DCLead Master in Digital Communication Leadership

Co-funded by the Erasmus+ Programme of the European Union

Comparative Analysis: The increase in phishing activities.

MASTER THESIS
to obtain the Erasmus Mundus Joint Master Degree

in Digital Communication Leadership (DCLead)

of

Faculty of Cultural and Social Sciences
Paris Lodron University of Salzburg

Technical Faculty of IT and Design
Aalborg University in Copenhagen

Submitted by
David Ayiku
12046395
davidayikuteye@gmail.com
Vognporten 14-856 2620 Albertslund

Prof. Reza Tadayoni
Prof. Sergio Sparviero
Prof Morten Falch

Department of Communication Studies

Salzburg, August 10th, 2023

TABLE OF CONTENTS

Executive Summary

As the world gets connected via the internet and the development of advanced information technology tools, and systems, Most countries are pressured to get connected, especially underdeveloped and developing countries. Digitization has its advantages and disadvantage. These underdeveloped and developing countries often adopt technologies to stay connected to the world without the structure to support it entirely, introducing more economic challenges. Some of the challenges that come with adopting digitisation are cybercrimes, most of the time initiated via phishing. Since the introduction of phishing in the nineties, many attempts have been made to curb it with the innovation of many tools, but it does not mitigate it that much. Phishing activities keep growing from year to year. This has affected many underdeveloped and developing countries as there are not fully developed structures and policies to deal with the fallout. This study seeks to probe structural issues that make it challenging to fight phishing attacks in Ghana and what the government can do to change this compared to the strategy used in Denmark, given what the Danish government has done to mitigate cybercrime.

Many resources are being lost to these attacks, giving Ghana a negative portrait on the central stage. Even though some measures are implemented to avert this, they have yet to make headway. A thorough review and qualitative expert interviews with in-depth questions were done to find a solution. For analysis, structuration theory was used. Structuration theory postulated the relationship between society and individuals. The enumerates that structure and agency are dependent constitutive dualities in that social phenomena are a relationship between structure(external forces) and agency(internal motivations); none is independent of the other, leading to coherent policymaking and healthy practice by the populations. We find that the main issue is education, and there is a need of well define laws and policies; a lack of expertise, and more resources need to be deployed, as well as a clean and centralised identification system and a well-defined role for various institutions for proper implementation of policies.

Keywords: Cybercrime, Phishing attacks, laws, policies, structure, digital illiteracy, Ghana, Denmark

1. Introduction

With the birth of the internet and digitalisation, how individuals interact with the world has changed. The Internet has become essential to individuals' daily activities, from ordering food to communicating with friends and family to being a vital part of the job process. It has also become the primary facilitator for building and maintaining knowledge and relationships. Nevertheless, due to the increase and rampant use of the internet for online activities, it has also posed threats in various aspects of our lives and in more ways than we can imagine. Phishing has become the most common type of cybercrime among other internet crimes for end users. Despite many security measures to secure internet users, there is still a growing trend in cyber attacks on individuals and organisations.

After decades since phishing activities were first introduced and various countermeasures developed to curb them, Phishing activities are still on the rise, and they have gotten worse during the COVID-19 pandemic. Because of the pandemic, more activities have shifted online, which has created more chances for phishing expeditions. Most organisations use emails as their standard way of communicating within and outside their organisation. Emails have become a source of vulnerability for both individuals and organisations. Most often than not, a breach of security measures in organisations occurs through hackers preying on the vulnerability of humans through phishing emails. The human element continues to be a key driver in 82 per cent of breaches, according to the Verizon data breach report for 2022 (Petri & Roer, 2022). It is evident that Phishing activities still pose a danger to cybersecurity because they can get past the standard security measures put in place and take advantage of people's vulnerabilities.

Much research has been conducted about phishing over the past decades by carefully studying the earliest researchers and also proposing various ways by which phishing activities can be filtered, identifying phishing sites and triggers that always push people to fall into these traps. Different companies have emerged in the quest to provide tools to prevent these activities (Lain et al., 2021).

Researchers and Security experts have tried in many ways to devise different strategies to combat these activities over the years, analysing their methods and motives to know how they often succeeded in carrying out these activities to curb them and educate the masses, as one of the most critical aspects of internet usage is the security of its users from fraudulent activities.

Some countries are doing better when it comes to protecting their populations from cybercrime than others. This study delves into what Denmark has done over cybercrimes that makes them more cyber resilient compared to other countries. However, in this study, we will look into what Ghana has done so far, what can be emulated from Denmark's strategy of clumping on cybercrime, especially phishing attacks, and how individuals and organisations can better protect themselves against phishing attacks. It explores different types and approaches of attackers and some techniques used in investigation. Some general regulations will be examined to learn about emerging countermeasures regarding Phishing activities. The following outline is how this research is structured, starting the research question with a brief background of the scope of the discussion—followed by the theoretical framework, which gives an overview of the theory. In essence, structuration theory was used because it gives the flexibility to analyse the necessary elements that create societal patterns, structure, and societal practices. Structure theory depicts how the Danish government, with collaborations with other institutions and the population, created a structural strategy to deal with phishing attacks to promote the continuity of digital solutions. After this, an Information review was presented regarding the current issues in cyberspace, from the different types of phishing attacks when they were first detected and how they have evolved over the years and measures proposed to resolve them. Next is some international law, the current situation in Denmark and Ghana, and the various laws and strategies employed. Methodology and research design This chapter has the steps to answer the research question, from categorising the various theory element through which data collected from interviewees were analysed, discussed and concluded.

1.1 Research question

With the rate at which phishing attacks are increasing all over the globe is critical that we draw attention to good internet infrastructure, rules and regulations across borders to provide a space for continuous digitisation and trusted cyberspace for transactions among countries and citizens. Measures adopted by most countries are failing, and data has shown a spike in phishing attacks, one typical attack leading to other cybercrimes across the globe in the first quarter of 2022. There is a need for a holistic strategy in dealing with cybercrime since digitisation has come to stay, and more advanced technologies are emerging, leading a more vulnerability in already vulnerable systems and economies. Amidst the increase in cybercrime, Denmark is one of the most digitised countries, which manages cybercrime significantly well compared to the attacks targeted at it. This research aims to investigate Denmark and Ghana has dealt with cybercrimes over the year, the current situation in both countries and what Ghana can adopt as a developing country trying to create a more sustainable and trusted digital economy. This led to the formulation of the following research questions.

Research Question:

How can Ghana learn from Denmark in an attempt to tackle phishing activities?

Sub-Research Questions:

a) What is the situation in Denmark and Ghana regarding cybercrime(Phishing activities)?
b) What can be done in Ghana to reduce phishing activities?

2. Theoretical Framework

In this research, the Structuration theory developed by Anthony Giddens will be used to understand the complex relationships between human agencies and institutions(citizens, the government, and private organisations). With the rate at which technologies evolve, It comes with challenges like regulations, policies, and structural readiness. A well-developed structure is needed to support it. Social structures are collections of transformation, interactions, norms, and resources arranged as characteristics of social systems; they do not exist independently of actions.

Giddens looked at how people interact, which later created rules and structures by which people gauge their behaviours from the smallest group to society to countries and how they interact, which may differ from one country to the other; this is termed the duality of structure; actions create structure, and structures enable and limit future activities.

Structuration theory posits the relationship between society and individuals. Giddens enumerates that structure and agency are jointly constitutive dualities in that social phenomena are a relationship between structure(external forces) and agency(internal motivations); none is independent of the other. Some of the most well-known decision-makers in the world, such as British Prime Minister Tony Blair, have drawn inspiration from Giddens' ideas. To comprehend the numerous complexities that emerge in modern digitisation, it is crucial to analyse how sociological theories are applied to real-world policy(Lamsal, 2012). However, human actors use social structures as a resource for their actions, creating and maintaining social structures(Jones & Karsten, 2008). The structure is described as modalities, rules, and resources that engage human activity. Regulations restrict actions, but the resources facilitate them, and the interaction shows structural qualities. Three types of structures identified in the social system are significance, domination, and legitimation.

Signification(communication) refers system's conceptual and symbolic order or the rules governing the predominant talk, language, and discursive practices. A method of prescriptively sanctioned institutions is called legitimation (sanction). These norms range from explicit legal responsibilities and limits to unwritten regulations entrenched in a particular organisation's culture. The final dimension, domination(exercise of power), deals with material and distributive resources related to political and economic institutions, most notably the state or the enterprise(Whittington, 2010). Giddens posits that structural characteristics of social systems result from practices they coercively organise, meaning they are continually recreated. Structures exist and are reformed due to the recreation of underlying codes.

Giddens says the Social actors practically apply society's structural elements (norms, regulations, and institutions) in their daily lives; this effectively "constitutes" society. (Structure is a set of rules and resources, procedures of action).

Figure 1 represents the dimension of the duality of the structure. The duality of structure consists of agency and structure, which structures through social practices. Over time, these social practices are how societies function due to actions performed deliberately or indeliberately. In that, Actions and structure are intertwined.(Jones & Karsten, 2008)

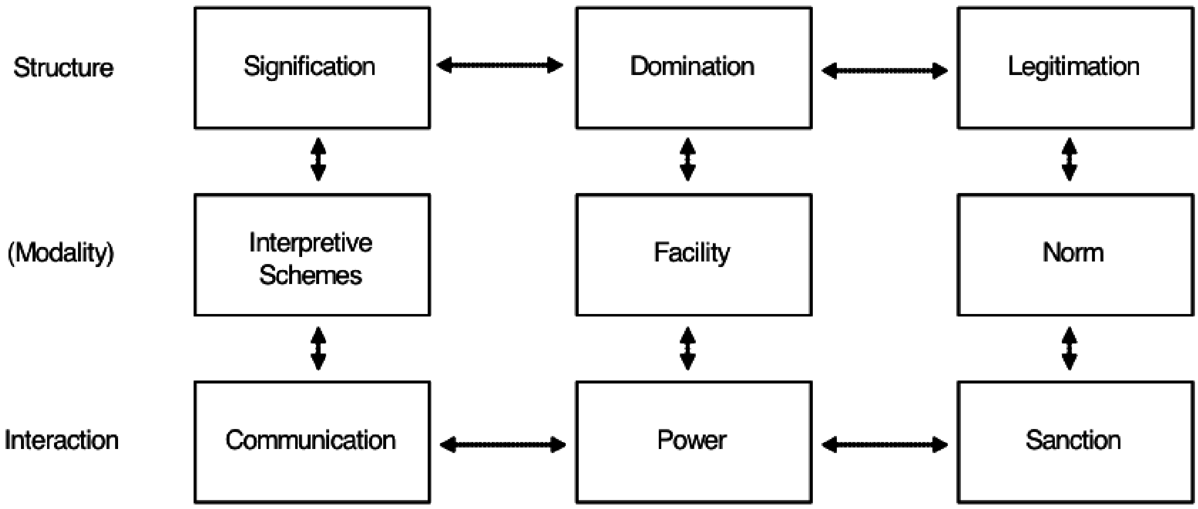


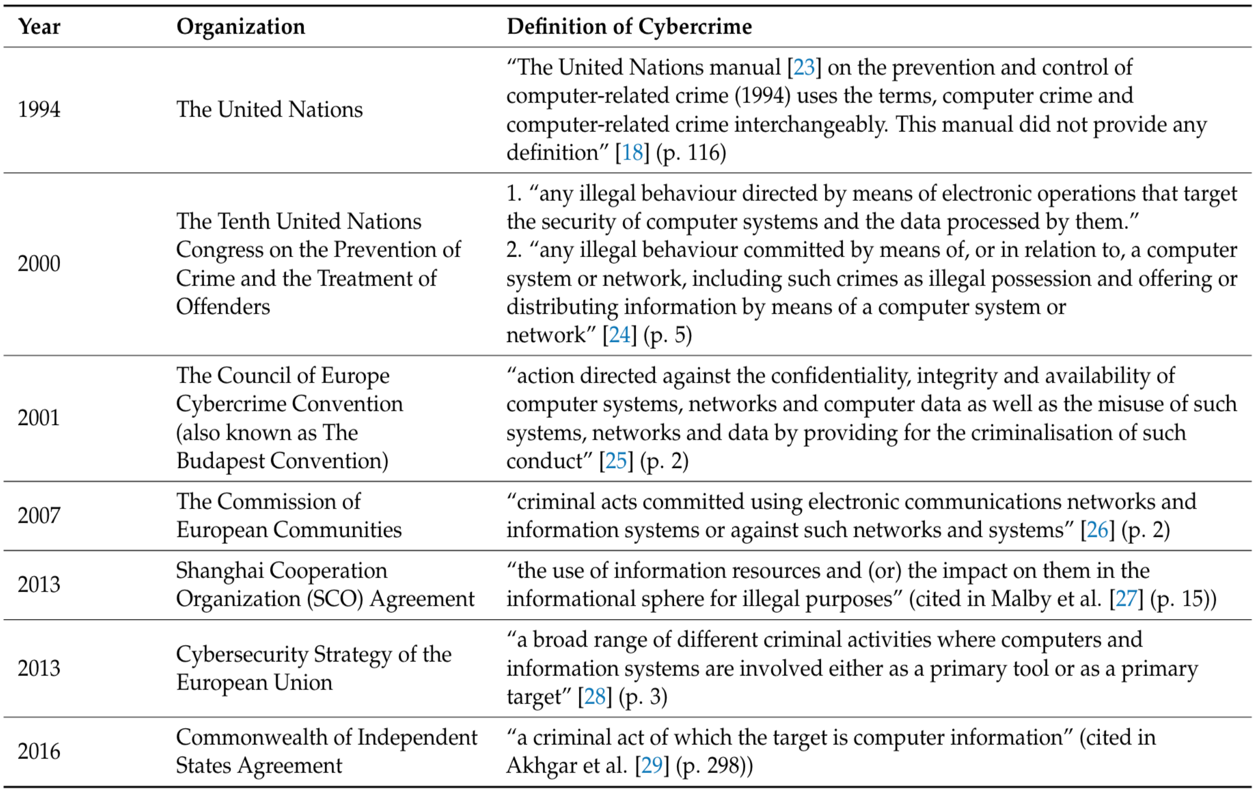
Figure 1. Dimension of the Duality of structure(Giddens,1984;p.29)

Dimensions		
★ Structure	★ Signification ★ Legitimation ★ Domination	- Rules and resources - Produce order, value, standard(sanctions, legal issues) - Gatekeepers like authorities(Exercise of power from resource control)
★ Modality	★ Interpretive Schemes ★ Facility ★ Norms	- Produce comprehensive understanding - Efficient institutions - Adequate measures/benchmark
★ Interaction	★ Communication ★ Sanction ★ Power	- Communications between stakeholders - Control of resources - Well, set up an institution to enact

3. Cybercrime

The issue of cybercrime is spreading widely throughout with the growth and expansion of digital technology. It has become more difficult be defined regardless it divulges to our society. There were attempts to properly define cybercrime and create the proper legal structure to deal with its occurrences, but more headway has yet to be achieved due to the constant and ever changes in cyberspace. This is because there is inconsistency in the definitions, terminologies and legislation across domains. (Curtis & Oxburgh, 2022; Phillips et al., 2022). Different types of cybercrimes exist: Internet fraud, Trojans, Phishing, DoS attacks, CyberStalking, Spamming, Ransomware, website defacement, Vishing, Smishing and the list goes on. Nevertheless, in this study, we focus on phishing attacks.

The table below shows the organisational definitions of cybercrime.



