# CyberBot: A Friendly Bot to Protect and Educate Digitally Vulnerable People from Cybercrime

Atulya Singh[1] and Tasmina Islam[1*]

[1] *King's College London, London, UK.*

**Abstract**

This paper proposes a browser extension-based bot "CyberBot" to protect and educate digitally vulnerable people from cybercrime. The proposed bot not only warns users of immediate dangers but also educates them about the nature of online risks and mitigation techniques. CyberBot fits with the user's everyday digital routine to deliver real-time notifications and advice on cybersecurity procedures. A user testing and a comprehensive user survey conducted in this study confirm the bot's effectiveness in enhancing users' understanding, knowledge, and confidence in their digital safety.

**Keywords**

Cybersecurity Awareness, Cybersecurity Education, Usable Security, Chatbot.

## 1. Introduction

In the face of escalating cyber threats, the digital realm's vulnerability to sophisticated cybercrimes such as hacking, phishing, and identity theft is more pronounced than ever and has magnified from isolated incidents into a global crisis. Hackers capitalise on security gaps, craft sophisticated phishing schemes, and commit identity theft, which amplifies threats, especially for those lacking cyber proficiency, such as the elderly, the less tech-savvy, small businesses, and novices to the internet [1][2]. The rapid escalation of cyber threats contrasted with the slow pace of cybersecurity innovation creates a dangerous digital landscape for the most vulnerable [3]. This can have disastrous financial and emotional effects on the affected people. As well as making the security systems robust, it is important to make the users aware of cybersecurity risks and train how to prevent themselves from becoming cybercrime victims. There are several training and awareness programmes available [4]. But most of these are standalone short courses or training sessions for users to learn and apply separately but not many solutions integrate training into their regular online activities. This paper investigates and proposes a friendly bot via a browser extension, aimed at empowering digitally vulnerable individuals with the knowledge to safeguard their online presence. The proposed bot aims to provide real-time alerts on emerging cyber threats and actionable cybersecurity advice, making it an accessible and user-friendly ally in the fight against cybercrime.

2nd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2024)
*Corresponding author.
atulya.singh@kcl.ac.uk (A. Singh), tasmina.islam@kcl.ac.uk (T. Islam)
0009-0004-8552-8716 (A. Singh), 0000-0002-6437-8251 (T. Islam)

The remainder of the paper contains Section 2 which gives a brief literature on cybercrimes and types of bots used to prevent it. Section 3 details the design and methodology, outlining initial design requirements and user test plans. Section 4 consists of the implementation and section 5 gives a summary of the results and an evaluation. Finally, section 6 will summarise and conclude the paper.

## 2. Related Work

This section provides a brief review of existing literature about cybercrime, their impact and different types of bots used in cybercrime protection.

### 2.1. Cybercrime

From financial gain to ideological goals that jeopardise both national security and big data, cybercrime is presented in the literature as a multidimensional danger. The vulnerability of these domains to cyber threats calls for strengthened security protocols and collaboration among sectors for threat intelligence and coordinated responses [5]. Cybercrime has a wide range of negative effects, including harm to society's trust and privacy in addition to the economics. To protect people and communities from these widespread dangers, there must be more awareness raised and educational initiatives undertaken due to the financial and social costs, which include privacy violations and deterioration of trust [6]. Beyond just monetary losses, the economic analysis of cybercrime considers larger effects including damaged user confidence and tarnished company reputation. The literature emphasises the necessity of a comprehensive cybersecurity strategy and points out the importance of workforce education, cooperative intelligence sharing, and preventive measures in reducing the financial burden of these crimes [7]. Lastly, studies classify the different forms of cybercrime and show how they affect a wide range of industries, including governments, corporations, and private citizens. This emphasises education and awareness as key elements in this battle and urges for heightened vigilance and coordinated efforts to safeguard against the varied and far-reaching impacts of cyber threats [8]. The body of research indicates that to defend against a constantly changing digital threat landscape, cybersecurity technologies and techniques urgently need to be advanced.

