Defense Methods Against Social Engineering Attacks

Chapter · January 2018

DOI: 10.1007/978-3-319-58424-9_35

2 authors:

Jibran Saleem
Manchester Metropolitan University
4 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Mohammad Hammoudeh
Manchester Metropolitan University
94 PUBLICATIONS **636** CITATIONS
SEE PROFILE

Defense Methods Against Social Engineering Attacks

Jibran Saleem*, Dr. Mohammad Hammoudeh
Manchester Metropolitan University
jibransaleem@gmail.com
m.hammoudeh@mmu.ac.uk

Abstract

In this chapter, multiple Social Engineering defense methods are comprehensively reviewed. Focus has been placed on examining data, which supports the hypothesis that security awareness is one of the key strengths one can develop, to assist themselves and others, in avoiding and countering increased Social Engineering attacks in this day and age. Various case studies have also been analyzed and evaluated, which demonstrates positive impact on the security outlook of employees, once continuous and sufficient security training is delivered. Evidence of effective counter-techniques have been gathered using a variety of sources, all of which can be employed by businesses and individuals to deter and prevent Social Engineering attacks from taking place.

1.1 - Defense Against Social Engineering Attacks

Social Engineers have the potential to cause some serious damage to their victims. This damage can be social, economical, or reputational. It is now, more than ever, vital to understand what precautions can be taken to prevent, alleviate, and contain the devastation that can be potentially caused as a result of a Social Engineering attack. This section thus outlines the common Social Engineering mitigation strategies that companies and individuals can employ to protect themselves from potential Social Engineering attacks.

1.1.1 - Physical Security

For any security-conscious business, a strong physical security must be enforced throughout the organization, without exception. If security is lax, attackers will have little trouble accessing the stations they need in order to launch their digital attack. In addition, once clear and concise security policies are established and implemented, they should be periodically tested in order to determine the state of security awareness among staff members. This is imperative to identify and resolve any potential gaps. It is equally important for members of staff to be contin-

ually reminded that the possibility of an attack is indeed real; it can occur at any time, without warning. Commenting on this issue, Kevin Mitnick asserts:

"People generally don't expect to be manipulated and deceived, so they get caught off guard by a Social Engineering attack." [1]

It is good practice to maintain signs throughout the premises, reminding employees not to plug-in any USB drives or any other digital device they find around the premises. Instead, they should submit them to the relevant department for expert analysis. In addition, they should be vigilant and report any suspicious behaviour to security, no matter how minor they perceive it to be. It is also a good idea to have employees acknowledge and sign a 'reminder of best security practises' each month.

Physical security could be bolstered with comprehensive CCTV coverage, coupled with a clearly defined human perimeter defence space on the premises. Installation of protective physical barriers, security lightings, alarms, motion detection systems, and the use of biometrics to identify employees could go a long way in protecting a business from a potential attack. Michael Erbschole states the following on physical security:

"The bottom line here is, no matter how good cyber security is, if an individual can walk in to a facility and gain access to systems, that individual has in effect circumvented cyber security defences." [2]

With sufficient physical controls in place, it may be possible for a company to repel a substantial Social Engineering attack. However, without implementation of strict physical security protocols, the company is effectively keeping their doors open to unauthorised visitors with malicious intent. They have free reign to visit and intrude the premises, offload malwares, Trojans, spywares, and circumvent the controls to access the desired data.

1.1.2 - Internal/Digital Security

Another logical step that should be taken in the fight against Social Engineering is the rolling out of a series of digital protective services and software tools. This should be implemented to negate the risk of attacks. It is also worth mentioning that although the use of digital security services may be effective in combatting certain types of Social Engineering attacks, they may turn out to be completely useless in other types of attacks. For example, a reliable spam protection guard with an updated blacklist, compounded with an antivirus/malware protection and a good firewall, may go a long way in protecting a company from phishing attacks.