Year	Organization	Definition of Cybercrime
1994	The United Nations	"The United Nations manual [23] on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition" [18] (p. 116)
2000	The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders	1. "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them." 2. "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" [24] (p. 5)
2001	The Council of Europe Cybercrime Convention (also known as The Budapest Convention)	"action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" [25] (p. 2)
2007	The Commission of European Communities	"criminal acts committed using electronic communications networks and information systems or against such networks and systems" [26] (p. 2)
2013	Shanghai Cooperation Organization (SCO) Agreement	"the use of information resources and (or) the impact on them in the informational sphere for illegal purposes" (cited in Malby et al. [27] (p. 15))
2013	Cybersecurity Strategy of the European Union	"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" [28] (p. 3)
2016	Commonwealth of Independent States Agreement	"a criminal act of which the target is computer information" (cited in Akhgar et al. [29] (p. 298))

Figure 2: Organizational definitions of cybercrime (Phillips et al., 2022).

A recent literature review by (Phillips et al., 2022) revealed no clear definition of cybercrime that is accepted in every domain. `further revealed are three domain of reports which are 1. One term that sums up the different actions and behaviours, 2. The definition that is mainly cited, and 3. Institutional and organisational purposes.

3.1 What is phishing?

Phishing has become one of the most rampant threats. Phishing is a cybercrime where hackers or attackers use deceptive methods to lure individuals into revealing vital and confidential information like credit card numbers, passwords, and credentials. These usually happen through emails and SMS Phishing can be referred to as a type of fraud where technical skills are used to manipulate the trust between individuals and institutions, systems, or websites. Phishing attacks take urgent forms or instil fear in individuals through emails, text messages, or voice calls that look genuine. Quick-response actions are required from victims. These messages or emails come with malicious attachments, so when victims click on or open them it leads them to fake sites where their data is collected, or vicious programmes are installed in their systems to gather the information.

Phishing activities' chances of success depend significantly on human vulnerabilities, a lack of awareness, or preying on already established trust. Platforms like social media, organisation websites, and LinkedIn are used to elicit information about victims. Cybercriminals have always used social engineering techniques for manipulation and crafted emails to their victims to boost their chances of success. Financial losses, identity theft, illegal access to accounts, and compromised personal and business data are just a few of the severe repercussions that can result from phishing attempts. Phishing assaults develop with technological advancements, becoming more sophisticated and challenging to spot.

Attacks come in different forms: mass attacks or targeted attacks. In mass attacks, the Attacker aims to collect a massive chunk of data from which they can draw specific attacks. Targeted attacks are modified to fetch a piece of information (Sun et al., 2016).

There are undoubtedly many phishing attacks, but only a few will be explained in this study. The security of the end-user has become paramount. With the continuous increase in phishing attacks and their high probability of occurrence, researchers in different sectors have invested in various dimensions concerning phishing attacks, from proposing and coming up with ways to curb them to creating awareness among the population. With all these investments and research conducted recently, it is clear that phishing attacks have increased Anti-Phishing Working Group 2022 first-quarter report, It was noticed that total phishing attacks had attained over one million, which shows to be the worst-ever quarter and the first time the quarterly total has surpassed a million. It has become crucial to understand why people still fall into phishing attack traps for us to improve their resilience and what can be done to help mitigate this (*APWG | Global Phishing Survey*, 2022).

3.2 Evolution of Phishing Attacks

Phishing was introduced as a variation on the term fishing, where attackers lure users (victims) using baits for personal or confidential information (Chiew et al., 2018). “It was initially used in 1996 when hackers used an algorithm to generate random credit card numbers to obtain America Online subscribers' passwords” (Alkhalil et al., 2021). “In 2014, a comprehensive study was conducted on phishing to establish how phishing can adequately be defined. They have established a few fundamental ideas the scholarly community has determined to define phishing: Phishing is a convertible form of fraud when deception is employed to trick a target into divulging credentials." (Lastdrager, 2014). In this definition, it was agreed that there are no specifics as mentioned, which is true as phishing has expanded beyond that in other descriptions like that of the Anti-Phishing Working Group (2022), where “phishing is defined as a criminal mechanism employing both social engineering and technical subterfuge to obtain users’ identity information and bank account details illegally”(Frauenstein, 2019, p:51).

Phishing attacks have evolved rapidly. Their methods keep changing to adapt to the countermeasures introduced to curb them, technological advancements, and the changing behaviours of individuals and organisations. Attackers have successfully employed cutting-edge technologies to exploit system flaws and user deception strategies. This has made phishing attacks a continuous plague in cyberspace (Alkhalil et al., 2021). Even though luring people to steal their personal information and passwords goes way back to the early “introduction of computer networking, of which AOHell’s was the first to be introduced” (Rekouche, 2011), Many other tools were created over the years due to technological advancement.

The availability of these tools has made it possible for people with this knowledge to engage in countless phishing activities that result in attacks. These activities have grown to involve professional criminals on the internet and have become “one of the top security threats affecting governments, corporations, institutions, and individuals” (Rekouche, 2011). Over the past two decades, the method “developed to trick AOL members by posing as an employee of the service provider to gain access to their accounts and credit cards has been similar to today’s attack” (Rekouche, 2011). These have been the basis for developing phishing tools over the years, but as users became acquainted with these activities, the attacker employed more sophisticated approaches. They research and investigate their subjects, gathering information from social platforms. In addition, they use social engineering and psychological tactics to conduct these acts to increase their chances, which seem to be working sofar.

3.3 First Phishing Attack Process

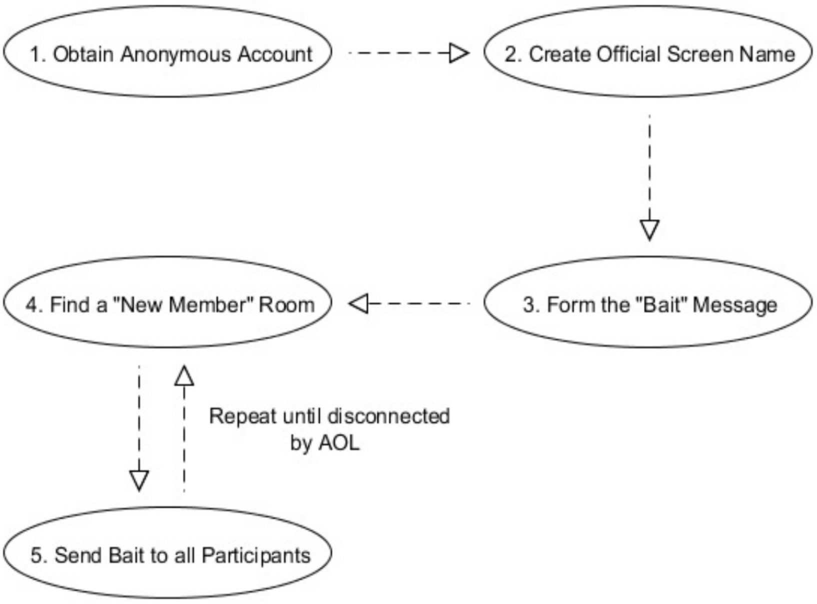

1. Obtain Anonymous Account
2. Create Official Screen Name
3. Form the "Bait" Message
4. Find a "New Member" Room
Repeat until disconnected by AOL
5. Send Bait to all Participants

Figure 3: Password and Credit Card Scam Process (Rekouche, 2011)

How it was carried out.

1. Attackers create an anonymous AOL account using a fake bank account number or credit card. They use an already-stolen account from a previous attack.
2. Attackers make a display name on the account that looks legitimate.
3. Attackers draft a message to bait users, like why it is necessary to get their billing information or passwords “verified.”. Example: "Hello, this is customer service from AOL. To prevent being terminated due to an issue with our records, please reply to this mail with your current username and password” (Rekouche, 2011).
4. Attackers locate the new member lounge chat room and open its occupant list.
5. The message is sent privately to each user in the room.

This process continues until AOL security staff notices and terminates the fake account.

In earlier days, phishing activities were relatively easy to notice as internet users became aware of them. As internet users grow, email, voice-over-IP, and SMS have become the most common communication tools for individuals and organisations. The number of phishing attacks has increased exponentially. Phishing attacks have transformed from stealing users' credentials by sending them automated messages to more interactive emails where users take action that can help attackers introduce ransomware into their system and now to the impersonation of familiar contacts or institutes. In 2018, a phishing attack targeting some organisations was conducted using PSImage, allowing attackers to hide malicious scripts in pixels executed later. This technique, in most cases, will not be detected. This shows another way phishing has evolved. In 2018, gift card phishing campaigns started and have developed throughout 2019. Along the way, Business email compromises pop up, enabling attackers to target a company's customers whose email accounts they have gained access to. This has affected over 500 organisations globally. Phishing attacks have evolved over the years in many innovative ways, and they became rampant in 2020 due to COVID-19, which has spread through countries across the globe, according to Microsoft. With the technological advancements and innovative ways that attackers target organisations, one must look at the whole picture, including the end user. A detailed survey was conducted on phishing techniques and how they work. They sort to find the link between the vectors of phishing and the technical approaches used in executing them. This is to help develop an excellent countermeasure to curb and prevent those channels from further exploitation (Chiew et al., 2018). Phishing attacks today can use different methods, as stated earlier, by scamming victims or using “malicious code to access their personal information” (Gupta et al., 2018).

3.4 Detection models

User interface

This section elaborates on the models and solutions proposed to help reduce phishing activities.

In Wu 2006 Fighting Phishing at the User Interface has brought some issues to bear since it is at the user interface where intentions are transformed into system operation. In this study, they decided to focus on deceptive phishing. These describe how phishing works from day one, luring individuals to give out sensitive information by impersonating legitimate institutions. In this study, they argue that the primary solution to phishing attacks is bridging the gap between the system models and the user's mind. Since it is the interface through which consumers interact with the system for the first time(Wu, 2006), it is at this point that their intentions are transformed into system operations. Therefore it is vital to fight phishing attacks from the user interface. While users must pay attention to the interfaces they come into contact with when performing their daily activities today, they need to pay more attention to graphical user interfaces.

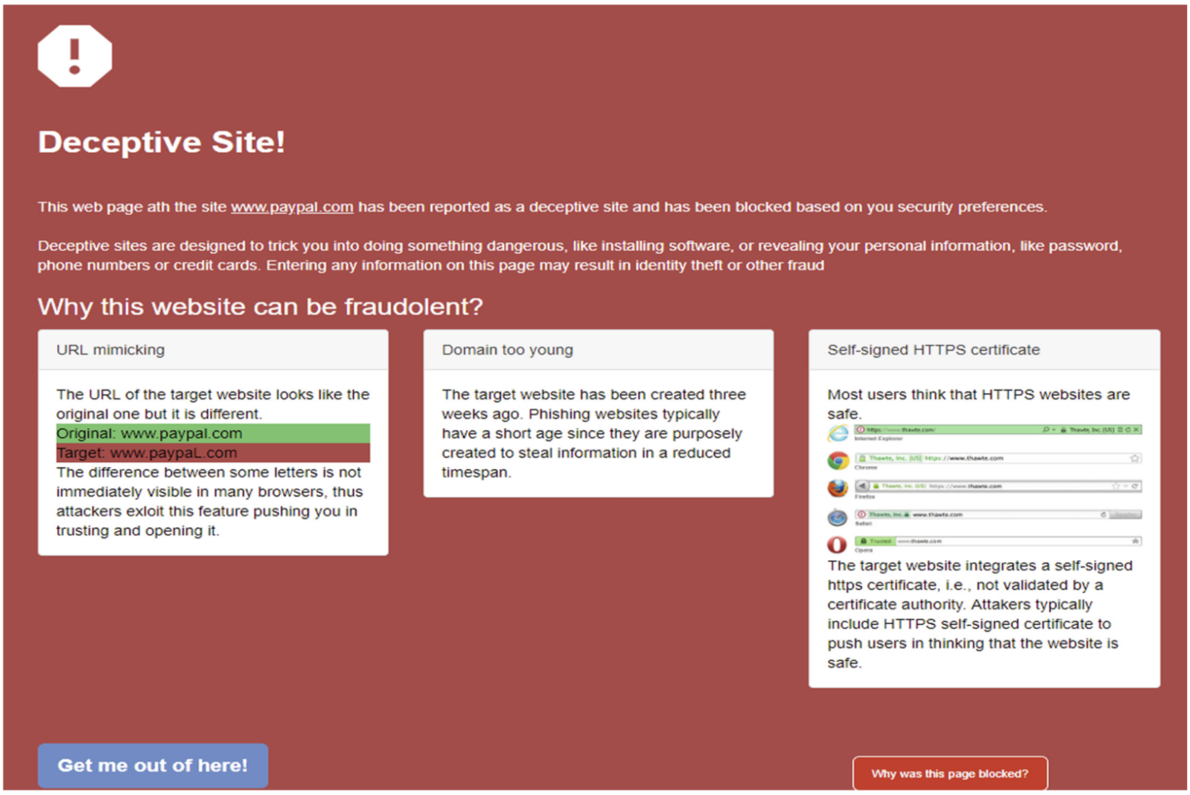
With the advancement of technology, it is more difficult to spot the difference between genuine websites and fake sites. So in the case of fighting phishing activities on the user interface looks unachievable. “Two primary approaches were used to close the semantic gap at the user interface. Reflecting the system model to the user is the first approach where Anti-phishing toolbars and the browser’s security indicator are implemented”(Wu, 2006). It gives information about website browsing and anti-phishing solutions.

Nevertheless, their research shows that this approach could be more effective against phishing attacks as it failed against advanced quality attacks. This approach also requires users to focus on the toolbar and have the technical know-how to give meaning to the message from the taskbar. This is impossible for people with knowledge in the computer field, most often than not and not even to talk about normal average users. Individuals can employ the second strategy when providing data online by informing the system of their intention. In this case, the system can check whether the submission meets the user’s intention. The system can effectively warn if any semantic gap is detected, which has proven effective(Wu, 2006). Two-factor authentication was proposed for users to use whenever they want to log into a website.

"Three user interface design principles were proposed to solve phishing" with the help of the findings and lessons learned from “the anti-toolbar studies and the project involving using cell phones for authentication.

One of these principles is Intention-centered design which says that instead of modelling the system to the user as depicted in the toolbar solution, The user should be allowed to tell the system his mental model"(Wu, 2006). In other words, the user should detect the path of the current operation he is trying to perform. It kind of sounds absurd in the first place since the action being performed in the first place was initiated by the attack, as he has successfully coerced his victim into going down that path. The second principle is integrating security into users' workflow; this may work on genuine sites the user might have been using but instead was being directed to fake sites created by the attacker. Furthermore, the path of least resistance will ultimately mean nothing as long as it is on the track made by the attacker(Wu, 2006).

Aneke et al. (2020) outlined an intelligent warning messaging mechanism to mitigate the rate at which phishing attacks are soaring and create awareness of the risk that comes with it so that users can make a more conscious and adequate decision. They sort to put in place intelligent behaviour that, apart from alerting the user of phishing attacks occurring, also explains why a particular site might be fake. This helps to address the design guidelines for better interface designs.



Deceptive Site!

This web page ath the site www.paypal.com has been reported as a deceptive site and has been blocked based on you security preferences.

Deceptive sites are designed to trick you into doing something dangerous, like installing software, or revealing your personal information, like password, phone numbers or credit cards. Entering any information on this page may result in identity theft or other fraud

Why this website can be fraudolent?

URL mimicking

The URL of the target website looks like the original one but it is different.
Original: www.paypal.com
Target: www.paypaL.com
The difference between some letters is not immediately visible in many browsers, thus attackers exloit this feature pushing you in trusting and opening it.

