MOSHI CO-OPERATIVE UNIVERSITY.

FACULTY; FBIS.

PROGRAMME BA-MED I

COURSE NAME; COMPUTER AND COMPUTER APPLICATION

COURSE ANTE; CIT 102

COURSE INSTRUCTOR; Mr. LUCAS MJEMA

STUDENT’S NAME; NOVATUS B. LYAMUYA

REGISTRATION NO; MOCU/BA-MFED/932/19

TASK; INDIVIDUAL ASSIGNMENT.

1: MEANING OF E-COMMERCE.

E-commerce is also known as electronic commerce or internet refers to the buying and selling of goods and services using the internet and the transfer of money and data to execute these transactions. E-commerce is often used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitated through internet.

Whereas E-business refers to all aspects of operating an online business, e-commerce refers specifically to the transaction of goods and services

TYPES OF E-COMMERCE.

There are various types of E-commerce models that can describe almost every transaction that takes place between consumers and business

Business to Consumer ;(B2C) when a business sells goods and services to individual consumer. Example you buy a pair of shoes from an online retailer, this means business sells products or services directly to the consumer over the internet.

Business to Business;(B2B) is a situation whereby one business makes commercial transaction with the other this typically occurs when a business is sourcing materials for their production process for output such as food manufacture purchasing salt, example providing raw materials to the other company that will produce output? A business resells goods and services produced by the others. Example a retailer buying the end product from the food manufacturer.

Consumer to Consumer;(C2C);Is the business model that facilitates commerce between private individuals whether it’s for goods or services , this category of e- commerce connects people to business to one another. When a consumer sells goods or services to the other consumer. Example you sell your old furniture to eBay to another consumer.

Consumer to Business;(C2B) means the business of developing, manufacturing, marketing, distributing and selling any product to or for the purpose of resale , directly or indirectly to any person for domestic use or any person who uses the product in the cause of providing services to domestic customers. Consumer to business occurs when a consumer sells their own products or services to a business or organization, example an influencer offers exposure to online audience in exchange for a fee or a photographer licenses their photo for a business to use.

2: INTERNET SECURITY.

Internet security; is a specific aspect of broader concepts such as cyber security and computer security being focused on the specific threats and vulnerabilities of online access and use of the internet.

Interment security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safe guard users from threats such as hacking into computer systems, email addresses or websites, malicious soft wares that can interfere and inherently damage systems. Is the practice of defending computers ,serves ,mobile devices networks and data from possible attacks, internet security applies in a variety of contexts from business to mobile computing and they can be grouped in the following types and they are like

Network security; is the process of securing computer network from intruders or malwares and viruses.

Application security; is the kind of security that ensures software's and devices are kept save from viruses.

Information security; this aims at protecting the privacy and integrity of data both in storage and transit.

Operational security; includes processes and decisions for handling and protecting data asset. The major aim of internet security is to minimize the dander and the possible threats that are likely to arise, example of these threats are like. Internet crime, internet attacks, internet terrorism, malwares, viruses Trojans, spyware and many others. Internet security requires a combination of several products and technologies to properly safeguard data, also its important to look into several strategies when taking proper measures to help keep network secure. The methods include.

Proper browser selection; some browsers have some of their own security that are very sensitive to hackers and other unauthorized people to invade. Also we advise to use a secure browser to reduce the risk of compromising the computer or network.

Having good email security; email creates a huge risk of getting viruses, worms, Trojans and other harmful viruses. E-mail messages can also be protected by using cryptography like signing email and also encrypting the body of an email message and encrypting the communication between mail servers.

Firewalls; acts as filters that protects devices allowing or denying access to network. By applying a specific set of rules to identify if something is safe or harmful, firewalls can prevent sensitive information from being stolen and keep malevolent code from being embedded onto networks.

Multi-factor authentication (**MFA**) is a method of controlling computer access by requiring several separate pieces of evidence to an authentication mechanism. Example websites and emails accounts can can be made more secure by requiring at least two factors of authentication by the user.

Usage of antivirus software products; that protects devices from attacks by detecting and eliminating viruses.

Password managers; that help store and organize passwords through encryption.

Avoiding using unsecure Wi-Fi networks; in public places unsecure networks cause you falling to man in the middle attacks.

The use of data strong password; it’s through Ensuring your passwords are not easily guessable by anything.

Conclusively; in the computer industry, internet security refers to the techniques for making sure that data stored in a computer cannot be read or used by anyone without any authorization, most measures may involve data encryption and putting of passwords. Data encryption refers to the translation of data into a form that can't be used by/ recognized by any deciphering mechanism and the use of passwords that gives the user the access to particular program or system.

3: INTERNET SECURITY THREATS.

. While the web present users with lots of information's and services, it also includes several risks. Cyber-attacks are only increasing with sophistication and volume with many cyber criminals using a combination of different types of attacks to accomplish a single goal. Through the list of potential threats is extensive, here are some of the most common internet security threats

Man-in- the- middle attacks; a man-in- the- middle attack is the type of cyber threat where a cybercriminal intercepts communications between two individuals in order to steal data , example on an unsecure Wi-Fi network an attacker could intercept data being passed from the victims device and the network.

Malware; it's the short form of malicious software, malware comes from various forms including computer worms, viruses, Trojans and dishonest spyware.

Computer worms; a computer software program that copes its self from one computer to the other it doesn't require human interaction to create these copies and can spread rapidly and in a great volume.

Spams; these are referred to as the unwanted messages in your email inbox. In some cases spam messages can include junk mail that advertise goods or services and you are not interest in them. These are usually considered harmless but some can include links that will install malicious software on your computer if they are added in.

Phishing ; phasing scams are created by cybercriminals attempting to socilitprivate or sensitive information , they can propose as your bank or web service and lure you into clicking links to verify details like account information or passwords .

Denial-of- service attack; a denial of service attack is where cybercriminals prevents a computer system from fulfilling legitimate requests by overwhelming the networks and serves with traffic. This renders the systems unusable preventing an organization from carrying out vital functions

Botnets; a botnet is a network of private computers that have been compromised infected with malicious software's , these computers are controlled by single user and are often prompted to engage activities such as sending spam messages or denial of services (Do's) attacks.

Spyware; is a program that secretly records what users does, so that cybercriminals can make use of this information. Example spyware could capture credit card details.

Ransom ware. It's a type of malware that locks down a user's files data with the threat of erasing it unless a ransom is paid.

Dridex malware; it's a financial Trojan with a range of capabilities. Affecting victims since 2014, it's through phishing emails or existing malware also it's capable of stealing passwords, banking details and personal data that can be used in fraudulent transactions it has caused massive financial losses amounting to hundreds of millions

Generally; the rate of internet security threats are becoming huge problem in the world and thus leading to some deployments in performing activities instead finding more better ways of dealing with the problem, to mention are some ways that can prevent the rapid spreading of these threats and they are such as, through training employers in interment security principles, installing and usage of regular update anti-virus and antispyware software on every computer used in your business, through downloading and installing software's updates for some operating systems and applications if they become available.

REFFERENCES;

1; A Look back on Cyber Security 2012 by Luis cordons – Panda Labs.

2; IEEE Security and Privacy Magazine –IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2013.

3; Swanson, Marianne. Guide for Developing Security Plans for Unclassified Systems, Special Publication 800-18. US Dept. of Commerce. Chapter 6 1997

4; Fraser, B. ed. RFC 2196. Site Security Handbook. Network

Working Group, September 1997. Chapter 4.1.