ASSIGNMENT 501 MEETING MINUTES

TEAM MEMBERS:

Noah King
Joshua Knight

Nevin Kishore

24th April – Topic Discussion

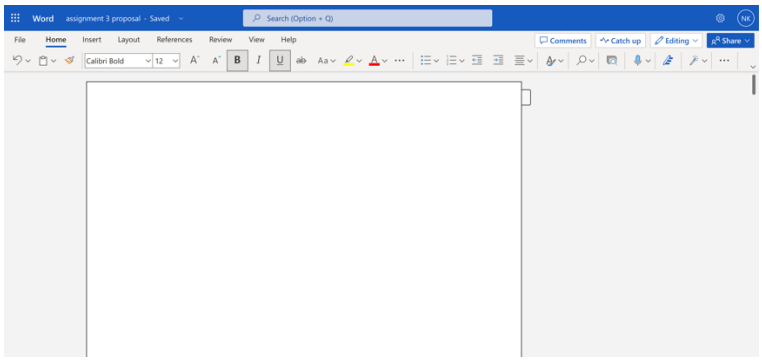
We went through possible topics we are able to narrow down and research about. We also discussed out strengths and weaknesses that we are able to utilise in terms of different aspects during out assignment creation.

Our possible topic ideas consist of:

- Artificial Intelligence
- Cybersecurity
- Cyberbullying

We leaned towards cybersecurity as it is a boarder topic with many examples to talk about. We narrowed out topic down to cyberterrorism in terms of social engineering.

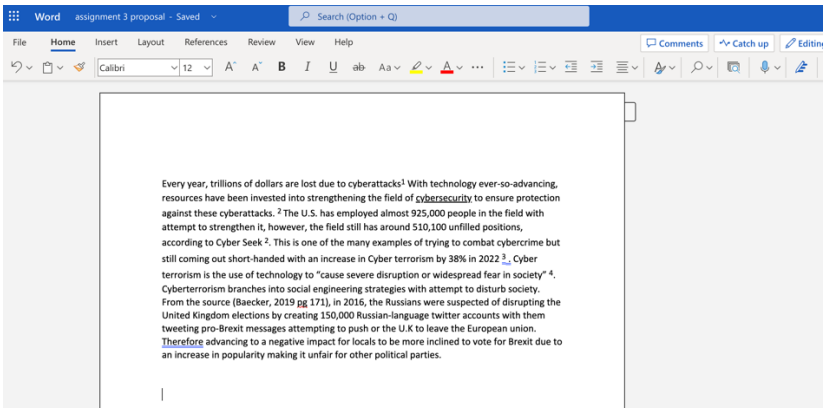
We created an Instagram group chat as well as an online word document in order for us to keep in contact and be able to update each other on parts of our work. We have also established roles of our group in terms of a primary researcher, coder and writer.



