

BASIC DIGITAL SAFETY



Importance of digital safety

According to Williams, (2022) due to its abundance of information and ability to facilitate communication and cooperation, the internet has grown to be a vital component of modern society. As the amount of personal information exchanged through the online mediums, it's critical to understand the hazards and take safety steps. Regarding this aspect, it's crucial to use strong passwords and be careful when disclosing sensitive information online because hackers have the ability to access personal accounts and steal confidential information which can result in financial losses as well as reputational damage also (Williams, 2022). Furthermore, it's critical to utilise precaution when responding to suspicious emails or requests for personal information because fraudulent hackers can utilise this information to conduct online fraud. People can keep themselves and others safe by being wise and fostering the digital safety approach even with the use of social media profiles and online presence. However, as argued by Ogochukwu and Idi, (2023) In an era of widespread digital surveillance, protecting one's privacy online is crucial. Following the basic rules of digital safety enables users to maintain control when disclosing personal information, reducing the risk of unwanted tracking and monitoring.



Countering Security Threats



Introduction

Welcome to the world of digital safety. In the recent era, staying safe from digital violence is crucial in the connected digital world of today. The entire world has greatly relied on digital technology for communication, shopping, banking, and other purposes. Thus the primary aim of this poster is to foster the understanding that it's critical to recognize the significance of fundamental digital safety procedures to protect the privacy and personal data.

Process of basic digital safety approach

Numerous cyberthreats, ranging from ransomware assaults to viruses and worms, hide on the vast expanse of the internet (Yadav *et al.*, 2022). This implies that there is only one thing left to do: make sure that everyone is doing the least amount of precautions when using the internet. The following five actions are suggested to improve basic digital safety:

When using websites to collect any kind of data, it is important to share personal information only with reliable and authentic sources. One important thing to be aware of is an SSL/security certificate (Sayal *et al.* 2020). This indicates that people should be on the watch for URLs that begin with "HTTPS" as opposed to "HTTP" (the "S" stands for "secure") and display a padlock icon in the address bar.

One of the main areas of vulnerability in cybersecurity is passwords. However, as argued by Sayal *et al.*, (2020) using the same password across several websites increases the risk of data breaches. Thus users need to select a strong password which could not be cracked easily.

However, users need to monitor the safety warning of using software regarding the update notifications which can not only help people to enjoy latest versions but also reduce the digital issues.



https://



Conclusion

From the above study, it has been concluded that the internet is a useful tool with a lot of good applications, but it also has risks that users should be aware of and take precautions to avoid. However, the findings provide an in-depth information about the digital safety procedure which reflects that entire digital security is relied on the usage pattern and safety measurement of the of the users.