### 2.2. Types of Bots used to prevent Cybercrime

A review article of Bot Protection [9] discusses CAPTCHA mechanisms and their role in web security, outlining various types and operational functions. It critically addresses CAPTCHA's limitations, like accessibility issues for users with disabilities and the potential for circumvention by sophisticated bots. The paper suggests that while CAPTCHA systems have their drawbacks, alternative methods and advancements, including machine learning and behavioural analysis, could enhance bot protection. However, the article could be strengthened with more concrete data or examples to substantiate these claims and a deeper comparison of emerging technologies to traditional CAPTCHA.

A survey of Botnet [10] provides an extensive examination of botnet detection methods, classifying them as signature-based, anomaly-based, DNS-based, and mining-based. It underscores the importance of understanding botnet behaviours and the proactive role of honeynets in cybersecurity, which extends beyond mere educational purposes. The paper

emphasises the promise of data mining techniques for future botnet detection but suggests a multi-faceted approach that incorporates various methods may offer greater resilience against evolving cyber threats. A more critical look at issues such as false positives in DNS-based detection could further enrich the analysis.

Studies reported in [11,12] underscore the importance of educational and preventative approaches in protecting victims from cybercrime. However, it can be observed from the literature review that current methods, while technically sophisticated, often neglect the user's understanding and active participation in their cyber defense and not much attention has been paid to integrating user education within cybersecurity tools. In other words, this gap highlights the need for tools that not only protect but also educate users, enhancing their digital literacy and engagement in cybersecurity practices. The following sections explore the proposed Friendly Bot Chrome extension to address this gap.

## 3. Design and Methodology

This section describes the design and methodology of the proposed friendly bot. An iterative approach was adopted recognizing the importance of including feedback from users in the development process. This process made it possible to continuously collect user feedback and improve the extension in response, ensuring it successfully satisfied their changing needs and preferences. Figure 1 shows the flow diagram of design of the chrome extension.

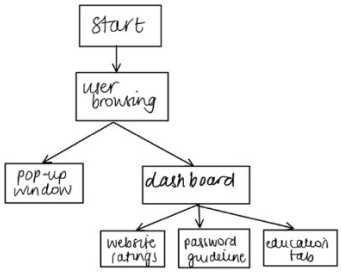


**Figure 1**: Flow diagram of the design

### 3.1. Requirements, Specification and Initial Design

The following elements are essential for the bot to effectively assist its user. A comprehensive literature review was conducted to understand the current landscape of cybersecurity challenges faced by digitally vulnerable individuals as discussed in section 2. This review helped to identify common cyber threats and the best practices recommended by experts in the field.

- **Real-time Protection**: Prompt detection of online threats, providing immediate alerts and recommendations to users for preemptive action.
- **Webpage Scanning**: Integral function to scrutinise web pages for any signs of malware, phishing activities, suspicious links, and other security risks, enhancing user safety.
- **Risk Evaluation**: Mechanism to assess the risk level associated with various online activities, aiding users in making informed decisions.

- **User Education**: Provision of educational content and best practices to improve digital security awareness and habits.
- **Performance Efficiency**: Optimisation for speed and responsiveness, ensuring smooth operation without hindering the user's browsing experience. The bot should work with the most recent browsers and utilize modern web development technologies like HTML, CSS, and JavaScript. A simple and intuitive user interface design, with brief instructions, visual aids, and a focus on usability, helps users comprehend the features and capabilities of the bot.
- **Password Strength Guidance**: Practical advice on creating robust, secure passwords by emphasizing the importance of password complexity, diversity of characters, and the risks associated with reusing passwords across multiple platforms. The Cyber Bot Helper extension doesn't directly access any user data to function. Rather, it concentrates on examining features of websites, such as password fields, to give people pertinent cybersecurity advice. The bot protects users' privacy and promotes online security by educating them only about password security procedures and providing help in creating strong passwords
- **Robust Security Measure**s: Prioritisation of robust security measures, including data encryption, user authentication and authorisation systems, safe development techniques, and frequent security assessments, to limit potential dangers. For threat analysis and detection, the bot should access third-party services and APIs while ensuring user privacy and security.
- **Continuous updates**: Implementation of a system for updating the bot's capabilities and features as new threats or technological advancements occur.