1st May – Proposal Writing

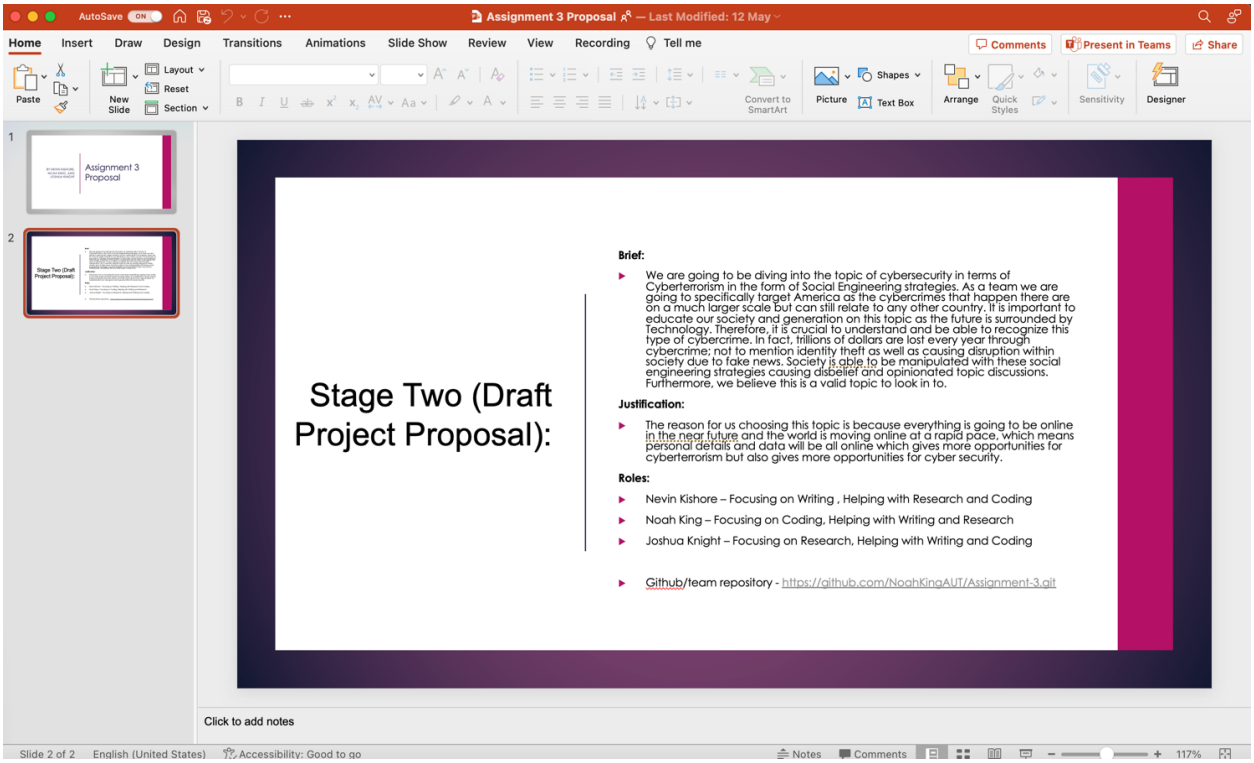
In class we started a proposal writing where we had Nevin writing and Noah creating the github link.

We created a paragraph with an explanation of our topic and what was to be covered. We had also created roles.



3rd May – PowerPoint Creation

After finding out the information had to be presented on a PowerPoint slide, Nevin created a base slide and shared the document to the group so that we were all able to edit it.



8th May – Proposal Presenting

Joshua and Nevin were able to present the proposal for the class

18th May – Research began

https://www.bbc.com/news/world-us-canada-57703836

from the bbc news

on July 3, 2021

main point pasted -**About 200 US businesses have been hit by a "colossal" ransomware attack, according to a cyber-security firm.**

Attack – ransomware and supply chain attack

Ransomware attack is when someone or a group of people try to gain access to a computer network so that they can hold it hostage and demand for money to gain back access. This attack is hard to accomplish but when done they can request for lots of money.

This is so far the biggest ransomware attack on supply chains in the us currently.

Over 200 supply chains were attacked, these supply chains support big business, so not just effecting the the suppily chains but business too.

Pasted - At a summit in Geneva last month, US President Joe Biden said he told Russian President Vladimir Putin he had a responsibility to rein in such cyber-attacks. Mr Biden said he gave Mr Putin a list of 16 critical infrastructure sectors, from energy to water, that should not be subject to hacking.
REvil - also known as Sodinokibi - is one of the most prolific and profitable cyber-criminal groups in the world.
The gang was blamed by the FBI for a hack in May that paralysed operations at JBS - the world's largest meat supplie

