Colloquium Paper
SS 2022

Psychology and Usability

Written by: Husnain Khan (ite104308)

Date: August 29, 2022

Supervisor: Prof. Dr. Gerd Beuster

Table of Contents

1. Introduction *3*

2. Cognitive Psychology *4*

3. Social Psychology *5*

3.1. The bystander effect 6

3.2. Gender, Diversity and Interpersonal variation 7

3.3. Phishing 8

4. Deception *8*

4.1. Online Deception 9

4.2. Deception in Practice 10

4.3. Types of Online Social Deception 11

4.4. Susceptibly to Online Social Deception 13

4.5. Deception Research 13

5. Passwords *14*

6. Conclusion *15*

7. References *17*

1. Introduction

Psychology refers to studying of mind and human behaviour. It involves studying and understanding mental processes, brain function and how humans behave in response to that. Psychology effects disciples from philosophy to artificial intelligence. It is discipline of science that is spread of many different themes including cognitive psychology, social psychology, decision science and behavioral science (Schacter, 2009). There are domains of psychology that specifically on how humans interact with each other and their environment. In this paper, we discuss how psychology is used by hackers and scammers to manipulate mind in order to be successful in their act. We will look at different branches of psychology and how these are used by hackers including Cognitive psychology and Social psychology (Anderson, 2020)

The term Social psychology refers to how human mind effects social interactions, and how society effects an individual. It focuses on how behaviour of an individual is influenced by other members of the society. Social psychology is used by hackers to manipulate mind in other to persuade individuals. On the other hand, cognitive psychology looks at mental processes such as memory, attention, and language that take place in order for a person to make a decision or any move. Decision science is another discipline of psychology that looks at how human process information presented to them and assess it in order to make a decision.

Hackers exploit the human mind by getting an understanding psychology. There are many examples in the real world where technology is being used to scam people because humans are more easily lured by a scam. Online frauds are a lot more common and easier to do because it is a lot easier to manipulate someone online versus in person. For example, significant component of inter-personal relationships is missing online. We can see that relationship with employers, banks and government is much more formalized online versus seeing someone in person at your local bank branch. This obviously creates a risk for being forged since you are not liable and do not know that person in your daily life. It is for example a lot easier to create a bogus bank website and scam people than actually creating a bogus bank branch in a neighbourhood (Anderson, 2020). In other words, technology has made it easier to manipulate with human mind and this is why internet scams as such are on the rise.

The principal mechanism that scammers and hackers are using to lure people into their scams is deception by playing with human mind and psychology. Deception is being used to compromise passwords, personal information and financial transactions (Anderson, 2020). Deception is when an agent speaks or acts a certain way to induce false belief in a target or victim. Deception and persuasion is a social phenomenon of our age. It can range from small lies to huge political propaganda. It is a lot easier for someone to deceive you online than in reality. For example, text-based interactions with anyone are a lot more deceiving than in person communication where victim can pick up social cues and facial expressions (Hancock, 2007). There are many ways digital deception occurs by manipulating human mind, some of which will be looked in later sections of this paper.

Psychology includes many topics from clinical psychology to neuroscience and the understanding of brain is very less and brain is a lot more complex. But nonetheless huge amount is still known that is exploited by hackers. In this paper we will explore some fundamental branches of psychology in order to understand the manipulation that occurs in order for victim to make irrational decisions which leads to them being exploited by scammers (Anderson, 2020).

2. Cognitive Psychology

Cognitive psychology is the discipline that deals with how humans think. There are neural networks that occur across the brain that help us form a decision or perform a task. Our memories are also stored in these networks. The neural networks are plastic and so is our brain, therefore they change over time and can be reconstructed and manipulated as well. (Anderson, 2020). It has been noted that cognitive psychology plays a major component in scam awareness. For example, research has shown that people with lower scam awareness early in life are at risk of developing Alzheimer's Disease later in life (Boyle, 2019). It is because mild cognitive impairment such as seen in Alzheimer's disease hinders a person from understanding the manipulation and they are more likely to be persuaded by a scammer and fall for their trap.

