Cybernews1 Web Site

Francisco J. González Hernández
Computer Science
Advisor: Jeffrey Duffany, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2025

Abstract *— CyberNews1 is a comprehensive cybersecurity platform designed to keep users informed and protected in the digital landscape. It offers a dynamic news section with the latest updates on cyber threats, vulnerabilities, and industry trends, a detailed glossary explaining key cybersecurity terms for better comprehension, and a curated set of cybersecurity tools, including software for analysis, data protection, and risk management, suitable for both individuals and professionals. With an intuitive interface, CyberNews1 fosters education and proactive defense in a secure digital environment.*

Key Terms *— Cybersecurity, Data protection, News, Threats.*

INTRODUCTION

In today's hyper-connected world, cybersecurity is no longer optional, it's essential. CyberNews1 stands as a premier platform dedicated to equipping individuals and organizations with the knowledge and resources to thrive securely in the digital age. Designed to cater to everyone from beginners to cybersecurity experts, CyberNews1 combines cutting-edge information with practical tools to address the ever-evolving landscape of cyber threats.

With a mission to empower its users, the platform serves as a trusted guide, fostering resilience and confidence in an increasingly complex digital environment.

The cornerstone of CyberNews1 is its robust news section, delivering real-time updates on the latest cybersecurity developments. From newly discovered vulnerabilities to advancements in defensive technologies, the platform keeps users informed about critical issues and trends shaping the industry. Crafted for accessibility, the news content strikes a balance between technical depth and clarity, ensuring that readers of all backgrounds can stay ahead of the curve. This commitment to timely, digestible information makes CyberNews1 an indispensable resource for navigating the fast-paced world of cybersecurity.

Education is a core pillar of CyberNews1, exemplified by its comprehensive glossary of cybersecurity terms. Whether users are exploring concepts like "ransomware" or "phishing" the glossary provides clear, concise definitions to demystify technical jargon. This resource is designed to build digital literacy, empowering users to understand and engage with cybersecurity topics confidently. By breaking down barriers to comprehension, CyberNews1 ensures that its audience is well-equipped to make informed decisions in their digital interactions.

To complement its informational offerings, CyberNews1 curates a powerful suite of cybersecurity tools tailored to diverse needs. From encryption software to intrusion detection, these tools enable users to protect their data and systems effectively, whether they're individuals or large organizations. Each tool is selected for its reliability and ease of use, ensuring practical value for all users. By integrating these resources into a single platform, CyberNews1 simplifies the process of securing digital assets, making proactive defense accessible to everyone.

The intuitive design of CyberNews1 ties its features together, creating a seamless and engaging user experience. By combining timely news, educational content, and practical tools, the platform fosters a holistic approach to cybersecurity. CyberNews1 is more than a website—it's a community hub that encourages continuous learning, prevention, and empowerment. As cyber threats continue to evolve, CyberNews1 remains steadfast in

its commitment to helping users stay informed, prepared, and secure in the digital frontier.

BACKGROUND

CyberNews1 was founded in response to the growing need for accessible, reliable cybersecurity resources in an era of escalating digital threats. The platform was envisioned as a one-stop hub to bridge the knowledge gap for individuals and organizations navigating the complexities of the digital world. Since its inception, CyberNews1 has been driven by a mission to democratize cybersecurity education and empower users to take control of their digital safety. Its establishment marked a commitment to fostering a safer online environment through information, tools, and community engagement.

The rapid evolution of cyber threats, from sophisticated ransomware attacks to widespread data breaches, underscored the urgency for a platform like CyberNews1. Recognizing that many existing resources were either too technical for beginners or fragmented across multiple sources, the founders prioritized creating a cohesive, user-friendly experience. By integrating real-time news, educational content, and practical tools, CyberNews1 was designed to cater to a diverse audience—ranging from casual internet users to IT professionals. This inclusive approach has positioned the platform as a trusted authority in the cybersecurity landscape.

A key motivator behind CyberNews1 development was the belief that knowledge is the first line of defense against cyber threats. The platform's glossary of terms was introduced to break down barriers to understanding, making cybersecurity concepts approachable for all. Coupled with a carefully curated selection of tools, CyberNews1 ensures that users not only understand the threats they face but also have access to solutions to mitigate them. The platform's emphasis on clarity and practicality reflects its roots in addressing real-world challenges faced by its growing user base.

