

The Importance of Cybersecurity

Posted on July 15, 2025

In recent decades, the internet has always offered positive impacts on people's lives around the world. Young populations, in particular, from every part of the world use social media as a platform to become known, to express their feelings, to promote discussions, to entertain people, and to encourage a healthy lifestyle. They use it to spread information, provoke meaningful discussions, or authenticate whether a piece of news is true or fake. The use of social media and the internet is not just limited to young people but adults, children, and old age people from all parts of life are addicted to it. However, in this era of advanced technology and communication, there are negative issues and impacts that emerge among internet users related to the use of the internet. People often indulge in gambling, pornography, hacking, online fraud, racial abuse, or other kind of nefarious activities due to misuse of the internet, social media, and related spaces. Such illegal activities usually occur due to a lack of knowledge, lack of awareness, and lack of "self-mechanism" among users to safeguard themselves from falling victim to such fraudulent acts (Heierhoff and Reher). The reason why such cases occur in the digital space is because internet users have a very low or moderate knowledge and awareness of the internet which leads them to cyber risks. In this context, cybersecurity education is very important to help users protect themselves against cybercriminals or unauthorized use of data available electronically. Cybersecurity, therefore, is an activity, state, process, or ability whereby information is protected against unauthorized use or illegal access and exploitation. Building on this context, this paper explores the importance of cybersecurity for individuals from different walks of life in order to educate and empower internet users on the responsible and secure use of digital or virtual platforms to foster a sense of cybersecurity.

Internet and social media platforms have vast benefits and potential for everyone who uses them in a legal way but are also harmful as their misuse can often lead to cyber risks, for instance, personal information exposure. The biggest threat, in this regard, is posed to vulnerable children who do not know how to use the internet and therefore fall victim to fraud and information exposure while doing activities on the internet such as gaming. Sometimes, parents are not aware of these acts as they are unaware of what their children do in cyberspace. This exposes children to bullying, fraud, harassment, and abuse, and they are often sexually exploited in the hands of criminals. Children cannot identify sexual predators on the internet because they use fake identities to prey on children or when seeking victims. Similarly, young people and adolescents often indulge in activities such as pornography, gambling, or gaming that expose them to cybercriminals. Cyber predators collect internet users' information for misuse and later harass and abuse users using their personal information. This makes people whether young children or adults vulnerable to fraud and abuse through technology and the internet while they independently explore the internet without monitoring or any boundaries (Rahman et al.). So, when enjoying the luxury of technology and the benefits of the internet, it is important for every internet user, whether a child or an adult, to be aware of potential risks and how to take safety measures when any such risk occurs to promote safe and responsible online behavior.

Cybersecurity is defined as the state of being protected against unauthorized access to personal information available electronically to avoid social problems and digital crimes (*What Is Cybersecurity?* – Cisco). On the other hand, cyber risk is defined as the “operational risk to information and technology assets” that has detrimental consequences to an individual or organization affecting the “confidentiality, availability, and integrity” of information systems. The increasing exposure to the internet can result in prominent cyber risk events such as identity theft, ransom, fraud, or crime that can greatly change an individual’s life. Oftentimes, people fall victim to online scams and share their Internet banking information which leads to stealing money and compromising an individual financially. To overcome these issues in the digital space, countries have made strict cybersecurity laws for individual and organizational realms to prevent information leaks and other cyber risks. Cybersecurity, therefore, protects individuals, systems, technologies, organizations, and societies from abnormal activities in the digital space. It is the maintenance of availability, integrity, and confidentiality of technological systems and computer resources owned by an individual or organization connected to other networks of individuals or organizations (*What Is Cybersecurity?* – Cisco). Thus, making the internet a safer and reliable space is the ultimate objective of cybersecurity education to protect every aspect of an individual’s life with far-reaching implications for people, organizations, societies, nations, and the global network of communications in order to fight cybercrimes and improve cybersecurity. Moreover, cybersecurity plays a role in maintaining global security in an increasingly interconnected world by preventing attacks and frauds that could have international consequences.

The users’ use of the internet and digital space is rapidly changing in response to “considerable societal, technological, and market innovation” (Rahman et al.) because of people’s frequent engagement with gaming, messaging, online videos, music, and search engines which is broadly positive. However, the issues emerge when a user uses these activities in an illegal manner such as a child may provide his/her information while playing a game on the internet to a person who is an abuser. The objective of cybersecurity is to make individuals aware and empower the users of the internet and technology on the potential dangers they may face while using internet communications technology or platforms such as social media, email, gaming, instant messaging, and more. It encompasses a vast range of processes, measures, practices, systems, and technologies that are specially designed to safeguard and protect the unification and confidentiality of information available online. Cybersecurity measures and practices are essential to protect important data such as “protected health information, personally identifiable information, and governmental systems from theft and damage” (Bada and Nurse). It also ensures personal privacy by empowering internet users to control how their personal data is collected, arranged, processed, and used by governmental and non-governmental organizations while protecting them from criminal and unauthorized access. Cybersecurity is not just about protecting data, it is about ensuring the ongoing integrity and functionality of information and information systems which is fundamental to the trust and reliability that people, organizations, businesses, and governments place in their digital interactions.