### 3.2. Database and Survey

As mentioned in 3.1, it is vital for the bot (extension) to detect malicious URLs and to facilitate this a Kaggle dataset [13] is employed that contains a comprehensive list of URLs. This enables the bot to compare visited URLs with known threats promptly alerting users to potential risks and enhancing their online protection.

A survey was designed as part of this study to investigate users' online behaviour, their understanding of cyber threats, and their interaction with the CyberBot. The survey was based on a standardised questionnaire designed specifically for this study. It included a combination of closed-ended and open-ended questions to capture both quantitative and qualitative feedback from participants. Relevant ethical clearance has been obtained for the survey from the institution before employment. The survey sought insights on various aspects including internet usage, cyber threat encounters, and the effectiveness of the bot. To extract both quantitative and qualitative feedback, the survey employed multiple choice and open-ended questions, via Qualtrics, questions ranging from the utility of the bot to personal cyber security learning, as well as demographic data and self-assessed tech proficiency.

### 3.3. User Test Plan

In the user test plan for the bot (chrome extension), the objective was to rigorously evaluate the core features such as real-time threat detection, webpage scanning, and risk assessment, while paying special attention to user education and performance. Emphasizing inclusivity, the tests

aimed to ensure the extension's ease of use for all, particularly targeting those less familiar with technology. Identifying any potential weaknesses was key to refining the extension and bolstering its role in cybersecurity.

Testing was conducted in a controlled environment using a single laptop with the latest stable releases of both Google Chrome and Windows. This controlled set up isolated variables, ensuring that any issues observed could be attributed to the extension's performance and not to external system variables. This also allowed a focused assessment of the extension's functionalities and user experience.

For each participant, individual user testing sessions will assess interactions with the Chrome extension using specific tasks reflective of real-world use. These tasks will evaluate key features such as understanding educational materials, responding to real-time alerts, and following secure password creation guidelines. Participants will verbalise their thought process using the 'think aloud' technique, offering insights into their engagement with the bot and decision-making. After completing these tasks, the survey mentioned in 3.2 will gather participants' feedback on their experience. Observations and feedback will inform any necessary refinements to enhance the bot's usability, particularly for digitally vulnerable users.

# 4. Implementation and Testing

Node.js, utilising Chrome's V8 engine for its efficiency and event-driven architecture, has been chosen as the development platform [14]. The Node Package Manager (NPM) played an important role in managing dependencies and installing necessary packages [15]. The development entailed scripting the extension's functions for user interaction, data retrieval, and processing. The dataset [13] mentioned in 3.1 was integrated to enable the bot to identify and alert users about cyber threats by comparing browsing data with known risks., The bot (chrome browser extension) was refined based on feedback and iterative testing transforming it into a reliable tool for preventing cybercrime.

## 4.1. Technical Implementation and User Interface Design

While popular browsers such as Chrome already provide password-generating tools and alerts for untrusted TLS certificates, the Cyber Bot Helper extension puts more emphasis on user education than technical functionality. The extension tries to inform users of the importance of these features and how to properly read and handle browser warnings, rather than just concentrating on technical details. By giving users more context and advice, the bot enhances the functionality that browsers already offer and empowers people to make decisions about their online security.

The technical implementation of the Chrome extension (CyberBot) is anchored by a JSON-formatted manifest file, outlining its components and facilitating their interaction. Essential details like the manifest version are specified to guide browsers in processing the extension [16]. The browser toolbar features an action button that allows user interaction through an icon and presents content via a popup, crafted with HTML, CSS, and JavaScript. Background scripts serve vigilantly to cross-reference URLs against a database, alerting users to threats through notifications.

Content scripts scrutinise web content with an emphasis on security, particularly detecting password fields to promote better password hygiene. The extension's robust backend, powered

by Node.js and Express [15], maintains module availability through node packet manager(npm). The backend server communicates through localhost on port 9091, categorizing web hosts using the dataset mentioned in section 3.1. When querying a host's status, the extension communicates to the backend with a dynamic hostname, receiving back an assessment of the host's safety.

