THE UNIVERSITY of ADELAIDE

ASSESSMENT 2 – PART A: PROJECT PLAN

Group 8.1

Dylan Rohan

Reminder:

Dylan Rohan, Samuel Miller
Business Data & Cyber Security (M)
18 Aug 2023 at 1:09

Hi Sam,

Im excited to learn from you and get into this unit, but I have some concerns I need to voice early. This is the only unit in the entire course with a group project, and I'm not sure I could have found out there was one prior to signing up. This wouldn't usually be a problem, however I'd planned on smashing out the assignments ahead of time because I will be in Ireland from the 8th until the 24th of September (the dates were not up to me).

I'm confident I can still do the unit, and I understand the purpose of the group assignment. But is it possible to preselect a topic so I can get started and not hold my group back? I'll be in an entirely different time zone otherwise.

The Ireland trip will provide me far more experience than a group assignment. While I'm there I'll be working at conferences about mental and physical disabilities and I'll be living with an Irish family. I will be around an entirely different culture. This being the case, do you think there is any chance I can do this group assignment as a group of 1 as I'll still be applying all those other skills in the same assignment period? Completely understand if there's no wiggle room there, but it is the simplest solution in my view. Please consider that I chose an online part time course for its flexibility, happy to provide my grades to demonstrate I've not taken the flexibility for granted (can also provide a letter from a previous tutor regarding my attitude, etc.).

Please advise as soon as possible as the clock is already ticking for me, as I'm also moving from Sydney into a new house in rural Geelong in week 1. I had made all the necessary plans and preparations, but find myself at an unavoidable disadvantage. I think I'll have to bring back a four leaf clover with me.

Warm regards,

Dylan Rohan

Written by Dylan Rohan

Word Count: [~500 word]

Introduction

Most people are unaware of the risks of the cyber landscape as individuals. A lack of data/ cybersecurity literacy represents the biggest threat to businesses and individuals. In this presentation, we hope to present to company employees on the topic of 'Social engineering attacks getting smarter'. We will provide listeners with:

- An understanding of why data has value
- An understanding of what 'Social engineering' means in this context
- A timeline and explanation of motives behind some of these attacks.
- A clear call to action
    - E.g., protecting their privacy, conducting themselves at work, how to respond to a cyber threat.

We hope that this enables employees to be cybersecure, take policy seriously, and improve cyber hygiene and cyber resilience.

Core information

Figure 1: The key points the project will cover.

1. Data Sources & information content - Presenter 1
    - In this section we will introduce the topic by discussing what kinds of data exist (Personally identifiable information, Internet of things data, business data, etc).
    - We will then show case the information that can be extracted (behavioural patterns, authentication keywords, business analytics).

2. Data usage and Value – Presenter 1 (Dylan)
    - We will demonstrate the utilitarian utility this information has for analytical and machine learning purposes (descriptive, diagnostic, predictive, and prescriptive purposes).
    - Demonstrate that data is an asset (financial gain it provides, marketing advantage, a metric for improvement, etc.)

3. Social engineering – Presenter 2 (Dylan)
    - Present a memorable definition
    - Explain why users should be concerned (the various levels of complexity and types of attack

4. Timeline of events – Presenter 3 (Dylan)
    - Showcase how these attacks have been evolving over time with relevant examples.
    - Each example should increase the anxiety levels of the users, its important they appreciate this threat.

5. Security measures and summary – Presenter 4 (Dylan)
    - Provide a release for that anxiety with actionable suggestions and resources
    - Summarise the key points of the presentation
    - Cement a sense of concern so that users feel a need continue to learn

Delivery

Computer science can be quite dry, it is important that we keep things concise and engaging. We will use interesting examples that require minimal understanding in order to improve recollection. The most important outcome is invoking a concern for cybersecurity which will be achieved in section 3-4 where we introduce social engineering and a timeline of events. Listeners are likely to seek information/help if we can achieve this goal and effectively reduce cyber risks on a personal and professional level.

Presentation Section	Time allocation
Introduction	5 min
Data sources & information content	
Data uses	10 min
Social Engineering	
Timeline of events	10 min
Security measures and summary	5 min

Conclusion

Targets of social engineering attacks are predominantly the uninformed and cognitively impaired (senior citizens, intellectually disabled, children, stressed individuals, etc). These attacks represent a large portion of cyber-attacks and we have a duty to reduce financial or emotional harm that may come to victims of such an attack. While there are systems that can be put in place to reduce these attacks, education is ultimately the best weapon. Educating has a two-fold effect. It reduces the success rate of attacks more broadly, and it reduces the funding available for future and more sophisticated attacks. This presentation prepares users by informing them of the assets they are in control of and the power they have, showcasing how social engineering attacks have evolved and continue to evolve, and provides actionable cyber hygiene tasks and resources that promote cyber resilience. This will protect users and businesses on a personal and professional level, greatly improving safety and security at minimal cost.