Hackers utilize the errors human make as these are rooted in very nature of human cognition, they develop schemata that utilizes these human cognition errors and develop a model to trap a victim. Some of these human cognition errors include:

- **Capture error:** Refers to errors that occur after you develop a skill and but slips can occur when manual skill fails, for example going straight to home from work instead of grocery because you are so used to taking the route to home every day. These types of errors and slips are exploited by Typo-squatters who register domains similar to popular typing errors, or a pop-up "Ok" box is another way to attackers exploit the victim's computer because they know people are in hurry to click the window to get their work done quickly (Anderson, 2020).
- **Post-completion error:** These types of error usually occur following interruptions or perceptual confusion. People are usually in a hurry after the accomplished a goal and these errors occur. For example, leaving ATM card in machine after getting the money. To avoid these types of errors ATM machines now a days give the card back first before giving out the money (Anderson, 2020).

3. Social Psychology

Social psychology looks at how society influences people's thoughts, behaviour and actions. Humans in general derive from belonging to a specific group of people, be it a religious group, tribe, team or gender (Anderson, 2020). People like to conform to the norms of that general group. For example, there are many experiments that shows us how people will change their behaviour just to conform to a group they belong to. One example of that includes Solomon-Asch conformity experiment, where he studies how people change their behaviour due to peer-pressure. In this experiment, and concluded that majority of the participants conformed to the view of peers. He concluded that majority of the people conformed for two main reasons. It was either because people wanted to fit in a group, known as normative influence or they believed that the other group is better informed than them. This is known as informational influence (McLeod, 2018). Another experiment known as Stanford prison experiment looked at the behaviour of students when given authority. The experiment concluded that most people will behave wicked if there is no authority and absence of orders. The experiment had students take roles of warden and inmates and noticed that students playing roles of wanderers rapidly became sadistic authoritarians (Anderson, 2020).

An example where social psychology is used to influence people's behaviour or actions is during Election campaigns. Presidential debates are bombarded by arguments with the intention to persuade people to change their political opinion (Ewell, 2015). Another example where social influence effect of decision is for example in marketing industry, where social media influencers promote products in order to persuade people to a buy product.

3.1. The bystander effect

The bystander effect refers to inhibition of behaviour of an individual in presence of others. Studies suggest that lone by-standers are more likely to help a person in need versus if there were multiple people present witnessing the event. It has been noted that people's judgement gets influenced when others are present and everyone likes to just follow what the rest of crowd is doing and not help, whereas if alone most by-standers help the victim. Studies suggest the more bystanders intervene, the successful they are at helping out in a situation (Anderson, 2020).

Figure 1. The by-stander effect.

3.2. Gender, Diversity and Interpersonal variation

There are biases noticed between both genders in many different disciplines of life. These gender biases sometimes are exploited by hackers to scam a specific group of people or gender. For example, most technology is designed by men for men and the designers tend to forget that at least half of their users are going to be females. This type of bias leads to women being more susceptible of such scams. Gender biases are seen in other fields such as medical equipment is mainly designed for men and therefore many women die because medical technology and medical test assume the patient is going to be a male (Anderson, 2020). An example of such gender bias is seen when talking about Coronary Artery Disease aka Heart disease specific tests. It has been found that more women die of heart disease because most test and clinical trials are specific for men and women's disease goes undetected while using those tests. Lack of gender-specific reporting in many clinical trials continue to limit the available knowledge needed to devise optimal management for women with heart disease (Wenger, 2003).

Gender has become a controversial topic in psychology research. Computer science has been considered a male dominant field, where most of the application and software are designed by geeky men keeping in mind that their users are going to be males. This leads to women being more prone to online scams. On the other hand, countries like Poland, Romania and Baltic states that women making up 1/3 of Computer science students where in India the ratio is 50% men: women. This suggests that differences are more cultural than genetic or developmental. Neuroimaging has also suggested that brains for both female and males are mosaic, just like our tissues in the body and everyone is equally capable of training the mind to be a certain way, be it aggression or empathy (Anderson 2020). A study suggests that anti-phishing advice given by banks to their customers is easier for men to follow than women.