Caused by REvil/Sodinokibi

24th May – Presentation Powerpoint Started

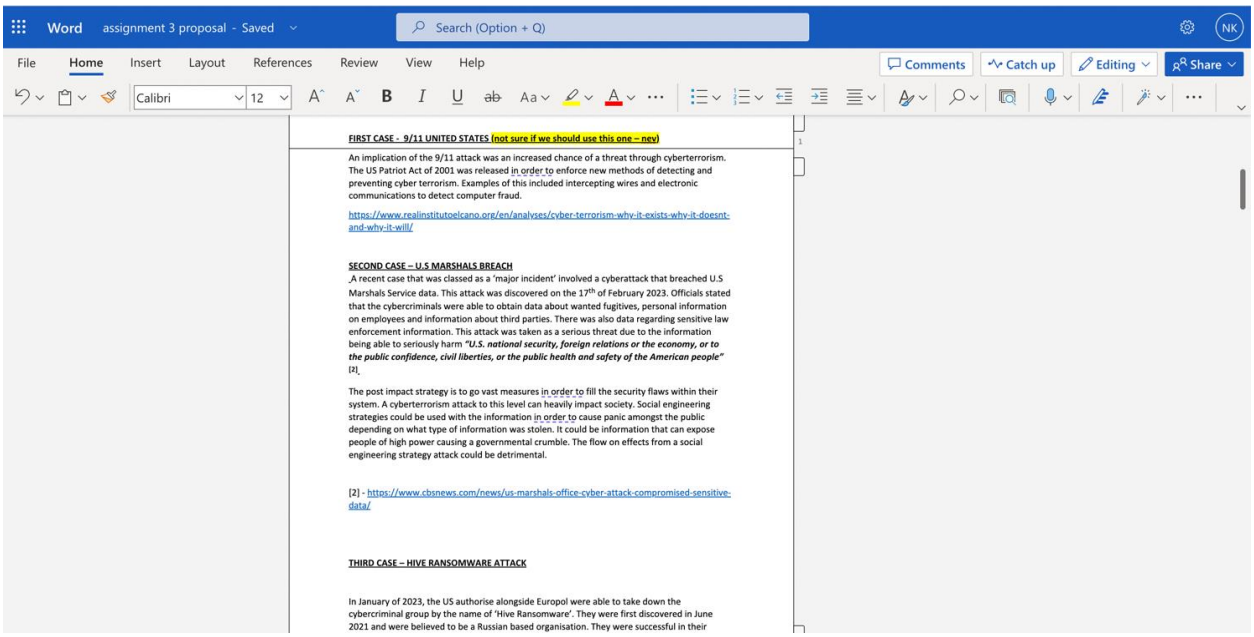
We created another PowerPoint document for the presentation and divided the workload so that we all had equal parts. Nevin had the first slide, Josh had the second slide and Noah had the third slide. We were able to all work on the slides at the same time making the task easier and more efficient. We also used out group chat for help when required.

29th May – Presentation Powerpointed Presented

Joshua and Nevin were able to present in class

1st June – Information For Website

We had started gathering more and more information to be used in the website. Noah has also used the template of the website to get a start.



FIRST CASE - 9/11 UNITED STATES (not sure if we should use this one – nev)

An implication of the 9/11 attack was an increased chance of a threat through cyberterrorism. The US Patriot Act of 2001 was released in order to enforce new methods of detecting and preventing cyber terrorism. Examples of this included intercepting wires and electronic communications to detect computer fraud.

https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/

SECOND CASE – U.S MARSHALS BREACH

A recent case that was classed as a 'major incident' involved a cyberattack that breached U.S Marshals Service data. This attack was discovered on the 17th of February 2023. Officials stated that the cybercriminals were able to obtain data about wanted fugitives, personal information on employees and information about third parties. There was also data regarding sensitive law enforcement information. This attack was taken as a serious threat due to the information being able to seriously harm ***"U.S. national security, foreign relations or the economy, or to the public confidence, civil liberties, or the public health and safety of the American people"*** [2].

The post impact strategy is to go vast measures in order to fill the security flaws within their system. A cyberterrorism attack to this level can heavily impact society. Social engineering strategies could be used with the information in order to cause panic amongst the public depending on what type of information was stolen. It could be information that can expose people of high power causing a governmental crumble. The flow on effects from a social engineering strategy attack could be detrimental.

[2] - https://www.cbsnews.com/news/us-marshals-office-cyber-attack-compromised-sensitive-data/

THIRD CASE – HIVE RANSOMWARE ATTACK

In January of 2023, the US authorise alongside Europol were able to take down the cybercriminal group by the name of 'Hive Ransomware'. They were first discovered in June 2021 and were believed to be a Russian based organisation. They were successful in their

according to a report from U.S agencies [3]. The HIVE was identified as a major threat as they were able to encrypt and compromise information of large IT and oil companies within the United States and of the European union.

This included million dollar deals to hack into large corporates[4]. The most commonly affected industries that the HIVE stole from include government facilities, telecommunication, manufactures, healthcare and information technology. Their most known attack was forcing a California healthcare facility to shut down.

The HIVE exploited networks by distributing phishing emails with malicious attachments. People would open these attachments without being able to recognise the malicious content and would in turn leave their device vulnerable to attacks [5]. Through accessing the attachment, HIVE were able to access the victims network meaning every device on the network was now accessible to the hackers.