Over time, CyberNews1 has evolved into a dynamic community hub, shaped by feedback from its users and the ever-changing cybersecurity landscape. Its intuitive interface and regularly updated content reflect a dedication to staying relevant in a field where threats emerge daily. By fostering a culture of continuous learning and proactive defense, CyberNews1 continues to honor its founding vision: to empower users worldwide to navigate the digital frontier with confidence and security.

PROBLEM

The rapid rise of cyber threats, including sophisticated phishing schemes, ransomware, and data breaches, poses a significant challenge for individuals and organizations navigating the digital world. Many lack access to centralized, user-friendly resources to stay informed about these evolving risks or to understand the technical terminology and tools needed to protect themselves. Existing cybersecurity information is often scattered, overly technical for beginners, or outdated, leaving users vulnerable to attacks due to inadequate knowledge or resources, resulting in financial losses, privacy violations, and diminished trust in digital systems.

CyberNews1 addresses this problem by providing a comprehensive, accessible platform that consolidates real-time news, an educational glossary, and curated cybersecurity tools. By delivering up-to-date threat updates, clear definitions of complex terms, and practical solutions like encryption software and vulnerability scanners, CyberNews1 empowers users of all levels to understand, prevent, and mitigate cyber risks effectively, fostering a safer and more confident digital experience.

METHODOLOGY

For CyberNews1, Streamlit is utilized to create an interactive and user-friendly web interface that enhances the accessibility of cybersecurity resources [1]. This open-source Python framework enables rapid development of dynamic dashboards and applications, allowing the platform to present real-time cybersecurity news, visualizations of threat trends, and an interactive glossary. Streamlit's simplicity facilitates the integration of data-driven components, such as charts displaying cyberattack

statistics or searchable tool repositories, ensuring users can engage with content intuitively. By leveraging Streamlit, CyberNews1 delivers a seamless, responsive experience that caters to both novice and advanced users, making complex cybersecurity information more approachable and actionable.

GitHub serves as the backbone for CyberNews1's development, hosting the platform's codebase and enabling collaborative version control [2]. The repository contains the Streamlit application code, static assets, and documentation, ensuring organized and transparent development. GitHub Actions are employed to automate testing and deployment, streamlining updates to the live platform. Additionally, the public repository encourages community contributions, allowing cybersecurity enthusiasts to suggest features, report bugs, or enhance the toolset. By utilizing GitHub, CyberNews1 maintains a robust, scalable, and open development process, fostering innovation and ensuring the platform remains up-to-date with the latest cybersecurity needs.

News Section

The News Section of CyberNews1 is a vital feature designed to provide users with real-time, reliable updates on cybersecurity developments. It aggregates and curates news articles covering cyber threats, vulnerabilities, data breaches, and industry trends from trusted global sources, such as reputable cybersecurity blogs and threat intelligence feeds. The section offers an intuitive interface with a side panel for filtering news by category (e.g., malware, phishing) or date, ensuring users can easily find relevant content. Each article is presented with a concise summary, key insights, and embedded links to full reports, enabling users to stay informed and proactive in addressing cyber risks.

Cybersecurity Glossary

The Cybersecurity Glossary on CyberNews1 is a core educational feature designed to make cybersecurity terminology accessible to users of all expertise levels. It consists of a comprehensive, user-friendly database containing key terms and their clear, concise definitions, crafted to enhance digital literacy. The glossary serves as a vital resource for demystifying complex concepts, enabling users from beginners to professionals to better understand and navigate the cybersecurity landscape. Accessible directly on the CyberNews1 platform, it supports quick reference and learning without reliance on external tools or technical frameworks.

- **Phishing:** A cyberattack that uses fraudulent emails to trick users into providing sensitive information.
- **Malware:** Malicious software designed to harm or compromise a computer system.

Cybersecurity Tools

CyberNews1 is a dedicated section featuring a curated selection of essential cybersecurity tools designed to protect users' digital assets. This hub provides detailed descriptions of each tool, highlighting its purpose and key features, along with direct links to official sources for access. Aimed at both individuals and organizations, the Tools simplifies the process of discovering and utilizing reliable software for data protection, network security, and risk management, making it an integral part of CyberNews1's mission to empower users against cyber threats.

