SECURITY

Assignment:- 1

# INTRODUCTION

As internet use is developing more and more, companies are opening their information system for their partners and suppliers. Therefore it is essential to know which of the company’s resources need to protect and to control system to be success and the user rights of the information systems

Therefore the goal of this report includes,

* The frauds of the buyers and sellers.
* IT security.

**Contents**

[THE CYBER ATTACK ON ISTANBUL ATATURK AND SABIHA GOKCEN AIRPORTS 5](#_Toc54517016)

[IT SECURITY 5](#_Toc54517017)

[NEED FOR IT SECURITY 5](#_Toc54517018)

[THE DIFFERENCE BETWEEN IT SECURITY AND INFORMATION SECURITY 6](#_Toc54517019)

[THE THREATS TO IT SECURITY 6](#_Toc54517020)

[MALWARE 6](#_Toc54517021)

[PROTECT MY NETWORK AGAINST MALWARE 6](#_Toc54517022)

[DETECT AND RESPOND TO MALWARE 6](#_Toc54517023)

[TYPES OF MALWARE 7](#_Toc54517024)

[VIRUS 7](#_Toc54517025)

[WORMS 7](#_Toc54517026)

[TROJAN VIRUS 7](#_Toc54517027)

[SPYWARE 7](#_Toc54517028)

[ADWARE 7](#_Toc54517029)

[RANSOMWARE 7](#_Toc54517030)

[FLIELESS MALWARE 8](#_Toc54517031)

[BENEFIT FROM IT SECURITY 8](#_Toc54517032)

[TYPES OF IT SECURITY 8](#_Toc54517033)

[NETWORK SECURITY 8](#_Toc54517034)

[INTERNET SECURITY 8](#_Toc54517035)

[ENDPOINT SECURITY 8](#_Toc54517036)

[CLOUD SECURITY 8](#_Toc54517037)

[APPLICATION SECURITY 9](#_Toc54517038)

[HACKING 9](#_Toc54517039)

[HACKER 9](#_Toc54517040)

[CIA TRIANGLE 10](#_Toc54517041)

[CONFIDENTIALIY 10](#_Toc54517042)

[INTEGRITY 10](#_Toc54517043)

[AVAILABILITY 10](#_Toc54517044)

[NETWORK 10](#_Toc54517045)

[TRUSTED NETWORK 10](#_Toc54517046)

[FIREWALL 11](#_Toc54517047)

[TOP ONLINE SHOPING SECURITY THREATS 12](#_Toc54517048)

[MAJOR THREAT TRANSACTION FRAUD 12](#_Toc54517049)

[MAJOR THREAT DIRECT SITE ATTACKS 13](#_Toc54517050)

[MAJOR THREAT PASSWORD ASSAULT 13](#_Toc54517051)

[MAJOR THREAT SOCIAL ENGINEERING 13](#_Toc54517052)

[OTHERS ONLINE THREATS YOU SHOULD KNOW 14](#_Toc54517053)

[BRUTE FORCE ATTACKS 14](#_Toc54517054)

[BOTS 14](#_Toc54517055)

[MALWARE 15](#_Toc54517056)

[PHISHING 15](#_Toc54517057)

[SPAM 15](#_Toc54517058)

[SECURITY MANAGEMENT 15](#_Toc54517059)

[SECURITY LEADERSHIP 15](#_Toc54517060)

[IMPLEMENT AN WAYS OF IT SECURITY MANAGEMENT SYSTEM 16](#_Toc54517061)

[FIREWALL 17](#_Toc54517062)

[TYPES OF FIREWALL 17](#_Toc54517063)

[PROXY FIREWALL 17](#_Toc54517064)

[STATEFUL INSPECTION FIREWALL 17](#_Toc54517065)

[UNIFIED THREAT MANAGEMENT FIREWALL 17](#_Toc54517066)

[NEXT GENERATION FIREWALL 17](#_Toc54517067)

[VIRTUAL FIREWALL 18](#_Toc54517068)

[VIRTUAL PRIVATE NETWORK (VPN) 18](#_Toc54517069)

[HOW DOES A VIRTUAL PRIVATE NETWORK (VPN) WORK 18](#_Toc54517070)

[WHAT IS SECURE REMOTE ACCESS 18](#_Toc54517071)

[IS VPN TRAFFIC ENCRYPTED 18](#_Toc54517072)

[TYPES OF VPNS 18](#_Toc54517073)

[REMOTE ACCESS 18](#_Toc54517074)

[SITE TO SITE 18](#_Toc54517075)

[IMPORTANCE OF CUSTOMER DATA VIEW ON EBAY SERVER SITE 19](#_Toc54517076)

[DATA SECURITY 19](#_Toc54517077)

[DATA PROTECTION 19](#_Toc54517078)

[WHAT PERSONAL DATA WE COLLECT AND PROCESS 19](#_Toc54517079)

[PURPOSES AND LEGAL BASIC FOR DATA PROCESSING AND CTEGORIES OF RECIPIENTS 19](#_Toc54517080)

[INTERNATIONAL DATA TRANSFERS 19](#_Toc54517081)