Domain too young

The target website has been created three weeks ago. Phishing websites typically have a short age since they are purposely created to steal information in a reduced timespan.

Self-signed HTTPS certificate

Most users think that HTTPS websites are safe.

The target website integrates a self-signed https certificate, i.e., not validated by a certificate authority. Attakers typically include HTTPS self-signed certificate to push users in thinking that the website is safe.

https://www.thawte.com/
Thawte, Inc (US)
Internet Explorer
Thawte, Inc. [US] https://www.thawte.com
Chrome
Thawte, Inc. (US) https://www.thawte.com
Firefox
Thawte, Inc. www.thawte.com
Safari
Trusted www.thawte.com
Opera
Get me out of here!
Why was this page blocked?

Figure 4. Polymorphic user interfaces(Aneke et al., 2020).

The figure above is a user interface sample that warns users about phishing attacks(Aneke et al., 2020). This sample shows columns explaining why the target site might not be genuine. They explained that the first column display two different URL but identically, of which the last letter of the original site was replaced with the upper caps of this same letter. All this happens on the interface of systems, so when they call for implementing a thorough anti-phishing mechanism, the interface is a call in the right direction. How many users can or would take their time to pay attention to all these details? In the second column, the display shows how young and the date the fake site was created, which is a significant go addon. With this information, users can make a consideration and make better decisions. The last column, tells depicts that even though HTTPS was used, it explains that the site might not still be legit. This was achieved by using an API to identify malicious areas. Instead of just displaying a generic message, a good design intelligent user interface was created to educate users, explain the possible attack and prevent a chronic clickthrough effect. One of the significant statement reminds unchanged “User must be able to see, understand and use to achieve efficacy of the security strategy.” In the future, they aim to improve the structure, content, language, and aspect of the messages to make them more effective and add a graphical element to the interface. Because One could still argue how effective this intelligent user interface would be, we have a user who can go into junk folders of the email box, retrieve messages that the system dims to phishing messages, and answer them. That leaves us questioning how phishing attacks are still increasing with the tool implemented to solve them(Aneke et al., 2020).

3.5 Types and Different Techniques of Phishing Attacks

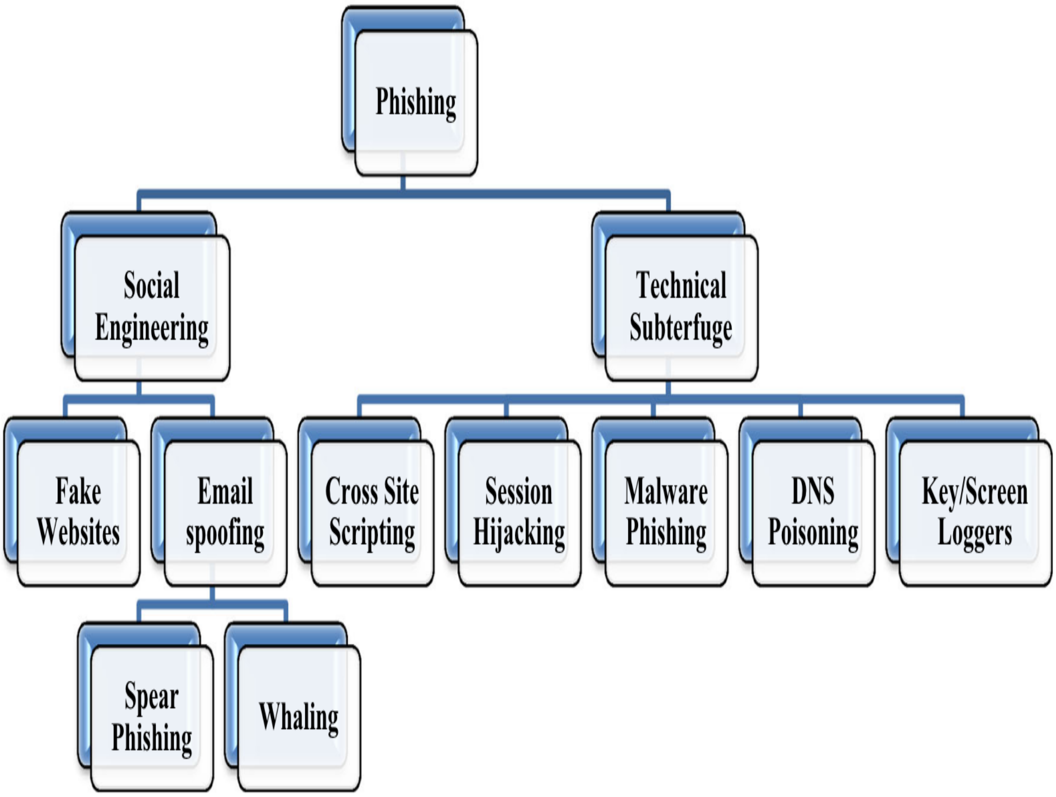


Figure 5: Classification of phishing attacks (Gupta et al., 2018)

I. Social Engineering

It is defined as the skills to lure a user into falling victim to malicious fraud, carry out an activity to inflict harm on the user, use deceptive manipulations to acquire sensitive information from individuals and gain unauthorised access to systems and data. Attackers do not only use technical means or tactics to deploy phishing attacks; technical tactics are usually combined with psychological tricks to prey on the vulnerability of humans. Despite the focus of many researchers on phishing attacks, they are coming up with better anti-phishing solutions to protect user-sensitive information from hackers. There were many phishing attacks during the COVID-19 pandemic. Criminals used social engineering techniques to take advantage of COVID-19 by not having a specific target so that anyone could become a victim of their attacks (Altani & Cresci, 2022). In Phishing Attacks and Root Causes, Abroshan et al. (18) identify some root-cause factors that make up phishing attacks, including human and psychological factors. In their quest, they reviewed the existing anti-phishing techniques. They found out that many of these tried to prevent or detect activities technically. They concluded that focusing on the sociological and psychological elements would be preferable. They believe this approach will be much more effective.

What can make an individual retrieve an email flagged by anti-phishing tools and still act on its instructions, as in the case of some phishing attacks? Yes, some anti-phishing tools do land some essential emails that sometimes do not deserve to be spam. That also speaks volumes about the poor algorithms behind some anti-phishing tools. Existing anti-phishing solutions are reasonable, but most are rendered useless in one way or another as phishers are constantly preying on people's psychology to get away with these attacks. Identifying this factor will help improve it and develop programmes to address it. Social engineering and technical tricks are some ways that attackers use to perpetuate successful phishing attacks. So it has become indispensable to “study psychological and sociological factors to discover why individuals still get caught in phishing nests.

II. Fake websites

These are websites that look to be identical to genuine websites. This is used to fool users into obtaining their credentials. Fake websites are one of the major sites for online scams. These sites look legit, but they are malicious control sites deployed by attackers. Phishing ads, links, and emails are embedded in them. (Gupta et al., 2018)

III. Email Spoofing

In this kind of phishing attack, emails are sent out to potential victims, and those emails are forged to appear to the receiver to be from a legitimate address. They are sent to lure the receivers to respond with valuable information, click links, or attach documents. " In 2021, email spoofing and phishing increased by 220 per cent (Jalda et al., 2022).

IV. Whaling

It is a high-end attack that targets bigger fish like the whales in an organisation,i.e., people at the enterprise level. These attacks target directors, CEOs, and CFOs, people occupying higher organisational positions (Karmakar, 2022). This is also termed CEO fraud. They aim at harvesting login information for business operation accounts like financial or `HR management systems. Since higher-ranking employees have control over and access to vast amounts of information about a company, One that has access to this can use it against the company by competitors to achieve a competitive advantage, which is also called industrial espionage (Sonowal, 2022).

V. Spear Phishing

Spear phishing is a step up from generic phishing or email fraud. This is usually associated with targeting a specific individual with emails from highly trusted sources. Most often than not, this is one of the most infiltrated institutions to be able to perform advanced Persistence threats (APTs) (Dewan et al., 2014). In Spear phishing attacks, first gather information about the user before the attack to create genuine-looking, sophisticated, and realistic messages to establish high confidence and trust in them. Targeted individuals are used as conduits, which has proven to have a much higher success rate than regular phishing. When trust is established, attackers can lure victims into giving out sensitive data like passwords and username card details. It can also trick individuals into downloading a malicious program or clicking malicious links, infecting user systems and obtaining sensitive or confidential information like login passwords. Attackers may spend lots of time researching their victims to find relevant information to design an irresistible email. Social media sites such as LinkedIn are the most common platforms where these things occur. Some examples depict how spear phishing attacks are carried out. In 2011, A spear-phishing attack involving RSA Security LLC, formerly RSA Security Inc., shows companies known for security are not left off the hook regarding phishing. RSA was attacked by targeting a small group of employees, of whom one, unfortunately, fell victim. Despite all the advanced security control implementations, attackers still find a way in. The email was retrieved from a junk mail folder by an employee with the subject ‘2011 Recruitment Plan’, an Excel file hiding a zero-day exploit. The file installed a backdoor through a vulnerability in Adobe Flash. Credentials were harvested successfully, and this attack threatened the security of defence contractors (Daniel, 2016).

Leading to the 2016 U.S. election, in John Podesta's case, The email suggested that John Podesta needed to change his email immediately because someone had just used his password to try to log into his account and also carried a shortened URL and Google link for the user to change his password through. Unfortunately, the shortened URL was clicked, enabling the attacker to access numerous email accounts of Clinton campaign employees (*John Podesta’s Phish Foreshadows Doom for 2020, Cofense*, 2020)

VI. Vishing

It is committed by using voice calls to pretend to be someone and committing a crime. Voice phishing is an attack that attempts to trick clients into providing confidential data like credentials and credit card numbers over the phone. This may sound impossible and old-fashioned, but with advanced technology, this has taken on different forms as we are more likely to trust a human voice.

Vishing is a phishing attack that uses voice technology to Persuade the victim to give over sensitive data over the phone, including card information, date of birth, social security numbers and other sensitive information. The following methods can be used, including voice messages, automated voice simulation technologies (including speech synthesis), and direct calls, can be used to conduct it due to VoIP networks' quick connection and disconnection times, lower call costs, and capacity to mask the trustworthy source of calls, early vishing attacks were conducted on them which can lead to compromising victims's bank account. (Mangut & Datukun, 2021).

VII. Smishing

With the growth of SMS over the years, businesses have considered it a cost-effective and more reliable way of communicating with customers. According to Gartner, the rate at which people open SMS messages is 98 per cent higher than emails at 20 per cent. Smishing is a phishing method used to send text messages to mobile phone lines, asserting to be an organisation's trusted individual or representative and sending SMS messages with malicious links to victims to collect their sensitive information. Examples of phishing bait include calling a number, clicking a link, and other requests for sensitive data or installing malicious software. Victims should report to cell phone carriers when they receive phishing texts. Smishing attacks are gaining popularity over the years(Mangut & Datukun, 2021).

VIII. Cross-Scripting Attack

The XSS vulnerability can even allow unauthorised access to a company's data through its web application. The hijacker accesses user sessions while engaging in various XSS attacks and deletes, adds, and modifies website data. Nevertheless, since they can access web pages, they can upload malicious code to alter the user interface and halt additional business operations. To take valuable information, the attackers would then access the organisation's servers (Maruf Hassan et al., 2022).

IX. Session Hijacking

Session hijacking is an attack to acquire unauthorised access between permitted session connections. This attack is also called cookie hijacking. This happens when an attacker wants to steal the identity and get unauthorised access to the resources. DoS attacks are used to obtain the session key. The attacker must break a specific access point to disconnect the mobile station. This is typically done to attack social networks and websites to gain access to both the website and the active session. This type of attack is one of the most frequent cyberattacks in today's networks. Most networks and websites are vulnerable to this attack (Gupta(Gupta et al., 2018).

X. Malware Phishing

Malware is used to steal confidential data from victims' devices and send it to the phisher. Hackers use malware, which contains an array of tools. Phishing is one of the tactics that spreads quickly and is simple to employ. The attacker will pose as a reliable company or person to trick their target into clicking a fake link to collect their sensitive information.

XI. Domain Name System Phishing (Pharming)

Pharming is a DNS-based phishing attack. In this attack, an entire network is breached using a single computer and infecting the machine with malware. Cache poisoning is used in this activity over the “Domain Name System, a naming scheme used to change sites like www.microsoft.com into numerical IPs to find and direct users to computer services and devices”(Karmakar, 2022). In a cache poisoning attack, a phisher changes the IP address associated with the website. Attackers redirect Visitors to a malicious portal in this manner to be able to collect their data.

XII. Key/Screen Loggers

This captures the individual's keystrokes while accessing their computer; this is done to gain access to login credentials or confidential information. Attackers use malware called keyloggers and screen-loggers to track user keystrokes and collect sensitive data. They can also be used for non-phishing reasons like tracking data and monitoring URL changes (Alkhalil et al., 2021).

3.6 Anatomy of phishing attack

This section talks about the phases of current real-time phishing and the activities that go into each stage of conducting it.

To carry out a phishing attack, attackers must host a phishing site. Infiltering servers can achieve this by downloading information using phishing tricks. Attackers share URLs as soon as their site is online through social media or direct messages in the form of ads or messages. Well-designed and convincing emails or messages with a sense of urgency that always urge or prompt users to act and lead them to give out sensitive information. Knowing the depth of phishing attacks might be the way to curb or eradicate them.

However, this is difficult considering the adaptive nature of attackers, the ever-evolving industry, and the human factors involved in dealing with this canker. First, attackers spoof or mimic websites so much that it is difficult to spot the difference. They spend hours, days and weeks studying their victims. A message is sent with a malicious link or link that will fool users onto a fake website where they will give away their sensitive information based on social engineering to convince users to take action. Most often, users respond. Phishing has become a complicated issue to solve, Despite the security measure put in place coupled with education and training. It is imperative to understand the nature of phishing attacks, how phishers undertake them, and the available defence tools. (Oest et al., 2018) Inside a Phisher’s Mind.

In 2016 there were more phishing attacks than in previous years, as published by the Anti-phishing Working Group. So this research was conducted to study the anti-phishing ecosystem at the point and also understand things from the attacker's perspective and how they could still manipulate their victims. One can say that years down the line, this is still happening, and it calls for thorough research and a well-proposed solution to this canker after analysing two datasets of over 2000 real-world “phishing kits” and 170,000 phishing URLs (provided to APWG).

Analysing these datasets gave them room to understand the attackers' goals and profile each attack. They concluded that attackers are aware of the tools being used by the security domain. They revealed that for attackers to be successful or avoid being detected, they will stop at nothing to achieve that by using compromised infrastructure when possible and registering highly-deceptive domain names(Oest et al., 2018). The essential contribution to knowledge is to help fight phishing attacks by familiarising ourselves with the patterns of attackers. Once again, this will also be difficult, as those patterns keep changing depending on what attackers want to achieve, even though it is all a purpose. This will develop more effective tools to fight against phishing. This is why it is imperative to know and understand the role of human activities in the quest of the fight and why users fall for this in the first place.