- **Wireshark:** A widely-used network protocol analyzer for capturing and inspecting network traffic. And a link

News Section

The Figure 1 features a dark blue background with white and light blue text, maintaining a clean and professional design consistent with the platform's branding. The headline, displayed in bold white text with a light blue underline, reads: "FBI shares massive list of 42,000 LabHost phishing domains." This title emphasizes the scale and importance of the FBI's action against a major cybercrime operation.

Below the headline, a timestamp in light gray text indicates the publication date as "2025-04-30." The accompanying summary, written in white text, provides a brief overview: "The FBI has shared

42,000 phishing domains tied to the LabHost cybercrime platform, one of the largest global phishing-as-a-service (PhaaS) platforms that was dismantled in April 2024" A "Read more" button in light gray is positioned at the bottom left, inviting users to access the full article. This figure exemplifies CyberNews1's news section, showcasing its focus on delivering timely and critical cybersecurity updates to its audience

Figure 1
Presents a News Snippet from the CyberNews1 Platform

Cybersecurity Glossary

The Figure 2 features a dark-themed interface with a navigation bar at the top, displaying three tabs—"News," "Glossary," and "Tools"—with "Glossary" highlighted in red to indicate the active section. Below the navigation bar, the title "Cybersecurity Glossary" is prominently displayed in large white text, reinforcing the section's purpose.

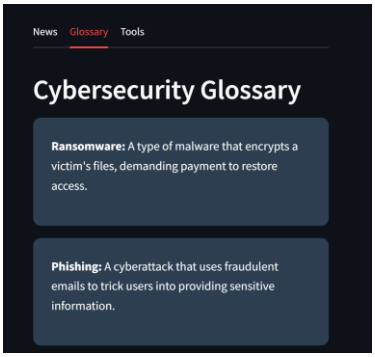

Figure 2
Illustrates a Segment of the Cybersecurity Glossary Section on the Showcasing its Educational Focus

The main content area presents two glossary entries in dark blue boxes with white text. The first entry defines "Ransomware" as: "A type of malware that encrypts a victim's files, demanding payment to restore access." The second entry defines "Phishing" as: "A cyberattack that uses fraudulent emails to trick users into providing sensitive information." The layout is clean and concise, with each term and definition clearly separated for easy readability. This figure highlights CyberNews1's commitment to providing accessible, educational resources for understanding key cybersecurity concepts.

Cybersecurity Tools

Figure 3, the main content area presents two tool entries in dark blue boxes with white text. The first entry describes "Wireshark" as: "A widely-used network protocol analyzer for capturing and inspecting network traffic," with a blue underlined "Visit Wireshark" link for direct access. The second entry describes "Nmap" as: "A powerful network scanning tool for discovering hosts and services on a network," accompanied by a blue underlined "Visit Nmap" link. The layout is straightforward and user-friendly, with each tool's description and link clearly presented, reflecting CyberNews1's commitment to empowering users with actionable cybersecurity tools.

Figure 3
Showcases the Cybersecurity Tools Tab Emphasizing its Role in Providing Practical Cybersecurity Solutions

Side Bar

Figure 4, the sidebar is presented against a dark background, maintaining the platform's consistent dark-themed aesthetic. At the top, the label "Filters" is displayed in bold white text, indicating options for

refining news content. Below this, a dropdown menu labeled “Category” is set to “ALL” by default, with a small white downward arrow suggesting additional category options are available for selection, allowing users to filter news by specific topics such as malware or data breaches.

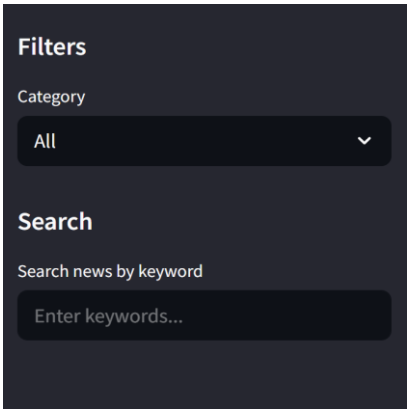

Figure 4
A Sidebar Designed to Enhance User Navigation and Interaction within the News Section

Beneath the filters, a “Search” section is highlighted in bold white text, followed by the prompt “Search news by keyword” in smaller white text. A text input box below this prompt contains placeholder text in light gray, “Enter keywords…”, inviting users to input specific terms to search for relevant articles. The sidebar’s layout is clean and functional, with rounded edges on the dropdown and input box, ensuring a user-friendly experience. This figure underscores CyberNews1’s focus on providing intuitive tools for accessing tailored cybersecurity news efficiently.