This type of bias goes beyond gender and has also been seen in different cultural backgrounds. Most of the systems are designed by white or Asian men and this might not be taken into consideration that people come for different educational and cultural backgrounds and this can lead to less educated people, older, children and women fleeing abusive relationships more vulnerable (Anderson, 2020). It is important to understand these biases and bring diversity in corporate world,

market research. It is important that while designing a product, we understand our users and their culture.

3.3. Phishing

Phishing refers to an email is sent to a user's account and by clicking on its malicious malware downloads in the user's computer hijacking the machine and compromising very important information. The targets of phishing tend to be both staff and your customers because everyone is in rush to click on a link and figure out easiest way to get work done. Phishing first appeared in the context of AOL password thefts. Some ways password phishing occurs is by sending spam to email and reporting password solicitation button on web. Initially phishing attacks were written in poor English and would ask all sort of information to the users for example their ATM PINS and emails and users started to be doubtful. Now attackers have learned this and they use better psychology and use genuine bank emails with changed URLs to persuade people (Anderson, 2020).

As we are familiar that it is easiest for scammers to attack victims in their most vulnerable state, therefore there was an increase in Phishing scams during COVID-19 pandemic. During these unpresented times and crises such as losing loved ones, losses of material, physical harm and dislocation, many people had negative impact on their mental health. In order to stay safe, people spent most of the time online be it for school, work or online shopping including many individuals that had very little experience conducting these activities online prior to the COVID-19 pandemic. This led to an increase in cybercrimes, phishing and fraud campaigns (Kaliňák, 2021).

4. Deception

Deception is a major skill used by scammers and con-artists to attack the vulnerable. It is important for us engineers to learn a little bit about deception in order to understand how our users can be a victim of it. The Sally-Anne experiment showed us that children acquire the ability that they are being deceived by the age of 5. It has been suggested that patients with Autism spectrum disorder or Asperger's syndrome develop this skill significantly later in life. Many computer scientists and engineers appear to be on the spectrum which would mean they are not as good at deception as a

neurotypical person (Anderson, 2020). This can lead to flaws in program designing which can be exploited by hackers to deceive our consumers.

Another type of deception is known as self-deception is the active misrepresentation of reality to the conscious mind. For example, people avoid getting medical tests in order not hear bad news. This is described as denial of unpleasant information by Sigmund Freud, in order to decrease anxiety about that event (Anderson, 2020). Self-deception and neutralisation are some of the strategies used by scammers to avoid the guilt they feel about their actions.

Another defense mechanism used by scammers to avoid guilt after their bad actions is minimisation. Minimisation is the process in which people justify their actions or make them appear less harmless. For example, many Nigerian scammers assume that people falling for the scams are racists therefore they deserve to be scammed (Anderson, 2020). The fraud triangle theory suggests that fraud only occurs when the offender is provided sufficient opportunity, pressure and rationalization to commit the crime (Kassem, 2012). For example, employees justify their fraudulent behaviour because they feel their employer underpaid them.

4.1. Online Deception

Online deception is on the rise in today's age. It is because it's a lot easier to deceive a person behind a computer screen than an individual in a face-to- face interaction. One survey suggests that participants in online chat rooms use deception to shield their identity, particularly women for safety purposes and to avoid harassment, whereas men use deception to be more expressive and reveal secrets about them (Hancock, 2007). Loss of social context is a one of the main reasons for online deception. People are franker and anonymity, invisibility, synchronicity and loss of authority lets us drop our guard express feelings from affection to aggression that we would normally not express for social reasons (Anderson, 2020).