With the above being said, these measures will prove to be completely inadequate against physical baiting or tailgating. This does not necessary mean that enterprises should not invest in software protection mechanisms, because they provide partial protection nonetheless. In protecting digital data and assets, the more security measures are undertaken, the better. Explaining the severity of complications that may occur if businesses are not using digital protection mechanisms, Charles elaborates:

"… some TEISME's (Technology Enabled Information Small Medium Enterprises) enable intruders to gain 'system administrator status', download sensitive files such as passwords, implant 'sniffers' (what is dubbed here as Internet dogs or spyware), to copy transactions, insert 'trap doors' to permit easy return, or implant programs that can be activated later for a variety of purposes." [3]

To negate some of the risks listed above, utilizing sandboxing mechanisms can be very productive. Sandboxing is the creation of an isolated virtual machine, use of which will protect the network from propagative malwares. It has a tendency to spread itself over the domain, even if an employee inadvertently plugs in a compromised USB flash drive into their computer. Use of sandboxing against some visual deception attacks is so effective, that some popular browsers [Chromium [4], Firefox [5]) have built in sandboxing technologies in order to prevent exploitation through internet browsers.

In 2010, Long Lu and his colleagues developed and tested an interesting browser-independent concept OS. The system named BLADE [6], which stands for 'Block All Drive-By Exploits' focused on preventing automatic unauthorised execution of binary files on the system. Drive-by downloads occur when a direct connection to the compromised website takes place, resulting in the installation of a malware without web user's authorization.

By taking the unconsented execution prevention approach, the author of the OS developed BLADE as a kernel driver. This kernel extension allowed the system to enforce a rule that barred any executable files on the system that did not have explicit user consent. Any downloads that do occur are directed to a sandbox where they are held and await further instruction from the authorised user. During the initial evaluation stage, the system preformed at 100% efficiency, prohibiting all 18,896 drive-by download attempts from compromised websites. There are no further updates on the project since the last preliminary evaluation. This indicates that the project did not materialise, possibly due to lack of funds or resources. Nevertheless, it remains an excellent concept; if it was made into an open source and was developed further to cover all executables, not just the ones downloaded from browsers, it could serve as an excellent tool to protect the system from technical manipulative tools used by Social Engineers.

Other dedicated measures can prove to be very effective mitigation strategy against Social Engineering attacks. Such measures include proactive monitoring, aggressive user authentication/accounting, and use of targeted machine-learning and analysis algorithms. Normal system behaviours can be observed, and it can self-educate to distinguish between legitimate and illegitimate user actions and data/packet inconsistencies. Machine and behavioural learning systems in particular have become so efficient that they are capable of detecting and stopping sophisticated Social Engineering attacks such as Spear phishing.

A group of tech enthusiasts led by Gianluca and Olivier [7] developed a vector machine-based learning system, which has the ability to identify and block spear phishing email. The authors describe the system as working by monitoring user habits and developing user profiles. The profile is based on the user's writing style, use of punctuations, character recognition, word frequency, inbox email content, usual times of email receipt and delivery, and other parameters. Once the profile is developed, it is updated every time an email is sent or received. When the algorithm reaches a prime state, it takes over and blocks every email it deems to be a spear phishing attack. The authors claimed to have achieved a false positive detection rate lower than 0.05% in the final evaluation stage, which is a remarkable achievement considering the diversity of content that can appear in a spear phishing attack email.

The internal security mechanisms described above, as well as many other security solutions available through online specialist vendors, can serve as a powerful shield that can be used to protect businesses from Social Engineering attacks. Upon implementation, these solutions may require continuous manual monitoring. An example of this may be daily, weekly, or monthly analysis of the detected and blocked attacks. Such procedures are necessary to ensure legitimate connections are not being unnecessarily stopped.

These digital protective measures may block the first few attempts made by Social Engineers. However, businesses must understand that Social Engineers and hackers are devoted to finding exploits, often dedicating their full time 'occupation' to doing so. This is especially the case if they have identified a good motivation to hack a particular company. The system may be able to block certain number of attempts, but then the attacker might gain an upper hand and find a technical exploit, allowing them the access they require. By continually analysing attack attempts and upgrading the infrastructure accordingly, businesses can better protect themselves from these attacks.

1.1.3 - Implementation of Efficient Security Policy and Procedures

Due to the ever-changing dynamics in today's IT world, it is crucial that the managers and employees alike are aware of their company's current security polices and procedures. The security policy contains procedures and guidelines that dictate data and asset protection methods of an organization. It is imperative to have a concise and clearly defined set of rules for maximum efficacy, and these rules should be available to all employees, irrespective of rank. That being said, the policies should also be protected from unauthorised access that could help the attackers gain insight into the inner workings of a company. The lack of a clear security policy can, in effect, become the cause of overwhelming non-compliance among employees, leading to successful attacks and fines from authorities.