[RIGHTS AS A DATA SUBJECT 19](#_Toc54517082)

[NETWORK MONITERING 20](#_Toc54517083)

[NETWORK MONITORING SYSTEMS 20](#_Toc54517084)

[PROTOCOLS FOR NETWORK MONITORING 20](#_Toc54517085)

[BENEFITS OF NETWORK MONITORING 20](#_Toc54517086)

[CLEAR VISIBILITY INTO THE NETWORK 20](#_Toc54517087)

[BETTER USE OF IT RESOURCES 20](#_Toc54517088)

[EARLY INSIGHT INTO FUTURE INFRSTRUCTURE NEEDS 20](#_Toc54517089)

[THE ABILITY TO IDENTIFY SECURITY THREATS FASTER 20](#_Toc54517090)

[DEMILITARIZED ZONE (DMZ) 21](#_Toc54517091)

[HOW DMZs WORK 21](#_Toc54517092)

[BENEFITS OF DMZs 21](#_Toc54517093)

[STATIC IP 22](#_Toc54517094)

[HOW STATIC IP ADRESSES WORK 22](#_Toc54517095)

[BENEFITS OF STATIC IP ADRESSES 22](#_Toc54517096)

[ADVANTAGES 22](#_Toc54517097)

[DISADVANTAGES 22](#_Toc54517098)

[NATWORK ADRESS TRANSLSTION (NAT) 23](#_Toc54517099)

[NETWORK ADRESS TRANSLATION (NAT) WORKING 23](#_Toc54517100)

[NETWORK ADRESS TRANSLATION (NAT) TYPES 23](#_Toc54517101)

[ADVANTAGES OF NAT 23](#_Toc54517102)

[DISADVANTAGES OF NAT 23](#_Toc54517103)

[NETWORK SECURITY 24](#_Toc54517104)

[HOW DOSE NETWORK SECURITY WORK 24](#_Toc54517105)

[BENEFITS FROM NETWORK SECURITY 24](#_Toc54517106)

[TYPES OF NETWORK SECURITY 24](#_Toc54517107)

[IMPROVE NETWORK SECURITY 24](#_Toc54517108)

[FIREWALL PROS AND CONS 26](#_Toc54517109)

[PROS 26](#_Toc54517110)

[CONS 26](#_Toc54517111)

[AVOID SELLER FRAUD AND BUYER FRAUD 26](#_Toc54517112)

[AVOID SELLER FRAUD 26](#_Toc54517113)

[AVOID BUYER FRAUD 26](#_Toc54517114)

**PART 1:-**

# THE CYBER ATTACK ON ISTANBUL ATATURK AND SABIHA GOKCEN AIRPORTS

The attack on Istanbul Ataturk and Sabiha Gokcen airports a few years prior the polish attack. In July 2013 the passport control systems at the departure terminals in both of these airports were shutdown by a cyber attack. Passenger were forced to stand in line for hours and the majority of flights were delayed. Even though the systems were restored the damage could be felt for many hours after. Unfortunately not all airports have implemented cyber security systems that would protect and control those operations and all related features. It simply means that even though many may have security measures in please cyber criminals hacktivists or cyber terrorist this as a perfect opportunity to attack the airports in many different ways.

Figure 1 helps illustrate the many risks to the Air Transport Industry

# IT SECURITY

It security is a set of cybersecurity strategies that prevents unauthorized access to organization assets such as computers, networks and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

# NEED FOR IT SECURITY

As hackers get smart, the need to protect your digital assets and network devices is even greater. While providing IT security can be expensive, a significant breach costs an organization far more. Large breaches can jeopardize the health of a small business. During or after an incident, IT security teams can follow an incident response plane as a risk management tool to again control of the situation.

# THE DIFFERENCE BETWEEN IT SECURITY AND INFORMATION SECURITY

Although IT security and information security sound similar, they do refer to different types of security. Information security refer to processes and tool designed to protect sensitive business information from the invasion, where as IT security refers to securing digital data , through computer network security.

# THE THREATS TO IT SECURITY

Threats to IT security can come in different forms. A common threats is malware, or malicious software which may come in different variations to infect network devices including

* Ransomware
* Spyware
* Viruses

These threats make it even more important to have reliable security practices in place.

# MALWARE

Malware is intrusive software that is designed to damage and destroy computer systems. Malwares is a contraction for malicious software Examples of common malware includes viruses, worms, Trojan viruses, spyware and ransomware.

# PROTECT MY NETWORK AGAINST MALWARE

Typically businesses focus on preventative tools to stop breaches. By securing the perimeter businesses assume they are safe. Some advanced malware however will eventually make their way into your network. As a result it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

# DETECT AND RESPOND TO MALWARE

Malware will inevitably penetrate your network. You must have defenses that provide significant visibility and breach detection. In order to remove malware you must be able identify malicious actors quickly. This requires constant network scanning. Once the threat is identified you must remove the malware from your network. Today’s antivirus products are not enough to protect against advanced cyber threats.

# TYPES OF MALWARE

## VIRUS

Viruses are subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system’s ability to operate. As result viruses can cause significant operational issues and data loss.

