups and carefully examine advertisements on social media. Pay extra attention when visiting a ‘Download’ service, they usually contain advertisement links mocking the download button, many of these directs you to download a malicious executable file (filename with the .exe extension)

Some malicious websites prevents you from closing their pages easily, try using the right buttons **CTRL + F4**. If that did not work either, then try **ALT + F** to close the browser and start fresh.
Examine the address (URL) of the website you visit.

Verify that the spelling and structure refer to the exact domain name you expect to access. For instance, http://paypal.papal.co.uk belongs to ‘papal.co.uk’ and not the known ‘paypal’ payment service, the word ‘paypal’ in this example is a name of a folder within the hierarchy of the given URL and it was used to give the impression you have visited paypal.

It is also a good technique to reach the website through Google, e.g. type in Gmail in the search engine and follow the link documented by Google which also has a feature trusted websites and addresses you have visited before.

Learn how to recognise secure connections.

Secure services and login pages has URL starting with HTTPS:// (note the letter ‘S’ at the end), this shows the connection is encrypted and that the domain has been authenticated, question whether the service you are using requires this feature to protect your session. Also, do not bypass browsers warnings relevant to ‘Certificate Errors’, it means, the website you are trying to access could not be authenticated as genuine.

Activate the SPAM filter provided by your email service provider, this is not always activated by default.

Do not respond to emails, social media messages and text messages with suspicious intentions. Your email reply will contain further detail about your email system including but not limited to your service provider and approximate location.

Always remember that a legitimate company dealing with sensitive information such as your bank will most-likely never email or call you to share or confirm sensitive information.

Plan to independently verify emails with the company if the matter sounds important and you suspect it can be real.

Keep your browser up-to-date

Use anti-phishing toolbars and other internet security tools, this is discussed in details in the chapter titled ‘How you can protect your computer and mobile devices from malware and data theft’.

Question the attachments you receive. Have you expected them? Do not trust an attachment because it came from a person you trust, remember, emails can be forged to appear as if they have been sent from someone you know.

Fake IDs

Fake IDs can be used both online and offline to gain unauthorised access to restricted areas. A social engineer could create a Facebook profile (or any similar social media accounts) and pose as someone you know. Accepting their request gleans private profile information to them. Similarly, a fake LinkedIn profile can pretend to be from a recruiting Agent or a professional active in an areas of interest to you. Using false IDs in real life is more risky to the social engineer and can as well be much more risky to you, make sure you confirm identities before you give access to your environment especially when you are alone.

Key points to remember:
Question the identity of the person sending you online requests, you can always play safe and attempt to confirm this using a second channel of communication you have such as emails and phones.

If you do not know the person (e.g. Recruiting Agent), confirm their role with the company they claim to work with. This step is more critical when physical access is requested, if the person claims to be from the Gas Company, ask them which company they work for, ask for an ID, look at their custom and car, and you could also confirm their visit with the company through phone. If a phone confirmation is not possible, ask them to inform you in advance for any visit.

Exploiting someone you know or deal with
It is not necessarily that you are the direct target of this attack, it is possible that any party holding information about you is targeted with social engineering techniques. This may include your family, friends, colleagues or a service provider you use.

- Talk to friends and family, if they are close enough, share with them to be alerted every time they share details on your behalf
- Have a look at the procedures adopted by service providers you use e.g. Gym do they have a policy strictly followed to maintain your privacy?

What other countermeasures should you consider to mitigate the damage of social engineering attacks?

- Always give yourself time to think, try not be pressured into responding to ‘urgent’ enquiries.
- Become vigilant and assess and authenticate communications.
- Do not share access control details, such as logins, passwords or PINs with anybody; they may become the target and might be more vulnerable than you are.
- Have a plan to dedicate some accounts/numbers for work while creating private ones for your personal life and close people and family
- Reading about common tricks, helps to increase your awareness. Your stalker is not necessarily a professional social engineer and they might very well repeat old tricks written somewhere.
- Do not respond to a warning from a program you didn't install or do not recognise even if it claims to protect your PC or offers to remove malware. It is highly likely to do the opposite.

What could you do if you suspect or identify a social engineering attempt?
If you recognise a potential phishing attack, it is a good idea that you move this email it to a separate folder (created for this purpose) within your mail system. This will allow a digital investigator to examine the email later in case you decide to report your case to the police. More on maintaining digital evidence in the chapter titled ‘How you can preserve digital evidence and why it is important’. Nevertheless, you can choose to report online fraud to www.actionfraud.police.uk and your service provider.