AMENDMENDS:

CHAP-1

General Purpose Software

General Purpose Software provides the framework for a great number of business,scientific, and personal applications. Spreadsheet, Databases, Computer-Aided Design (CAD) and Word processing software etc. fall into this category.
Some of the examples of General Purpose Software are as follows:

• Word Processor: A word processor is a computer application used for the production including composition, editing, formatting, and possibly printing of any sort of printable material.

• Spreadsheet Program: A spreadsheet is a computer application that generally simulates accounting and financial information on the worksheet. It displays multiple cells that together make up a grid consisting of rows and columns, each cell containing alphanumeric text, numeric values or formulas.

• Database Management System: A Database Management System (DBMS) is a system or software designed to manage a database, and run operations on the data requested by numerous clients.

• Internet Browser: An Internet Browser or a Web Browser is a software application that enables a user to display and interact with text, images, and other information .

• Electronic mail, abbreviated as email, is a method of composing, sending, storing, and receiving messages over electronic communication systems.

The three basic types of software are: Commercial, Shareware and Open Source

- **Commercial software** comes prepackaged and is available from software stores and through the Internet.
- **Shareware** is software developed by individual and small companies that cannot afford to market their software world wide or by a company that wants to release a demonstration version of their commercial product.
- **Open Source software** is created by generous programmers and released into the public domain for public use. There is usually a copyright notice that must remain with the software product.

CHAP-2 The various types of relationships are discussed as as below:

(i) **One-to-one relationship,** as in a single parent record to a single child record or as in a husband record and wife record in a monogamous society.

(ii) **One-to-many relationships**, as in a single parent record to two or more child records – for example, a teacher who teaches three single-section courses.

(iii) **Many-to-one relationships**, as in two or more parent records to a single child record-for example, when three administrators in a small town share one minister.

(iv) **Many-to-many relationships,** as in two or more parent records to two or more child records – for example, when two or more students are enrolled in two or more courses

Entity-Relationship Model or Database:

- An E-R model is a specialized graphic that illustrates **the interrelationships between entities in a database.** It is conceptual representation of data.
- Entity-relationship modeling is a database modeling method used to produce a type of **General Purpose Software**.
- **Entity**: The entity is defined as a object and is described by a set of attributes. An entity may be a physical object such as a house or a car, an event such as a house sale or a car service etc.
- **Relationship**: A relationship is the association among several entities. For examples, a works relationship between an employee and a department and many more.
- The set of all entities or relationships of the same type is called the **entity set or relationship set.**
- The degree of relationship indicates the link between the two entities for a specified occurrence of each. The degree of relationship is also called **"Cardinality**".
- Cardinality specifies how many instances of an entity relate to one instance of another entity.

Object Oriented Database:

- It is based on the concept that the world can be modeled in terms of objects and their interactions.
- Objects are entities possessing certain attributes to characterize them and interacting with each other.
- An Object- Oriented database provides a mechanism to store complex data such as images,
- audio and video, etc

Communication Interface Devices (MODEM)

Types of MODEMs: MODEMs are classified on the basis of different criteria such as the place where they are installed, the manner in which they accept information and the way they transmit signals. Based on these criteria, MODEMs are classified into the following types:

1. External vs. Internal Modems (on the basis of place where they are installed)
External Modem: This is connected to the serial port of the computer by means of a cable. It is connected to the telephone cable and can be switched off or on easily too. The lights on the external modem also inform about the status of transmission of data.

Internal Modem: An internal modem is a device installed inside a desktop or laptop computer, allowing the computer to communicate over a network with other connected computers.

2. Standard vs. Intelligent Modems (on the basis of the manner in which they accept information)

Standard Modems: Most modems used today are called Standard modems which are usually operated by commands entered from a microcomputer keyboard. Users control the functions (dialing, etc.) of a modem through the keyboard.

Intelligent Modems: Intelligent modems are also called Advanced modems. They have inbuilt microprocessor chips and internal Read Only Memory (ROM) contained in the modem. These modems are more expensive.

3. Short-Haul and Wireless Modems (on the basis of the way the signals are transmitted)

Short-Haul Modems: Short-haul modems are devices that transmit signals down the cable through any COM1 port.They are also called line drivers that can send data for a distance of more than one mile. This type of modem can be used within or across several buildings in a company or a university campus.

Wireless Modems: Wireless modems transmit the data signals through the air instead of by using a cable. They sometimes are called a radiofrequency modem. This type of modem is designed to work with cellular technology, and wireless LANs.

Communication Channel (Medium)

(ii) Unguided Media: Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. Some of the common examples of unguided media are Radio wave, Microwave and Infrared wave.

