Forum: General Assembly First Committee

Issue: The question of digital and cybersecurity on search engines and social media

Student Officer: Kaveen Parthiban

Position: Deputy Committee Chair

Introduction

People are increasingly being interconnected with their friends and loved ones through the World Wide Web (WWW). They are able to share photos, videos, and events seamlessly at the push of a button, transferring information instantly via applications such as Facebook and Instagram. Individuals have also gained access to a multitude of articles, webpages, databases and information through the use of search engines such as Google, allowing for further research and to increase our understanding of the world. However, the ease with which this happens often blinds us from realising how the information we provide on the WWW is used and the threat search engines pose on our lives and privacy. It is the question of cybersecurity that search engines and social media provide for us individuals.

In terms of social media, many people are unaware of the availability of the information they put on their social media accounts to the world and how it is used. In addition, companies sometimes do not give cybersecurity the value it deserves. This is in light of the Cambridge Analytica data breach, which saw the information of over 70 million users utilised by the company of the same name unbeknowingly to the users. There was negligence by Facebook to fully address the privacy issue it identified in 2015. Moreover there is a lack of cybersecurity education for individuals that use social media. This includes identity-driven cyber threats such as spoofing, phishing and impersonation as well as permissions to their information.

Search engines also pose an equal threat on our lives. Although we are able to access a variety of resources, there is the risk of malware and viruses being inflicted upon us individuals and the companies we work for. This is where Search Engine Optimisation (SEO’s) comes into play. This is a technique of designing a website to improve its rankings in search engines. Malicious website operators can use wording in its sites that reflect the current trends in society. Such as when a video or image “goes viral”, people will search for it, and hence these operators will create a website to attract individuals who search
for them. This can easily compromise the individuals’ computer and steal personal information. It is thus highly important that user education is maximised to lower the risk of such malicious attacks.

Definition of Key Terms

Cybersecurity

Cybersecurity comprises of technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks. It can be the installation of firewall or even basic user education on how to avoid cyberattacks.

Social Media

Social media are web-based communication tools that enable people to interact with each other by both sharing and consuming information. This includes Facebook, Gmail, Snapchat and Instagram.

Search Engines

A program or website that searches for and identifies items in a database that correspond to specified keywords or characters, mainly used for finding particular sites and information on the World Wide Web.

Search Engine Optimisation (SEOs)

The technique of designing a website to improve its ranking in search engines. This is a common marketing strategy for websites and not inherently or always malicious. If a website operator wants to attract more visitors, he or she will want the search engines to steer people to the site. However, this can be misused to improve rankings of a malicious website that can infect an individual’s computer.

Encryption

It is the process of encoding data, making it scrambled. In a lot of cases, encrypted data is also paired with an encryption key, and only those that possess the key (a collection of unique algorithms) will be able to unscramble the data to make it readable and accessible. This makes data transfer secure, and provides users with an additional sense of security and privacy with the management of their data by companies. This makes users more confident in providing personal information to websites and to friends over social media. On the business perspective, this allows them to easily and quickly exchange data with other businesses which can lead to increased revenue and increased customer satisfaction.
World Wide Web (WWW)

It is combination of all resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP). The WWW has made information easily accessible by many people; allowing people to seamlessly communicate with others around the world and assisting in the process of globalisation. However, this has also made users susceptible to data theft and manipulation, as many websites appear safe and secure but in fact are malicious and do not serve their described purpose.

Background Information

Cybersecurity is gaining increasing importance in today’s society. The nature and cost of cyberattacks are varied, with personal data such as birth certificate numbers, social security numbers and bank details being unlawfully obtained and companies facing falling share prices as a consequence. Although such cyberattacks may initially target one individual, it can spread to other individuals in the company; affecting business. The Office of Cyber Security and Information Assurance estimate that cybercrime costs UK businesses more than £21 billion per year. Ineffective cybersecurity from individuals can compromise their own privacy and in turn livelihood, whilst ineffective cybersecurity from business can affect profits and damage individuals who use their services. Such is the case of cybersecurity in social media and search engines.