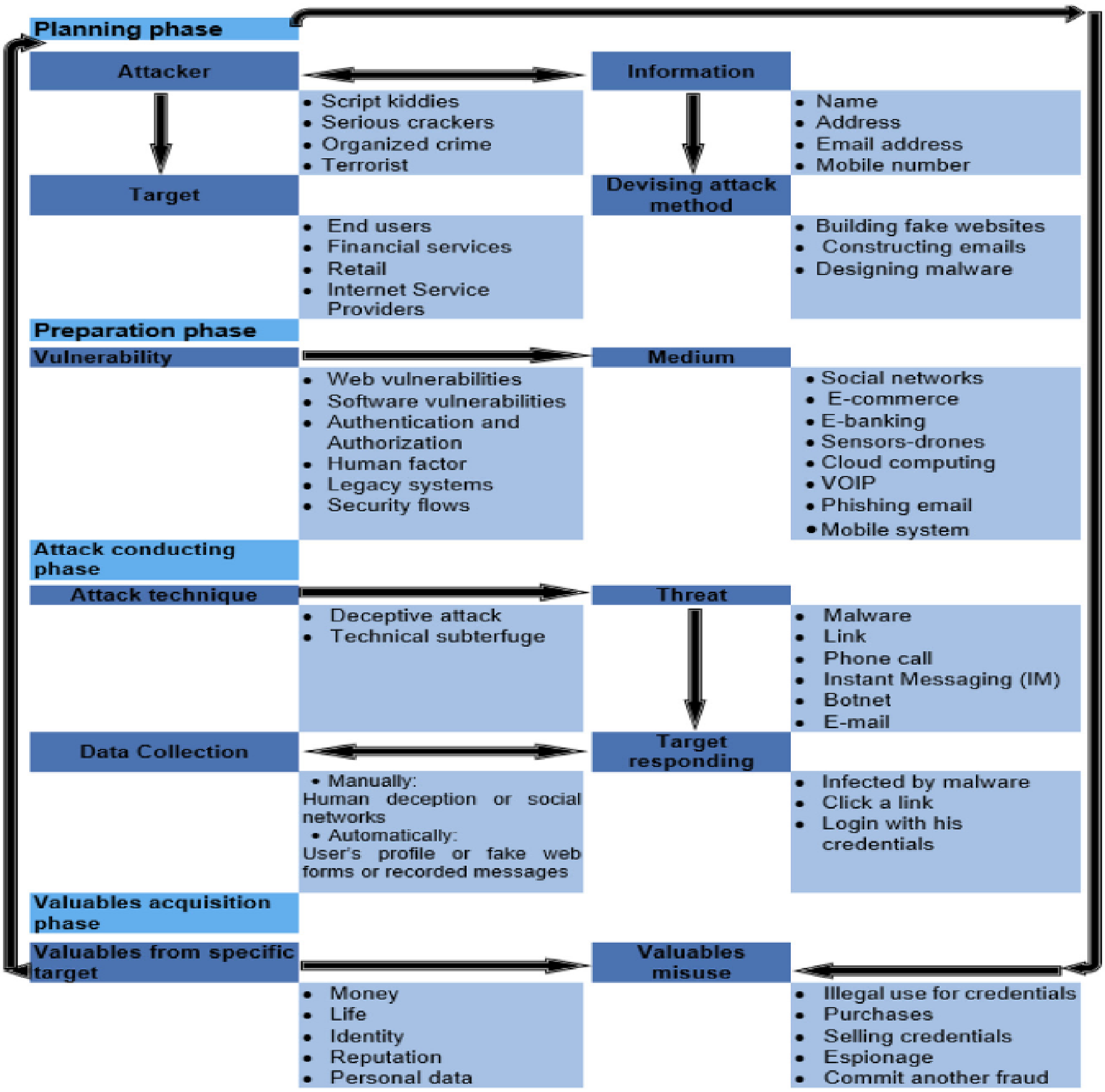


Figure 6. Proposed phishing anatomy (Alkhalil et al., 2021)

I. Planning stage

The first step in phishing attacks is to gather information about the targets, which might be anything from names and email addresses to company clients. In this stage, attack strategies are also developed. For example, Fake websites are created, malware is designed, phishing emails are created, and distant machines are compromised using hacking tools and malicious ways. The most efficient attack is organised crime, which can potentially harm victims seriously. A group of professional hackers working together to develop complex attacks and conduct phishing campaigns against individuals and companies is known as an organised cybercrime organisation. For various reasons, including causing harm, conducting cyber espionage, acquiring information, locating people, and other destructive goals, terrorists use spear phishing to launch their attacks. These crimes may be directed at people, governments, or other institutions.

II. Preparation of Attack Stage

Phishers uses vulnerabilities to compromise computers, take over target apps, or launch a denial-of-service attack. Examples include cross-domain vulnerabilities, browser vulnerabilities, buffer overflow vulnerabilities, and zero-day software vulnerabilities. Attackers require a channel to transmit the threat to the victim and execute the attack. One of the more promising technologies is cloud computing, although it has privacy and security concerns. Malicious customers may use virtualisation flaws to launch security attacks on the applications and data of other customers. Microsoft SharePoint was used by attackers in 2017 to send messages that infected hundreds of campaigns with malware.

III. Conducting Attack Stage

Phishing uses attack methods to present the target with a threat that can be used to undermine security and privacy: Malware, botnets, eavesdropping, unwanted emails, and viral links.

IV. Acquisition of Valuables Stage

The most crucial information is that the phisher obtains vital information from victims and then unlawfully utilises it to make purchases, fund transactions, or sell credentials on the black market. Data on victims might be gathered manually or automatically. Recorded messages are used in VoIP and phone hacks to gather user data (Alkhalil et al., 2021).

6.7 The Human Factor in Phishing

This paragraph addresses the part that people play in phishing attacks. Technology is developing and becoming more widely accessible, which increases the dangers it poses to its users. The more we understand humans' role in cybersecurity, the better our chances of curbing cybercrimes. Research has demonstrated the complexity of cyberattacks and their effects on the government, industry, and users. Phishing cannot be solved solely through technical means. The research sole base on a technical viewpoint must be replaced with one that acknowledges the significance of human elements in all facets of technology use because these activities are carried out by preying on technical and behavioural susceptibility (Dupont & Holt, 2022). Even with the warning signs and awareness campaigns, many people still fall into phishing nets of attacks because of “cognitive susceptible factors and a discrepancy between human behaviour and technologically imposed standards” (Whitty, 2019). According to (Dupont & Holt, 2022) in Leukfeldt & Holt (2020), The phrase "human factor" has a fairly broad definition and refers to aspects of the individual, organisational, and societal dimensions. It shows how people act independently, the social structures that allow people to work together, and the various institutional assemblages that shape how people respond to society.

Phishing attacks create severe risks to people's and organisations' security. Although contemporary antiphishing technologies have great accuracy rates and could solve this issue, people frequently need more time to trust these capable tools' predictions. (Chen et al., 2020). They investigate the factors influencing users' reliance on anti-phishing tools to address the issue of not trusting or relying on anti-phishing tools. A study was conducted to evaluate the impact of tool characteristics (i.e., the precision and frequency of forecasts for phishing emails) and create a model based on the ideas of trust and mistrust. (Chen et al., 2020). In contrast to the widely held belief that tools are not accurate enough, they discover that users' under-reliance is not a result of the low accuracy of tools because consumers still used tools insufficiently even when there was 100% accuracy. Instead, they discover that although accuracy raises users' faith in tools, complete dependence is constrained by users' mistrust, which is stoked by a lack of transparency regarding the functions of tools and the number of forecasts offered. As a result, their research demonstrates the limits of accuracy in inspiring reliance. It explains the under-dependence phenomenon by demonstrating that some users trust and rely on their poor judgement rather than the predictions made by highly accurate tools(Chen et al., 2020).

4. The Global Effect of Phishing

After the discovery of the internet, the whole world has advanced in technology and communication. This has led to many forms of business worldwide and increased online payment leading to the security and user data, one of the most important, if not the most important, in these days and age. One common menace in nations today due to the internet is cybercrime, most carried out by phishing attacks one way or the other. There is a need for a cohesive understanding of this crime to deal with it effectively globally.

The figure below is the survey conducted by the Anti-phishing working group(APWG). Phishing has affected every aspect of life in one way or the other, indirectly or directly. Phishing attacks affect every country, from the smallest to the biggest, from the developed to the developing countries and all sizes of businesses and individuals. Over 4.7 million phishing attacks were reported in 2022, marking the highest record mark since 2019; the Number of phishing attacks has increased over the years. The Anti-phishing working group has sampled about 1,350,037 attacks in the fourth quarter of 2022.

The financial sector, among others, is not excluded from this menace as they suffered 27;7 per cent of the total attack in 2022. In a study, they examined how phishing alarms published in open databases affect the market value of multinational corporations. It was demonstrated that the publication reporting phishing attacks results in a substantial loss of market value of a minimum of 411 million US$ for a corporation based on a sample of 1942 phishing alerts involving 259 businesses in 32 different countries(Chen et al., 2020).

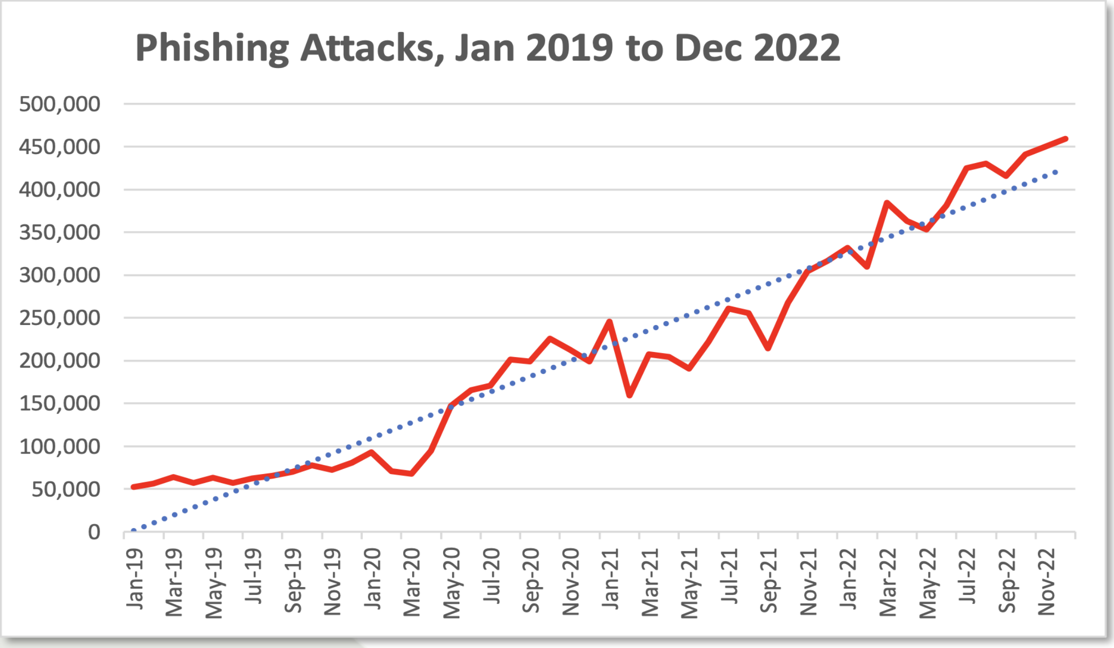


Figure 7: Phishing attacks reaching the highest peak quarterly in 2022(APWG, 2022).

4.1 International Laws on Phishing

Phishing is a global cybercrime that poses significant challenges for law enforcement agencies and policymakers worldwide. While no specific international law is solely dedicated to phishing, several existing legal frameworks and international agreements can be applied to combat this cybercrime. Here are some key international laws and initiatives relevant to addressing phishing:

1. Council of Europe Convention on Cybercrime: This international treaty aims to harmonise laws concerning cybercrime and enhance international cooperation. It addresses various cybercrimes, including phishing, and facilitates cooperation in information sharing, extradition, and mutual legal assistance among member states, otherwise called the Budapest Convention(Vatis, 2010).

2. General Data Protection Regulation (GDPR): While not specific for phishing attacks, the GDPR sets regulations for protecting personal data within the European Union. It requires organisations to implement robust security measures to safeguard personal information, and individuals have the right to be informed about data breaches that may result from phishing attacks(Regulation, 2018).

3. National Legislation: Individual countries have enacted laws and regulations to address cybercrimes, including phishing, within their jurisdictions. These laws vary from country to country but generally cover offences related to unauthorised access, identity theft, fraud, and computer-related crimes.

It is important to note that the enforcement of laws related to phishing largely depends on the jurisdiction in which the crime occurs and the countries' willingness to cooperate in investigating and prosecuting cybercriminals. Given the transnational nature of phishing attacks, international cooperation and information sharing among law enforcement agencies are crucial in combating this global threat effectively. Efforts are ongoing to strengthen legal frameworks, improve collaboration, and raise awareness to address phishing and other forms of cybercrime at the international level.

5. Denmark

Phishing has become problematic due to the digital economy and IT infrastructure expansion. There is no doubt that Europe has been at the forefront of digitalisation, As Covid-19 pandemic has evolved most economies in European countries by migrating most processes online. Many employees work from home, and many e-platform tools were created. In research was conducted where there seeks out outlined cybersecurity environment with its main threat(phishing) by providing a relationship between the individual and their ability to notice phishing messages targeted at them by their level of digital literacy. They also noted that computer literacy skills and education of end users could help reduce these threats. Attackers are constantly amending their ways to ensure they succeed. This paper seeks to prove factors that aid in spreading cyber fraud using support vector machines.

According to Eurostat (2021), 25% of European Union individuals reported receiving fraudulent phishing messages. Denmark has 45% of its citizens reporting receiving fraudulent messages(phishing). 2% of the population reports financial loss due to rerouting to phoney websites and stolen identities. The figure below shows a survey conducted among European countries' populations. They assume that these data show the ability of populations to notice potential phishing messages compared to the actual phishing attacks that happened in the country."A nation's general population's capacity to recognise a potentially harmful internet message is directly correlated to its capacity for digital literacy"(Romania. et al., 2021). This implies that if the rate of detection is high using any means via humans or machines, the higher the digital literacy rate and vice versa.

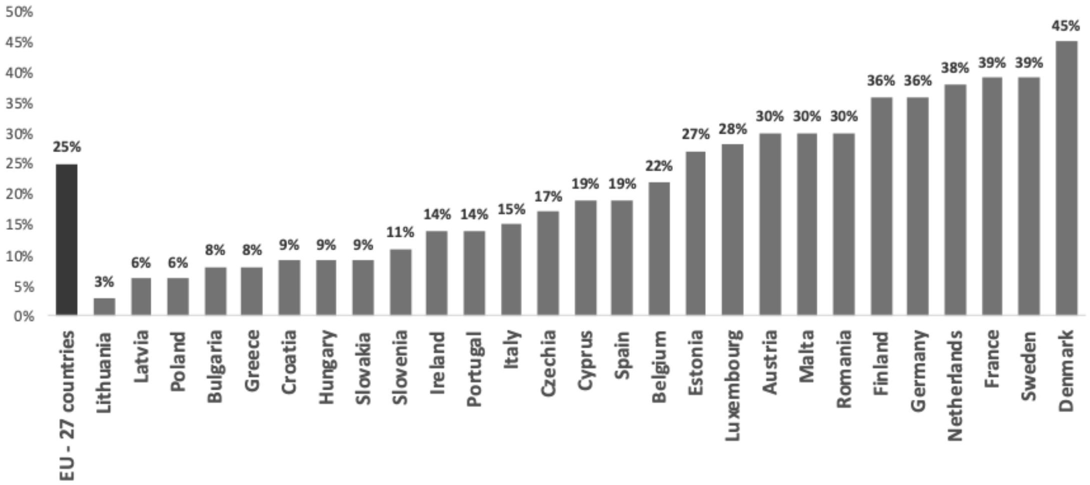


Figure 9: Phishing messages Received(Eurostat, 2021).