## WORMS

Worms are a malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses worms do not need host programs to disseminate. A worm infects a device via a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses worms can severely disrupt the operations of a device and cause data loss.

## TROJAN VIRUS

Trojan viruses are disguised as helpful software programs. But once the user downloads it the Trojan virus can gain access to sensitive data and then modify block or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms Trojan viruses are not designed to self-replicate.

## SPYWARE

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device’s operations spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a key logger which records your keystrokes to reveal passwords and personal information.

## ADWARE

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous in some cases adware can cause issues for your system. Adware can redirect your browser to un safe sites and it can even contain Trojan horse and spyware. Additionally significant levels of adware can slow down your system noticeable. Because not all adware is malicious it is importance to have protection that constantly and intelligently scans these programs.

## RANSOMWARE

Ransomware is malicious software that gains access to sensitive information within a system encrypts that information so that the user cannot access it and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key then they know. When the attacker receives payment the data is unlocked.

## FLIELESS MALWARE

Fileless malware is a type of memory-resident malware. As the term suggest it is malware that operates from a victim’s computer’s memory not from file on the hard drive. Because there are no files to scan it is harder to detect then traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. In late 2017 the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNS Messenger.

# BENEFIT FROM IT SECURITY

IT security prevent malicious threats and potential security breaches that can have a huge impact on your organization. When you enter your internal company network IT security helps ensure only authorized users can access and make change to sensitive information that resides there. IT security works to ensure the confidentiality of your organization’s data.

# TYPES OF IT SECURITY

## NETWORK SECURITY

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability reliability and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users ability to access or use the network.

Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to public cloud.

## INTERNET SECURITY

Internet security involves the protection of information that is sent and received in browsers as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls antimalware and antispyware.

## ENDPOINT SECURITY

Endpoint security provides protection at the device level. Devices that may be secure by endpoint security include cell phones, tablets, laptop, computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

## CLOUD SECURITY

Applications, data and identities are moving to the cloud meaning users are connecting directly to the internet and are not protected by the traditional security stack. Cloud security can help secure the usage of software as a service application and the public cloud. A cloud access security broker secure internet gateway and cloud based unified threat management can be used for cloud security.

## APPLICATION SECURITY

With application security applications are specifically code at the time of their creation to be as secure as possible to help ensure they are not vulnerable to attacks. This added layer of security involves evaluating the code of an app and identifying the vulnerabilities that may exist within the software.

# HACKING

Hacking refers to activities that seek to compromise digital devices, such as computer, smartphones, tablets, and even entire networks.

# HACKER

A security hacker is someone who explores methods for breaching defenses and exploiting weaknesses in a computer system or network.

**PART 2:-**

# CIA TRIANGLE

Confidentiality, integrity and availability the CIA triangle is a security model creates to guide information security polices within a company. The three elements of CIA triangle confidentiality, integrity and availability are consider the three most important components of security.

Figure 2 CIA triangle

## CONFIDENTIALIY

Confidentiality is the security principle that controls access to information. It is designed to ensure the wrong people cannot gain access to sensitive information while ensuring the right people can access it.

## INTEGRITY

The second component of the triad integrity assures the sensitive data is trustworthy and accurate. Consistency, accuracy and trustworthiness of data should be maintained over its lifecycle. Sensitive data should not be altered in transit and security measures such as file permissions and user access controls should be taken to make sure that it cannot be modified by unauthorized users.

## AVAILABILITY

In order for an information system to be useful it must be available to authorized users. Availability measures protect timely and uninterrupted access to the system. Some of the most fundamental threats to availability are non malicious in nature and include hardware failures unscheduled software downtime and network bandwidth issues.

# NETWORK

Two or more computers that are connected with another for the purpose of communicating and share the data electronically.

# TRUSTED NETWORK

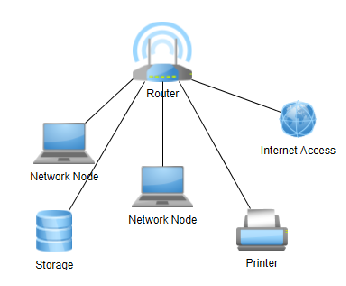
A trusted network is a network of devices that are connected to each others open only to authorized users and allows for only secure data to be transmitted.

A trusted network should have the following features:

* Authentication: The network should require users to login so that only authenticated users are allowed to use the network.
* Encryption: The data should be encrypted so that secure data cannot be intercepted and transmitting to unauthorized users.
* Firewall: The computer and servers on the trusted network should include hardware like firewall which is a software program or piece of hardware that helps screen for security.
* Private Network: The computers and servers on the trusted network should be equipped with software like Virtual private network (VPN) which allows for remote work with secure data transmission.

## FIREWALL

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific based on a defined set of security rules.

Decided that the first step was to configure a firewall so that unauthorized users (like hackers) and viruses can be kept out of the network. At the same time it must allow users to access resources outside of without any problem.

The operating system of all the computers and servers to include a firewall. The firewall will be default block all out side programs but can be configured to allow valid programs through. When the firewall is turned on many programs from the outside will be blocked and not allowed to communicate to the computer and servers inside the firewall.