Mitnick has written comprehensively on the utility of a well-researched security policy. He has an extensive and dedicated chapter in his book, the art of deception [8], aimed at policy writers and researchers. On the importance of having an organised and coherent security policy, Mitnick notes:

"Designed at lowering exposure to semantic attacks, well-maintained policy and organizational procedures help to mitigate and significantly lower the risk of a potential exploit occurring, without relying on the technical capabilities of users." [8]

The above statement makes clear that not only are the security policies important for a company's survival, they are an integral tool in protecting the employees from any potential harm. Therefore, it is of paramount importance for the managers to be aware of any change in the company's security policy. It is also their responsibility to ensure that the changes are communicated to their employees, and that they are implemented consistently across the board. In a survey paper published in December 2015, Ryan and George write:

"Policy and procedures need to be flexible to unknown and unforeseen attacks and, therefore, appropriate to the changing threat landscape. Fixed guidelines can quickly become out of date as new attack methods are constantly being developed." [9]

We have thus learned that one of the greatest benefits of enforcing security policies and procedures is that it not only protects the company from intruder attacks, but also from potential lawsuits. Examples of which include policy on data pro-

tection, prohibition of business related information on social media, and policies on the use of BYOD (Bring Your Own Device). Such procedures can prevent lawsuits that may arise in case of a successful attack and crackdown from local authorities due to business non-compliance.

A well-maintained and regularly updated policy is the end result of compressive research, updated laws, and lessons learned from previous attacks. It is derived from policies of other successful businesses in the same industry, and can result in greatly reduced security risks.

Implementing security policies is directly related to computer use at work. An employee wilfully accessing a compromised website, or a victim of a phishing attack, will put the enterprise at risk due to their workstation being connected to the network. Potent and effective computer access and authorization policies, along with competent firewall and robust and reliable enterprise antivirus, should be sufficient to put a stop to any inadvertent exposure to potential harm to the company's IT infrastructure.

1.1.4 - Penetration Testing

When a company has employed enough security measures and feels confident that it has protected itself from an attack, it is still a good idea to search for a second opinion from an established and professional penetration tester. The primary purpose of a penetration test is to determine technical vulnerabilities and weaknesses in the network, systems, and applications being used by the business. As well as testing the resilience of the company's digital assets, many firms that test penetration also offer their services to determine the security outlook of business employees.

By employing the same tactics as a malicious Social Engineer, but with the company's consent, an official penetration tester will attempt to access the system by human manipulation, direct hacking, or use of other tricks. Such tricks range from telephone pretexting and phishing, to bating, tailgating, and other browser-based exploitation attacks. Once the simulated attack is completed, the firm leading the attack presents the employer with a report detailing the vulnerabilities identified, probable causes of weaknesses, and remedial strategies. The business can follow up on the feedback to patch-up the identified fragility.

If the focus of simulated attack was internal employees as well as infrastructure, then the company may also discover which human manipulation technique was used to gain access to the desired information. The information obtained can be very useful in hardening the network and employees in preparation for a real life attack. Commenting on the importance of penetration testing, Steve notes:

"Its not enough to secure often and update often, though these two items certainly go a long way towards ensuring a secure environment. Another basic point of security in depth is to test often. Testing ensures that the security policies are being enforced and the implementation of those security policies is successful." [10]

In today's age, there is an unprecedented complexity and frequency of attacks targeting businesses, and with the exponential growth of cyber-led criminal activity, it is ever more important for businesses to take every security precaution available to them. Steve's abovementioned statement clearly emphasizes the utility of having an updated and secure system. It is also clear from the remark that penetration-testing allows companies to identify weaknesses in the day-to-day implementation of the security policies.

It is reported by Navigant that the average cost of security breaches in 2013 was $6,200,200 [11]. Navigant also reports that Cenzic Security's testing performed in the same year led to the discovery of technical flaws in 96% of the cases. An average loss of $6,200,200 is a substantial amount, whereas security testing would only cost a fraction of this amount. These incredible statistics provide every reason for security-conscious businesses to develop the habit of undergoing regular penetration tests.

Further research indicates that more than half of all UK businesses have been hit by a ransomware attack in 2015 [12], a malicious program that is commonly transmitted through phishing attacks. A separate study shows that one in five UK businesses hit by ransomware attacks are forced to close [13]. This due a variety of reasons, ranging from high ransom demands, to loss of data, negative publicity, and lawsuits.