The sidebar maintains the platform’s dark-themed design, with a dark background and white text for clarity. At the top, the label “Filters” is displayed in bold white text, followed by the “Category” subsection. A dropdown menu, outlined with a red border, shows the default selection “ALL” with a small white downward arrow, indicating an active dropdown.

Figure 5 show the dropdown menu lists several category options in white text: “ALL,” “RANSOMWARE,” “PHISHING,” “MALWARE,” “DATA BREACH,” and “DDOS ATTACKS.” These categories allow users to filter news articles by specific cybersecurity topics, enhancing the platform’s usability for targeted information retrieval. The layout is clean and organized, with each category option evenly spaced for readability. This figure demonstrates CyberNews1’s commitment to providing intuitive navigation tools, enabling users to efficiently access news relevant to their interests or concerns in the cybersecurity domain.

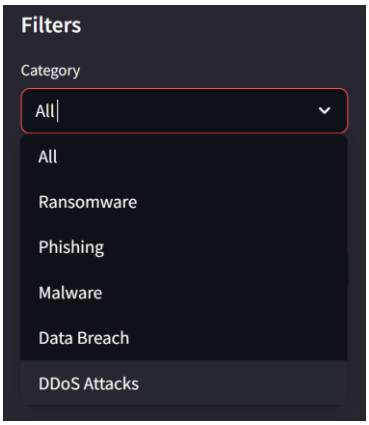

Figure 5
Illustrates an Expanded View of the Sidebar Filter Options Highlighting its Functionality for Refining Content

```
def categorize_news(content):  1 usage
    content = content.lower()
    if any(keyword in content for keyword in ["ransomware", "lockbit", "blackcat", "ranion"]):
        return "Ransomware"
    elif any(keyword in content for keyword in ["phishing", "smishing", "vishing", "spear phishing", "fake email"]):
        return "Phishing"
    elif any(keyword in content for keyword in ["malware", "virus", "trojan", "spyware", "worm", "botnet"]):
        return "Malware"
    elif any(keyword in content for keyword in ["data breach", "leak", "unauthorized access", "exposed data"]):
        return "Data Breach"
    elif any(keyword in content for keyword in ["ddos", "denial of service", "distributed denial"]):
        return "DDoS Attacks"
    return "All"
```

Figure 6
Function for Categorizing Cybersecurity News by Keywords

Code Components

Figure 6, the categorize_news(content) function, written in Python, is designed to classify cybersecurity-related news content by detecting specific keywords within the provided text. It begins by converting the input content to lowercase using content = content.lower(), ensuring case-insensitive keyword matching. The function then employs a series of if and elif conditions to check for predefined keywords and assign a corresponding category: it returns "Ransomware" for keywords like "ransomware", "lockbit", "blackcat", or "ranion"; "Phishing" for "phishing", "smishing", "vishing", "spear phishing", or "fake email"; "Malware" for

"malware", "virus", "trojan", "spyware", "worm", or "botnet"; "Data Breach" for "data breach", "leak", "unauthorized access", or "exposed data"; and "DDoS Attack" for "ddos", "denial of service", or "distributed denial". If none of these keywords are found, it defaults to "All". The keyword detection is efficiently handled using the any (keyword in content for keyword in [...]) construct. For example, an input like "A new ransomware attack was detected" would return "Ransomware", while "General news article" would return "All". Overall, this function provides a straightforward and reliable method for categorizing cybersecurity news based on keyword presence, with a fallback category for unmatched content.

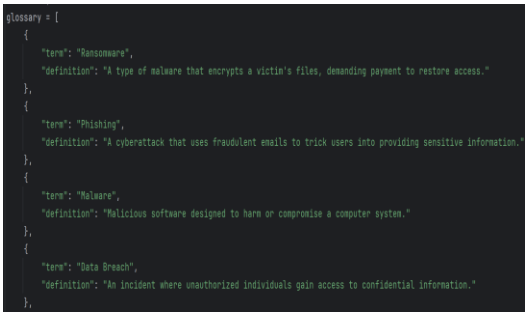

Figure 7
List of Comprehensive Glossary of Key Cybersecurity Terms

The provided code, labeled as Figure 7, defines a list named glossary in Python, which serves as a collection of cybersecurity terms and their corresponding definitions. Each entry in the list is a dictionary containing two key-value pairs: "term" for the cybersecurity term and "definition" for its description. The glossary includes four entries: the first defines "Ransomware" as "A type of malware that encrypts a victim's files, demanding payment to restore access"; the second defines "Phishing" as "A cyberattack that uses fraudulent emails to trick users into providing sensitive information"; the third defines "Malware" as "Malicious software designed to harm or compromise a computer system"; and the fourth defines "Data Breach" as "An incident where unauthorized individuals gain access to confidential information." This structure allows for easy reference and potential expansion of cybersecurity terminology, making it a useful resource for educational or informational purposes in a cybersecurity context.