Figure 3 A Computer Network in an Office

A firewall is like a door that protects a home. Anyone who has enter into the house will need a key to enter the building. But like a home owner other people can have copies of that key to be allowed in.

For example professor from inside the campus classroom may be not able to use chat software to communicate to an international student if the computer the professor uses has the firewall option turned on. To make it possible for the chat to work the professor dose not have to turned the entire firewall off. That would be leaving the door wide open for any burglar nearby.

Instead the professor only needs to add an exception to the firewall to allow the chat software program to communicate through the firewall like giving that software a key. The professor can now communicate with others outside of the firewall while his computer and data is secure within the college network.

**PART 3:-**

# TOP ONLINE SHOPING SECURITY THREATS

Online shopping security isn’t something to be taken lightly. Major data leaks have fundamentally damaged trust in digital security. Consumers are comfortable making payments through familiar systems (PayPal, Amazon, Google, apple, ect.) but take b bit more convincing to risk their credit card details with unknown companies. After all they know what’s at stake.

Failing to secure an online shopping business can directly impact sales or worse ruin your reputation. Once it’s know that a business cannot be relied upon to keep data secure no one will want to buy from them again.

Get serious about protecting your online shopping business. Learn the basic of what you need to know about online shopping security threats and solutions.

Figure 4 Major Threats to Online Shopping industry

# MAJOR THREAT TRANSACTION FRAUD

Vast amounts of money change hands online with each passing second as much as we like to think that technology has moved past transaction being dangerous to consumers it hasn’t. There are two primary forms of payment fraud. The first is stolen credit cards whose details are used to make unauthorized payment. The second is transactions on insecure systems that are interrupted or get redirected.

Online buyers now have access to systems offering unprecedented financial convenience. Bank support is available through live chat and you can even cancel payments through apps. But this doesn’t fully protect from this type of fraud. The reasons is simple even the most diligent among us will forget to check our bank records on occasion and it only takes one lapse in attention for a cybercriminal to make numerous payment.

Online shoppers are now aware of the importance of website security makers such as the HTTPS indicator. Still such indicators can often be spoofed in a manner that’s sufficiently convincing for most people. This type of forgery can make it quit trickly to tell when a website is providing a secure service. Consumers need to be educated and get batter at being vigilant online.

# MAJOR THREAT DIRECT SITE ATTACKS

While is passive approach online shopping sites can sometimes be subjected to direct attacks in the form of DDoS campaigns. Here’s how it work those who want to put a store under siege will program many internet capable devices to near constantly attempt to use the store site.

This orchestrated attack will overwhelm the store’s hosting and prevent the site from loading for most regular visitors. It’s mainly about keeping it so busy that it can’t focus on the visits that actually matter. This attack type can also burn through hosting data allowances causing other costly issues for businesses. These campaigns are relatively rare but not so much so that they’re not a threat.

What’s the end goal of a DDoS attack? It depends on the situations. Sometimes it will be inconvenience that store and damage its reputation as matter of corporate sabotage. More often a DDoS attack will be coupled with a blackmail demand pay a certain sum and the attack will be disabled.

# MAJOR THREAT PASSWORD ASSAULT

Password strategy has been frustrating security consultants since the very beginnings of the internet all due to the irritating balance needed between protection and convenience. It you choose long and complex password you can end up forgetting them and losing all access. Creating easy to remember passwords leaves systems highly vulnerable and open to attack.

There are two methods for this type of attack to occur. The first is brute forcing using a program to run through thousands upon thousands of passwords in the hope of eventually getting it right. And second what can reasonably be called informed guessing using pieces of information from a user’s life gleaned off social media to identify the words most likely to appear in their passwords.

And if a key admin passwords is discovered the resulting access can prove massively damaging because it might not be noticed for sometime. Significant alterations can be made systems can be taken offline data can be stolen and money can be transferred all with minimal risk to the person with access. It’s like breaking into someone’s house by picking the lock there’s no apparent damage but it happens when you’re supposed to be home.