The HIVE had social engineering strategies in the way that they attacked large groups of people through these attachments and even at times requested for ransom money. Phishing is a form of social engineering strategy in the way that they are able to obtain confidential information and influence peoples behaviour.

[3] - https://therecord.media/cisa-hive-ransomware-has-netted-more-than-100-million-from-over-1300-victims

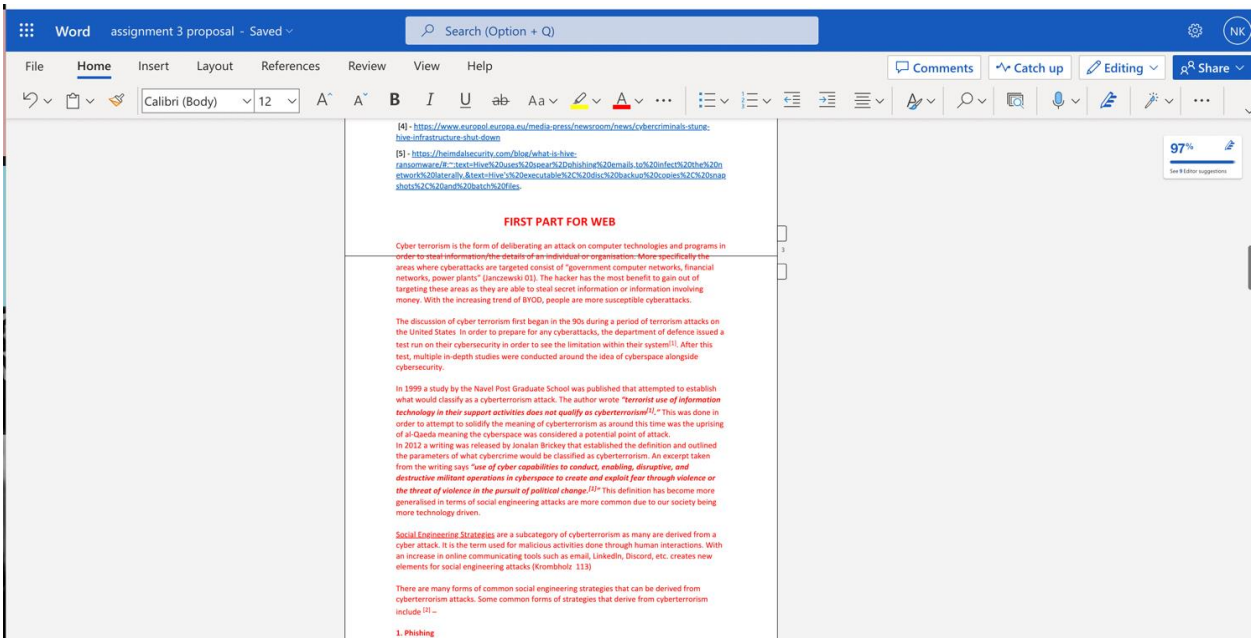
[4] - https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down

[5] - https://heimdalsecurity.com/blog/what-is-hive-ransomware/#:~:text=Hive%20uses%20spear%2Dphishing%20emails,to%20infect%20the%20network%20laterally.&text=Hive's%20executable%2C%20disc%20backup%20copies%2C%20snapshots%2C%20and%20batch%20files.

9

6th June – Website writing started

We have started to finalise information and sources for the website. We also spent some time helping each other understand referencing. Nevin finished his part first and was able to assist Josh in helping to write out one part.



[4] - https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down

[5] - https://heimdalsecurity.com/blog/what-is-hive-ransomware/#:~:text=Hive%20uses%20spear%2Dphishing%20emails,to%20infect%20the%20network%20laterally.&text=Hive's%20executable%2C%20disc%20backup%20copies%2C%20snapshots%2C%20and%20batch%20files.

FIRST PART FOR WEB

Cyber terrorism is the form of deliberating an attack on computer technologies and programs in order to steal information/the details of an individual or organisation. More specifically the areas where cyberattacks are targeted consist of "government computer networks, financial networks, power plants" (Janczewski 01). The hacker has the most benefit to gain out of targeting these areas as they are able to steal secret information or information involving money. With the increasing trend of BYOD, people are more susceptible cyberattacks.