Designing the UI for the Chrome extension was critical, aiming to offer users a straightforward, accessible interface. The design emphasised simplicity to ensure usability across all skill levels. The UI incorporated a notification system to alert users of potential threats and provide advice, balancing visibility with unobtrusiveness to maintain the browsing experience. A focus was on initial TLS verification and URL safety checks, which are essential for online security. The TLS protocol protects data transfer, and the extension checks for a site's valid TLS certificate to prevent security risks. It also compares the visited URL against a database of known malicious sites.

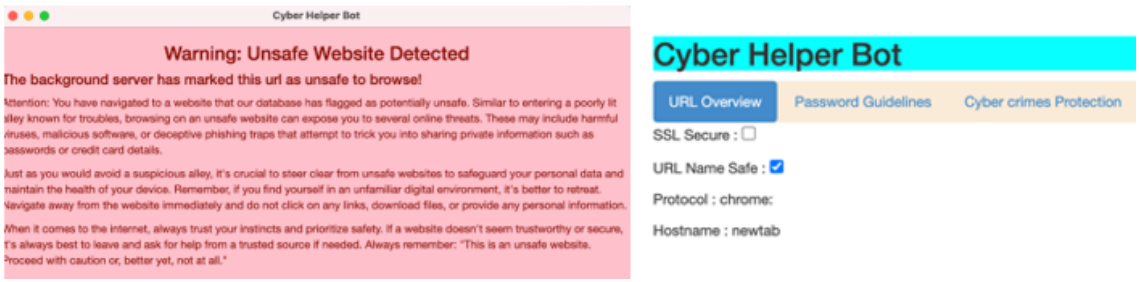


**Figure 2**: Warning sign that is displayed when clicking on a malicious website.

Originally, the design required user engagement with TLS concepts, but recognising the complexity for those without a security background, the design evolved. In the final implementation, TLS and URL checks run automatically in the background, with the extension alerting users through clear, simple messages about any security concerns (as shown in Figure 2), ensuring protection while simplifying the user experience.

## 4.2. Functionality and Features

The purpose of the Chrome extension is to improve web security and encourage safer browsing, especially for those who might feel vulnerable online. Automating background processes like

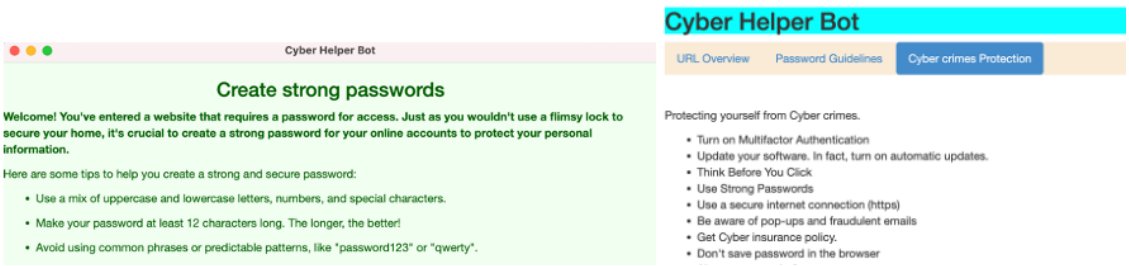


**Figure 3**: Password guide displayed during login or new password creation on a password-protected website on the left and the right is the educational tab.

URL safety analysis and TLS certification verification frees users from the need for tedious security checks or in-depth knowledge of the intricacies of web security.
Users are provided with easy-to-understand warning messages about possible online hazards that are brief and straightforward, regardless of their level of technological expertise. Together with important security advice for creating strong passwords, these alerts help users be safer online without interfering with their online activities highlighting the importance of proactive measures, the extension introduces users to Cyber Insurance, offering insights into its benefits and providing direct links to relevant resources as shown in Figure 3. This feature aims to empower users with the knowledge and means to secure their digital presence proactively [17].

