Applied Social Engineering

Thursdays [Every day is like Sunday…]
Dr. Filipo Sharevski fsharevs@cdm.depaul.edu
Discord Channel https://discord.gg/8sgrZqr

A hands-on course in which students investigate social engineering attacks in a controlled lab environment and develop technical, policy, and risk management responses. This is the Number 1 Problem in the national security, especially in the election year. Topics social engineering mechanics, principles of persuasion, preparation, traditional social engineering attacks and defenses, Ambient Tactical Deception (ATD), policy response, risk management, ethics and societal impact of social engineering. Students work on an individual defense to a practical social engineering scenario of their choice for their final project.

Assignments

This is the tentative schedule for the class:

W	Module	Assignment
1	Introduction	Homework 1
2	Principles of Persuasion in Social Engineering	Homework 2
3	Social Engineering Targeting	Homework 3
4	Traditional Social Engineering Attacks	Homework 4
5	Trolling, Misinformation, Rumors	Homework 5
6	Ambient Tactical Deception	Homework 6
7	Propaganda and Pseudo-events	Homework 7
8	Ethical Aspects of Social Engineering	Homework 8
9	Social Engineering and Nonverbal Behavior	Homework 9
10	Group Project [ATDBot]	

The weights of each assignment for contributing to the final average are as follows:

Assignment	Weight in final grade
Homework	45%
Project	45%
Presentation	10%

Assignments are due Sunday in the week assigned, 11:59 PM. Clear language, concise writing. Your choice of formatting. A .pdf file submitted in the D2L folder. NO late assignments accepted. Bargaining for grades is not allowed and is considered academic dishonesty.

Grading

Grading is based on a percentage basis, which is then convert to a letter as:

Percentage	Grade	Percentage	Grade	Percentage	Grade
100-92	A	91-90	A-		
87-82	B	81-80	B-	89-98	B+
77-72	C	71-70	C-	79-78	C+
67-62	D	61-60	D-	69-68	D+
				59-0	F

Project/Presentation

In this class everyone will participate into a group class project called ATDBot. Everyone will receive a Virtual Machine (VM) that has to use as part of this project. The VM must be used for the clasroom project ONLY – No external use is allowed. I will divide the class in pairs and each one has to use the ATDBot to ofline manipulate a (1) Wikipedia Artricle; (2) a news article. I will provide you a manual how to do so. Once you have the manipualated versions of article you will exchange those with your partner. When you have their, and they have yours, you will proceed to answer several questions about their articles and elaborate about your mainpulation strategy [I will provide you a Qualtrics where you will provide your answers]. Becase this is your class project you need to elaborate more in detail. I will assign and give you the ATDBot VM+manual mid-quarter. This is the first time I ran such a class project so be friendly and open to participate. The quality of experience and your contribuiton will help future classes extend this work [plus, the more you give here, the more you learn what's coming post-trolling on social media].

Week-by-week schedule

Week 1: Introduction

Social Engineering concept. Social engineering targets and goals. Taxonomy of social engineering attacks: types, attackers, channels, vectors.

Homework 1:
Is Kevin Mitnik that smart or we people are letting him take us for a ride? Watch the documentary and provide your commentary: https://www.youtube.com/watch?v=tIVAjgiatqM
Don't write: "He is cool, I think this is real; Hackers are there to get you" - I know that already. Academic level of commentary is expected. You are not writing a Facebook post or a blog.

Week 2: Principles of Persuasion in Social Engineering

Social engineering theory. Elaboration Likelihood Model (ELM) and persuasion techniques. Compliance principles: Commitment, reciprocation, consistency, and social proof, likability and trust, fear, authority, and scarcity.

Homework 2:
Why persuasion in marketing is okay, but in social engineering not? Review the assigned reading to argument up your position:
https://www.jstor.org/stable/26059056?seq=1#metadata_info_tab_contents [access it through DePaul's Library. Figure it out how, you ought to protect us from social engineering]
Sure enough, use real-world examples of social engineering and marketing persuasions.

Week 3: Social Engineering Targeting

Open Source Intelligence (OSNIT). Target profiling. Elicitation. Pretexting.

Homework 3:
OSNIT in action - use the framework and Maltego to profile a target - yourself: https://www.paterva.com/downloads.php#tab-2 (or pick an OSNIT tool of your choice: https://github.com/v2-dev/awesome-social-engineering). See what you can find about you or a person of interest and how that can be used for a potential social engineering campaign against you/them. Report the findings (redacted, of course - I have no intentions of lurking into students' OSNIT profiles; just the sites and general description of what info is available). Write a hypothetical pretexting scenario.

Week 4: Traditional Social Engineering Attacks

An ontological model of a social engineering attack. Social Engineering attacks framework. Social engineering templates. Creating a test social engineering campaign - phishing. Post-phishing exploitation.