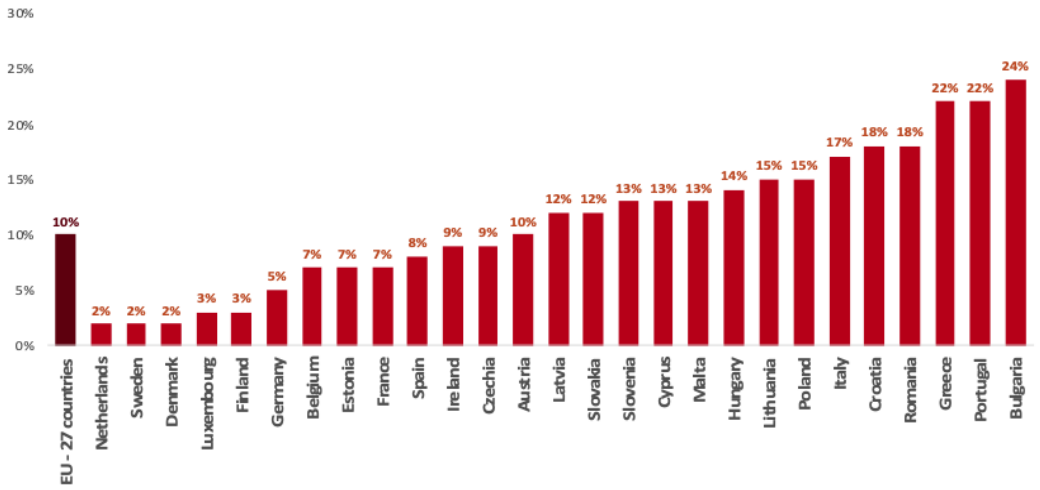
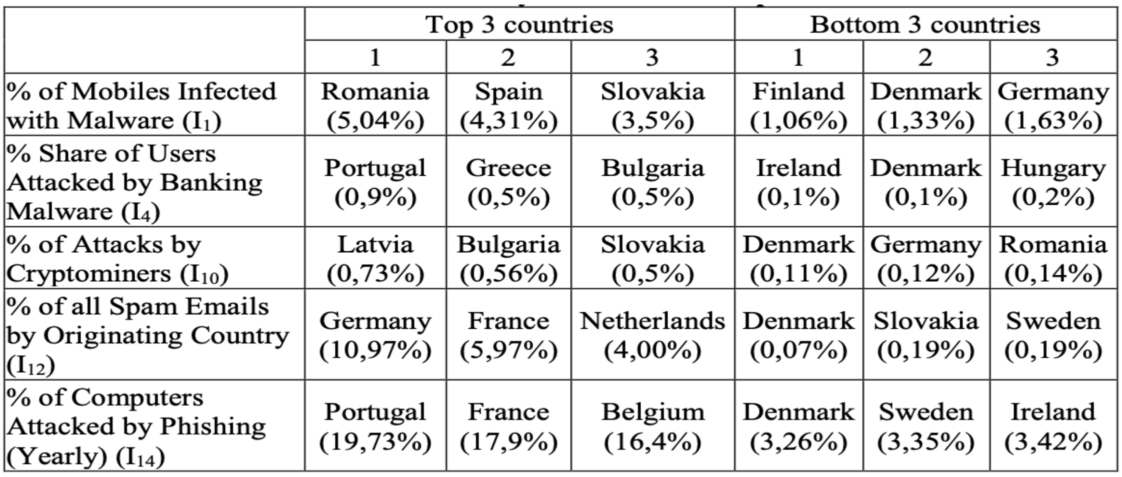


Figure 10: People who never use the internet(Eurostat, 2021)

In the Figure above, Whiles Denmark recorded the highest number of fraudulent messages declared by its citizens, and Lithuania recorded 3 per cent, followed by Latvia, Poland, and Bulgaria with 6%, 6%, and 8%, respectively. Among the European Union, 10% of the average citizens have never used the internet. At the same time, the rest of the citizens have varied levels of digital skills and uses the internet. Going into the specifics in the Figure above, the Netherlands, Sweden, and Denmark all recorded the lowest illiteracy rate of 2 per cent, respectively. In contrast, Bulgaria recorded 24% of its citizens with the highest illiteracy rate. These go to validate their hypothesis that countries with lower illiteracy rates have a large chunk of their populations with a certain level of digital skills and proficiencies, even though there might be certain exceptions(Romania. et al., 2021).

In 2021, research was conducted to help improve security management by considering a massive piece of information that was analysed to help notice cyber-attacks early on. Some factors were considered to promote cyber attacks using Support vector machines. Results showed that the increase in cybercrime results from the increase in online banking usage, increase in internet user skills, and expansion of online activities. About 14 indicators were used example: mobiles infected with malware, users attacked by banking malware, Spam Emails by Originating Country (Yearly), attacks by crypto miners, countries targeted by malicious mailings, and computers attacked by phishing (yearly), just to mention a few.(Kuzmenko et al., 2021)



	Top 3 countries			Bottom 3 countries		
	1	2	3	1	2	3
% of Mobiles Infected with Malware (I_1)	Romania (5,04%)	Spain (4,31%)	Slovakia (3,5%)	Finland (1,06%)	Denmark (1,33%)	Germany (1,63%)
% Share of Users Attacked by Banking Malware (I_4)	Portugal (0,9%)	Greece (0,5%)	Bulgaria (0,5%)	Ireland (0,1%)	Denmark (0,1%)	Hungary (0,2%)
% of Attacks by Cryptominers (I_{10})	Latvia (0,73%)	Bulgaria (0,56%)	Slovakia (0,5%)	Denmark (0,11%)	Germany (0,12%)	Romania (0,14%)
% of all Spam Emails by Originating Country (I_{12})	Germany (10,97%)	France (5,97%)	Netherlands (4,00%)	Denmark (0,07%)	Slovakia (0,19%)	Sweden (0,19%)
% of Computers Attacked by Phishing (Yearly) (I_{14})	Portugal (19,73%)	France (17,9%)	Belgium (16,4%)	Denmark (3,26%)	Sweden (3,35%)	Ireland (3,42%)

Figure 11. State of Cybercrime in European Countries as of 2020(Kuzmenko et al., 2021)

The analysed attacks, as represented in the figure above, show that when it comes to cybercrime, Denmark is one of the countries that recorded the lowest number. (Kuzmenko et al., 2021)It is essential to note that cybercrime is a constantly evolving threat, and Denmark, like all other countries, has continuously adapted its cybersecurity measures to stay ahead of cybercriminals. Public-private partnerships and international cooperation are also vital in tackling cyber threats effectively.

5.1 What is Being Done to Address Cybercrime in Denmark

Denmark is a highly developed and technologically advanced nation which relies significantly on digital technologies and the Internet. Digital technologies and solutions have fueled the expansion of the public sector and competition in the private sector. Citizens rely on digital solutions to communicate with public authorities and businesses. Because individuals know the data given to authorities are secure and being processed with utmost privacy, it has created fundamental trust between the citizens and the leaders. Like in many other countries, cybercrime in Denmark is a growing concern due to the increasing reliance on digital technologies and the internet.

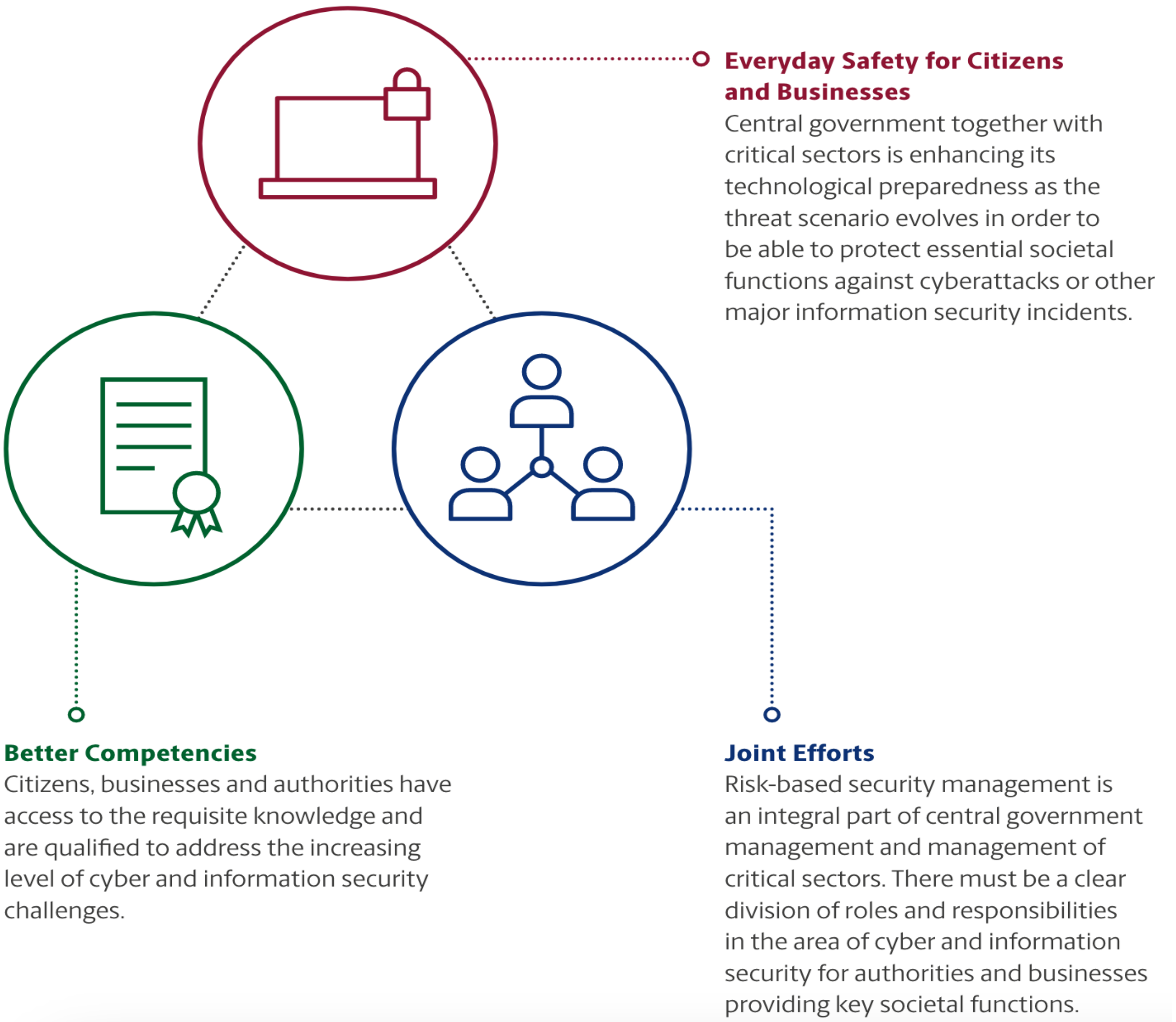
Denmark faces various cyber threats, from phishing and malware attacks to online fraud and data breaches. Denmark is one of the most targeted countries regarding cyber-attacks, so phishing attacks are prevalent to lure individuals into giving away sensitive personal data. In all of this, the Danish government has taken continuous steps to curtail cybercrime, setting up a centre for cyber security under the Danish defence intelligence service to monitor and mitigate cyber threats. Creating awareness among citizens and education is essential in fighting cybercrime. Every organisation and the government provide end users and businesses with resources to protect them against cyber threats.

Reporting cybercrime incidents is encouraged to help authorities like the Centre for cyber security to prevent cyber incidents and investigate.

In 2018, the Danish government was on the agenda for businesses, citizens and all authorities to become familiar with and capable of dealing with threats that come with digital Technologies and solutions as they heavily rely on digital solutions in handling day-to-day activities. The repercussions of not having a planned approach to address security issues are dire. So the government needed a coordinated and collaborative effort to prioritise cyber security. It is clear that even though the government have the sole mandate of protecting security at the national level, the individual's actions affect them and the people around them, just as companies are responsible for securing their organisation from cyber threats.

They are three focused areas that were considered to be critical to the readiness against cyber threats. These areas are 1. Technological preparedness, 2. Raising awareness, 3. To Improve cooperation and coordination between responsible authorities. During the process, 25 more strategies will be implemented to support the initiatives in place already. In the quest to strengthen the cyber defences of Denmark, an amount of 1.4 billion Danish kroner was invested over six years(2018-2023).

Denmark has taken a queue from the European Union “NIS Directive on the security of network and information systems security. It says that Providers of vital societal services and functions must take action to manage the security of the networks and information systems they employ to deliver their services”(Romaniuk & Manjikian, 2020, p. 116). A national strategy for the security of networks and information Systems must be developed by member states. To prepare Denmark to tackle future challenges on different levels, the government devised a strategy to help the cyber security space growth be resilient. This planned strategy has specific steps to improve security in business regarding information technology and digital solutions. For the government to ensure it is achieved, they had a decentralised talk to further this strategy across the country, starting with municipal to the regional cyber and information security strategy.



Everyday Safety for Citizens and Businesses

Central government together with critical sectors is enhancing its technological preparedness as the threat scenario evolves in order to be able to protect essential societal functions against cyberattacks or other major information security incidents.

Better Competencies

Citizens, businesses and authorities have access to the requisite knowledge and are qualified to address the increasing level of cyber and information security challenges.

Joint Efforts

Risk-based security management is an integral part of central government management and management of critical sectors. There must be a clear division of roles and responsibilities in the area of cyber and information security for authorities and businesses providing key societal functions.

Figure 8: Benchmarks to strengthen cyber security

5.2 One Main Technology to Ensure Security at the National Level

There are many types of identity. However, in cyber security, identity is vital online as it shows who one is and the kind of resources one can access depending on one's privilege.

Denmark has recently introduced an authentication method called MitID(electronic identification solution), which all citizens must use to prove who they are when trying to get some access online, i.e. online banking and public self-service solutions. This was a move from NemID, which has been used for over ten years and, at the time, met the security requirement and regulation by the eIDAS(electronic IDentification, Authentication and trust services) but now has to be replaced by the MitID because the eIDAS demands in security level in eiD have changed over the years. Denmark constantly adapts new ways and technology to stay up-to-date with ever-changing cyberspace and challenges for citizens to use the internet with trust and confidence. This is not to say that the solution has fixed the cyber threat that Denmark faces, but more research is being done, and updates are being made to make it as resilient as possible(Mogensen & Aranha, 2023).

5.3 Legal Reforms in Denmark

Denmark, among other countries, is part of the European Union, meaning some, if not all, laws and regulations are derived from EU directives and regulations. Phishing in Denmark is addressed by the

1. Danish criminal code(Straffeloven): This code includes provisions relevant to different types of cybercrime, including phishing. Section of this code stated categorically about

- Fraud: This section discusses fraudulent acts, like phishing scams, in which people trick others into getting private data or sensitive information.
- Obtaining Login Information by Deception: This section deals explicitly with offences related to obtaining login credentials or accessing computer systems through deceit, such as phishing.
- Illegal Access to IT Systems: This provision covers unauthorised access to computer systems, which can be applicable if phishing is used to gain unauthorised access to someone's digital accounts.
- Illegal Data Interception and Use: This section addresses the unlawful interception and use of electronic communications or data, which could apply to phishing attempts involving electronic messages.

According to the sternness of the offence, individuals who engage in phishing may be sentenced to jail or fines if proven guilty under these rules.

2. Personal Data: Personal Data processing act governs the protection and handling of personal data in Denmark. It establishes guidelines for collecting, storing, and using personal information, including measures to prevent unauthorised access or disclosure through phishing or other fraudulent activities.