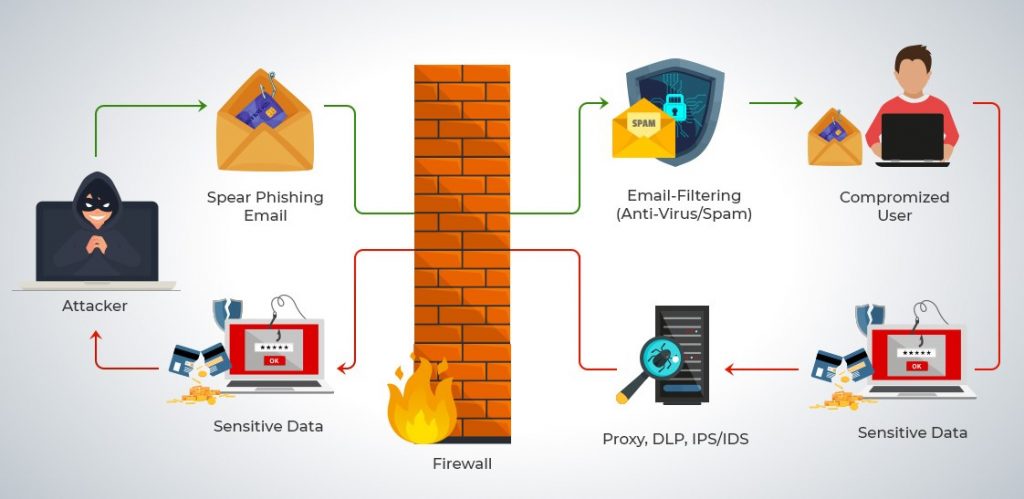
# MAJOR THREAT SOCIAL ENGINEERING

Social engineering is a broad method for gaining access to systems money or assets through deception at a social level instead of directly through technology. One of the most common forms of social engineering is phishing which which involves pretending to be someone trustworthy when contacting someone and exploiting that trust to get something from them.

In the recent phishing most commonly occurred through phone calls letters and even house visits. An example of a phishing attack is calling someone and claiming to be from their bank saying they need to confirm credit card details. When online shopping and online developed and became more popular it grew more sophisticated.

At this point phishers can learn about which retailers a shopper uses and spoof emails from them. Emails that are loaded with risks such as fraudulent forms to keylogger installers. They can also pose as online shopping through social media or setup stores that appear very similar to legitimate sites by using slightly different URLs and steal data. These cybercriminals often use misspellings and build a store that copies the design of a trusted online shoppers i.e: copying Amazon’s design and making it live at [www.amazon.com](http://www.amazon.com).

# OTHERS ONLINE THREATS YOU SHOULD KNOW

For online shopping dealing in daily monetary transactions security must become the number one concern. Intensive security measures need to be implemented to obstruct threats effectively and keep transactions protected. Here are others common threats online shopping sites face:

## BRUTE FORCE ATTACKS

Brute force attacks target an online store’s admin panel. Why? They want to figure out the password and gain access the directness of the attack makes it brute force. After using software to connect to a site it using code crunching programs to crack passwords by using every possible combination imaginable. The solution is easy protect your system by creating strong and complex passwords changing them regularly.

## BOTS

Bots can be both good and bad. The good ones are those that crawl the internet and determine how to rank your site in search engines. Bots can also scrap websites too for inventory information and pricing and after prices on a site freeze popular items in shopping carts and thereby damage site sales and revenues.

The solution is to protect exposed APIs and mobile apps and examine traffic source regularly looking for spikes and then blocking those hosting providers and proxy services.

## MALWARE

There are different types of malware that want to penetrate the backend to steal sensitive site data and customer information.

Malware are those that use malvertising, ransomware, cross site scripting, SQL injections, targeting credit card info and personal data. Malicious JavaScript coding is the most common. WordPress sites using online shopping and shopify regularly get targeted by malware injections via widgets and plugin upgrades. The solution is to use professional antivirus and anti malware software switch to HTTPS secure servers and admin panels and use SSL certificates while using employing multi layer security.

## PHISHING

Receiving fake you must take action emails either to your company or customers is widely used ploy and form of trickery used by hackers. It does require follow through and unintentionally offering up login information or personal identification information. The solution here is employee training and educating consumers.

## SPAM

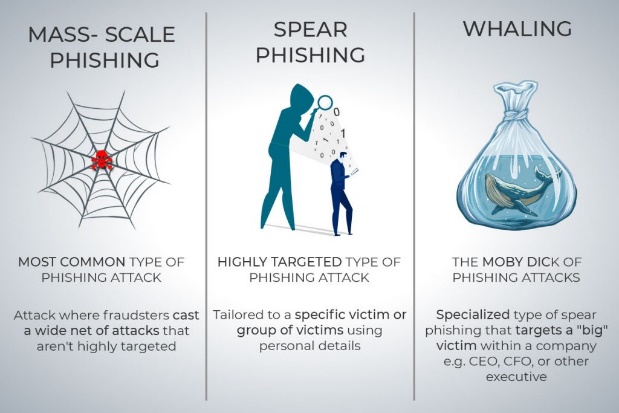
Contact forms and text boxes for blog comments are wide open to spammers. They can leave infected links that others can click on ruining your reputation and site security. Also known as SQL injections these cyber-attacks want to access databases via query forms. These links quietly wait for employees in inboxes and can affect site speed also. The solution is employee training and downloading spam filtering tools and anti virus software updating it regularly.

Figure 5 PHISHING

# SECURITY MANAGEMENT

Security manager helps to enable consistent policy and troubleshooting of security events offering summarized reports across the security development. Using its centralized interface organization can scale efficiently and manage a wide of security devices with improved visibility.

# SECURITY LEADERSHIP

A security leader shares tips for adopting a mindset creating risk management strategies and selling infosec to IT and executives.

# IMPLEMENT AN WAYS OF IT SECURITY MANAGEMENT SYSTEM

* Secure executive support and set the objectives
* Define the scope of the system
* Evaluate assets and analyze the risk
* Define the information security management system
* Train and build competencies for the roles
* System maintenance and monitoring
* Certification audit

**PART 4:-**

# FIREWALL

a firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow to block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internet networks that can be trusted and und untrusted outside networks such as the internet.