As there is increase of money flowing through the internet, there has been increases incidences of fraud reported online in the recent years, some of which include fraudulent internet auctions, credit card frauds, identity thefts and stealing personal information of an individual. Some deception and manipulation tactics used online by scammers to persuade the victims include (Hancock, 2007):

- **Masking:** Eliminating critical information regarding an item (for example social media influencers failing to inform the viewers that the item they are promoting is a paid advertisement).
- **Dazzling:** keeping critical information regarding an item (For example, free trails leading to automatic enrolment without giving clear information to the customers)
- **Decoying:** distracting the victim attention from the transaction, for example by offering free products
- **Mimicking:** creating fake identity by using identify theft mechanism (For example creating a "mirror bank" website that is identical to original website and stealing personal information of user)
- **Inventing:** Making up information about an item (For example advertising a product they do not have or does not exist)
- **Relabelling:** exaggerating a transaction to mislead person (For example, selling questionable material online as in good shape).
- **Double play:** convincing the victim that they are taking advantage of deceiver (for example, sending emails designed to look like internal memos).

4.2. Deception in Practice

Deception involves an abuse of techniques developed by compliance professionals. Marketing is another word for deception. There are many techniques used by marketing agents in advertising to scam the consumer. 6 main classes of techniques used to influence people include (Anderson, 2020):

- **Reciprocity:** most people feel the need to return favours to others
- **Commitment and consistency:** people feel guilty if they think they are being inconsistent.
- **Social proof**: most people want to belong to a group and want approval of others in that group
- **Liking:** Most people want to accept something that a good-looking or likable person offers
- **Authority:** Most people obey someone who is an authoritative figure
- **Scarcity:** People are afraid of missing out; therefore, they will buy something that is advertised as limited supply.

4.3. Types of Online Social Deception

There are merely 5 types of online social deception that takes place. This part of paper is inspired by (Gou, 2020). These include:

- **False Information**: False information on the social networking sites, also known as mis-information or disinformation can mislead people's belief. It can be categorized as fact-based or opinion-based. Some of types of false information include:
    - Fake news: Propaganda or large-scale hoaxes are for example seen commonly during US presidential elections. Twitter and Facebook banned thousands of pages to block us propaganda during the US elections.
    - Rumors: defined as unverified news that spreads over different networks online.
    - Information manipulation: false information that is deliberately spread by malicious user to propagate opportunistic disinformation for financial interests or political purposes
    - Deceptive online comments or fake reviews: or google about a product so people are more likely to buy the product because other people had good experience with it.
- **Luring:** common luring techniques in online world include:
    - Spamming: Malicious users send spam messages ranging from advertising to phishing messages in order to gain access to personal information of the user
    - Phishing: Online phishing attacks webpages or emails can lure users to reveal sensitive information such as Social insurance number and financial information. These can lead to economic losses and threaten security of users.
- **Fake Identity:** Use of fake identity is common online and carry from harmless intent to malicious activity. These include:
    - Fake profile: Creating fake identities for example on Facebook for their benefit for financial gain or breaching public personal data such as addresses, date of birth and pictures of victim and their family/ friends. This is also known as Sybil attack.

- Profile Cloning: Creating a duplicate of existing profile in same or different social media platform and use it to send request and deceive them. After construction relationship with the victim, the attacker can steal sensitive data. This has been used in many serious cybercrimes such as cyberbullying, cyberstalking and blackmail. Profile cloning poses serious financial, social and physical threat to the victim.
- Compromised Accounts: Hacking of legitimate account and establishing connection with other legitimate users.

- **Crowdturfing:** paid workers who perform malicious activities online, they belong to an astroturfing campaign and spread fake information to mislead people's belief. This is done on different social networking websites including instant messages, groups, blogs and online forums. It is challenging to detect these accounts as these posts are camouflage with normal posts.
- **Human Targeted Attacks:** Cybercriminals start their crime by establishing true relationship with the victim first by social deception and then attack them. Some examples are:
  - Human Trafficking: Online human trafficking involves kidnappers using advertising services online and kidnapping great number of victims.
  - Cyberbullying: This involves online harassment of victims and publicly harassing them on these platforms.
  - Cyber-grooming: involves establishing relationships with victims with the intent of having improper sexual relationships with them or produce pornography content.
  - Cyberstalking: Attackers exploit information of legitimate users and harass them stalking.

The table below provides a visual representation of types of online deception and how frequently are they used.