The emergence of technology and the internet allows human beings to enjoy two realms of life, the real world and the virtual life through search engines such as Yahoo and Google, video sharing

platforms such as Instagram and YouTube, and online gaming as well as music which has made entertainment and information available to the consumers of technology at the comfort of their homes. However, the growing world of cyberspace and the advancements in technology have also posed serious and negative effects on users of the internet which has raised the significance of cybersecurity education in the digital world. The negative effects can lead to serious cyber risks for both individuals and organizations by implementing strategies that can mitigate the risks of damage, theft, exploitation, and unfair use of financial data preventing financial loss. Cybersecurity is crucial in today's digital and modernized age as it encompasses the technologies and practices particularly designed to protect devices, systems, and data from malware attacks, unauthorized access, or damage to one's personal or intellectual property (Heierhoff and Reher). Organizations that prefer their customers and emphasize a positive workforce environment observe cybersecurity practices to protect individuals within their organizational structure and the organization itself to protect against malware attacks, ransomware, data breaches, identity theft, financial losses, and other potential cyber risks (Dawson and Thomson). It is also crucial for protecting critical infrastructure and national security to protect government infrastructure and secrets. Data breaches in the national or international infrastructure of a country can lead to the unauthorized use of governmental secrets and thus cyber threats go beyond borders. So, cybersecurity strategies must be adopted to counteract such sophisticated and evolving threats and dangers.

In a world where almost 60% of social interactions, businesses, and industries occur online with the aim to deliver safe and reliable products and services, ensuring security and confidentiality while maintaining high standards, cybersecurity has become a significant means of ensuring data protection, privacy concern, and data security as well as data availability while preventing cyber risks. People in today's world need the internet for almost every single task ranging from small enterprises to educational institutions, healthcare settings, transportation systems, communication systems, and energy suppliers. So, they require a system to protect personal data, guarantee confidentiality, secure infrastructures, and uprightness of sensitive information for which cybersecurity is crucial. This can be achieved by individuals, organizations, governments, and nations by adopting cybersecurity practices and measures as cybersecurity provides "intrusion detection" mechanisms and defense mechanisms by merging cutting-edge communication and computing technologies. In order to make the internet and related platforms safer and more reliable ensuring responsible use and access to the internet has become an integral part of the digital landscape with new cybersecurity technologies and systems to effectively investigate and prosecute cyber risks posed to individuals, organizations, and nations due to the internet. Therefore, cybersecurity education and awareness have become crucial in almost every part of an individual's life to maintain social responsibility, financial security, and economic stability so that internet users can have safe, reliable, and responsible access to technology without any fraud, information leak, abuse, harassment, or exploitation (Bada and Nurse).

In conclusion, the paper has offered a comprehensive overview of the importance of cybersecurity in almost every field of life which is the need of the hour because, with the advancement of technology and dependence on the internet, the associated security and cyber risks have also increased. The emergence of the internet has brought about tremendous opportunities and possibilities that have

opened a new gateway for global success, but the world of the internet has also posed new attack vectors and vulnerabilities that compromise the confidentiality and uprightness of connected networks within global communication systems. The Internet has emerged as a critical technology in modern society in this digital age with fundamental implications for cybersecurity in the realm of interconnected devices that collaborate to exchange and monitor information. Indeed, the internet and information communication systems have undergone explosive growth over the recent decades with inventions and advancements in technology, fundamentally transforming individual life, businesses, economies, societies, and the critical infrastructure of the world. The growing scale and significant speed of the transformation of the “global village” to “cyber civilization” has made the internet an indispensable source for almost every critical task ranging from health sectors, human resource management, educational sectors, banking, and smart systems. With the growing influence of technology and the internet on people’s lives, cybersecurity has become a crucial aspect of digital lives that requires continuous attention and adaptation to new threats and dangers. Thus, cybersecurity is crucial for safeguarding the safety of individuals and the security of organizations since every arena of life is highly dependent on the internet and digital technologies.

Works Cited

Bada, Maria, and Jason RC Nurse. “Developing Cybersecurity Education and Awareness Programmes for Small-and Medium-Sized Enterprises (SMEs).” *Information & Computer Security*, vol. 27, no. 3, 2019, pp. 393–410.

Dawson, Jessica, and Robert Thomson. “The Future Cybersecurity Workforce: Going beyond Technical Skills for Successful Cyber Performance.” *Frontiers in Psychology*, vol. 9, 2018, p. 284332.

Heierhoff, Sebastian, and Alina Reher. *Balancing Digital Innovation and Cybersecurity Capabilities through Organizational Ambidexterity-An Investigation in the Automotive Industry*. 2022.

Rahman, Nurul Amirah Abdul, et al. “The Importance of Cybersecurity Education in School.” *International Journal of Information and Education Technology*, vol. 10, no. 5, 2020, pp. 378–82.

What Is Cybersecurity? – Cisco.

<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>. Accessed 7 May 2024.