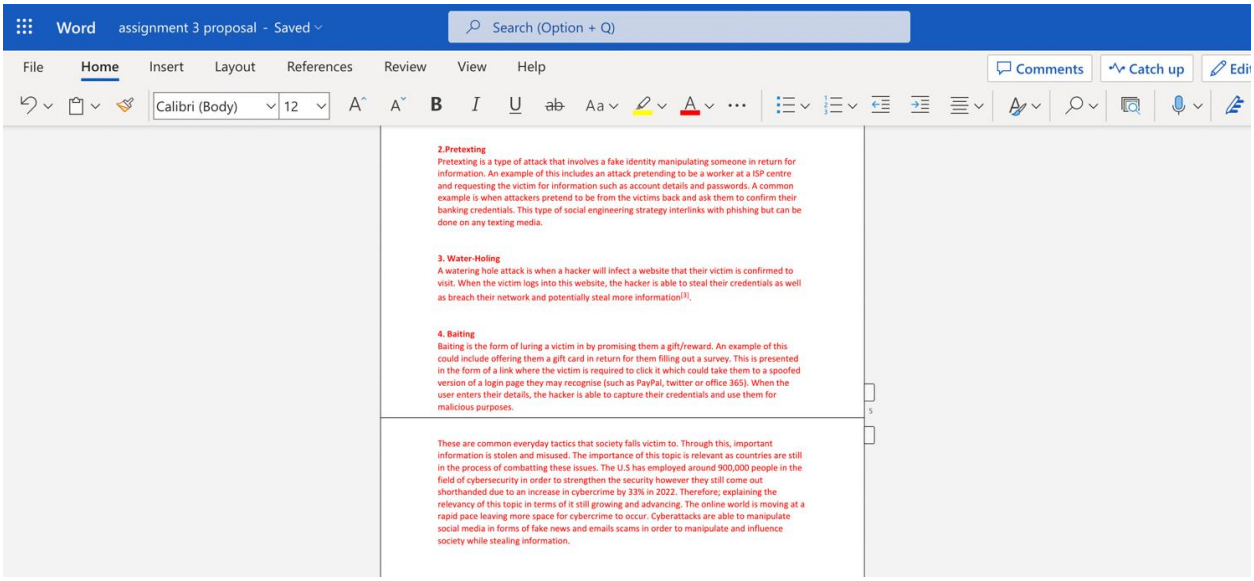
The discussion of cyber terrorism first began in the 90s during a period of terrorism attacks on the United States In order to prepare for any cyberattacks, the department of defence issued a test run on their cybersecurity in order to see the limitation within their system[1]. After this test, multiple in-depth studies were conducted around the idea of cyberspace alongside cybersecurity.

In 1999 a study by the Navel Post Graduate School was published that attempted to establish what would classify as a cyberterrorism attack. The author wrote ***"terrorist use of information technology in their support activities does not qualify as cyberterrorism[1]."*** This was done in order to attempt to solidify the meaning of cyberterrorism as around this time was the uprising of al-Qaeda meaning the cyberspace was considered a potential point of attack.
In 2012 a writing was released by Jonalan Brickey that established the definition and outlined the parameters of what cybercrime would be classified as cyberterrorism. An excerpt taken from the writing says ***"use of cyber capabilities to conduct, enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change.[2]"*** This definition has become more generalised in terms of social engineering attacks are more common due to our society being more technology driven.

Social Engineering Strategies are a subcategory of cyberterrorism as many are derived from a cyber attack. It is the term used for malicious activities done through human interactions. With an increase in online communicating tools such as email, LinkedIn, Discord, etc. creates new elements for social engineering attacks (Krombholz 113)

There are many forms of common social engineering strategies that can be derived from cyberterrorism attacks. Some common forms of strategies that derive from cyberterrorism include [2] –