Homework 4:
Look around for the latest phishing trends. Use GoPhish to create and test the campaign with your own email (or set up a dummy email account): https://getgophish.com Report the steps, cues, and methods you used to create your campaign. Include screenshots from the GoPhish dashboard documenting the successful execution of the test phishing campaign.
Write a hypothetical post-phishing exploitation scenario.

Week 5: Trolling, Misinformation, Rumors

Trolling – behaviour, manifestation, traits. Online expressions. Misinformation. Rumors. Effect on decision making.

Homework 5: Find a particularly interesting trolling / misinformation / disinformation / rumor case. Write a report on how it relates to the social engineering principles we discussed in the previous classes.

Week 6: Ambient Tactical Deception

ATD Concept. Technical Implementation. ATD persuasion and compliance principles. Goals and target profiling. ATD threat model. ATD types, channels, vectors. Creating an ATD test campaign of choice - swap/insert/modify in email/webpage/social media. Post-ATD exploration (psychological operations and cyberwarfare). ATD defenses.

Homework 6: Come up with your ATD example. Show me how good of ATD attacker you are. NO Trump tweets – out of bounds, a very low hanging fruit. You can use our ATD code for manipulating text as a browser extension (uploaded in D2L).

Week 7: Propaganda and Pseudo-events

History of propaganda. Foreign, domestic, war-times. Use of propaganda for social engineering. Mass media and propaganda. Pseudo-events. Celebrities.

Homework 7: Watch at least one part of The Century of the Self and tell me what do you think: https://www.youtube.com/results?search_query=the+century+of+self Again, I know Ed Bernays is cool. Don't summarize me the movie or the part; this is not an IMDB review. Tell me how it fits into the narrative discussed in class.

Week 8: Ethical Aspects of Social Engineering

Trolling – behaviour, manifestation, traits. Online expressions. Misinformation. Rumors. Effect on decision making.

Homework 8: Is it ethical to use Twitter as a means of propaganda? Start thinking this and make sure your answer is not clouded by your detest/favor of public political figures [This is academic course, you have to move beyond being a "propagandee"]. Think broadly and write about the implications of using utilitarian or deontological approach in public relations.

Week 9: Social Engineering and Nonverbal Behavior

Amydhala hijack. Emotional responses. Misuse of Empathy.

Homework 9: Write a reflection on how think people can prevent amygdala hijack for social engineering. No conspiracy theories or unsupported ideas. This is a serious psychological condition. Go and look how has manifested in other domains.

Week 10: Final Project presentation

We will gather for a final Zoom meeting where each of you will share and reflect on the ATDBot usage, outcome, experience, recommendations for additional features, etc.

Books

List of books [not required, use abebooks.com or triftbooks.com to buy some of them] about social engineering and manipulation:

- **Propaganda**: ISBN: 9780970312594
- **The Age of Propaganda.** ISBN: 9780805074031
- **Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.** ISBN: 9780190923631
- **Crystalizing Public Opinion**. ISBN: 9781935439264
- **Influence: The Psychology of Persuasion**. ISBN: 9780061241895
- **Manufacturing Consent.** ISBN: 9780375714498
- **The Image: A Guide of Pseudo Events in America.** ISBN: 9780679741800
- **This is Not Propaganda: Adventures in the War against Reality**. ISBN: 9781541762114
- **Amusing Ourselves to Death: Public Discourse in the Age of Show Business**: ISBN: 9780143036531
- **Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information**. ISBN: 9781699035306
- **The Ellipsis Manual:** ISBN: 9780692819906
- **The Art of Deception: Controlling the Human Element of Security.** ISBN: 9780764542800
- **Permanent Record.** ISBN: 9781250237231
- **LikeWar: The Weaponization of Social Media.** ISBN: 9780358108474

Other Important Information

Attendance: I expect you will attend every class [or watch it on Panopto].

Class Cancelation: Unless DePaul closes because of weather or any other force majure, we will have class.

Academic Integrity: I expect that you have read and understood DePaul's Academic Integrity policy: http://academicintegrity.depaul.edu/ .

Changes to Syllabus: I reserve the right to change the syllabus and you will be timely informed of such changes. I don't expect significant deviations of the course agenda.

Academic Policies:
http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx

Students with disabilities: Contact the instructor or the Center for Students with Disabilities (CSD) at: csd@depaul.edu prior to the class start.

Preferred Name & Gender Pronouns: I will gladly honor your request to address you by an alternate name or gender pronoun: http://policies.depaul.edu/policy/policy.aspx?pid=332

Online Teaching Evaluation (OTE): Please evaluate the course in CampusConnect when you receive a notification towards the end of the quarter.