Presentation

[Slide 1] Hi everyone, my name is _____ and today I'm going to talk about social engineering and how to defend against attacks of this nature. I'll mainly be covering the tactics as a workplace and employee but will also cover personal steps that can be taken for every day.

[Slide 2] Social engineering is usually defined as exploiting human vulnerabilities to gain access to a target as opposed to exploiting technical vulnerabilities. There are many different styles of social engineering, which include:

- Phishing, where malicious links are sent to targets
- Quid pro quo, where they promise something in exchange for information
- Tailgating, where an authorized person helps an unauthorised person through an electronic barrier
- Baiting, similar to 'Trojan Horse' style attacks
- Pretexting, pretending to be someone else to obtain information
- Blackmail, where they threaten to reveal a secret
- And lastly, dumpster diving, where the attacker will physically search for information about the target (Tiwari, 2018)

[Slide 3] While there are many different types of social engineering, the most common is phishing (Infosec, 2019). A study was conducted, and the results found that 27% of people will click on a malicious or bogus link when sent under the pretence of a trusted company (Lopez, 2019). While phishing has been found to be the most successful (Lord, 2019), many social engineers will combine different aspects of social engineering and construct a tailored experience for a specific target and situation. It has been found that almost 1 in 5 people will fall victim to a social engineering attack (Ashford, 2018).

[Slide 4] So what makes social engineering such an easy attack to pull off? Social engineering relies on common human behaviours, such as trust, curiosity and ignorance. Many people are often also striving to be helpful and like to gain something from nothing (Gulati, 2003). Attackers are aware of the way humans react to certain triggers and use this knowledge to their advantage. How are we supposed to defend against attacks which are tailored to our weaknesses? There are many layers to defending against social engineering attacks, including policy, training, and traps ('including social engineering land mines').

[Slide 5] Policies are the building blocks for a great social engineering defence. Having rules in play assist in both security as a whole and also being able to identify suspicious behaviour. These policies can include password rules, destroying of information, access approval and so much more. The most important part of a policy is the assurance that it is enforced by every individual, otherwise it loses its value. As an example, some companies include in their policies that employees are held responsible for any information or access that is handed over, which makes them more aware of the security implications, leading to a greater defence against social engineering attacks. Having the right policies in place can lead to less damage caused by successful attacks.

[Slide 6] While a policy is required in any social engineering defence, untrained employees will decrease the value in it. For a great social engineering defence to exist, there must be no weak links, as all it takes is one vulnerability and then the attacker can get the information they're after. Aside from initial training in social engineering attacks, employees must always be up to date with new social engineering techniques and ensure to complete training regularly as to ensure it is not forgotten. Training should include recognising the signs of social engineering such as urgency or asking for unauthorised information so that the correct steps can be taken to prevent the attack. It can sometimes be difficult to motivate people to learn about social engineering attacks when they feel separate from it or invulnerable to them. Demonstrating to these people can show how easily it can happen and provides the motivation for them to be vigilant and educated.

To go even further, inoculation is another tactic that can be implemented into training methods. This involves fake social engineering attacks organised by the technical team to give other employees a real-life example of what it can look like, similar to how vaccines work.

[Slide 7] Social engineering land mines are tricks put in place in order to expose social engineers. Traps, or land mines, are most successful when put into place in conjunction with trained individuals and a solid foundation of policies in place. An example of a land mine is assigning the responsibility of knowing everyone to an employee, so that non-authorised personnel or attackers are easily identified. For land mines to be effective, they must be undetectable by the attacker, so that they aren't able to con their way past the land mine.

On a more personal note, to keep your own data safe as opposed to defences in the workplace, it is important to never give out credentials like bank login details or email passwords, even to trusted people. Some other helpful tactics for personal defence can include only downloading from trusted sites, using anti-phishing tools and not falling for things that sound too good to be true. Being cautious and knowledgeable are the first steps to remaining safe and having a good defence.

[Slide 8] Defending against social engineering is a constant battle but it must be fought. Through tactics like policies, training and other defence mechanisms like traps, the likelihood of a successful social engineering attack can be greatly reduced. Although, it's important to keep in mind that it's not the end of the world if an attack is successful as long as you have policies in place that minimise the damage of successful attacks.

References

Arthurs W, 2 August 2001, A Proactive Defence to Social Engineering, https://www.sans.org/reading-room/whitepapers/engineering/proactive-defence-social-engineering-511

Ashford W, 9 April 2018, More than one in 10 employees fall for social engineering attacks, https://www.computerweekly.com/news/252438572/More-than-one-in-10-employees-fall-for-social-engineering-attacks?utm_source=datafloq&utm_medium=ref&utm_campaign=datafloq

Frumento E, 14 May 2018, Estimates of the number of Social Engineering based cyber-attacks into private or government organizations, https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/94-estimates-of-social-engineering-attacks

Gragg D, December 2002, A Multi-Level Defence Against Social Engineering, https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920

Gulati R, 31 October 2003, The Threat of Social Engineering and Your Defense Against It, https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

Gupta B et al, n.d., Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions, https://arxiv.org/pdf/1705.09819.pdf

Lopez C, 16 February 2019, Social Engineering Attacks by the Numbers: Prevalence, Costs, & Impact, https://datafloq.com/read/social-engineering-attacks-numbers-cost/6068

Lord N, 15 July 2019, Social Engineering Attacks: Common Techniques & How to Prevent an Attack, https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

Milkovic D, 3 December 2018, 13 Alarming Cyber Security Facts and Stats, https://www.cybintsolutions.com/cyber-security-facts-stats/

Netsparker, n.d., Social Hacking of Support and Implementation Teams, https://www.netsparker.com/blog/web-security/social-engineering-customer-facing-teams/

Olavsrud T, 19 October 2010, 9 Best Defenses Against Social Engineering Attacks, https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

Paganini P, 6 February 2019, The Most Common Social Engineering Attacks, https://resources.infosecinstitute.com/common-social-engineering-attacks/ - gref

Poston H, 19 March 2019, Protecting Against Social Engineering Attacks, https://resources.infosecinstitute.com/protecting-against-social-engineering-attacks/#gref

Tiwari A, 30 May 2018, What Is Social Engineering? What Are Different Types Of Social Engineering Attacks?, https://fossbytes.com/what-is-social-engineering-types-techniques/