### 4.3. Performance Testing

Performance testing aimed to assess the effectiveness, speed, and accuracy of the "Cyber Bot Helper," especially its capability to provide real-time alerts and insights on potential cyber threats.
**Test Case 1: Detection of Malicious Websites:** The first test case verified the bot's ability to recognise and notify users about dangerous URLs from the Kaggle dataset. Preconditions included the bot being active and the testing carried out on the Kaggle malicious URL dataset. Upon navigating to a listed harmful URL, the expected outcome was that the bot should generate immediate alerts. The bot successfully displayed the warning pop-up for each dangerous URL accessed, marking the test as a pass.
**Test Case 2: Password Policy Display**: The second test case evaluated the bot's ability to present password guidance when a user visited a webpage related to password input or creation. Preconditions ensured the bot was operational. The test was conducted by opening a webpage where the user is prompted to create or input a password. The bot was expected to provide password recommendations or guidelines for creating a strong password. The actual result confirmed the bot's functionality, as it presented the password guideline prompt upon accessing the password section on a website, resulting in a pass status for the test.

### 4.4. User Engagement and Data Insights

This section describes the all-encompassing strategy used to guarantee that the Chrome extension is a flexible and inclusive tool. Strict ethical guidelines established by the university were followed when recruiting a broad group of participants for testing, with an emphasis on individuals who were more vulnerable to online risks since they had less digital expertise. To confirm the extension's usability and effectiveness for all user types, it was evaluated in a variety of scenarios.

Data was meticulously gathered through Qualtrics, an intuitive platform chosen for its strong analytical capabilities, ensuring feedback was reflective of the diverse user base while adhering to privacy standards. Each participant interacted with the extension on a dedicated laptop, providing a controlled environment that isolated variables for accurate usability assessment.

The Chrome extension, which is based on Node.js, was iteratively improved to satisfy the dual goals of improving online security and user education using this focused and ethical technique. The process underscored the paper’s alignment with creating a safer digital space, demonstrating a harmonious fusion of technological advancements, ethical research practices, and user-centred design.

## 5. Results, Analysis and Evaluations

This section analyses the findings from the survey and user testing and evaluates the implemented CyberBot chrome extension indicating some future improvement. The age range of the 29 participants who completed the survey was 18 to 65. The wide range of participants in the study guaranteed that the insights obtained were inclusive of a wide range of users.

### 5.1. Survey Results

The choice was taken to use user testing and survey methods to evaluate the efficiency and usability of the created Chrome extension. A reliable method for learning how the actual user