To defeat the cancer of cybercrime, companies must go above and beyond normal business practices to stay on top of the game. The security challenges in today's digital world are dynamic, daunting, and convoluted to say the least. Therefore, robust cyber security and continual testing of infrastructure and employees should be a company's top priority. A holistic and comprehensive strategy that deals with risk management, cyber security will help businesses go a long way in protecting themselves from the dangers of cybercrime and Social Engineering attacks. With the aid of automated technology, vital security gaps can be identified and dealt with accordingly.

1.1.5 - User Training and Security Awareness

People are more easily accessible and exploitable than machines, and thus the human element in businesses remains most vulnerable to Social Engineers. Policies than ensure strong passwords, two-factor authentications for work login, top of the range firewalls, and IDS, are all made redundant if employees do not appreciate the importance of maintaining the safety of their pin, passwords, and access cards. A company's security is only as strong as their weakest link, which in this case is the employee.

Since the inception of modern technology, social Engineers and hackers have understood that the human link in any technological equation is always the most exploitable element. Humans are the mouldable key that can be easily manipulated to gain entry to any network, system, or data. As such, the trend to access targets by 'technology only' is changing. Obtaining information from someone under false pretences, manipulation, deceit, and coercion is now conventional. The following quote aptly summarizes the rationale behind the increased number of attacks on employees as opposed to infrastructure:

"Why waste your efforts on cracking passwords when you can ask for it" - Unknown

In essence, the most effective mitigation strategy when dealing with Social Engineering is education. With periodic and systematic security training and frequent reminders urging the need to stay on guard and staying vigilant against suspicious behaviour, businesses can effectively turn their weakest link in to the strongest. It is vital for employees to understand the significance of protecting sensitive information, as well as the importance of knowing how a Social Engineer might strike. With a greater awareness, they can develop the knowledge of various attack vectors and establish the capability to differentiate between a dispersed or a direct attack. Employees can learn that a Social Engineer will not directly ask for a code; they will not blurt: "Give me access code for the server room, please?" Rather, they will tie little pieces of information they have acquired over time, decipher cues and signals given to them by multiple employees, and then connect the pieces of the jigsaw puzzle to unearth the information they have been after.

The single most important measure that can protect the company from a Social Engineering attack is a *continued* awareness program on information security. The word "continued" is purposefully stressed; a recent study [14] found that after attending a business training session, employees in general tend to forget 50% of the information in an hour, 70% in 24 hours, and 90% in a week. So although preparatory work for training as well as the actual delivery itself can be manually intensive and costly, it is nevertheless the necessary plunge that companies must take if they wish to fortify themselves against Social Engineering attacks.

Guido Robling, a respected name in the field of academia with over a hundred publications to this date, holding numerous academic awards, presents this comment on the significance of security awareness:

"Only two things really help against Social Engineering: awareness and vigilance. Users need to know about Social Engineering, how it works, and be on alert when "strange" phone calls or emails occur." [15]

The message Guido is trying to deliver could not be anymore clearer; absolute security can never be guaranteed, but by playing smart and educating employees on security awareness, companies can turn their ignorant workers into educated and resourceful watchmen. In essence, employees are turn from liabilities into assets.

1.2 - Analysis of mitigation strategies

In the section above, the five different strategies that firms can employ to protect themselves from Social Engineering attacks have been presented and discussed. Here, the objective is to elaborate further on the most effective and useful approach that can truly turn the tables on attackers.

1.2.1 - The Most Potent Approach - Security Awareness

As the internet world is expanding, so is the horizon of knowledge of those who are curious. Previously, people would have to make a concentrated effort to learn hacking and social engineering. Now, with the internet within easy reach (and so full of information) learning exploitation techniques has become much simpler. Accessible tutorials and the availability of dedicated online social engineering tutoring websites means that 'spare time and dedication' is all that is needed for one to master the art of social engineering.

The need for businesses to be wary of this ever-growing threat is now fundamental. A lack of wariness will eventually result in catastrophe. Therefore, out of the many actions a company can take, security awareness is perhaps the most effective against social engineering attacks. As mentioned repeatedly in this chapter, businesses can take every single security measure available to them, but if their employees are not educated on the risks of disclosing internal sensitive information to strangers, all existing security measure are meaningless.

It is also essential to understand that security awareness is not just for employees who use phones and computers. From high-profile managers to security guards, cleaners and catering staff, everyone within an organization must have a

solid understanding of risks arising from social engineering attacks. By involving all staff members in a security training (including non-IT staff) not only helps them understand the need to remain vigilant, but also ensures that they embrace the security program as a whole; which will consequently improve the security outlook of the entire organization.