These are described as follows:

- **Radio Waves:** Radio waves are an invisible form of electromagnetic radiation that varies in wavelength from around a millimeter to 100,000 km, making it one of the widest ranges in the electromagnetic spectrum. Radio waves are most Commonly used transmission media in the wireless Local Area Networks.

- **Micro Waves:** Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz. These are used for communication, radar systems, radio astronomy, navigation and spectroscopy.

- **Infrared Waves:** Infrared light is used in industrial, scientific, and medical applications. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected. **Infrared tracking, also known as infrared homing**, refers to a passive missile guidance system to track the target.

Transmission Techniques

Transmission Techniques: A communication network consists of a collection of devices (or nodes) that wish to communicate and interconnect together. The primary objective in any communication network is simply moving information from one source to one or more destination nodes. **Based on the techniques used to transfer data, communication networks can be categorized into Broadcast and Switched networks**. In **Broadcast networks**, data transmitted by one node is received by many, sometimes all, of the other nodes.

In switched-communication networks, however, the data transferred from source to destination is routed through the switch nodes. The way in which the nodes switch data from one link to another as it is transmitted from source to destination node is referred to as a switching technique. Three common switching techniques are Circuit Switching, Packet Switching, and Message Switching.

Message Switching:

- In message switching, end-users communicate by sending each other a message, which contains the entire data being delivered from the source to destination node.
- As a message is routed from its source to its destination, each intermediate switch within the network stores the entire message, providing a very reliable service.
- There is no direct connection between the source and destination nodes. The **intermediary nodes (switches)** have the responsibility of conveying the received message from one node to another in the network.
- Therefore, each intermediary node within the network must store all messages before retransmitting them one at a time as proper resources become available. This **characteristic is often referred to as store-and-forward.**
- Electronic mail (e-mail) and voice mail are also examples of message switching systems.

Three Tier Architecture:

Disadvantages:

- Creates an increased need for network traffic management, server load balancing,

and fault tolerance.
- Current tools are more complex.
- Maintenance tools are currently inadequate for maintaining server libraries.

Features of Data Centres:

Backup Systems: A data center should have the provision of automatically providing backup data services to all shared hosting solutions. Full back up may be taken for full system restoration and off-server and off-site backup services should also be available as well.

Continuous monitoring 24x7: 24x7x365 monitoring must be there in data centers for the security of the data. Such a monitoring will be done for all the hardware including routers, switches, UPS systems and servers.

Environment – Cooling: Cooling infrastructure is a significant part of a data center. The cooling infrastructure creates the optimal computing environment, for servers which is installed.

Data Center Protection challenges and Best Practice Solutions:

Some of the top challenges faced by large enterprise IT managers and the best practices for overcoming them are as follows:

(i) Control skyrocketing data growth:

- Data growth is the biggest data center hardware infrastructure challenge for large enterprises.
- Data deduplication technologies that helps in reducing data storage needs by eliminating redundant data.

(ii) System performance and scalability:

To avoid data center sprawl in the data protection environment, IT managers should look ahead 3-5 years and choose a data protection “target” system that will scale to accommodate the performance and capacity they will need without adding new system.

(iii) Network congestion and connectivity architecture:

- The new generation of servers with multicore processors demands significantly high input/output (I/O).
- Vendors should help its customers to be strategic with their network infrastructure.

(iv) IT administration and staff time at premium:

Minimum requirements for large enterprise data protection platforms include:

- Automatic load balancing and tuning.
- Automatic system monitoring and “phone home” functionality. Choose systems that preemptively identify potential hardware issues and notify administrators before a problem arises.

- Provide dashboards and reporting.

(v) Inadequate Disaster Recovery plans:

- Large enterprises that have been using physical tape backup systems in branch offices are particularly vulnerable to downtime and data loss in the event of a disaster.
- Enterprise IT managers should consider the use of remote-office backup, deduplication, replication and restore operations from a data center headquarters.

(vi) Resource balancing:

- The enterprise chief technical officer today needs to strike a working balance between reduced operational budgets, maximizing availability, ensuring round-the-clock monitoring etc..
- This is why even some of the largest enterprises in the world choose to host their mission-critical
  and sensitive data with established data centers.

Threats and Vulnerabilities:

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. Network
security threats can be categorized into four broad themes:

- **Unstructured threats -** These originate mostly from inexperienced individuals using easily available hacking tools
  from the Internet. Many tools available to anyone on the Internet can be used to discover weaknesses in a company's network.