Social Media

The pool of potential social media victims is huge. The number of social media users is expected to grow from 2.04 billion worldwide in 2015 to 2.55 billion by 2018. That’s about a third of Earth’s population.

In addition, as companies become more digitised to target these social media users, they continue to build their social media presence. According of Altimeter, 38% of companies plan to spend more than 20% of their total ad budgets on social media channels. This focus makes social media a lucrative target for cyber criminals. One of the most effective methods is fraudulent accounts. These scammers would conceal themselves as corporate brands to defraud consumers. Proofpoint’s Social Media Brand Fraud Report for 2016, in fact found that of the 4,840 fraudulent accounts associated with top 10 brands (which included BMW, Amazon, Shell and Samsung in this study) 19% were fraudulent. Often they will offer free and/or discounted gifts, offer software updates or customer support by filling in personal details in a survey, or install malware to extract information from your computer unlawfully. The methods that this can occur include through phishing, malware, scams and counterfeit products.
WhatsApp

WhatsApp added end to end encryption for all of its messages in April 2016. This means that all messages are encoded and can only be decoded by the receiver. This adds additional security for users, preventing governments and even the parent company Facebook from reading your messages. This was in light of the San Bernardino shooting, where the Federal Bureau of Investigation (FBI) asked Apple to unlock one of the shooter’s iPhone 5C.

However, the concern now amongst people is that such end to end encryption programs allow for terrorists to converse secretly. The UK’s Home Secretary, Amber Rudd notes that the governments must make sure they “don’t provide a secret place for terrorists to communicate with each other.”

Cambridge Analytica

In 2014, Aleksandr Kogan developed a Facebook application called “thisisyoudigitallife” where users were paid to fill out a survey. This data was then collected alongside data of the friends of those users and in this fashion, over 50 million Facebook user profiles were subject to this data collection. Kogan then sold the data to Cambridge Analytica, to which a whistleblower of the company Christopher Wylie in 2018 said the data was used so it could target US voters with personalised political advertisements and pro-Trump material based on their psychological profiles.

Although Facebook says that Kogan received this information legitimately, Facebook said he lied to the firm and violated its policies in the transfer of this data to Cambridge Analytica. Even when Facebook banned the app in 2015 upon the knowledge of such malpractice and requested for the data to be deleted, it is reported that the data was not removed. This data breach highlights how easily data can be obtained and manipulated through social media, and also brings to light the necessary cybersecurity measures that need to be implemented to combat future data breaches such as stricter policies by Facebook.

Search Engines

Search engines form the basis of how we utilise the WWW. We use them to search for resources we need for our assignments, tasks, personal needs et cetera. However, search engines can facilitate the illegitimate acquisition of data from our computers and our user accounts. This can come from SEO, whereby malicious website operators make their websites more attractive by having them ranked higher in search engines. By clicking on such websites, they could inflict malware and viruses. Also, such malicious operators can hack popular websites and obtain information by “acting” as the purported website. The worrying part is that according to Sitelock only around 1 in 5 infected websites are
blacklisted by search engines, whilst Wordfence says that of the 1605 people they surveyed whose website was hacked, only 46.5% of them reported being flagged by Google. This highlights how easily and unknowingly a user can stumble upon a malicious website and compromise their data. Moreover, it is estimated that around 18,500,000 websites are infected with malware at a given time each week further highlighting how those without cybersecurity education can easily be targeted.

Small businesses are often those that are infected by malware and viruses. This is because they are the ones that do not have the necessary funds to improve their security measures as they start out their business. This is worrying as the sheer number of small businesses out there are large, and many of them are also unaware of the importance of cybersecurity.