Gragg [16] talks extensively in his research about the need to have a well-established security awareness amongst all workers. He suggests that each organization must have a specific security policy addressing social engineering. He goes on to suggest that every employee must complete security awareness training, while those who are easily manipulated should also go through resistance training.

Sarah Granger, a media innovator and author, states that:

"Combat strategies… require action on both the physical and psychological levels. Employee training is essential. The mistake many corporations make is to only plan for attack on the physical side. That leaves them wide open from the social-psychological angle." [17]

This is an apt observation. Adding to this statement, Martin asserts that the case for information security in businesses is very strong. He claims that if physical security is the engine, staff awareness is the oil that drives this system forward [18]. Expressing his thoughts, Shuhaili states that with the ever-changing security landscape and people's increasing adoption of technology, the need to maintain an up to date levels of awareness is imperative [19]. Similarly, the European Union Agency for Network and Information Security (ENISA) claims that educated employees will help enhance the consistency and effectiveness of existing information security controls, and potentially stimulate the adoption of cost-effective controls [20]. In essence, a comprehensive training program will gradually reduce expenditure on IT security.

The real-world benefits arising from educating employees on internet security practices are unending. Not only will companies save money due to a reduction in security breaches (and resulting fines), they will also protect themselves from having to respond to any negative press and intrusive scrutiny from authorities – which often occurs after a breach. Further, a sterling reputation amongst company clients for being competent and strict on security, supported by periodic penetration test results, means that the prospects of growth in clientele could be endless.

In comparison, take for example the case of Talk Talk. This organization firmly established itself as a budget broadband provider and a leader in fibre-optics over a relatively short period of time. Nonetheless, they started gathering negative attention from the media and public after three consecutive high profile security

breaches in a single year. These breaches resulted in a loss of 101,000 customers, and a financial loss of an estimated £60 million. [21]

To further support our view that security awareness among employees is an effective strategy in combating social engineering attacks, we will devote the next section of this chapter to practical case studies. We will evaluate the security improvements before and after the employees attended a security awareness course. Analysis of these cases will demonstrate that security awareness is the crucial and most effective tool in the fight against social engineering attacks and, therefore, are an indispensable component of a healthy business.

1.2.2 - Case Studies

Company A – A small financial institution [22]. Company A had been aware of targeted phishing and spear phishing attempts aimed at SME's. However, were unable to train their employees in security awareness, except for some key staff in their IT department. As part of a new initiative, some of the recently employed staff had been given very limited and basic exposure to IT security. Thereafter, the company decided to make security training mandatory for its entire workforce, contracting with an IT security training provider. As part of the training process, phishing tests were conducted before and after the training was delivered. According to the report, initial tests indicated that 39% of the company employees are highly likely to click on a phishing email, which could result in a major security breach.

In response to the recommendations, the company introduced a mandatory training session for managers lasting 40 minutes, with a condensed 15-minute version tailored for the other employees. After all staff members received their security awareness training, another test was conducted to determine how would employees respond to phishing emails. The report shown that not a single one of the employees clicked on a phishing link. The probability of employees becoming victim to a phishing attack fell from 39% to 0%. Reportedly, the company averaged 1.2% over the next twelve months in subsequent simulated phishing attacks - a considerable improvement.

Company B - A shipping and logistics business [23]. Company B had over 3,000 employees, most of whom were issued with company-supplied PDAs and laptops. After a new security manager took charge of his office, he noted a prevalence of poor IT practices amongst employees. For example: misuse of user access rights; passwords being shared openly between employees; sharing access credentials; use of simple passwords (e.g.123456); staff members leaving computers unlocked when away from desks, and unauthorised disclosures made to third parties. An audit also discovered that in most cases it was an employee's ignorance or un-

intentional error that led to the incident. This had been the standard of IT security for years, so the company decided to act and began working on a large-scale IT security awareness campaign. After consultation, the company implemented the PDCA (Plan, Do, Check, Act) standard for information security management, prescribed in the ISO 27110:2005 [24].