Appendix

Table 2: Specifics of each section.

Section	Examples	References
Data sources & information content	• PII • Natural World data • Engagement data • IoT data • Audible and visual data • Traffic and network data • Business data	

Data uses	• PII
	  ○ Personal records
	  ○ Likely behaviours
	  ○ Authentication keywords
	  ○ Recommendation algorithms
	• Natural World Data
	  ○ Plan and forecast (natural disasters)
	  ○ Targeted marketing/behavioural patterns
	  ○ Targeted disruption
	• Engagement Data
	  ○ Recommendation algorithms
	  ○ Marketing analytics
	  ○ Adversarial attacks
	• Business Data
	  ○ Financial data and business analytics
	  ○ Business metrics and KPIs
	  ○ Competitive advantage, data for ransom
	• IoT Data
	  ○ Health records
	  ○ Convenience
	  ○ Disability support
	  ○ Outlier logging	

	○ Behavioural patterns ○ Surveillance ○ Target detection ○ Hacking the software	
Social Engineering	Human hacking Simple definition: Psychological manipulation to obtain access to sensitive data or systems for nefarious purposes. Types: • phishing, spear phishing, whaling, vishing, business email compromise fishing • pretexting • Impersonation on help desk calls • shoulder surfing • eavesdropping • dumpster diving • stealing important documents • diversion theft • fake software • baiting • quid pro quo • pretexting • tailgating • Pop-Up windows • Robocalls • reverse social engineering • Vishing	(Salahdine & Kaabouch 2019) (Krombholz et al. 2015) (Koyun & Al Janabi 2017) (Bhusal 2021) (Mouton et al.) (IBM 2023) (FBI 2021)
Timeline of events	1184 BC – The trojan Horse 1500 BC – Spanish prisoner con 1970s - physical attack (floppy disks, drives, bulletin board systems) & Nigerian prince letters 1980s – Nigerian prince faxes	(Pienta, Thatcher & Johnston 2020)

	1992 – Motorola source code and Kevin Mitnick's capture 2011 – RSA phishing scam 2013 – Target Third-party breach 101 million users' PII), New York Times (Fake fed ex email) (Krombholz et al. 2015), The Associate Press (twitter breach), Apple, Facebook, Twitter (whittaker) 2014 – Sony pictures Phish (North Korean government) 2016 – US presidential election email leak (Russia & shortened urls) 2019 – Toyota BEC scam 37 million, the third attack that year 2020 – Sharktank spear phish $388,000 2020 – twitter bitcoin scam (no one is untouchable) Etc.	
Security measures and summary	• Improved language choices and seduction techniques • Deepfakes • New surveillance techniques • Cloned speech • Autonomous attacks • Ability for AI to improve	(Geng, Huang & Fernando 2022) (Neekhara et al. 2021) (Mirsky & Lee 2022) (Zeng 2022)

Bhusal, CS 2021, 'Systematic review on social engineering: Hacking by manipulating humans', *Journal of Information Security*, vol. 12, pp. 104-114.

FBI 2021, *Internet Crime Report 2021*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Geng, J, Huang, D & Fernando 2022, 'DensePose From WiFi', *arXiv pre-print server*, 2022-12-31.

IBM 2023, *Cost of a Data Breach Report 2023*, IBM, https://www.ibm.com/reports/data-breach, viewed 06/09/2023 2023.

Koyun, A & Al Janabi, E 2017, 'Social engineering attacks', *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, vol. 4, no. 6, pp. 7533-7538.

Krombholz, K, Hobel, H, Huber, M & Weippl, E 2015, 'Advanced social engineering attacks', *Journal of Information Security and applications*, vol. 22, pp. 113-122.

Mirsky, Y & Lee, W 2022, 'The Creation and Detection of Deepfakes', *ACM Computing Surveys*, vol. 54, no. 1, pp. 1-41.

Mouton, F, Malan, MM, Leenen, L & Venter, HS 'Social engineering attack framework', in IEEE.

Neekhara, P, Hussain, S, Dubnov, S, Koushanfar, F & McAuley, J 2021, 'Expressive neural voice cloning', in *Asian Conference on Machine Learning,* PMLR, pp. 252-267.

Pienta, D, Thatcher, JB & Johnston, A 2020, 'Protecting a whale in a sea of phish', *Journal of Information Technology*, vol. 35, no. 3, 2020/09/01, pp. 214-231.

Salahdine, F & Kaabouch, N 2019, 'Social engineering attacks: A survey', *Future internet*, vol. 11, no. 4, p. 89.

Zeng, Y 2022, 'AI Empowers Security Threats and Strategies for Cyber Attacks', *Procedia Computer Science*, vol. 208, pp. 170-175.