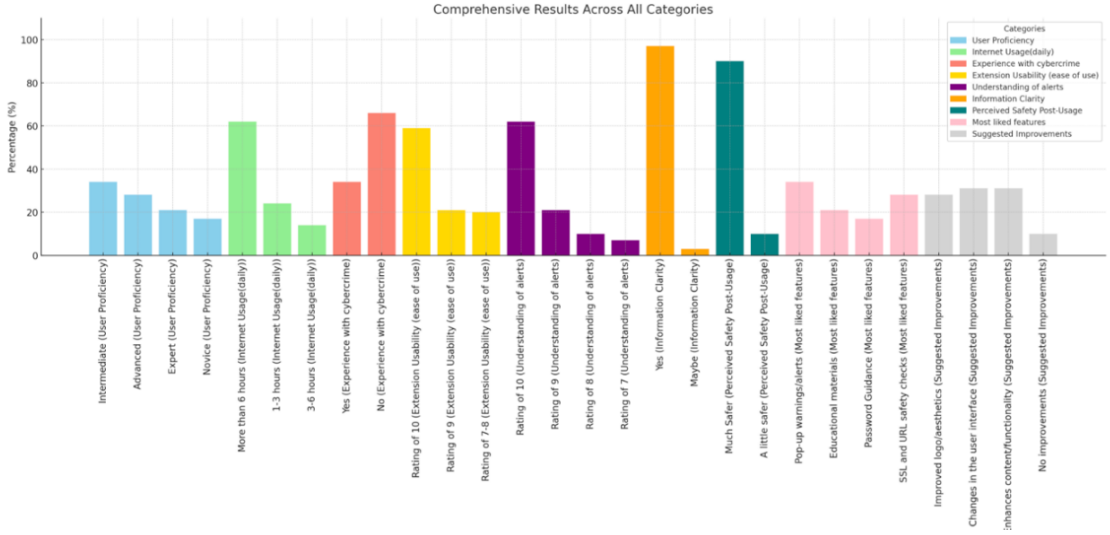


**Figure 4**: Survey results.

interacts with and sees a system is user testing which allows quantifiable measurements and first-hand accounts of how well the bot extension worked. The survey method, on the other hand, was created to assess the users' perceptions and knowledge about cyber security before and after using the bot extension. This enabled a methodical way to get thorough responses from a larger audience than was possible with just user testing. Initially, a random sample of participants was involved, from which those who were digitally vulnerable were later identified based on their responses to the survey. These responses allowed for an assessment of their digital competence and susceptibility to online threats. The survey was instrumental in soliciting additional feedback, while user testing focused on the Chrome extension's functionality and usability. The utility and usability of the extension were evaluated using both qualitative and quantitative data gathered from these methods, providing a clearer picture of the extension's potential to enhance the safety of digitally vulnerable individuals online.

Figure 4 presents the survey results, serving as the foundation for further analysis and discussion to explore the implications of these findings and the overall impact of the bot extension on online safety and awareness. Demographic data reveal that gender and tech proficiency levels are key factors in digital vulnerability. The survey indicates that women, representing 55.2% of the respondents, may have a greater engagement with online security issues compared to men, who make up 41.4% of the 29 respondents. It also became apparent

that while advanced users might be less prone to common cyber threats, overconfidence in their digital skills can still leave them exposed.

User proficiency ranged from novice to expert, indicating a need for the Chrome extension to accommodate this diversity. Real-world feedback underscored the prevalence of cyber threats, with a significant portion of respondents having been directly affected. The extension received high marks for ease of use and clarity of warnings, leading to an increase in perceived safety among users.

The bot's educational role was a standout feature, bridging the knowledge gap even for self-identified "advanced" users and reinforcing the importance of continuous learning in cybersecurity. User feedback suggests a preference for integrated, non-intrusive alerts and an appreciation for educational content that empowers rather than merely protects.

Overall, positive feedback from users affirmed the bot extension's utility and highlighted areas for future enhancement. The aim is to enhance the extension, emphasising its educational role while maintaining security, for a seamless integration with browsing.

### 5.2. Evaluation

The CyberBot Chrome extension has notably succeeded in its fundamental goal, with users reporting a heightened sense of security during their online activities. This aligns with the primary aim of the study to bolster online safety. However, the extension's role extended beyond protection; it became a pivotal educational resource. Users were not only shielded from threats but also became more knowledgeable about digital security principles. they were able to identify safe URLs and understand the need for TLS certifications, reflecting the extension's success in enhancing digital literacy.

The extension plays a significant teaching role by providing users with long-lasting cybersecurity skills in addition to temporarily improving web safety. Feedback indicates that while the tool's protective features were effective, its capacity to inform and educate users on cybersecurity is equally valuable. It emphasises how useful the application is as an educator because it allows for on-the-go learning and provides real-time alerts and help. This ability to blend progressive learning with instant safety highlights the tool's critical role in developing a user base that is not just secure but also skilled at autonomously identifying and thwarting cyber threats.

Feedback also revealed areas for improvement, especially concerning more fluid user interactions and design improvements. Users expressed a preference for an appealing interface and less intrusive notifications, and they suggested that including these features could improve user engagement and experience even more. This emphasises the extension's dual role in the digital sphere as a defender and an educator.

## 6. Conclusion

Navigating around the digital world can be difficult, especially when it comes to protecting vulnerable users from online attacks. Addressing this critical issue, this paper describes the development of a Chrome extension-CyberBot tailored for such individuals, integrating both technical innovation and empathetic design. The extension has shown to be successful in raising users' awareness of security and educating them with the information and resources needed to

identify and mitigate online threats. It performs the dual role of being both a line of defence and an educational tool, providing knowledge about the details of online risks, such as the complexity of URLs and the importance of TLS certification.