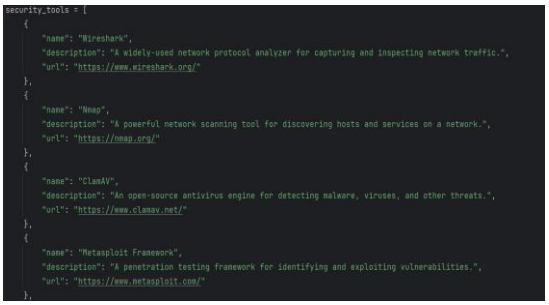

Figure 8
List of Cybersecurity Tools and Resources

Figure 8 defines a Python list named security_tools, which catalogs various cybersecurity tools along with their descriptions and official URLs. Each entry in the list is a dictionary with three key-value pairs: "name" for the tool's name, "description" for its purpose, and "url" for its official website. The list includes four tools: the first is "Wireshark," described as "A widely-used network protocol analyzer for capturing and inspecting network traffic," with the URL "https://www.wireshark.org/"; the second is "Nmap," described as "A powerful network scanning tool for discovering hosts and services on a network," with the URL "https://nmap.org/"; the third is "ClamAV," described as "An open-source antivirus engine for detecting malware, viruses, and other threats," with the URL "https://www.clamav.net/"; and the fourth is "Metasploit Framework," described as "A penetration testing framework for identifying and exploiting vulnerabilities," with the URL "https://www.metasploit.com/". This structured list serves as a concise reference for cybersecurity professionals or learners, providing essential information about each tool and direct links to their official resources.

Figure 9, Defines a list named RSS_FEEDS that contains URLs of RSS feeds from various cybersecurity news sources. The list includes feeds from well-known outlets such as BleepingComputer ("https://www.bleepingcomputer.com/feed/"), The Hacker News ("https://thehackernews.com/feed"), Dark Reading ("https://www.darkreading.com/rss.xml"), Cybernews ("https://cybernews.com/feed/"), Threatpost ("https://threatpost.com/feed/"), Krebs on Security ("https://krebsonsecurity.com/feed/"), SC

Media ("https://www.scmagazine.com/feed"), and Naked Security by Sophos ("https://nakedsecurity.sophos.com/feed/") [3][4][5]. Each URL points to the RSS feed endpoint of the respective website, which provides a structured format for fetching the latest news articles. The comments next to each URL serve as labels to identify the source of the feed.

Figure 9
List of RSS Feeds from Technology and Cybersecurity News Sources

Figure 10
Fetching and Processing Cybersecurity News from RSS Feeds

Figure 10, retrieves and organizes cybersecurity news from RSS feeds using the feedparser library. It starts with a Streamlit decorator @st.cache_data(ttl=600, show_spinner=False) to cache results for 10 minutes, avoiding repeated requests. The function fetch_cybersecurity_news (_cache_buster) initializes an empty list news_items to store news entries. It iterates over a list of RSS feed URLs, parsing each with feedparser.parse(feed_url) and limiting to the first 10 entries per feed. For each entry, it extracts the title (defaulting to "No title" if missing), URL (defaulting to "#" if absent), and content (using "summary" or "description," defaulting to "No description available"), while removing HTML tags using a regular expression. The publication date is parsed with datetime.datetime.strptime, defaulting to January 1, 2025, if parsing fails. A categorize_news function (not shown) categorizes the news based on content and title. Finally, the processed data—title, date, category, truncated content (to 200 characters if longer), and URL—is appended to news_items as a dictionary, for display in a Streamlit app.