A firewall can be hardware, software or both.

# TYPES OF FIREWALL

## PROXY FIREWALL

An early type of firewall device a proxy firewall servers as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such content caching and security by preventing direct connections from outside the network. However this also may impact throughput capabilities and the applications they can support.

## STATEFUL INSPECTION FIREWALL

Now through of as a traditional firewall a stateful inspection firewall allows or blocks traffic based on state port and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator defined rules as well as context which refers to using information from previous connections and packets belonging to the same connection.

## UNIFIED THREAT MANAGEMENT FIREWALL

A UMT device typically combines in a loosely coupled way the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

## NEXT GENERATION FIREWALL

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next generation’s firewalls to block modern threats such as advanced malware and application layer attack.

According to Gartner Inc’s definition a next generation firewall must include.

* Standard firewall capabilities like stateful inspection.
* Integrated intrusion prevention.
* Application awareness and control to see and block risky apps.
* Upgrade paths to include future information feeds.
* Techniques to address evolving security threats.

While these capabilities are increasingly becoming the standard for most companies NGFWs can do more.

## VIRTUAL FIREWALL

A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware, ESXi, Microsoft Hyper-V, KVM) or public cloud (AWS, Azure, Google) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software defined networks.

# VIRTUAL PRIVATE NETWORK (VPN)

A virtual private network or VPN is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

# HOW DOES A VIRTUAL PRIVATE NETWORK (VPN) WORK

A VPN extends a corporate network through encrypted connections made over the internet. Because the traffic is encrypted between the device and the network traffic remains private as travels. An employee can work outside the office and still securely connect to the corporate network, even smartphones and tablets can connect through a VPN.

# WHAT IS SECURE REMOTE ACCESS

Secure remote access provides a safe way to connect users and devises remotely to a corporate network. It includes VPN technology that uses strong ways to authenticate the user or device. VPN technology is available to check whether a device meets certain requirements also called a device’s posture before it is allowed to connect remotely.

# IS VPN TRAFFIC ENCRYPTED

Virtual network is sent securely by establishing an encrypted connection across the internet known as a tunnel. VPN traffic from a device such as a computer, tablet or smartphones is encrypted as it travels through this tunnel. Offsite employees can then use the virtual network to access the corporate network.

# TYPES OF VPNS

## REMOTE ACCESS

A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may laptops, tablets or smartphones. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting.

## SITE TO SITE

A site to site VPN connects the corporate office to branch office over the internet. Site to site VPNs are used when distance makes it impractical to have direct network connections between these offices. Dedicated equipment is used to establish and maintain a connection.

# IMPORTANCE OF CUSTOMER DATA VIEW ON EBAY SERVER SITE

## DATA SECURITY

We protect your personal data through technical and organizational security measures to minimize risks associated with data loss misuse unauthorized access and unauthorized disclosure and alteration. To this end we use firewalls and data encryption for example as well as physical access restrictions for our data centers and authorization controls for data access.

## DATA PROTECTION

We have appointed data protection officers in several countries to oversee the protection of your personal data. If you have any questions about this User Privacy Notice or about data protection at eBay in general, you can contact the data protection officer responsible for your country at any time.

## WHAT PERSONAL DATA WE COLLECT AND PROCESS

We collect your personal data when you use our Services, create a new eBay account, provide us with information via a web form, add or update information in your eBay account, participate in online community discussions or otherwise interact with us. We also collect personal data from other sources.

## PURPOSES AND LEGAL BASIC FOR DATA PROCESSING AND CTEGORIES OF RECIPIENTS

We process your personal data for various purposes and based on several different legal bases that allow this processing. For example, we process your personal data to provide and improve our Services, to provide you with a personalized user experience on this website, to contact you about your eBay account and our Services, to provide customer service, to provide you with personalized advertising and marketing communications, and to detect, prevent, mitigate and investigate fraudulent or illegal activity. We also share your information with third parties, including service providers acting on our behalf, for these purposes. In addition, we may share your personal data among eBay group companies in order to fulfil our contract with you under the User Agreement and, if applicable, the Payments Terms of Use.

## INTERNATIONAL DATA TRANSFERS

Some recipients of your personal data are located outside your country or have offices in countries where data protection laws may provide a different level of protection than the laws in your country. When transferring personal data to such recipients, we provide appropriate safeguards.

## RIGHTS AS A DATA SUBJECT

Subject to possible restrictions under national law, as a data subject, you have the right to access, rectification, erasure, restriction of processing and data portability with regard to your personal data. In addition, you can withdraw your consent and object to our processing of your personal data on the basis of our legitimate interests. You can also lodge a complaint with a supervisory authority.

**PART 5:-**

# NETWORK MONITERING

Network monitoring provides the information that network administrators need to determine in the real time whether a network a network is running optimally. With tools such as networking monitoring software administrators can proactively identify deficiencies optimize efficiency and more.

# NETWORK MONITORING SYSTEMS

Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation such as traffic bandwidth utilization and uptime. These systems can detect devices and other elements that comprise or touch the network as well as provide status updates.