After implementing mandatory security training sessions (lasting 120 minutes per module), the company saw notable improvement in employee's attitude towards information security. In the sessions, trainers actively encouraged employees to use more sensible and strong passwords. Pre-training assessment figures reveal that 57.9% of staff members were using simple passwords, which were cracked by the penetration testers in around two hours. The audit commissioned soon after the training shows that use of simple passwords fell immediately to 20%. Overall, after security training, the company noticed considerable improvement among staff in terms of compliance to security policy. After the company introduced a continued security awareness program for its entire workforce, the rates of unintentional security breaches, unauthorised disclosure, and bad IT practices fell significantly.

Company C - A large global manufacturing company [25]. Company C had over 5,000 employees across the globe and been in the manufacturing business for decades. Despite robust authentication and filtering systems, the company began noticing malware attacks on its infrastructure - mostly through phishing attacks and browser infections. There was no employee awareness on IT security at all, and the company had neither policy nor plan in place to educate users on the on the ill-effects of thoughtlessly clicking on a URL. It was estimated that these infections were costing the firm in excess of $700,000 annually in repair costs alone.

Fearing the worst, the company decided to supress the growing number malware infections. They contracted an online security awareness training provider that offered the course in multiple languages. Since the majority of the workforce had been using the company's computers for emails and internet browsing, the company focused its efforts on increasing security awareness on three key areas: email security, safer web browsing, and URL training. With close collaboration with the security course provider, the company managed to train 95% of their employees in twelve months. It is reported that prior to the training program, the company was dealing with 72 malware infections per day. In a review undertaken four months after the program commenced, the company noted a reduction of 46% in malware infections globally. This resulted in substantial savings, which would have previously been spent on strenuous system repairs and recovery.

1.2.3 - Review of Case Studies

All three case studies listed above have one thing in common: the businesses had no effective security awareness plan in place. This resulted in IT malpractices, infections, and attacks on their infrastructure. We then notice that significant reduction in the IT related problems was observed once the institutions implemented an effective security-training program .It is also evident that all three businesses received quick returns on the investment they made in the awareness course delivery. This was true in terms of overall savings on the cost of remedial actions. Finally, their staff also developed a healthy sense of suspicion against cyber attacks, which in itself is everything a sensible and smart employer should encourage and expect from their employees.

What should also be understood here is that the review of these case studies had only one main focus, namely the overall impact after the delivery of awareness courses. If employers also begin integrating other defence methods described in this chapter, the benefits arising from that decision would be positively far reaching and its effects would be long-term. The protection achieved through a comprehensive multi-level and prolonged defence strategy could potentially bring businesses to near immunity against cyber and Social Engineering attacks.

1.2.4 - Methods To Improve User Awareness

Social Engineers are on constant search for new technical and psychological vulnerabilities so they can continue exploiting their targets. Unfortunately, uneducated and naive workers make the task of manipulation easier for the Social Engineers. Unwittingly, uninformed workers extend a helping hand to malicious Social Engineers and end up becoming part of skirmish, which brings enduring hardship to the business, that trusted them.

However, as argued thoroughly in this chapter, there are numerous measures, which businesses can take to prevent themselves from becoming victim of Social Engineering attacks. One of which is security awareness, which can be delivered in a number of ways. This sections lists different approaches that are available to employers, should they choose to convert uneducated workers into knowledgeable and security aware employees.

i. Onsite training

An arrangement can be made to prepare an internal staff member who can conduct regular in-house coaching to in turn educate other staff members on security awareness. Alternatively, external trainers can also be hired for the same purpose. The key here is that these sessions should

not be lengthy; they should be delivered in small, bite-sized sessions with regular breaks. That way, the message will be easily absorbed by the audience, and they will not suffer from training fatigue.

Another important factor to consider is that the sessions must not contain technical jargon. Employees who are not involved in a technical role are not required to understand how to operate a firewall, or how malware containment programs work. The training must be delivered in simple, easy to understand language with clear objectives and focus on spotting and preventing Social Engineering from occurring.

ii. Intranet

A company's intranet can be very resourceful in facilitating security awareness programs. For example, a company can integrate a security course, prepared locally or externally by accredited personnel, and list the program as learning guide in a prominent section of the intranet. The managers must then encourage the workers to review the content on recurring basis, so that the information is engraved in the minds of workers. The intranet is also a good medium to circulate security notifications to workers regarding recent security risks, with instructions on how to deal with the threat and who to report the incident to.