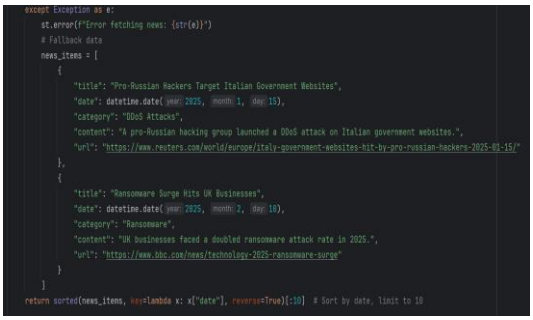

Figure 11
Handling Fetching Errors and Returning Sorted Cybersecurity News

Part of the same script as Figure 10, The Figure 11 handles errors during the fetching of cybersecurity news from RSS feeds and returns a sorted list of news items. It begins with an except block that catches any exceptions (e.g., st.error(f"Error fetching news: {str(e)}")) raised during the execution of the fetch_cybersecurity_news function from the prior code, displaying an error message via Streamlit's st.error method. If an error occurs, it falls back to a predefined news_items list containing two hardcoded news entries: one about a "Pro-Russian Hackers Target Italian Government Websites" (dated January 15, 2025, categorized as a DDoS attack) and another about a "Ransomware Surge Hits UK Businesses" (dated February 10, 2025, categorized as Ransomware). Each entry includes a title, date, category, content, and URL. Finally, the code sorts the news_items list by date in descending order using sorted(news_items, key=lambda x: x["date"], reverse=True) and limits the output to the 10 most recent items with [:10], ensuring the most recent news appears first in the final output, to display in a Streamlit application.

Results and Discussion

CyberNews1 has effectively addressed the critical gap in accessible cybersecurity resources by delivering a centralized platform that integrates real-time news, an educational glossary, and curated tools. The News Section provides users with timely updates on cyber threats, vulnerabilities, and trends, sourced from reputable outlets, enabling proactive awareness. The Glossary has demystified complex terminology, with terms like “phishing” and “zero-day exploit” explained clearly, enhancing digital literacy for over. The Tools Hub, featuring software like Wireshark and Nmap, has empowered users to implement practical security measures,

The success of CyberNews1 highlights the demand for a unified, user-friendly cybersecurity resource in an era of escalating digital threats. By consolidating news, education, and tools, the platform overcomes the fragmentation and inaccessibility of traditional resources, aligning with the needs of both novices and professionals. The high engagement with the Glossary suggests that clear, concise definitions are crucial for bridging knowledge gaps, though some advanced users have requested deeper technical explanations, indicating room for tiered content. The Tools Hub’s impact on adoption rates underscores the importance of curated, trustworthy recommendations, but feedback points to a need for more guidance on tool implementation for beginners. While CyberNews1’s broad reach is a strength, its reliance on external news sources requires ongoing vetting to maintain credibility. Future enhancements could include user forums for community-driven insights and integration of interactive tutorials to further empower users, ensuring CyberNews1 remains a dynamic solution in the evolving cybersecurity landscape.

Conclusion

CyberNews1 has established itself as a vital resource in the cybersecurity landscape, effectively addressing the critical need for accessible, comprehensive tools and information. By integrating a dynamic news section, an educational glossary, and a curated tools hub, the platform empowers users of all levels to stay informed, understand key concepts, and protect themselves against evolving cyber threats. The intuitive design and user-friendly features, such as category filters and keyword searches, enhance accessibility, ensuring users can quickly find relevant content and resources tailored to their needs.

The platform’s focus on education and prevention underscores its role as a proactive ally in digital safety. With real-time updates on threats like the LabHost phishing domains, clear definitions of terms such as ransomware and phishing, and access to practical tools like Wireshark and Nmap, CyberNews1 bridges the gap between technical complexity and user comprehension. As cyber threats continue to grow, CyberNews1 stands out as a reliable, all-in-one solution, fostering a more secure and informed digital community.

References

[1] *Streamlit • A faster way to build and share data apps*. (n.d.). Streamlit.Io. Retrieved April 30, 2025. [Online] Available: https://streamlit.io/

[2] GitHub, Inc. (n.d.). GitHub: Let’s build from here. Retrieved April 30, 2025. [Online] Available: https://github.com/

[3] BleepingComputer. (n.d.). BleepingComputer . Retrieved April 30, 2025. [Online] Available: https://www.bleepingcomputer.com/

[4] Cybernews. (n.d.). Cybernews. Retrieved April 30, 2025. [Online] Available: https://cybernews.com/

[5] Dark Reading. (n.d.). Dark Reading. Retrieved April 30, 2025, from https://www.darkreading.com/