Network administrators rely on network monitoring systems to help them quickly detect devices or connection failures or issues such as traffic bottlenecks that limit data flow. These system can alert administrators to issues via email or text and deliver reports via network analytics.

# PROTOCOLS FOR NETWORK MONITORING

Protocols are sets of rules and directions for devices on a network to communicate with one another. Network hardware can’t transmit data without using protocols. Network monitoring systems use protocols to identify and report on network performance issues.

# BENEFITS OF NETWORK MONITORING

## CLEAR VISIBILITY INTO THE NETWORK

Through network monitoring, administrators can get a clear picture of all the connected devices in the network, see how data is moving among them, and quickly identify and correct issues that can undermine performance and lead to outages.

## BETTER USE OF IT RESOURCES

The hardware and software tools in network monitoring systems reduce manual work for IT teams. That means valuable IT staff have more time to devote to critical projects for the organization.

## EARLY INSIGHT INTO FUTURE INFRSTRUCTURE NEEDS

Network monitoring systems can provide reports on how network components have performed over a defined period. By analyzing these reports, network administrators can anticipate when the organization may need to consider upgrading or implementing new IT infrastructure.

## THE ABILITY TO IDENTIFY SECURITY THREATS FASTER

Network monitoring systems can provide reports on how network components have performed over a defined period. By analyzing these reports, network administrators can anticipate when the organization may need to consider upgrading or implementing new IT infrastructure.

# DEMILITARIZED ZONE (DMZ)

In computer networks a DMZ (demilitarized zone) also sometimes known as a perimeter network or a screened subnetwork is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks usually the public internet. External facing servers resources and services are located in the DMZ. Therefore they are accessible from the internet but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data through the internet.

# HOW DMZs WORK

DMZs are intended to function as a sort of buffer zone between the public internet and the private network. Deploying the DMZ between two firewalls means that all inbound network packets are screened using a firewall or other security appliance before they arrive at the servers the organization hosts in the DMZ.

If a better-prepared threat actor passes through the first firewall, they must then gain unauthorized access to those services before they can do any damage, and those systems are likely to be hardened against such attacks.

Finally assuming that a well resourced threat actor is able to breach the external firewall and take over a system hosted in the DMZ they must still break through the internal firewall before they can reach sensitive enterprise resources. While a determined attacker can breach even the best secured DMZ architecture a DMZ under attack should set off alarms giving security professionals enough warning to avert a full breach of their organization.

# BENEFITS OF DMZs

The primary benefit of a DMZ is that it offers users from the public internet access to certain secure services while still maintaining a buffer between those users and the private internal network. The security benefits of this buffer manifest in several ways including:

* Access Control for Organization.
* Prevent attackers from performing network reconnaissance.
* Protection against IP spoofing.

# STATIC IP

A static IP address is a 32 bit number assigned to a computer as an address on the internet. This number is in the form of a dotted quad and is typically provided by an internet service provider (ISP).

# HOW STATIC IP ADRESSES WORK

Because static IP addresses are not the default provided by most ISP companies, if an individual or organization wants one they first have to call their ISP and ask to assign their device such as router for example a static IP address. Once the device is set up with a new and unchanging IP address they will have to restart their device once. Computers or other devices behind the router will use the same IP address. Once the IP address is in place it doesn’t require any steps to manage since it doesn’t change.

There is a limit to the number of static IP addresses available however meaning requesting a static IP address will often cost money. IPv6 is an idea to get around this issue. IPv6 lengthens IP addresses from 32 bits to 128 bits (16 bytes) and increases the number of available IP addresses significantly making static IP addresses easier and less expensive to obtain and maintain. A large portion of internet traffic still uses IPv4 today but more internet traffic is shifting to the use of IPv6 meaning both are in use today.

# BENEFITS OF STATIC IP ADRESSES

## ADVANTAGES

* Businesses that rely on IP addresses for mail FTP and web servers can have one, unchanging address.
* Static IP addresses are preferred for hosting voice over IP, VPNs and games.
* They can be more stable in the case of an interruption in connectivity meaning packet exchanges won't be lost.
* They allow for file servers to have faster file uploads and downloads.
* A static IP will make it easier for any geolocation services to access where a device is.
* Static IPs are better for remote access to a computer.
* A static IP address-enabled device does not need the device to send renewal requests.
* Static IP addresses can be simpler for network administrators to maintain considering running servers.
* And it is easier for administrators to track internet traffic assigning access to users based on IP address.

## DISADVANTAGES

* It limits the amount of IP addresses. A static IP address assigned to a device or website is occupied until otherwise noted even when the device is off and not in use.
* Most people do not need a static IP address now.
* Because the IP address is constant and cannot easily be changed a static IP address is more susceptible to hackers or follow-up attacks.
* It can be complicated to set up a static IP manually.
* It may be difficult to transfer server settings from a static IP device to a new one if the original device becomes obsolete.
* Devices with a static IP are easier to track.
* Static IPs are more costly, as an ISP will typically need static IP users to sign up for a commercial account and pay one time fees. Monthly internet service costs may go up as well.
* Security concerns with both static and dynamic IP addresses can be addressed by implementing router firewalls, using a VPN or by using an internet security suite. Although these don't absolutely guarantee security, they can help significantly.