1. Phishing

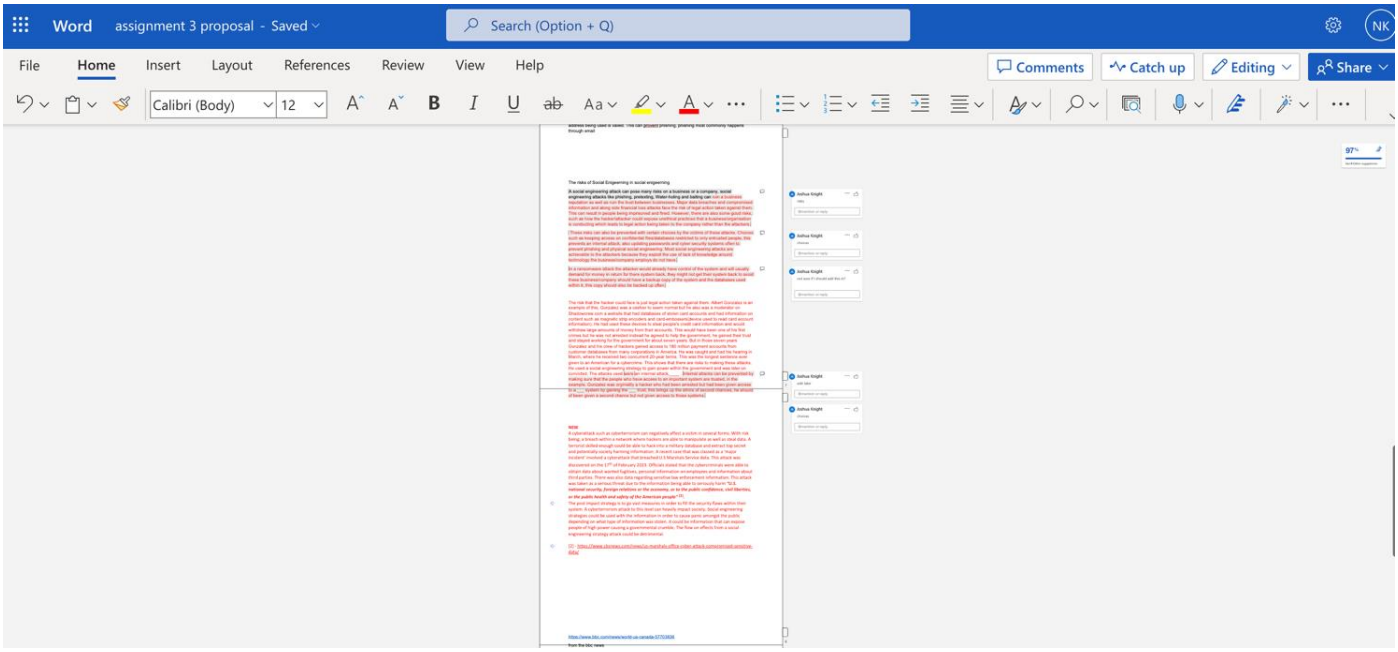


2.Pretexting
Pretexting is a type of attack that involves a fake identity manipulating someone in return for information. An example of this includes an attack pretending to be a worker at a ISP centre and requesting the victim for information such as account details and passwords. A common example is when attackers pretend to be from the victims back and ask them to confirm their banking credentials. This type of social engineering strategy interlinks with phishing but can be done on any texting media.

3. Water-Holing
A watering hole attack is when a hacker will infect a website that their victim is confirmed to visit. When the victim logs into this website, the hacker is able to steal their credentials as well as breach their network and potentially steal more information[3].

4. Baiting
Baiting is the form of luring a victim in by promising them a gift/reward. An example of this could include offering them a gift card in return for them filling out a survey. This is presented in the form of a link where the victim is required to click it which could take them to a spoofed version of a login page they may recognise (such as PayPal, twitter or office 365). When the user enters their details, the hacker is able to capture their credentials and use them for malicious purposes.

These are common everyday tactics that society falls victim to. Through this, important information is stolen and misused. The importance of this topic is relevant as countries are still in the process of combatting these issues. The U.S has employed around 900,000 people in the field of cybersecurity in order to strengthen the security however they still come out shorthanded due to an increase in cybercrime by 33% in 2022. Therefore; explaining the relevancy of this topic in terms of it still growing and advancing. The online world is moving at a rapid pace leaving more space for cybercrime to occur. Cyberattacks are able to manipulate social media in forms of fake news and emails scams in order to manipulate and influence society while stealing information.


Word
assignment 3 proposal - Saved
Search (Option + Q)
File
Home
Insert
Layout
References
Review
View
Help
Comments
Catch up
Editing
Share
Calibri (Body)
12