- **Structured threats -** These originate from individuals who are highly motivated and technically competent and
  usually understand network systems design and the vulnerabilities of those systems. They can understand as well as create hacking scripts to penetrate those network systems. Usually, these hackers are hired by organized crime, industry competitors, or state-sponsored intelligence organizations.

- **External threats -** These originate from individuals or organizations working outside an organization, which does not have authorized access to organization's computer systems or network. They usually work their way into a network from the Internet.

- **Internal threats -** Typically, these threats originate from individuals who have authorized access to the network.
  These users either have an account on a server or physical access to the network. An internal threat may come from a discontented former or current employee or contractor.

Vulnerabilities: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or
system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

- **Software Bugs -** Software bugs are so common that users have developed techniques to work around the
  consequences, and bugs that make saving work necessary every half an hour or crash the computer every so
  often are considered to be a normal part of computing. For example - buffer overflow, access validation error, input validation errors are some of the common software flaws.

- **Timing Windows -** This problem may occur when a temporary file is exploited by an intruder to gain access to the file, overwrite important data.

- **Insecure default configurations -** Insecure default configurations occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems. Unfortunately, most intruders know these passwords and can access systems effortlessly.

- **Bad Protocols -** Some protocols, or the standards by which information is exchanged over the Internet, lack any security at all. For example, unsolicited commercial email know as SPAM.

- **Trusting Untrustworthy information-** This is usually a problem that affects routers, or those computers that connect one network to another. When routers are not programmed to verify that they are receiving information from a unique host, bogus routers can gain access to systems and do damage.

- **End users -** Generally, users of computer systems are not professionals and are not always security conscious. For example, when the number of passwords of an user increases, user may start writing them down, in the worst case to places from where they are easy to find. In addition to this kind of negligence towards security procedures users do human errors, for example save confidential files to places where they are not properly protected.

IDS Components

Intrusion Detection Systems are generally made up of following major components:

- **Sensors:** These are deployed in a network or on a device to collect data. They take input from various resources, including network packets, log files, and system call traces. Input is collected, organized, and then forwarded to one more analyzers**.**

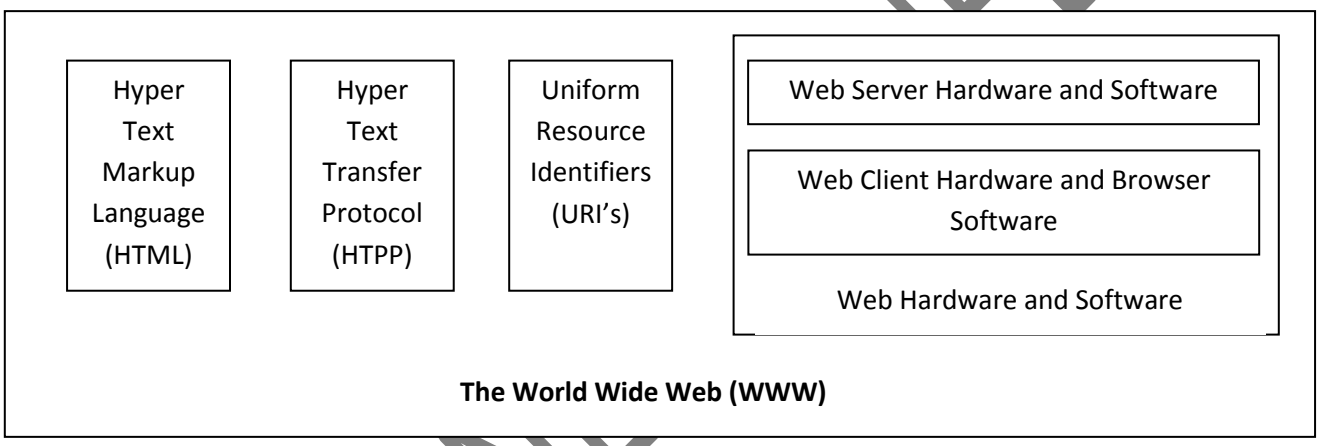
- **Analyzers:** Analyzers in IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance on mitigation steps.

- **User interface:** The user interface of the IDS provides the end users a view and way to interact with the system. Through the interface, the user can control and configure the system. Many user interfaces can generate reports as well.

- **Honeypot**: In fully deployed IDS, some administrators may choose to install a "Honeypots", essentially a system components setup as trap for intruders. Honeypots can be used as early warning systems on an attack. Many IDS vendors maintain honeypots for research purposes and to develop new intrusion signatures.

Chapter: 4 Internet and Other Technologies

World Wide Web: The World Wide Web (WWW or W3), most often called as Web, is defined as a network of computers all over the world. Fig. shows the major components of WWW.