3. Danish Electronic Commerce Act: Danish Electronic Commerce Act covers various aspects of online commercial activities, including provisions related to fraudulent practices such as phishing. It sets online businesses' requirements and obligations to protect consumers from deceptive practices.

4. Danish Data Protection Act: The General Data Protection Regulation requirements of the European Union are implemented in Denmark by this Act. It regulates the processing of personal data and imposes obligations on businesses to guard against phishing scams and safeguard the privacy and security of personal information.

6. Ghana

With the high internet penetration in Ghana, which gave birth to a growing digital economy, it has faced severe cybercrime implications of all kinds. The introduction of Mobile money payment, popularly known as MoMo to make banking easier, has attracted the attention of many. Ghana has been in international media for the wrong reason, often due to internet fraud. In 2019 Bank of Ghana reported that they had recorded 2,295 cases of fraud, amounting to a 5.4 per cent increment, among which they have cases like impersonation and email fraud, which was labelled as a high-risk type due to the highest value of attempted fraud amounting to GH¢ 50.54 million. These crimes increase due to a lack of clear and proper cybersecurity strategies and collaboration among the various stakeholders. Identity theft and smishing(SMS phishing) have cost the country and individuals much money, which the banks and telecom operators have never taken full responsibility for. To an extent, the state has shown good faith in trying to curtail the crimes by developing legislation to address the scams. In 2017 the policy brief by the Kofi Anna international peacekeeping training centre came out with a report after thorough research in which they had examined legislative initiatives, examine the types of cyber security threats that exist in Ghana, review how well the country is doing in addressing them, and make suggestions to the government on how to proceed. With the construction of a multi-million dollar 600-rack national data centre in Accra and the rollout of fibre optic rings to connect government ministries and offer internet access to all government departments, Ghana has seen a rapid development of internet access in recent years. Ghana has yet to create a reliable legal framework to manage cybercrime, although cybercrime has become a significant problem. To retain consumer trust in the security of the internet, ensure national security, and grow the Ghanaian economy, it will be essential to address these concerns. As Africa's second-largest source of financial fraud and cybercrime, Ghana is at a higher risk of becoming the target of coordinated cyberattacks. Targeting more affluent and valued victims both inside and outside of Ghana, cybercrimes have developed into sophisticated businesses. Many cyberattacks go unreported, which has detrimental effects on the Ghanaian economy. Cyberattacks seriously threaten the economy, the public sector, and the country's security. Cybercriminals have become more cunning in recent years. The primary government website was hijacked by a malicious Turkish hacking group in January 2015, highlighting the demand for a more contemporary approach to cyber security. The state requires legal acts to tackle cybercrime, but national laws disregarding international standards fall short. Many judicial systems still use common law offences to prosecute their counterparts in cyber crimes because they have

not yet developed a new strategy for dealing with cybercrime. Ghana has fallen into this trap since no laws are primarily intended to handle online crimes.
The government has not yet established a framework for adhering to international norms or developing an official cyber security plan. Regional entities have adopted legal frameworks for combating cybercrime. However, no African country has ratified the AU treaty. The ECOWAS Draft Directive disregards widely used tools for real-time data collecting. The AU convention's clauses regarding computer data preservation and expanding government power could encourage discrimination and other human rights violations. By ratifying the Budapest Convention on Cybercrime and harmonising its laws with those of the rest of the world, Ghana can make efforts to combat cybercrime better. Create a central organisation to coordinate and distribute cyber security resources between government departments, undertake benchmarking and accreditation, and build a framework for globally adopting acknowledged cyber security standards. (Motiwala, 2017)

Cybersecurity in Ghana

Phishing, Smishing, Vishing, Mobile money fraud, Identity fraud, fake gold merchants, and estate fraud are among the types of cybercrime that have dominated the cybercriminal infrastructure in Ghana. Identity fraud, often known as "romance fraud," requires the victim to "hook" a possible partner or lover from the United States or Europe and convince them to send money to keep their relationship going. Fake gold sellers deceive their victims, primarily from developed countries, by starting relationships with them online using email, chat rooms, social media, and marriage sites. Estate scam mainly targets Ghanaians residing outside Ghana and wanting to invest there. These criminal operations use online resources to steal money from Westerners and Ghanaians living abroad. One of the novel trends in Ghana's cybercrime problem is how criminals utilise the internet to steal money from individuals and organisations through bank, identity, and credit card theft. There is a belief that cybercriminals use spirits openly to cheat their victims. This conviction demonstrates the necessity of considering the technological, political, economic, and legal factors in any approach to combat and address cybercrimes in Ghana. There are cultural environments that encourage the development and spread of cybercrime in Ghana; nevertheless, Ghana has been one the countries at the forefront of fighting cybersecurity issues when it comes to Africa due to its growing information technology industry, it has become one of the countries that most African countries look to when it comes to fighting cybercrime.

However, as the world gets connected via the internet, from which Ghana was not exempt, Cybercrime has increased exponentially, affecting every aspect of Ghanaian society. To tackle this issue in the diaspora and internally to maintain the peace and stability of the country, many criminal institutions were established, and laws were enacted coupled with partnerships with international bodies to help put the necessary infrastructure to deal with these issues. The transition from disengagement to quick modernisation and centralisation has been the turning point of Ghana's approach to cyber security. The government established a network in 2008 to centralise the regulatory organisations that help monitor online behaviour, cybercrimes, and new electronic services but have yet to help much as there is still evidence of increases in cybercrimes.Nearly all government entities now solely receive internet and data services from the National Information Technology Agency as of 2011. This effort established "digital certificates" to identify and safeguard communication between government and non-governmental groups and permitted regulatory organisations to function under government domains.

The creation of NITA gave the government the green light to launch a strategy to combat cybercrime on a local, regional, and global level. Ghanaian economy and citizens have suffered due to the surge in cybercrime. The government has created regulations, national papers, and cybersecurity institutions to address the country's problems, such as cybercrime and internet threats. Adopting these policies institutionalises and integrates Ghana's political, economic, and social institutions with the expanding cybersecurity apparatus. It is imperative to examine the historical development of legislation influencing Ghana's attitudes regarding cybersecurity to comprehend better this abrupt policy change in tackling the enormous variety of cybercrime that seeks to emerge in Ghana.

6.1 Phishing in Ghana

As the world strives to achieve a certain level of digitisation. African countries like Ghana are not left behind. Every technological achievement comes with its downsides. The emergence of “COVID-19 has expedited the adoption rate and the expansion of Information communication technologies in the health sector”(Yeng, 2023). Among all the African countries, Ghana has attracted many international organisations like Twitter, Google, and Oracle to set up a headquarters of a sort or technology-enabled hub. The World Health Organization (WHO) has confirmed increased mobile devices, tablets, embedded devices, and laptop usage(Yeng et al., 2022). Ghana’s population as of 2021 was pegged at 30,792,608. According to Ghana's statistical report, based on the 2021 census, there are about 15 million internet users in Ghana. Ghana currently has the greatest mobile penetration in West Africa. Mobile adoption reached 55% by the end of 2019, exceeding the regional average of 44.8%. This implies that a sizable population may have access to digital services, which may lead to the expansion of the digital economy (Omondi, 2020). In that regard, there is the need to put proper structures like the construction of Digital Forensic Labs, better ICT infrastructures and good regulations to deal with crime challenges.In Ghana, a simulation of SMS phishing was carried out among healthcare professionals. The result shows that 61% of the targeted health workers were susceptible to phishing attacks(Yeng et al., 2022). SMS phishing(Smishing) is the most common way of conducting phishing attacks in Ghana. The adoption and expansion of the digital economy in Africa, especially Ghana, have also increased cybercrime, and many, for a long while, have thought our infrastructure has supported it to the fullest. Yes, many can argue that cybercrime is a huddle yet for any country to cross. However, we cannot disregard the fact that it always gets the better of developing countries whose national ICT infrastructure, institutions, and regulatory frameworks are not cut out for it. The proliferation of these cybercrimes makes us ask whether digital society is a blessing or a curse. These crimes of which, the most common ones are Smishing, popularly known in Ghana as mobile money fraud. Cybercrime, among many others, remains a threat to digital society. Crimes like identity theft, email scams, investment scams, jobs scams, shopping scams, compromises of sex images used as leverage in blackmail, and social media impersonation, particularly on Facebook(Whaling), where people pose as CEO of organisations or captains of law enforcement agencies, and many more just dupe or lure people and ripped off for financial gains. “In 2018, a report showed that cybercrime constituted about 82 per cent of fraud-related cases in the country”(Ennin & Mensah, 2022). According to Ghana's Criminal Investigation Department(CID), a huge sum of money was lost due to cyber fraudsters' activities in 2020 compared to 2019. The Director in charge of the CID unit alluded to the increase in these cybercrime cases due Covid-19 pandemic, which has forced most people and organisations to do electronic transactions (*Criminal Investigation Department*, 2021). The timely increase in these cases and have caused huge financial losses in Ghana. One could say with no doubt that these are just a few of the many incidents reported and captured. Furthermore, it is believed that many of these victims do not report this case because they believe it to be a lost cause right from the jump. In many instances, people allege to be the culprit get away with these crimes, and victims do not often report or follow up on these cases. The Director of the CID revealed that cyber violence and e-threats have increased, including crimes like denial of service, false news, and pre-registered SIM cards. The department made 135 and 241 arrests in 2019 and

2020, respectively. He attributed the increase in their arrests to collaboration between the U.S. Embassy, the Council of Europe, and the National Cyber Security Centre.
He noted that there is a need for collaboration with major security stakeholders to help reduce the number of crimes. As demonstrated by (Ennin & Mensah, 2022) in their exploratory study of victims' perspectives on these issues found deficient responses to the information they gathered from the CID. "The department made it known to them that usually victims involved High-profile persons who cannot handle the disgrace of others discovering they have been duped online. Moreover, in some cases involving expatriates who want to pursue their cases are advised by their ambassadors/representatives to Ghana not due lack of confidence in the Ghanaian legal system which has been tainted with alleged corrupt practices and undue delay of cases." Most of the time, these crimes result from someone posing as a different entity, be it the CEO of an organisation with a business proposal to which these victims fall prey. In most cases, it has become difficult to punish these cybercriminals because of the abstract nature of the Internet and the hurdles involved in getting the root cause of these cases. This is a looming danger. If we do nothing, we will face rapidly proliferating episodes of theft and deception, eroding public trust in the Internet.

6.2 Legal Reforms in Ghana(What is been done to address this)

The security dealings in Ghana have been between the public and the private sector. The National Information Technology Agency (NITA), a technology agency, was established by the Ministry of Communication to show Ghanaians and the rest of the world how seriously the country takes the development of cybersecurity as a countermeasure to the rise of cybercrime(phishing scams). The Data Protection Commission is instructed with the regulatory oversight and appropriate implementation of policies, procedures, and processes of Data Controllers. NITA is responsible for implementing Ghana's Information Technology policies and ensuring the sustainable growth of Information Communication Technology. The National Information Technology Agency was Ghana's effort to create a formalised structure for the regulation of information and communication technology provision, the guarantee of high standards of service, the promotion of standards of efficiency, and the assurance of the provision of high-quality technology and campaigns. To supplement national expertise, Ghana has made strides in forming communicative pipelines and initiatives with international institutions to develop Ghana's infrastructure in the face of increased cyber threats. Non-Governmental organisations, professional certifications, and training are pivotal tools that will improve" The creation of awareness and the development of online skills for everybody by creating a national program and gateway for cyber security awareness that is directed at all parties and that content producers use different formats and methods." but this never seems to make a head start yet. Ghana has defined different elements of its Critical National Information Infrastructure, which gives aims and objectives for improving the cybersecurity structure in developing an effective cybersecurity policy and structure. With these areas in mind, some areas covered by Ghana's cybersecurity initiative include regulatory and technology frameworks, facilitating a security culture, and international cooperation. Ghana's cybersecurity policies rely on the following legislation.

The Electronic Transactions Act of 2008 (ETA)

The main objective of the act of facilitating digital interactions and associated transactions is for the benefit of the public. It also removes and prevents barriers to electronic communication and commerce and promotes legal certainty in electronic communication and transactions. The act is to help develop a safe, secure, and effective environment and ensure that vulnerable groups are considered. Cyber offences are addressed, even though this Act does not necessarily touch on phishing but other crimes like stealing, representation (pretences), forgery, unauthorised access, denial of service, and obtaining electronic payment medium falsely, which is “Making a false statement to obtain the authorisation of an electronic payment medium for oneself or another person constitutes a crime and is liable to punishment or imprisonment. This act does not directly address phishing, but since phishing is a cyber offence, the Electronic Transaction Act can punish culprits. In Ghana, an individual falsely represents himself as someone or a trusted entity to dupe others(Romaniuk & Manjikian, 2020).

Data Protection Act of 2012 (DPA).

The act was passed to protect the public's privacy. Regulations govern how personal data is handled, including how to gather, store, utilise, or disclose individual information. This is to ensure a proper guideline for individual data usage. However, there are theories on the street that most financial fraud, as we call it, is mainly perpetrated with the help of staff in organisations with data on the individual or organisations(Adu, 2022).

Cybersecurity Act, 2020

Parliament approved this Act, and the president assented. It aims to create a cybersecurity authority to oversee national cybersecurity policies, advance cybersecurity research and development, and guarantee a safe, resilient digital economy. The authority is also responsible for creating awareness of security issues and joint forces with international bodies to help enhance the country’s cybersecurity. They are to monitor cybersecurity threats outside and within the country keenly.

“Due to these critical collaborations, other significant steps have also been implemented since the founding of the National Information Technology Agency Act”(Romaniuk &

Manjikian, 2020). Each of these institutions plays a specific role in the proactive deployment of measures against cybercrimes and the widespread dissemination of knowledge about the threats they pose and viable solutions across the nation. We looked at legislative attempts to institutionalise cybersecurity norms within the country to give an overview of the framework and policies guiding cybersecurity in Ghana.

In order to emphasise cybersecurity and then reduce cybercrime, Ghana's legislative initiatives establish a framework of authorities, regulatory organisations, oversight mechanisms, and scientific metrics. Establishing the Data Protection Act as an essential component of the legislation symbolises transition in Ghana. It highlights the level of importance with which the government treats cybersecurity, even though it needs to be clarified to what extent the act and its associated measures are being implemented and monitored. Ghana's complete approach to addressing cybersecurity issues through its institutions and active legislative structures speaks volumes about Ghana's peculiar historical dynamics and the perceptions of cybercrime that are shared globally.

However, “the lack of competence from law enforcement and the absence of robust substantive measures in implementing these statutory requirements remain significant obstacles in the fight against cybercrime”(Romaniuk & Manjikian, 2020).

The government's foresight in passing such a law demonstrates its comprehension of cybersecurity's serious consequences for various sectors, including finance, health, national security, and education.

7. Methodology and Research Design

The methodological techniques used in this research paper are outlined in this chapter. To meet the objective of this study, a qualitative approach was used as qualitative research emphasises words, descriptions, concepts, or ideas, whereas quantitative research uses data and figures. Generally, qualitative methods are used in the study to explore and understand a problematic scenario.

In contrast, quantitative methods are used to test or validate hypotheses. Semi-structured interviews were conducted with experts in this domain as these are things they deal with on a day-to-day basis to show a deeper analysis of the value of knowledge relevant to achieving the objective of this research. This study first seeks to understand the literature and data available in this field and to establish how this research will add relevant and undeniable knowledge to this research field. A semi-structured interview was employed as it gave the researcher room to a list of open-ended questions to elicit more information from interviewees.