With an emphasis on user-centricity, the study used an iterative methodology that allowed the tool to adapt to user feedback and testing. This helped not only in identifying areas for improvement but also gained general approval of the CyberBot. This bot is integrated into the users' everyday digital routine. This ensures real-time delivery of essential cybersecurity notifications and educates users about cyber risks and mitigation processes in real-time without having to learn these at a different time or setting, enabling users to navigate the digital landscape securely and with confidence. Integrating the Large Language Model and the dynamic dataset may be a potential extension of the bot to provide a dynamic defense against the constantly changing landscape of cyber threats and improve user education.

## References


[1] The latest Cyber Crime Statistics (updated August 2023): AAG it support (2023) AAG IT Services. Available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (Accessed: 14 May 2023).

[2] Dashora, K., 2011. Cybercrime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1), pp.240-259.

[3] Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M., 2022. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University-Computer and Information Sciences.

[4] Cyber resilience: Change behaviour, prevent cyber incidents. (No date) Phished.io. Available at: https://phished.io/product-overview (Accessed: 20 January 2024).

[5] Brewster, B., Kemp, B., Galehbakhtiari, S. and Akhgar, B., 2015. Cybercrime: attack motivations and implications for big data and national security. In Application of big data for national security (pp. 108-127). Butterworth-Heinemann.

[6] Saini, H., Rao, Y.S. and Panda, T.C., 2012. Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), pp.202-209.

[7] Gañán, C.H., Ciere, M. and van Eeten, M., 2017, October. Beyond the pretty penny: The economic impact of cybercrime. In Proceedings of the 2017 new security paradigms workshop (pp. 35-45).

[8] Yadav, H. et al. (2021) Various types of cybercrime and its affected area, SpringerLink. Available at: https://link.springer.com/chapter/10.1007/978-981-15-9774-9_30 (Accessed: 05 June 2023).

[9] Saini, B.S. and Bala, A., 2013. A review of bot protection using CAPTCHA for web security. IOSR Journal of Computer Engineering, 8(6), pp.36-42.

[10] M. Feily, A. Shahrestani and S. Ramadass, "A Survey of Botnet and Botnet Detection," 2009 Third International Conference on Emerging Security Information, Systems and Technologies, Athens, Greece, 2009, pp. 268-273, doi: 10.1109/SECURWARE.2009.48.

[11] Maqsood, S. and Chiasson, S., 2021. Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens. ACM Transactions on Privacy and Security (TOPS), 24(4), pp.1-37.

[12] Das, S. and Nayak, T., 2013. Impact of cybercrime: Issues and challenges. International Journal of engineering sciences & Emerging Technologies, 6(2), pp.142-153.
[13] Siddhartha, M. (2021) Malicious urls dataset, Kaggle. Available at: https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset?resource=download (Accessed: 13 August 2023).
[14] Getting started with the concepts | chrome extension 101 | video 01 | tutoriex (2022) YouTube. Available at: https://www.youtube.com/watch?v=ARDlbhF9f4A&list=PLlntQfRHhjjB4pxzH6qR2lly1ZgaZAjkG (Accessed: 15 May 2023).
[15] Chrome extension tutorial - 1 - introduction (2016) YouTube. Available at: https://www.youtube.com/watch?v=8q1_NkDbfzE&list=PLC3y8-rFHvwg2-q6Kvw3Tl_4xhxtIaNlY&index=3(Accessed: 15 June 2023).
[16] itsdaniel0itsdaniel01 and sergserg110k7777 gold badges317317 silver badges330330 bronze badges (1957) Chrome extension: Open new popup window, Stack Overflow. Available at: https://stackoverflow.com/questions/5186296/chrome-extension-open-new-popup-window (Accessed: 15 June 2023).
[17] 9 ways to protect yourself from cybercrime (no date) Policybazaar.Available at: https://www.policybazaar.com/corporate-insurance/articles/ways-to-protect-yourself-from-cyber-crime/ (Accessed: 1 August 2023).