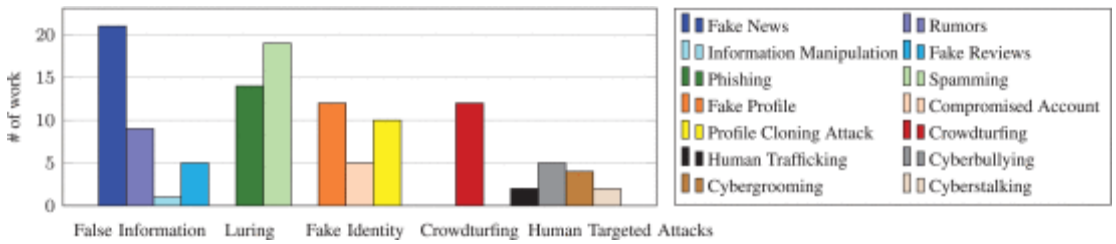

Figure 2. Types of Online Social Deception.

4.4. Susceptibly to Online Social Deception

The goal an attacker is to successfully conduct an attack and therefore they use psychology, diversity, and gender biases to figure out which population will be highly susceptible to their scam. In this section, we will discuss various types of susceptibility traits to online deception attacks. These include:

- **Demographic factors:** Young people between ages 18-25 are susceptible to phishing than other age groups. On the other hand, children are potential victims for cyber-grooming. Old women in particular are also found to be more vulnerable population to phishing (Gou, 2020).
- **Cultural factors:** Societies that tend to have collectivistic culture are more prone to online deception. It is because collectivistic societies are tightly connected and tend to trust each other more than individualist cultures where privacy is more valued.
- **Socio-economic factors**: Lower socioeconomic status, such as lower income families and lower education background are more susceptible to online deception
- **Social isolation**: individuals socially isolated and looking to make friends, relationships online tend to engage in more online activities and are more vulnerable to attacks such as cyber-grooming (Gou, 2020).

4.5. Deception Research

Since 9/11 there has been a lot of work done in deception. Lie detectors and polygraph measures have been used for crime investigation. Polygraph test measures stress via heart rate and skin conductance. It can also measure distraction using eye movements and guilt by upper body movements. Another way to prevent deception is to train machine learning classifier on real customer behaviour. This has been used for credit-card fraud engines (Anderson, 2020). Another method by which deception can be detected online is via products such as Microsoft IIS or Apache (Ishikawa, 2017).

5. Passwords

Passwords are one of the main targets of hackers to gain access to people accounts. They are in place to provide security to user's privacy but when compromised it can pose a major security threat to user's information. The problem with passwords being our main source of authentication mechanism is that it requires the user to remember the password. What we know about human memory is that people cannot remember items changed frequent. If the password is more complex for example with letters and symbols, it becomes non-memorable whereas easier passwords are easier to hack (Anderson, 2020).

Back in the days password recovery methods included security questions like first car or maiden name, this type of information is easy guessable than the password itself. In 2008 Yahoo email of US vice-president Sarah Paulin was hacked by guessing security questions like her date of birth and her school. This type of information is easily available over the internet and therefore it becomes easier to guess these compared to the password itself and defeats the purpose of "security questions". This is why most social media is moving away from this type of security methods. Many banks websites are no using sending code to person's phone via SMS every time security check is required. Google search shows that SMS stop all bulk of guessing by bots, 96% of bulk phishing and 76% of targeted attacks. Hackers seem to be finding a solution to this as well. Since 2020, SIM-swap attacks are becoming more common where attacker pretends to be from your mobile phone company and gets a replacement SIM card for your account. This type of hacks first started in 2007 in Nigeria and are becoming common rest of the world (Anderson, 2020).

Many accounts are compromised because their passwords are guessed. Recent examples include cryptocurrency wallets where anonymous bitcoin bandit managed to steal $50 Million by trying weak passwords and successfully hacking into accounts. There are examples of people losing billions of dollars' worth of cryptocurrency simply because they forgot their passwords. This brings us to the other problem that if possible is too complex humans forget it or have difficulty entering the systems locking them out of their account (Anderson, 2020).