Major Functional Components of the World Wide Web

1. **HTML:** HTML stands for HyperText Markup Language and is the main markup language for web page. HTML lets the creator of a Web page specify how text will be displayed and how to link to other Web pages, files, and Internet services.

2. **HTTP:** All computers in the Web communicate with each other using a communication standard called Hypertext Transfer Protocol (HTTP). HTTP is defined as the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

3. **URIs:** Uniform Resource Identifier (URI) is a string of characters used to identify a resource either by location, name or both.
   URIs can be classified as names (URNs) and locators (URLs), or as both.
   a. **URN:** A Uniform Resource Name (URN) is a specification of URI that identifies the resource by name i.e. it functions like a person's name, and
   b. **URL:** A Uniform Resource Locator (URL) is a specification of URI that defines the network location of a specific resource like address and access individual Web pages and Internet resources.
   c. The format of a URL is: protocol/Internet address/Web page address.

      For example - http://www.icai.org/seminars.html

4. Web Hardware and Software:

Web pages reside on **servers** that run special software that allow users to access Web pages and to activate links to other Web pages and to Internet services.

Computers reading the Web pages are called a **Web Client**. Web clients view the pages with a program called **a Web**

Browser. The first such browser capable of displaying graphics within a Web page was Mosaic. This request is

standard HTTP request containing a page address. A page address looks like: http://www.name.com.

Difference between Internet and WWW:

The Internet & the World Wide Web (the Web), though used interchangeably, are not synonymous.
Internet is the hardware part - it is a collection of computer networks connected through either copper wires, fiber optic cables or wireless connections.
The **World Wide Web** can be termed as the software part – it is a collection of web pages connected through hyperlinks and URLs.
Table highlights some of the major differences between Internet and WWW.

	Internet	WWW
Nature	**Hardware**	**Software**
Comprises of	Network of Computers, copper wires, fiber - optic cables & wireless networks	Files, folders & documents stored in various computers
Governed By	Internet Protocol	Hyper Text Transfer Protocol
Dependency	This is the base platform and is independent of WWW	It depends on the Internet to work

Table Internet vs. WWW

HTTP – Hyper Text Transfer Protocol:

The WWW is driven by two fundamental technologies: HTTP and HTML.

HTTP is the Hypertext Transfer Protocol that controls how Web servers and Web browsers communicate with each other.

HTML is the Hypertext Markup Language that defines the structure and contents of a Web page.

Simple Mail Transfer Protocol:

The Simple Mail Transport Protocol (SMTP) controls the transfer of email messages on the Internet.

SMTP is defined as text-based protocol in which an e- mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable channel, typically a **Transmission Control Protocol (TCP) connection.**

An SMTP transaction consists of three command/reply sequences (see example below.) They are:

- MAIL command, to establish the return address.
- RCPT command, to establish a recipient of this message. This command can be issued multiple times, one for each recipient.

- DATA to send the message text. This is the content of the message, as opposed to its envelope. It consists of a message header and a message body separated by an empty line.

File Transfer Protocol (FTP): The File Transfer Protocol (FTP) is used widely on the Internet for transferring files to and from a remote host. FTP is commonly used for uploading pages to a Web site and for providing online file archives.
An FTP URL has the basic form: ftp://user:pass@host/directory/file.

Network News Transfer Protocol (NNTP): The Network News Transfer Protocol (NNTP) is the basis for tens of thousands of newsgroups that provide a public forum for millions of Internet users. NNTP consists of two components: a list of newsgroups supported by a specific newsgroup server (newsgroups are typically selected by an Internet service provider); and a database of messages that are currently available for any particular newsgroup.

Common Gateway Interface (CGI): The Common Gateway Interface is used with many Web servers to provide processing beyond the normal HTTP Web interface. CGI requests are submitted from Web browsers to Web servers. When a server receives a CGI request, it typically executes a script to process the request and return a result to the browser.

Transmission Control Protocol (TCP): The TCP provides reliable transmission of data in an IP environment. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing.

Internet Protocol (IP): The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed.

VoIP (Voice over Internet Protocol): Voice over IP (VoIP) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. This allows delivery of voice communications over IP networks, for example, phone calls.(eg: yahoo call)

Address Resolution Protocol (ARP): The Address Resolution Protocol is a request and reply protocol that runs encapsulated by the line protocol. It is communicated within the boundaries of a single network, never routed across internetwork nodes. For two machines on a given network to communicate, they must know the other machine's physical (or MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically
discover the MAC-layer address corresponding to a particular IP network-layer address.

