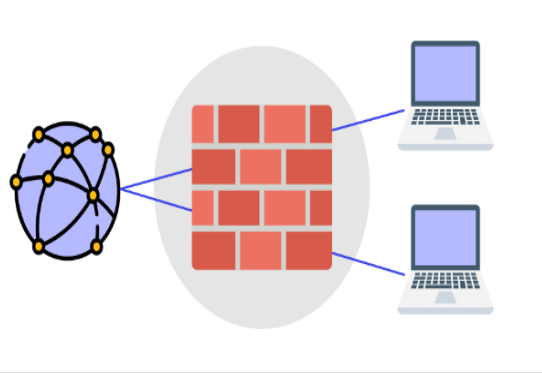


Certificate of Higher Education
Skills for the Work Place
Module- Digital skills
TASK2 (Poster)
Student: Vasilka Stancheva
ID: 2227031

Basic Digital Safety

Introduction

Digitalisation in every aspect of the world is the future and rapidly developing factor with the help of new and more advanced technology. Therefore, the proper definition of Basic Digital Safety will be described along with its importance in the current and future sectors of the organisation. Many types of digital safety will also be highlighted in the information poster section with elaboration.



Types of Basic Digital Safety

Antivirus Software

Systems and devices that are connected to the internet are coming screeching halt due to the data infection caused by viruses that are delivered through malware. Therefore, an effective and useful antivirus program software can detect and clean unwanted and harmful internet viruses and also can help to identify suspicious online site programs.

Updated Firewall

One of the vital tools that is utilised for monitoring web traffic, blocking prohibited access, and detecting authorised users. Updated and effective firewalls also can protect devices from next-generation viruses. Throughout, the previous many years firewalls have been used by cyber experts to maintain internet safety (Melendez, 2019).

Vulnerability Scanner

While utilising the Internet within an organisation, there can be found many less strong spots that can be affected by Internet threats. Identifying flaws and prioritising the identified flaws for countermeasures-related aspects regarding organisations become easier with the help of vulnerability scanners (Watson, 2023).

Conclusion

While discussing digital safety, it was important to be knowledgeable about the proper definition of internet security. Therefore a detailed description of basic digital safety along with its importance and requirements has been delivered in the poster section. Three types of basic digital safety also have been highlighted after discussing the importance of digital safety.

Definition of Basic Digital Safety

Digital safety refers to the process by which an individual’s personal information or important data available on online sites, media and applications are kept secure from internet-related threats. Protecting individuals’ computers, mobile devices, tablets, and any other systems that are connected to the internet and consist of personal information and important data from intruders is known as digital safety. Intruders or internet-related threats can be malware, hacking, phishing, harmful and illegal contents which can also affect online relationships (Kazmeyer, 2023).

Requirement of Basic Digital Safety

While understanding the requirements of digital safety, first one should understand how their information can be utilised illegally and threats can be faced by them.

Fake ID creation can be prevented

Personal information is always valuable for everyone and no one wants their valuable information utilised by the intruder for illegal activities. With the help of individuals' data illegal users and intruders can create fake identities to perform illegal activities safely. Therefore, original data holders can be accused of a crime that they never executed. The importance of digital safety for keeping safe personal information to avoid fake accusations is considered vital.

Keeping personal data safe

Nowadays large number of youths and children are using the internet for online searches and becoming the victims of internet threats. Therefore, many of them get harmed psychologically and psychically. Digital safety is required to resolve these issues regarding internet threats and prevent youths from using risky online activities.

Prevention from online bullying

One of the major internet threats that can be found across the globe is online bullying by intruders. Private information of the youths is collected by the intruders illegally and youths become the victims of online bullying. Digital safety can be beneficial for preventing this online bullying factor.

Prevention from hacking

Hacking is another big problem for recent business and government sectors due to their vital role in the nation’s economy. Hackers can be prevented by advanced theft protection and improved firewalls introduced by internet security engineers.



References

Kazmeyer, M., (2023). Online Safety in the Workplace. [Online] Available at: <https://smallbusiness.chron.com/online-safety-workplace-47356.html> [Accessed 20 August 2023].

Melendez, S., (2019). Types of Computer Fraud & Crime. [Online] Available at: <https://smallbusiness.chron.com/types-computer-fraud-crime-78730.html> [Accessed 20 August 2023].

Watson, C., (2023). Why There Should Be a Network Security Policy in Place in All the Networked Companies. [Online] Available at: <https://smallbusiness.chron.com/there-should-network-security-policy-place-networked-companies-58989.html> [Accessed 20 August 2023].