Advertisements

Advertisements are used by search engines as a main form of revenue. As such, the chances of false and misleading advertisements are high and this can directly influence our behaviours and actions. For example, China’s Baidu was found to have advertised misleading medical information which led to the death of a college student. Wei Zexi died in April after being led to an experimental cancer treatment in Baidu’s paid search results. This prompted China’s Cyberspace Administration (CAC) to unveil a set of new rules covering web search and mobile apps in 2016. The CAC said search engines will be “prohibited from providing banned information in various formats including links, summaries, cached pages, associative words, related searches and relevant recommendations” whilst being “required to report websites and applications that contain prohibited content when spotted”.

Also since the above incident was caused by a misleading paid advertisement, the new legislation also stresses that search engines operating in China must investigate clients offering paid-for advertisement, set a clear upper limit on such advertisements and clearly distinguish which are paid-for advertisement and which come from “natural searches”.

Major Countries and Organizations Involved

European Union (EU)

The European Union (EU) in 1995 implemented their "Data Protection Directive" which regulates the processing of personal data within the region, that became an important component of EU privacy. This will be explored further in the previous attempts to solve the issue.
Following this, the EU adopted “The General Data Protection Regulation (GDPR)” in May 25th 2018, which strengthens a number of rights already introduced in the “Data Protection Directive”. It means individuals will find themselves with more power to demand companies reveal or delete the personal data they hold, as well as ensuring data is not publicly available without clear informed consent. Once again this will be further explored in the previous attempts to solve this issue.

**United States (US)**

In 2002 the US implemented the “Homeland Security Act”, which included the “Federal Information Security Management Act (FISMA)”. However, the rules stated are not rigid in securing data and require only a “reasonable” level of security. For example, FISMA says that it “requires the development and implementation of mandatory policies, principles, standards, and guidelines on information security” by companies, leaving a lot of room to interpretation.

In 2014 the US also implemented the “Cybersecurity Enhancement Act”, which provides an ongoing but voluntary public-private partnership to improve and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

**China**

China has been known to censor and effectively ban search engines such as Google and Facebook from its citizens. Whilst the common perspective is that this limits individual freedom, officials in China maintain that they “are needed to ensure security against growing threats, such as terrorism” and to prohibit the spread of “rumors, obscenities, pornography, violence, murder, terrorism and other illegal information”.

**Timeline of Events**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>The EU implemented the “Data Protection Directive” which regulates the processing of personal data within the region, that became an important component of EU privacy.</td>
</tr>
<tr>
<td>2002</td>
<td>The US implemented the “Homeland Security Act” as well as the “Federal Information Security Management Act (FISMA)”. This requires companies to build necessary policies, standards and guidelines on their information security.</td>
</tr>
</tbody>
</table>
2014
The US implemented the “Cybersecurity Enhancement Act” which calls for public-private partnership to improve cybersecurity research and development, workforce development and education and public awareness and preparedness.

August 2016
China’s Cyberspace Administration (CAC) implemented strict regulations on the nature of paid advertisements allowed on search engines in China following the death of a misled college student.

September 28th 2017
The US implemented the Main Street Cybersecurity Act which aims to assist small businesses in reducing their cybersecurity risks. It will provide resources as well as promote a workplace cybersecurity culture.

May 25th 2018
The EU adopted the “The General Data Protection Regulation” which calls for greater consent from users if their data is to be made public, and gives users the power to delete the personal data that they hold of them.

Relevant UN Treaties and Events

In terms of UN resolutions or treaties, there are very few. Most policies or legislation that tackle cybersecurity are adopted by member states themselves.

- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, March 2010 (A/RES/64/211)
- Combating the criminal misuse of information technologies, 22nd January 2001 (A/RES/55/63)

Previous Attempts to Solve the Issue

In 1995 the EU adopted their “Data Protection Directive” which regulates the processing of personal data in the EU. This came about after the Organisation of Economic Cooperation and Development (OECD) issued seven recommendations for personal data protection which includes:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject’s consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;

6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data

7. Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

Although this was implemented in the “Data Protection Directive”, it is to be noted that the US did not endorse these guidelines in their own legislations.