In this research, thorough research was conducted to find and understand the current level of knowledge available and the evolution over the years with various technologies deployed to counteract this huddle. These will help to put in context the relevance of this research as the result of this research will be based on how Denmark has dealt and is dealing with the issues of cybercrime, especially phishing attacks, the current deficiency in Ghana society and what can ghana adopts and implement as it is still challenging to get a grip on the increase in phishing activities that have taken many forms in the Ghanaian society despite the enormous attempts to curb it. Some other relevant issues were also touched on as this will help form a good generalisation and properly put context to understand this issue even more so, as it does not just pertain to Ghana, a good reference point is needed to understand this help understand this. The theoretical framework and literature evaluation were developed using scholarly search tools and platforms. Research Gate, Sci-Hub, IEEE Xplore, Taylor, Francis + NEJM, Frontiers, Springer Link, and UBsearch, were used along with Google Scholar, Science Direct, Sage journals, and Science Direct. Some keyword combinations that were used are "cybercrime in Ghana", ''Cybersecurity issues, "Phishing crime/ activities/ fraud/scam'', "cybersecurity policies/law/infrastructure", and "phishing activities in Denmark". Of the total number of relevant articles, book chapters, and conference papers, over 270 were found and downloaded, out of which 150 were considered and 60 were selected and used for research. The ones that meet the criteria used in the research's theoretical framework served as the basis for the selection. Top priority was given to the sources that provided in-depth analyses of the issues.

7.1 Research Design

A qualitative approach has been employed, providing a framework for data to be collected and analysed to provide a comprehensive description and interpretation of a study(Vaismoradi et al., 2016). This study focuses on understanding the steady increase in cybercrime in Ghana and what can be learned from a developed country like Denmark when dealing with phishing activities(cybercrime). Even though this research field is not necessarily new, this study will help look at issues through the structural lens of structure, strategy, and policies that can help curtail cybercrimes. The structural lens can the different forms and angles, but this study will analyse the problem through structuration theory, as discussed in earlier pages. To help understand the issues properly. A thorough literature review was conducted from the broader spectrum before narrowing it down and data on how the increase of cybercrime has become an issue in Ghana.

The strategies that the Danish authority has employed to help get a grip on cybercrime and what they are still doing were derived from the literature, as this will give a general perspective on the scale of the issue after the research question was posed. A theoretical framework was developed to allow data collection and perspective analyses of the research findings. Interview questions were formulated regarding the literature review's fallout, which aligns with the theoretical background for better analysis. The theoretical study has given the basis for identifying and developing the themes and applying them to the interview transcripted. Notes and interview transcripts were analysis base on the issues and the theory. Codes were generated to organise data accordingly(Vaismoradi et al., 2016)

Usage of Theory in Analysis

Dimension	**Analysis Explanation**
Signification - Interpretive Scheme - Communication,	The signification dimension of this research is to put into perspective laws, policies, and resources that are available in the fight against cybercrime and phishing to be a precise, comprehensive understanding of these policies and the communication between the various stakeholders.
Domination - Facility - Power	The domination dimension concerned materials, allocative resources, and exercising power by various authorities and institutions from control resources. In this case, the gatekeepers and the government hold the authority to make sure they are clear-cut laid down procedures.
Legitimation - Norms - Sanctions	Every society has its values and standards they live by, which directly and indirectly affect every aspect of their life. Legitimation will measure the degree of implementation of the appropriate standards, laws, policies, and sanctions, which could help shape this domain for the better.

8. Interview Guide Questions

Dimension	Interview Questions
Signification - Interpretive Scheme - Communication	● Are the laws or policies helping in the fight against phishing? ● Are well-constituted bodies available to collect and share knowledge for proper understanding and investigations? ● Are there issues with implementing our technological systems that make them more vulnerable?
Domination - Facility - Power	● Are the gatekeepers doing enough to curb it? ● Is digital illiteracy level a contributing factor to this problem? ● What do you think about the resources dedicated to the fight against these phishing scams that have ravaged cyberspace?
Legitimation - Norms - Sanctions	● What can the government do to avert these crimes properly? ● How often do these crimes get the punishment requires to serve as a deterrent?

The questions above will help answer the research questions and to put things into proper perspective, and the theory will be used to analyse the outcome. Since the dimensions of the structures intertwine with each other. It will help us to understand the holistic issues in this regard.

8.1 Data Collection

For better comprehension of this topic and a good analysis of data, excellent and relevant sources for data collection were needed. Employees of Phishing companies, lawmakers, software engineers, and testers were approached in the United Kingdom, Canada, Australia, Denmark, the United States of America, and Ghana via LinkedIn. Data collected from these sources was to establish how grave this issue is across countries and borders. Nonetheless, this would have made the research broader with the scope of time we have to reconsider and narrow down the data collection sources since we were trying to investigate this issue from a specific point of view. This would have been a good approach considering how research has shown that this field is one of the popular fields of interest with the rise in digitisation worldwide. However, some countries' infrastructure is better than others. Attention was focused on experts in Ghana and Denmark to give us in-depth and valuable information since they mainly deal with this in their day-to-day activities. The techniques allow for collecting evidence from different sources, as the qualitative approach best fits. Interviews were taken with industry experts and reviewing articles, quarterly reports from recognised organisations, regulatory acts, News articles, book chapters, and documentary videos. Apart from experts, Lawmakers and Lectures were contacted, as well as the Directors of various cybersecurity authorities, all from Ghana. In total, 40 participants were contacted, out of which ten responded and agreed to participate in the study. However, 5 participants later cancelled after several failed attempts to schedule a meeting.

The remaining participants' meetings were organised based on availability, and open-ended questions were designed and posed during the interview sessions. Sessions were recorded with the participant's permission and later transcribed for analysis. Notes were taken and compared with transcriptions, and detected errors were corrected by listening and reading the transcript of the recorded sessions.

8.2 Interview

Interview Findings Summary

Interview I		
Dimension	**Question**	**Quotes**
Signification - Interpretive Scheme - Communication	● Are there issues with the ways we implement our technological systems that make them more vulnerable?	● *That statement can partially stand or not.* ● *but there was a case where we investigated and realised that some of these people are into mobile fraud and Other types of fraud, they have insiders in the various telecoms who have been helping them.*
	● Are the laws or policies helping in the fight against phishing?	● *For the law, there is. In 2020, Ghana had its first Cybersecurity Act* ● *it has been going through several implementations* ● *the reason why most criminals can go away with the various crimes they commit successfully is a result of our identification problem.*
	● Are there well-constituted bodies available to collect and share knowledge for proper understanding and investigations	● *Ghana has a cyber security authority, and- incidents relating to cyber crimes it is reported to them, and they do bring out feedback on it.* ● *do some investigations* ● *get some data and bring it out to the public to make the public aware.* ● *Just that, unfortunately, that information doesn't reach everyone. One thing is that gap in education*

Domination - Facility - Power	● Are the gatekeepers doing enough to curb it?	● *the various service providers are doing their possible best.*
	● What do you think about the resources dedicated to the fight against these phishing scams that have ravaged cyberspace?	● *I think the resources there are because most of the cyber crimes in Ghana are not sophisticated. People who fall victim to these phishing, vishing, and smishing, mainly when they are narrated, you just realise that it was as a result of due diligence.*
	● Is digital illiteracy level a contributing factor to this problem?	● *Yeah, that is very true. It's a very great contributing factor.*
Legitimation - Norms - Sanctions	● What can the government do to avert these crimes properly?	● *the government has started putting in some initiatives, and one of them includes using the month of October every year to create awareness of cybersecurity and cyber crimes* ● *The cybersecurity authority has been periodically organising some outreach to go to some remote areas to educate the people there on cybersecurity issues in the local dialect, not just in the English*
	● How often do these crimes get the punishment requires to serve as a deterrent?	● *The laws are working. I said at first we didn't have many laws used to prosecute such people, but with the implementation of the Cybersecurity Act, we're able to have something to serve as a basis to prosecute such people.*

Interview II		
Dimensions	Questions	Quotes
Signification - Interpretive Scheme - Communication	● Are there issues with the ways we implement our technological Systems that make them more vulnerable?	● *NO, we try to create a more robust and secure system.*
	● Are the laws or policies helping in the fight against phishing?	● *laws in Ghana regarding data privacy and all that. I think, um, assess and education is quite on, on the lower aspect as well* ● *I don't think people are even aware of what the law says.* ● *we are never clear on what the law is about.*
	● Are there well-constituted bodies available to collect and share knowledge for proper understanding and investigations	● *Yes, they are* ● *NSP provides a platform for scam reporting* ● *I don't think it's really working effectively. But the one that really works more is that of the NSP, where you can, um, kind of make a complaint.*
Domination - Facility - Power	● Are the gatekeepers doing enough to curb it?	● *the NSP hasn't done much* ● *so people posted, be certain people calling from, from the*

		NSP. - *Presenting Ghana and when they call, they tried to get access to your accounting pills, make requests, financial requests* - *Serious attention whereby someone is able to, to take money from somebody's account and the money cannot be tracked*
	- What Do you think about the resources dedicated to the fight against these phishing scams that have ravaged cyberspace?	- *I don't think we've done enough. That's from a general point of view, I don't think we've done enough in Ghana.* - *It's more like we, we've accepted, um, we find a way to live with it* - *You just have to be smart enough to protect yourself.* - *more like a post-action than a pre-action to kind of prevent them.*
	- Is digital illiteracy level a contributing factor to this problem?	- *you can't take that out.* - *digital illiteracy is, is part of the problem* - *even update their software thinking it's gonna cost them more data to update than their security.*

Legitimation - Norms - Sanctions	- What can the government do to avert these crimes properly?	- *to have that education out there to let people understand* - *I don't think people are getting access to the information as they should.* - *I think the law will need to look at the law and also need to be enforced.*
	- How often do these crimes get the punishment requires to serve as a deterrent?	- *cybercrime, like 80 or 90% of them go unpunished.* - *the process to get justice is not, it's not, um, seamless. It's not transparent.* - *So the majority of the cyber can go unpunished because the process of getting justice is just*

Interview III		
Dimension	Questions	Quotes
Signification - Interpretive Scheme - Communication	- Are there issues with the ways we implement our technological systems that make them more vulnerable.	- *Yes. Because of the nature of our users, most people do not stick with, uh, the standard policies that are said.* - *find it, to be too much work going through the proper procedure. So we*

		tend to cut corners, and that's what makes us vulnerable.
	● Are the laws or policies helping in the fight against phishing?	● *There are laws, yes. The laws are good. The laws are solid, but again, it's just Dr who don't know about them.*
	● Are there well-constituted bodies available to collect and share knowledge for proper understanding and investigations	● *Yes, I know of the police cyber bureau where they have the capability and then the men to investigate such acts.* ● *most of the things that happen go unreported because people don't even know about them at the first.*
Domination - Facility - Power	● Are the gatekeepers doing enough to curb it?	*No, no. I can use, uh, a few of the NCA and other things, uh, internet service providers where all of these guys are around and even they are the west corporates because they are services that they, Are the avenues that are being used by most people in this endeavour.*

	● What do you think about the resources dedicated to the fight against these phishing scams that have ravaged cyberspace?	● *No, not at all. I mean, even with the basic form of fighting, which is education, I don't think that's, most people even know about, phishing in the first place.*
	● Is digital illiteracy level a contributing factor to this problem?	● *yes. All right,*
Legitimation - Norms - Sanctions	● What can the government do to avert these crimes properly?	● *government can do would be to educate the people,* ● *they become victims, and they know where to go to seek redress.*
	● How often do these crimes get the punishment requires to serve as a deterrent?	● *would say daily. It happens every day, and then I put on a report and then it just goes away.*

Interview IV		
Dimension	Questions	Quotes
Signification - Interpretive Scheme - Communication	● Are there issues with the ways we implement our technological systems that make them more vulnerable.	● *Yes, most of than not, security becomes a secondary thought in implementing some products.*
	● Are the laws or policies helping in the fight against phishing?	● *I think the laws are usually on cybercrime in general and not specific to phishing. I believe the laws would be stiffer as we grow in these areas.*
	● Are there well-constituted bodies available to collect and share knowledge for proper understanding and investigations	● *Yes, some institutions are created for these, but there are no distinct roles for them, and citizens don't trust them to do their work to the fullest.*
Domination - Facility - Power	● Are the gatekeepers doing enough to curb it?	*I think the gatekeepers are doing enough. It is also up to the users of the space to be super vigilant and talk more about these phishing acts.*

	● What do you think about the resources dedicated to the fight against these phishing scams that have ravaged cyberspace?	● *Resources are never enough, as these scammers get creative most of the time. The best resource is awareness creation. Once there is a new phishing technique, it is very important to let the world know about it to create awareness.*
	● Is digital illiteracy level a contributing factor to this problem?	● *yes. Digital illiteracy is not a contributing factor. We just need to be more intelligent with these scams*
Legitimation - Norms - Sanctions	● What can the government do to avert these crimes properly?	● *Government can create more awareness and be more strict with various laws and policies.*
	● How often do these crimes get the punishment requires to serve as a deterrent?	● *Since there are no clear regulations on this, making it complicated. There delay and corruption in the legal system is also contributing factor.*

9. Discussion

Signification,

The signification dimension of this research is to put into perspective laws, policies, and resources available in the fight against cybercrime and phishing to be a precise, comprehensive understanding of these policies and the communication between the various stakeholders. In the literature review, we found that phishing activities are still increasing and difficult to tackle because, under organisational structure, institutions with the obligations to enforce laws and policies have overlapped roles that tend not to be efficient. Even though there were cases where investigations were done, the culprit was punished, as enumerated by one of the interviewees. In an attempt to disagree with the statement, answer the question and add an example.

Moreover, the Interviewee elaborated that in most cases, they have investigated that these crimes were committed with the help of an insider in the organisations, ”there was a case where we investigated and realised that some of these people are into mobile fraud and Other types of fraud, they have insiders in the various telecoms who have been helping them ”. The laws and policies that were developed are still very new, and the structures available do not support the effective implementation of the rules and policies. As an interviewee said, “In 2020, Ghana had its first Cybersecurity Act. It has been going through several implementations; most criminals can go away with the various crimes they commit successfully because of our identification problem,” As outlined by one of the respondents. How can people who commit crimes be tracked and identified if essential user identification is still problematic?

In addition, when crimes like this happen, most people do not report them because people do not even know about them; as the interviewee elaborated ’’laws in Ghana regarding data privacy and education are quite on, on the lower aspect as well ”. With any new phishing activities emerging, the cybersecurity authority tries to notify the population.

However, education only reaches some, as posited by interviewee I, II, III, and IV; the educational gap is also a problem. Interviewees agreed that laws were created recently due to increased crime, but they need to be entirely up to the task and the structures in place to support the implementation of these laws and policies. However, there added that people are unaware of these rules” I do not think people are even aware of what the law says. We are never clear on what the law is about”.

Moreover, one interviewee elaborated that the rules are unclear and the institution is ineffective. “I do not think it is working effectively. But the one that works more is that of the NSP, where you can kind of make a complaint”. As stated, “Crime is increasing due to a lack of clear and proper cybersecurity strategies and collaboration among the various stakeholders.” (Motiwala, 2017). So formulating laws and policies makes no meaning if there are no excellent structures to support the implementation and the efficient communication and interpretation between the institutions to enforce these policies and laws, unlike Denmark, where rules and regulations are clearly stated, and directives from the EU are adhered to. There is coherence in the institutions made available and enabled to receive reports and makes the most out it to educate the populist as stated by the interviewee, “In Denmark are mechanisms in place to educate every for example, in every organisation people are tested to see the level of education and the ability to identify in phishing emails and report it ” and there is a clear planned strategy to prepare the citizen.