# NATWORK ADRESS TRANSLSTION (NAT)

To access the Internet one public IP address is needed but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this the translation of private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also it does the translation of port numbers i.e. masks the port number of the host with another port number in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

# NETWORK ADRESS TRANSLATION (NAT) WORKING

Generally, the border router is configured for NAT i.e the router which has one interface in local network and one interface in the global network. When a packet traverse outside the local network then NAT converts that local IP address to a global IP address. When a packet enters the local network, the global IP address is converted to a local IP address.

# NETWORK ADRESS TRANSLATION (NAT) TYPES

* Static NAT
* Dynamic NAT
* Port address translation (PAT)

# ADVANTAGES OF NAT

* NAT conserves legally registered IP addresses.
* It provides privacy as the device IP address sending and receiving the traffic will be hidden.
* Eliminates address renumbering when a network evolves.

# DISADVANTAGES OF NAT

* Translation results in switching path delays.
* Certain applications will not function while NAT is enabled.
* Complicates tunneling protocols such as IPsec.
* Also router being a network layer device should not tamper with port numbers but it has to do so because of NAT.

# NETWORK SECURITY

Network security is an any activity designed to protect the usability and integrity of your network and data.

* It includes both hardware and software technologies.
* It target a variety of threats.
* It stops them from entering or spreading on your network.
* Effective network security manages access to the network.

# HOW DOSE NETWORK SECURITY WORK

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements polices and controls. Authorized users gain access to network resources but malicious actors are blocked from carrying out exploits and threats.

# BENEFITS FROM NETWORK SECURITY

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

# TYPES OF NETWORK SECURITY

* Firewalls
* Email security
* Anti virus Anti malware software
* Network segmentation
* Access control
* Application security
* Behavioral analytics
* Cloud security
* Data loss prevent
* Intrusion prevention systems
* Mobile devices security
* Security information and event management
* VPN
* Web security
* Wireless security

# IMPROVE NETWORK SECURITY

* Perform auditing and mapping.
* Keep the network up to date.
* Physically secure the network.
* Consider MAC address filtering.
* Implement VLANs to segregate traffic.
* Use 802.1X for authentication.
* Use VPNs to encrypt select PCs or servers.
* Encrypt the entire network.

**PART 6:-**

# FIREWALL PROS AND CONS

## PROS

* Protection for vulnerable service.
* Protection against routing based attack.
* Controlling access to system.
* Centralization of security software.
* Privacy.
* Statistic collection.
* Policy enforcement.

## CONS

* Complex to configure.
* May block service that would be helpful as well.
* Back door attack may also be possible.
* Cannot protect against viruses.
* Could cause performance problems.
* Tends to concentrate security in a single port.

# AVOID SELLER FRAUD AND BUYER FRAUD

## AVOID SELLER FRAUD

* Keep Platforms and Software Up to Date.
* Get Tougher with Password Requirements.
* Require the Card Verification Value (CVV).
* Use the Address Verification System (AVS).
* Consider Setting Limits.
* Monitor Transactions and Reconcile Bank Accounts Daily.
* Managing Your Risk.
* PCI Compliance and Your online Store.

## AVOID BUYER FRAUD

Never send your card number PIN or any others card information to anyone by email



If you are not buying anything don’t submit your card details. There are for example games and fake lotteries online which sole purpose is to get your credit card information.



Many online shopping sites will ask to store your payment details. Think twice before deciding and make sure you understand the risk this might imply such as the site becoming compromised by cybercriminals. Most well known brands have a strong customer security policy.

Buy from trusted sources. Use brands and shops that you are familiar with or have used before and check the ratings of individual sellers on sites such as eBay or Amazon. For internet purchase make sure you use the internet security protocol called 3D secure verified by visa/secure code/safe key. Ask your bank or your card issuer about it.



Whenever possible do your online shopping at sites that use full authentication (verified by visa/master card secure code).

If the web site dose not support full authentication make sure the data transfer is appropriately protected. Check that there is an icon of an unbroken key or locked locket the bottom of your browser window and that in the address bar the URL begins with https:// instead of http://.



Don’t send money to anyone you don’t know. If someone approaches you online and asks for the money think whether you would give the same amount of money to an unknown person on the street.



When purchasing something online from another person don’t send money upfront to the seller. If possible reserve the right to receive the goods first.



Use credit cards when purchasing things online. Most credit have a strong customer protection policy if you don’t get what you ordered the card issuer will refund you.



Before providing your card details to pay for a continuous service over the internet (such as virus protection software) find out how can you can stop that service and the recurring charges related to it.



Always save all documents related to your online purchases. They may be needed to establish the terms and conditions of the sale or to prove that you have paid for the goods.

Some online shops outside of Europe may request a copy of your card and passport by fax in order to ensure that the order is placed by the actual card holder. Never send your card details in an unencrypted email if you do not supply these details the online shop will probably not ship your order.