This directive, however, has been superseded by the “The General Data Protection Regulation (GDPR)” in May 25th 2018 by the EU. Since this is not a directive but a regulation, it does not require national governments to pass any legislation and is automatically applicable and binding. Therefore, the GDPR applies to any organisation operating within the EU, but also to those organisations outside of the EU which offer goods or services to customers or businesses in the EU. This ultimately means that most corporations around the world would need to adhere to the GDPR.

Under the terms of the GDPR, organisations have to ensure that personal data is gathered legally and under strict conditions of consent, whilst those who collect and manage it will be obliged to protect it from exploitation, as well as to respect the rights of data owners. Moreover, organisations must explicitly tell consumers how their customer data is being used, and give them the option of deleting their personal data if they no longer want it processed. In addition, following a hack or data breach, organisations will be required to notify the appropriate national bodies as soon as possible in order to ensure EU citizens can take measures to prevent their data from being misused. This piece of legislation does however come with criticism. It puts small and upcoming businesses in a tough position to develop or acquire technology to meet these requirements. They may not be having sufficient funds from the start to adhere with this regulation therefore limiting the effectiveness of the strategy as a whole.

On September 28th 2017 the US Senate passed the Main Street Cybersecurity Act which will have the The National Institute of Standards and Technology (NIST) to “disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks.” These resources targeted at small businesses in the US are to promote a workplace cybersecurity culture and to promote awareness of cybersecurity risks and methods of prevention.

Possible Solutions
The most effective solution to phishing, scams and being subject to malware is user education. Individuals need to be educated on deals that look “too good to be true” and avoid providing their bank and personal details to such places, even when Google or other search engines fail in blacklisting them. In addition, they need to understand that shortened URL’s like Google’s https://goo.gl could make the link read better, but could disguise a link to a malicious website that can instantly infect malware into your computer. Whilst such cybersecurity risks are endless and getting more advanced and complicated, employers in particular should consistently educate their employees of the latest threats and risks and provide free courses and programs that incentivise the uptake of cybersecurity education. This includes being reminded to update their social media passwords regularly and to make them lengthy and complicated. This will ensure that the company they are working for, has a reduced risk of a data breach or hack that could compromise millions of individuals. As such employees gain cybersecurity education, which makes them more employable as the global economy becomes more digitised and requires people who know how to avoid such risks.

This also means that companies such as Facebook and Instagram should set out clear and understandable guidelines that make it easy for consumers to manage their privacy and security. Whether it be allowing the public to view their photos or sending data to third party applications, consumers need to be fully aware of how to manage such events. Since these social media applications are global, they also need to effectively translate their guidelines into other languages, making it easy for everyone to understand.

Consumers should also be reminded to consistently update their computer and mobile softwares as they are released. This is to ensure they are given the latest security measures that can combat the new risks the WWW poses.

Search engines also need to reevaluate their SEO ranking algorithms. This is because the more successful a website is, the higher it is ranked in search results. This makes them easy targets for hackers and gives them a larger scope to infect or scam individuals. Therefore, search engines do need to consistently and regularly perform website checks, as it is reported by Sitelock that only 1 in 5 websites that are infected are blacklisted by search engines.

In addition, whilst the GDPR is the latest most effective personal data protection regulation in the EU, there is a lack of such regulations globally. The US in particular, coming off the recent Cambridge Analytica Data Breach, is an example of this. Therefore, there needs to be a strong resolution that brings together organisations such as the European Union who have regulations in place with those that do not, and in particular Less Economically Developed Countries (LEDCs) who are starting to digitalise.

If Whatsapp is to lead by example, member states should be highly encouraged to adopt encryption methods within their regulations. According to a 2009 report from the U.S. National
Intelligence Council leaked by Edward Snowden, it mentions that secure encryption technology is the “best defense to protect data.” This will thus give an extra layer of protection and confidence to those using social media where personal data is constantly being processed.

Bibliography