A study done showed users are aware of what constitutes a good or bad password but they are still motivated to engage in bad password management behaviours because they do not see any immediate negative consequences. This is known as negative externalities. They choose to prefer convivence over security (Espana, 2016).

6. Conclusion

In conclusion, psychology is study of human mind and behaviour and how we use the environment around us to make decisions. Psychology plays a major role in fields especially artificial intelligence and computer science because it involves interacting with other humans. Psychology includes many different branches but the ones that needed to be understood by us while coming up with programs is cognitive psychology and social psychology.

Cognitive psychology involves learning about how humans think. It has been shown that users with mild cognitive impairment tend to fall for more scams. Some of the errors in human cognition that hackers utilize include capture error and post-completion error. Therefore, it is important for us to understand human cognition and come up with programs that suit best for all diversity. Social psychology looks at how people get influenced by other people around them. People tend to belong to a group and like to conform to the norms of that group. It has been shown that people tend to change their behaviour around others and get persuaded by the group or people around them. This can be explained by the bystander effect where it has been seen that a lone bystander is more likely to help a victim in need than if there are more people around.

This brings us to lack of diversity and gender equality friendly system designs which leads to people being vulnerable to attacks by hackers. Many programs are made by males and this leads to women being more vulnerable to online scams such as phishing. This is also seen in people with different socio-economic background and educational backgrounds. Older women, less educated people and people of different cultural background are more likely to be attacked by scammers. During COVID-19 pandemic phishing scams were on rise because people are more vulnerable and where using computers for merely all aspects of their life, be it school, work or shopping.

Deception is another technique used by scammers to persuade people into victims. Some of these techniques include Masking, Mimicking, Dazzling, Decoying, Inventing, Relabelling and Double play. Online deception is on rise because it is a lot easier to people behind computer screen then in face to face interaction. People also tend to franker and anonymous which leads to us letting our guard down. There has also been an increase in identity thefts, credit card frauds and stealing personal information. Online social deception occurs by scammers using techniques such as spreading false information, luring, fake identity and crowd-turfing. Passwords are another source of target for hackers to compromise privacy of users. It is difficult for people to remember passwords or come up with complex password which is where the hackers take advantage to attack them.

We as engineers are people making system for the people therefore it is important for us to understand psychology so we can come up with better systems to provide better experience to our users and also protect them from hackers.

7. References

1. Schacter, Daniel L., Daniel T. Gilbert, and Daniel M. Wegner. *Psychology*. Macmillan, 2009.

2. Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020.

3. Hancock, Jeffrey T. "Digital deception." *Oxford handbook of internet psychology* 61.5 (2007): 289-301.

4. Boyle, Patricia A., et al. "Scam awareness related to incident Alzheimer dementia and mild cognitive impairment: a prospective cohort study." *Annals of internal medicine* 170.10 (2019): 702-709.

5. McLeod, Saul. "Solomon Asch-Conformity Experiment." *Simply Psychology* 28 (2018).

6. Ewell, Patrick J., Jessica A. Minney, and Rosanna E. Guadagno. "Social influence online." *Encyclopedia of Information Science and Technology, Third Edition*. IGI Global, 2015. 6762-6772.

7. Wenger, Nanette K. "Coronary heart disease: the female heart is vulnerable." *Progress in cardiovascular diseases* 46.3 (2003): 199-229.

8. Kassem, Rasha, and Andrew Higson. "The new fraud triangle model." *Journal of emerging trends in economics and management sciences* 3.3 (2012): 191-195.

9. Guo, Zhen, et al. "Online social deception and its countermeasures: A survey." *IEEE Access* 9 (2020): 1770-1806.

10. Ishikawa, Tomohisa, and Kouichi Sakurai. "Parameter manipulation attack prevention and detection by using web application deception proxy." *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication*. 2017.

11. Kaliňák, Viliam. "Psychology of Phishing Attacks During Crises: The Case of Covid-19 Pandemic." (2021).

12. España, Lezlie Y. "Effects of password type and memory techniques on user password memory." *Psi Chi Journal of Psychological Research* 21.4 (2016): 269-275.