9.1 Domination,

The domination dimension concerned materials, allocative resources, and exercising power by various authorities and institutions from control resources. In this case, the gatekeepers, the government and other regulatory bodies or institutions hold the authority to ensure clear-cut procedures are laid down. One of the Respondents said the various service providers are doing their best and the resources allocated are enough, "The various service providers are doing their possible best *and* the resources there are because most of the cyber crimes in Ghana are not sophisticated.".

The other interviewees agreed that the various institutions are not doing enough to help curb these crimes. As much as the Network Service Providers and the rest are trying their best, we found in the literature review that this is not good enough. Moreover, one can imagine that if most of the crimes are committed with the help of insiders in the network service providers or telecom companies, how can what they have done be enough to help reduce or resolve the cybercrimes? Identity theft and phishing, especially smishing and vishing, are still increasing, and telecom operators and bank portals are being used to perpetuate this act. However, they do not want to take full responsibility for it. To an extent, the state has shown good faith in trying to curtail these crimes by developing legislation to address the scams, but there is a need for a precise plan or strategy to tackle this crime. The Interviewees agreed that digital illiteracy is also a significant contributing factor to this issue, which establishes that the resource to educate the population is also on the lower even though they are institutions that are responsible for these but still have little to no effect. Hence with the overlap roles, resource mobilisation and use usage has to be reevaluated and mapped accordingly for practical use. Ghana should work with regional and international entities to improve its cyber security capabilities and reduce risks. Establish best practice rules, prioritise discretion, reduce disruptions, and give law enforcement and military authorities thorough training to help the Ghanaian economy deal with potential illegal activity. Ghana must create a strategic framework for addressing cybersecurity challenges to maintain national security and economic progress.

Whereas in Denmark, their digital illiteracy is reduced to the barest minimum as it has been proven that, though Denmark received the highest number(45%) of phishing messages, very few succeeded(2%). The interviewee also confirmed that there is constant training going on in every organisation and institution to help citizens to be able to recognise the report these attacks or attempted attacks. Literature has also pointed out that the Danish government has to invest a considerable sum of money in research and equipping all the necessary institutions assigned to make Denmark safe and to continue the reliability of digital solutions. The government has committed to making Demark safe for the people to have confidence in the give out the data

and know there is a safer environment in which their data is being processed. And so far, the result has been proven, leading to introduction of a new electronic identification platform (MITID) at the national level for further protection.

9.2 Legitimation

Every society has its values and standards they live by, which directly and indirectly affect every aspect of their life. Legitimation will measure the degree of implementation of the appropriate standards, laws, policies, and sanctions, which could help shape this domain for the better. With a low trust level in the use of digital solutions, as found in the literature, “Despite the majority of consumers being mobile subscribers this does not translate into usage as consumer lack education, understanding, awareness, and trust in the system due to poor implementation.” due to the challenges with privacy issues and scams that Ghanaians experience on a day to day basis that goes unreported and not to talk of it being punished. Nevertheless, there are fundamental laws that could be used for prosecution if culprits are found guilty, So the government must train the necessary expertise to handle things when it comes to technological legislation, as observed in the literature that includes the absence of robust substantive measures and institutions in the implementation of these statutory obligations, as well as the expertise of law enforcement.

For the government as an authority to help avert crime, Interviewees agree that education is critical to help create specific standards and values in the daily life of the average person, Despite the challenges of digitisation. As elaborated by interviewee I,” The government has started putting in some initiatives, and one of them includes using the month of October every year to create awareness of cybersecurity and cyber crimes”. However, this education must be daily, as pointed out by Interviewee III, “would say on the say attackers happen daily. One the respondent also elaborated the education has to be in other languages, “The cybersecurity authority has been periodically organising some outreach to go to some remote areas to educate the people there on cybersecurity issues in the local dialect, not just in the English” It happens every day, and then are put on reports, and then it just goes away.” Attackers are always looking for innovative and more accessible ways to scam people. Education will help cultivate in the minds of people cybersecurity values and standards and awareness of legal redress if they fall victim. One respondent noted that many citizens believe that getting just of any kind in these issues will lead to a waste of time and more resources. “Cybercrime, like 80% or 90% of them go unpunished, and the process to get justice is not, it is not seamless and transparent.” Furthermore, the government needs the judiciary system to be smooth, fair, and accessible to people, and above all, proper investigations must be carried out, and justice served to the culprits.

10. Limitation

The results of this study only use Ghana and Denmark as case studies for their conclusions. Although this problem exists in every nation, it is not a model for other nations. Having to meet experts and conduct interviews physically would have been a great source of data collection. Limited expert interviews due to last-minute cancellations, and some responded only some out of 36 experts, including directors and lawmakers, were contacted, and a large population sample of expert interviews would have given fascinating data for interpretation analysis. Moreover, they could not interview the Director of the Ghana Cybersecurity Authority and a member of parliament, as it would have been an excellent source of data collection.

Nevertheless, this does not negate the other sources from which data was collected. However, data gathered through experts interviewed are relevant to the study discussion as articles were reviewed to prove the data collected from the experts interviewed. A survey of the general population would have also been a good data collection point for analysis Since this issue affects more of the general population. An interview with more experts in Denmark would have also given a more solid view to establishing the structure, laws, and policies that make Denmark a strong study point concerning Ghana in the cybercrimes, not to say these countries are free from the attacks. However, they manage to curtail cybercrime largely compared to the attacks directed at them.

11. Conclusion

As the era of digitalisation has dawned on us, with the increase in the use of information Technology in aspects of life, cybercrimes, especially phishing attacks, are undoubtedly on the rise. The threats that come with digitisation do not only affect businesses and end users but also the government. Moreover, in every country, there is a need to address these cybercrimes. The most common ways used by attackers are via phishing.

To curb these growing activities, the government, as the highest authority in control of the state, must put structures in place to mitigate these crimes, as these will be with us as long as digitisation is concerned. It is the case of Denmark; Data shows that the Danish government, in collaboration with its defence institutions, devised a strategy to fight against cybercrime, leading to its success. The End users and the private institutions also have a significant role in making this vision feasible.

In Ghana, the private sector and the end users also have to play a huge role in ensuring this happens. Some measures are in place to help mitigate these things, but they never seem to work. Phishing activities are still on the increase. So this study aims to determine the structural issues that make it difficult to combat phishing scams in Ghana and what the government, as the foremost authority, can do to help fight these crimes.

Throughout the information review, some indications point out that Ghana is putting in many efforts to digitalise its economy. However, a lot is being lost to cybercrime, making the average population lose interest in digital systems and portals. Several researchers elaborate on the various attempts to digitalise every aspect of the economy. However, in conclusion, we also saw failures in these actions due to poor implementation, lack of expertise, the unclear and precise role of institutions and cybersecurity issues, low digital literacy rate amount the majority of the population, and many more. Data was collected, and empirical evidence was gathered through a thorough review of articles and blogs and conducting semi-structured interviews to elicit information to understand and put this study in the proper perspective. This study seeks to expand from the theoretical point of view to properly understand the significant issues of the structures that had to deal with these cybercrimes.

In theoretical review found three dimensions through which we analyse our findings from the interview. These dimensions are signification through which this research is to put into perspective laws, policies, and resources available in the fight against cybercrime and phishing to be a precise, comprehensive understanding of these policies and the communication between the various stakeholders. Legitimation measures the degree of implementation of the appropriate standards, laws, policies, and sanctions, which could help shape this domain for the better. Furthermore, domination involves materials, allocative resources, and exercising power by various authorities and institutions. We found out the government has a significant role, the private sector and the user.

The government as an authority need to establish transparent, precise institutions for dealing with these issues. There is a need for a decentralised solution. The ways and avenues of reporting these crimes must be made more accessible and easy for users. Policies and laws need to reconsider and made clear to promote swift prosecution and protect citizens from the attacker. Furthermore, Education is critical, as well as research and collaboration with foreign agencies to improve and train expertise in dealing with cybercrimes. People need to be educated about the various ways these attacks are carried out and, most importantly, about their right to privacy organisations must be held accountable when there is a leak or breach of privacy, as it sometimes leads to successful attacks.

To conclude, the government's efforts to curtail these crimes as the world gets more and more connected and the quest to digitise the economy to leverage the use of information technologies can only be possible in partnership with private companies well, equipped and established institutions with well-defined laws and policies for investigation and prevention rather than post-action not to after math actions are not essential but building resilient structure to support the digital economy is much worthy.

The above strategy is what the Danish government has employed over the year, and it is still used and shown to have worked.

12. Bibliography

Adu, J. N. (2022). *Cybercrimes and the Rule of Law in West-Africa: The Republic of Cote d'Ivoire as a Case-Study.*

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Information Security*, *16*(5), 324–345. https://doi.org/10.1049/ise2.12073

Aneke, J., Ardito, C., & Desolda, G. (2020). Designing an Intelligent User Interface for Preventing Phishing Attacks. In J. Abdelnour Nocera, A. Parmaxi, M. Winckler, F. Loizides, C. Ardito, G. Bhutkar, & P. Dannenmann (Eds.), *Beyond Interactions* (pp. 97–106). Springer International Publishing. https://doi.org/10.1007/978-3-030-46540-7_10

APWG | Global Phishing Survey. (n.d.). Retrieved November 7, 2022, from https://apwg.org/globalphishingsurvey/

Chen, R., Gaia, J., & Rao, R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. https://doi.org/10.1016/j.dss.2020.113287

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Criminal Investigation Department. (2021, February 20). DailyGuide Network. https://dailyguidenetwork.com/cyber-fraudsters-stole-19-8m-in-2020/

Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, 0032258X221107584. https://doi.org/10.1177/0032258X221107584

Daniel, B. (2016). *Spear phishing: Real life examples*. Infosec Resources. https://resources.infosecinstitute.com/topic/spear-phishing-real-life-examples/

Dewan, P., Kashyap, A., & Kumaraguru, P. (2014). Analyzing social and stylometric features to identify spear phishing emails. *2014 APWG Symposium on Electronic Crime Research (ECrime)*, 1–13. https://doi.org/10.1109/ECRIME.2014.6963160

Dupont, B., & Holt, T. (2022). The Human Factor of Cybercrime. *Social Science Computer Review*, *40*(4), 860–864. https://doi.org/10.1177/08944393211011584

Ennin, D., & Mensah, R. O. (2022). Cybercrime in Ghana and Victims Accounts. *Mediterranean Journal of Social Sciences*, *13*(3), 1. https://doi.org/10.36941/mjss-2022-0019

Frauenstein, E. D. (2019). An Investigation into Students Responses to Various Phishing Emails and Other Phishing-Related Behaviours. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), *Information Security* (Vol. 973, pp. 44–59). Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_4

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2017). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267.

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

Jalda, C. S., Kumar Nanda, A., & Pitchai, R. (2022). Spoofing E-Mail Detection Using Stacking Algorithm. *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, 01–04. https://doi.org/10.1109/ICSSS54381.2022.9782173

John Podesta's Phish Foreshadows Doom for 2020—Cofense. (2019, June 13). https://cofense.com/john-podestas-phish-foreshadows-doom-2020/

Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS Quarterly*, 127–157.

Karmakar, S. (2022). Phishing Attacks and It’s Working Methodology and How Spear Phishing Is Happening in Modern IT Hubs. *International Journal of Mechanical Engineering*, 9.

Kuzmenko, O., Kubálek, J., Bozhenko, V., Kushneryov, O., & Vida, I. (2021). AN APPROACH TO MANAGING INNOVATION TO PROTECT FINANCIAL SECTOR AGAINST CYBERCRIME. *Polish Journal of Management Studies*, *24*(2), 276–291. https://doi.org/10.17512/pjms.2021.24.2.17

Lain, D., Kostiainen, K., & Capkun, S. (2021). *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study* (arXiv:2112.07498). arXiv. http://arxiv.org/abs/2112.07498

Lamsal, M. (2012). The structuration approach of Anthony Giddens. *Himalayan Journal of Sociology and Anthropology*, *5*, 111–122.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 9. https://doi.org/10.1186/s40163-014-0009-y

Mangut, P. N., & Datukun, K. A. (2021). The Current Phishing Techniques–Perspective of the Nigerian Environment. *World Journal of Innovative Research (WJIR)*, *10*(1), 34–44.

Maruf Hassan, Md., R. Ahmad, B., Esha, A., Risha, R., & S. Hasan, M. (2022). Important factors to remember when constructing a cross-site scripting prevention mechanism. *Bulletin of Electrical Engineering and Informatics*, *11*(2), 965–973. https://doi.org/10.11591/eei.v11i2.3557

Mogensen, T. K. T., & Aranha, D. F. (n.d.). *User-centric security analysis of MitID: The Danish passwordless digital identity solution*.

Motiwala, A. (2017, February 1). *Cyber Security in Ghana: Evaluating Readiness for the Future*. Africa Portal; Kofi Annan International Peacekeeping Training Centre (KAIPTC). https://www.africaportal.org/publications/cyber-security-ghana-evaluating-readiness-future/

Oest, A., Safei, Y., Doupé, A., Ahn, G.-J., Wardman, B., & Warner, G. (2018). Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. *2018 APWG Symposium on Electronic Crime Research (ECrime)*, 1–12. https://doi.org/10.1109/ECRIME.2018.8376206

Omondi, G. (2020, February 11). The state of mobile in Ghana's tech ecosystem. *Mobile for Development*. https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-in-ghanas-tech-ecosystem/

Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, *67*, 101766. https://doi.org/10.1016/j.tele.2021.101766

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), Article 2. https://doi.org/10.3390/forensicsci2020028

Regulation, G. D. P. (2018). General data protection regulation (GDPR). *Intersoft Consulting, Accessed in October*, *24*(1).

Rekouche, K. (2011). Early phishing. *ArXiv Preprint ArXiv:1106.4692*.

Romaniuk, S., & Manjikian, M. (2020). *Routledge Companion to Global Cyber-Security Strategy*. https://doi.org/10.4324/9780429399718

Sonowal, G. (2022). Types of Phishing. In G. Sonowal (Ed.), *Phishing and Communication Channels: A Guide to Identifying and Mitigating Phishing Attacks* (pp. 25–50). Apress. https://doi.org/10.1007/978-1-4842-7744-7_2

Sun, J. C.-Y., Yu, S.-J., Lin, S. S. J., & Tseng, S.-S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249–257. https://doi.org/10.1016/j.chb.2016.02.004

The Bucharest University of Economic Studies, Bucharest, Romania., Paraschiv, D., Toader, L., Nițu, M., & Negrea, Ștefan. (2021). *Internet Fraud and Phishing Attacks—A*

European Perspective. 394–400. https://doi.org/10.24818/BASIQ/2021/07/051

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), p100. https://doi.org/10.5430/jnep.v6n5p100

Vatis, M. A. (2010). The council of Europe convention on cybercrime. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy Http://Www. Nap. Edu/Catalog/12997. Html*.

Whittington, R. (2010). Giddens, structuration theory and strategy as practice. *Cambridge Handbook of Strategy as Practice*, 109–126.

Whitty, M. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*, 00–00. https://doi.org/10.1108/JFC-10-2017-0095

Wu, M. (2006). *Fighting Phishing at the User Interface*. 199.

Yeng, P. K. (n.d.). *Healthcare Security Practice Analysis, Modelling and Incentivization*.

Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into Phishing Risk Behaviour among Healthcare Staff. *Information*, *13*(8), 392. https://doi.org/10.3390/info13080392