Internet Control Message Protocol (ICMP): The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that **provides message packets to report errors and other information regarding IP packet processing back to the source.**

User Datagram Protocol (UDP): The User Datagram Protocol is another transport layer protocol that provides a connectionless method of communicating between machines. It allows us to send datagrams, packets, between machines. The operation of UDP is much different than TCP. UDP is simpler, but it is essentially unreliable.

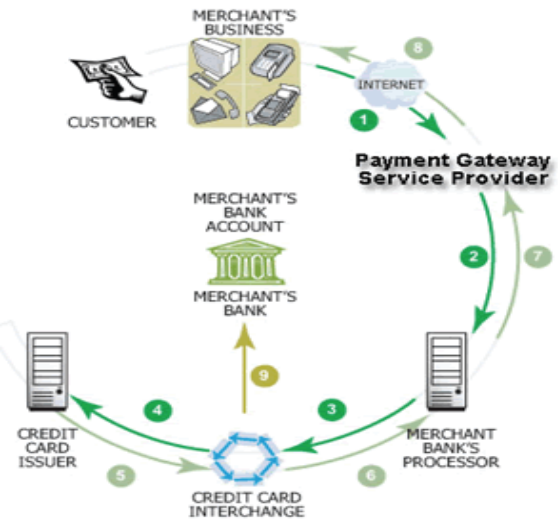
Telnet: Telnet is a protocol that allows us to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet). We use software called a telnet client on our computer to make a connection to a telnet server (i.e., the remote host). Once our telnet client establishes a connection to the remote host, our client becomes a virtual
terminal, allowing us to communicate with the remote host from our computer.

Credit card

How a credit card is processed?

Step 1: Authorization – This is the first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card issuing bank, where it is authorized or denied, and the merchant is allowed to process
the sale.

1. The cardholder requests a purchase from the merchant.
2. The merchant submits the request to the acquirer.
3. The acquirer sends a request to the issuer to authorize the transaction.
4. An authorization code is sent to the acquirer if there is valid credit available.
5. The acquirer authorizes the transaction.
6. The cardholder receives the product.



Step 2: Batching – This is the second step in processing a credit card. At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

1. The merchant stores all the day's authorized sales in a batch.

2. The merchant sends the batch to the acquirer at the end of the day to receive payment.

Step 3: Clearing – This is the third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through
the network back to the acquirer.

1. The batch is sent through the card network to request payment from the issuer.
2. The card network distributes each transaction to the appropriate issuer.
3. The issuer subtracts its interchange fees, which are shared with the card network, and transfers the amount.
4. The card network routes the amount to the acquirer.

Step 4: Funding – This is the fourth and final step in processing a credit card. After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.
1. The acquirer subtracts its discount rate and pays the merchant the remainder.
2. The cardholder is billed.

Acquirer: A bank that processes and settles a merchant's credit card transactions with the help of a card issuer.

Cardholder: The owner of a card that is used to make credit card purchases.

Card network: Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.

Discount fee: A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.

Interchange fee: A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards. They generally range from 1 to 3 percent.

Issuer: A financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

Using a credit card to make a purchase over the Internet follows the same scenario. But on the Internet, added steps must be taken to provide for secure transactions and authentication of both buyer and seller. To address these growing security concerns and pave the way for uninhibited growth of electronic commerce on the net, the two
leading credit card brands, Visa and MasterCard, teamed up some years ago to develop a common standard to process card transactions on the Internet, called the **Secure Electronic Transaction (SET) standard**.

Objectives of SET

SET addresses major business requirements:
SET is a standard which will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.

1. Provide **confidentiality of payment information and enable confidentiality of order information** that is transmitted along with the payment information.
2. Ensure the **integrity of all transmitted data.**
3. Provide **authentication that a cardholder** is a legitimate user of a branded payment card account.
4. Provide **authentication that a merchant can accept branded payment card** transactions through its relationship with an acquiring financial institution.
5. Ensure **the use of the best security practices and system design techniques to protect all legitimate parties** in an electronic commerce transaction.
6. **Facilitate and encourage interoperability among software and network providers.**

E-Commerce Risk and Security Considerations

The different dimensions of E-commerce security are as follows:

- **Integrity** - The ability to ensure that information being displayed on a web site or transmitted or received over

  the internet has not been altered in any way by an unauthorized party.
- **Non-repudiation** - The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions.
- **Authenticity** - The ability to identify the identity of a person or entity with whom we are dealing in the internet.
- **Confidentiality** - The ability to ensure that messages and data are available only to those who are authorized to view them.
- **Privacy** - The ability to control the use of information about oneself.
- **Availability** - The ability to ensure that an e-commerce site continues to function as intended