iii. Screensavers

Screensavers can play a big part in promoting security awareness among employees. They can be used to display short reminders on topics such as keeping the password safe, disallowing tailgating, challenging anyone without a company badge/pass, reporting any suspicious behaviour to relevant departments, and so on. Efforts must be made to ensure bigger, bolder fonts and appropriate and relevant imagery are used in order for the content to be viewed and understood from a reasonable distance.

iv. Posters

Displaying bright and vibrant posters with big fonts can be an effective attention-grabber. Putting brief and targeted messages on security issues concerning the business can act as an effective strategy in creating awareness among employees. General security reminders on posters should be rotated routinely, which will provide employees the opportunity to digest multiple security messages with ease and convenience. How-

ever, posters with more important and specific reminders can be placed in a prominent part of the work place on a semi-permanent basis.

v. Manual reminders

Concise and direct reminders can also be delivered to the workforce through printed sheets. In cases where staff intranet or other resources are not available, this could be an affordable model to keep the employees informed about the risks associated with Social Engineering. Managers could also implement a system where these manual/physical reminders are circulated in the workplace with a staff name list and date. That way, everyone who has read and understood the content can sign the form acknowledging that they have reviewed security awareness reminders, and those who have not can be re-approached with the reminders.

vi. Online courses

Employers also have an option to choose from one of the many online security training providers. Online courses not only allow self-paced learning and flexibility, but some providers offer intranet integration and specialist software in the package as well. Managers can thus track the progress of their employees from their own computers. Although many online training websites charge a fee for supplying courses, there some excellent and free resources available online too such as www.cybrary.it. These websites can be very effective in developing a worker's knowledge on risks related to Social Engineering, and has an added benefit of zero cost to employers, proving to be very beneficial for cash-strapped businesses.

The reality is, that with the presence and availability of such a variety of training methods as well as many more ingenious ways of awareness development, businesses have no excuse to leave their workers uneducated on the hazards of Social Engineering. Once training is finalized and the work force is adequately aware of the risks posed by attackers, the employer automatically gains an upper hand in this battle; the business is less likely to suffer from an attack due to their trained staff exercising due diligence to protect the company.

1.3 - Chapter Summary

This chapter contains detailed analyses of potential Social Engineering mitigation techniques used by companies to protect themselves from attacks. In addition, it has also been concluded in this chapter, after rigorous consultation of published papers on the topic of Social Engineering prevention and reviews of various case

studies, that security awareness is the most significant tool in the combat against Social Engineering. The last section of this chapter lists and examines various approaches that are available to deliver security awareness coaching and reminders to employees in an office environment.

The steps outlined in this chapter are by no means exhaustive; it would be more beneficial to combine all the defence measures listed in this report to achieve maximum protection. A multi-layered defence program will undoubtedly be more effective against Social Engineering attacks compared to a single defence method. To become competent in defence, employees must understand exploitation methods used by Social Engineers. It is often the case that the sole reason attackers manage to gain entry to a target is because they are successful in exploiting the weaknesses found in employees. Therefore, companies must spend their time and effort to ensure that their workforce truly understands and appreciates the threat of Social Engineering. By recognising the general exploitation methods that Social Engineers use to execute attacks, workers can play a huge part in the defence, namely by taking preventative measures.

Using creativity in their own refined methods, businesses can also trigger various behavioural defence instincts in their workers. An excellent way to achieve this is by conducting regular brainstorming sessions, so that employees can present new defence ideas and learn from each others' experiences. The unfortunate reality though, is that there is no such thing as absolute "fool-proof" security. However, if all the defence methods outlined in this chapter are implemented with efficiency and sincerity, those security measures will make it much more difficult for a Social Engineer to successfully penetrate a company.

References

[1] Kevin Mitnick (2005) Art of Intrusion C: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, 1st edn., New Jersey, US: John Wiley & Sons.
[2] Michael Erbschloe (2004) Physical Security for IT, 1st edn., Dorset, UK: Digital Press.
[3] Charles A. Shoniregun (2014) Impacts and Risk Assessment of Technology for Internet Security (Advances in Information Security), 1st edn., New York, US: Springer.
[4] The Chromium Projects (Unknown) Sandbox FAQ, Available at:https://www.chromium.org/developers/design-documents/sandbox/Sandbox-FAQ(Accessed: 11th July 2016).
[5] Mozilla Wiki (Unknown) Security/Sandbox, Available at:https://wiki.mozilla.org/Security/Sandbox (Accessed: 11th July 2016).
[6] Long Lu, Vinod Yegneswaran, Phillip Porras, Wenke Lee (2010) BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections, Available

at:http://ants.iis.sinica.edu.tw/3bkmj9ltewxtsrrvnoknfdxrm3zfwrr/17/BLADE-ACM-CCS-2010.pdf (Accessed: 11th July 2016).

[7] Gianluca Stringhini, Olivier Thonnard (2015) That Ain't You: Blocking Spearphishing Through Behavioral Modelling, Available at:http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/spearphishing-dimva2015.pdf(Accessed: 11th July 2016).

[8] K. Mitnick and W. Simon (2002), The art of deception. Indianapolis: Wiley.

[9] Ryan Heartfield, George Loukas (2015) 'A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks', ACM Computing Surveys, 48(3), Article 37.

[10] Steve Suehring (2015) Linux Firewalls: Enhancing Security with Nftables and Beyond, 4th edn., Boston, US: Addison Wesley.

[11] Navigant (2014) Cyber Security Trends for 2014 – Part 1, Available at:http://www.navigant.com/insights/hot-topics/technology-solutions-experts-corner/cyber-security-trends-2014-part-1/ (Accessed: 12th August 2016).

[12] TOM MENDELSOHN (2016) More than half of UK firms have been hit by ransomware—report, Available at: http://arstechnica.co.uk/security/2016/08/more-than-half-of-uk-firms-have-been-hit-by-ransomware-report/ (Accessed: 12th August 2016).

[13] Warwick Ashford (2016) One in five businesses hit by ransomware are forced to close, study shows, Available at: http://www.computerweekly.com/news/450301845/One-in-five-businesses-hit-by-ransomware-are-forced-to-close-study-shows (Accessed: 12th August 2016).

[14] Art Kohn (2014) Brain Science: The Forgetting Curve–the Dirty Secret of Corporate Training, Available at: http://www.learningsolutionsmag.com/articles/1379/brain-science-the-forgetting-curvethe-dirty-secret-of-corporate-training (Accessed: 13th August 2016).

[15] Guido Robling, Marius Muller (2009) Social engineering: a serious underestimated problem., Available at:https://www.researchgate.net/publication/220807213_Social_engineering_a_serious_underestimated_problem(Accessed: 13th August 2016).

[16] David Gragg (2002) A Multi-Level Defense Against Social Engineering, Available at:https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920 (Accessed: 15th August 2016).

[17] Sarah Granger (2002) Social Engineering Fundamentals, Part II: Combat Strategies,Available at: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies (Accessed: 15th August 2016).

[18] Martin Smith (2006) The importance of employee awareness to information security,Available at: http://digital-library.theiet.org/content/conferences/10.1049/ic_20060320(Accessed: 16th August 2016).

[19] Shuhaili Talib, Nathan L. Clarke, Steven M. Furnell (2010) An Analysis of Information Security Awareness within Home and Work Environments, Available at:http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5438096&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5438096(Accessed: 16th August 2016).

[20] ENISA (2010) The new users' guide: How to raise information security awareness (EN),Available at: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide(Accessed: 16th August 2016).

[21] Kate Palmer, Cara McGoogan (2016) TalkTalk loses 101,000 customers after hack,Available at: http://www.telegraph.co.uk/technology/2016/02/02/talktalk-loses-101000-customers-after-hack/ (Accessed: 17th August 2016).

[22] KnowBe4 (2016) CASE STUDY Financial Institution, Available at:https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/CaseStudy_Financials.pdf?t=1471185563903 (Accessed: 17th August 2016).

[23] Mete Eminagaoglu, Erdem Ucar, Sxaban Eren (2010) The positive outcomes of information security awareness training in companies e A case study, Available at:http://www.csb.uncw.edu/people/cummingsj/classes/mis534/articles/Ch5UserTraining.pdf(Accessed: 17th August 2016).

[24] ISO (2013) ISO/IEC 27001:2005, Available at: http://www.iso.org/iso/catalogue_detail?csnumber=42103 (Accessed: 17th August 2016).

[25] Wombat (2016) Global Manufacturing Company Reduces Malware Infections by 46%,Available at: https://info.wombatsecurity.com/hs-fs/hub/372792/file-2557238064-pdf/WombatSecurity_CaseStudy_Manufacturing_46PercentMalwareReduction_090815.pdf?submissionGuid=ffd67461-ca8b-4466-9d8b-a4ad57a5d9df (Accessed: 18th August 2016).