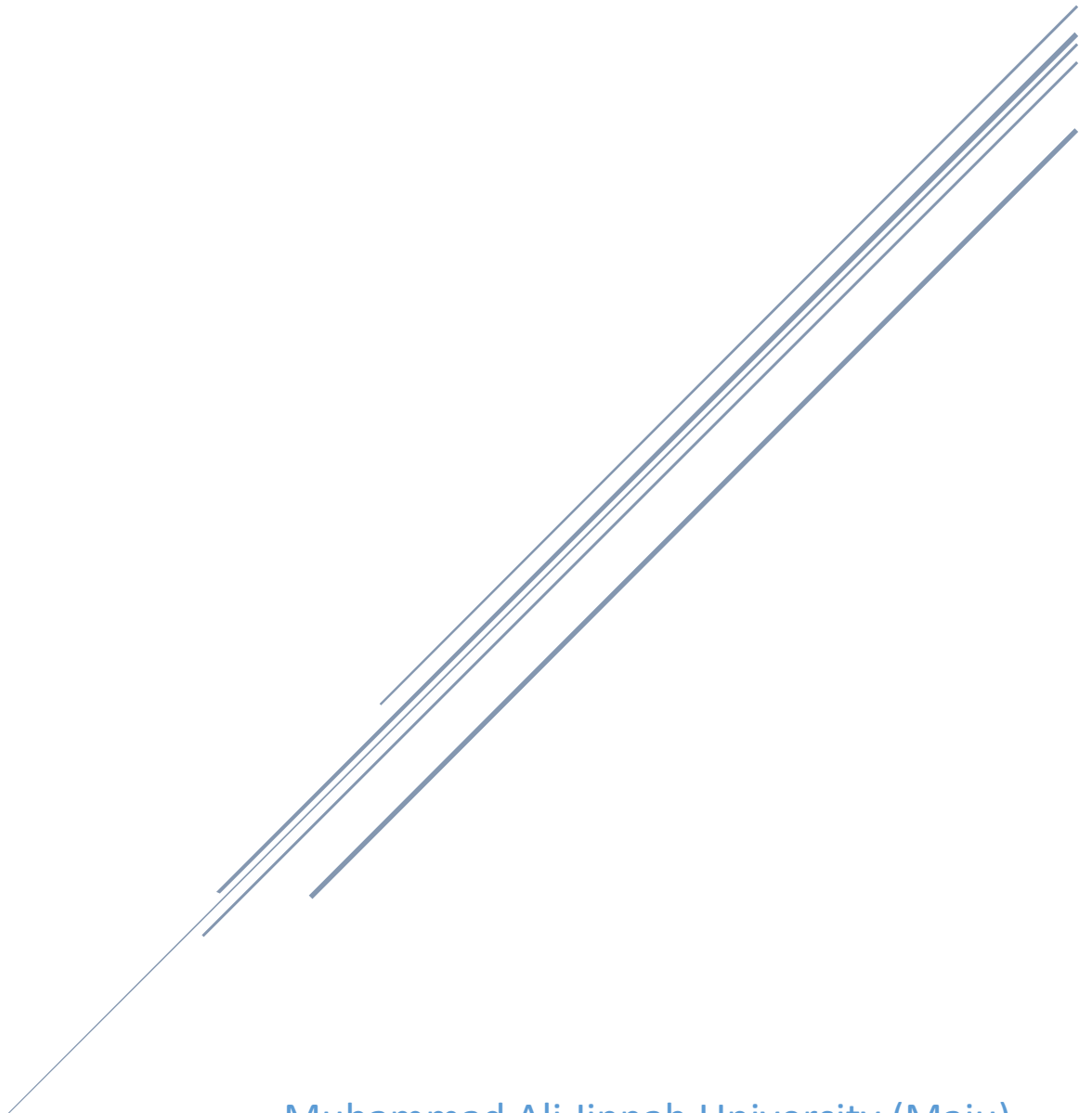


CYBER SECURITY

Formal Report



Muhammad Ali Jinnah University (Maju)
Technical Report Writing



Mohammad Ali Jinnah University
Chartered by Government of Sindh - Recognized by HEC

Formal Reports on Cyber Security

Subject: Technical Report Writing

Section: CM

Teacher: MUDASSIR JALAL

Member 1: Muhamad Fahad (FA19-BSSE-0014)

(FA19BSSE0014@maju.edu.pk)

ABSTRACT

Cyber Security is the back bone of information technology. Securing the information from the authorized Organization / people has become a challenge now days. When someone wants cyber security it means they wants to prevent them self from the '**cyber crimes**' which are increasing day by day. Governments and Other private companies are taking many actions in order to control the cybercrimes. This Report mainly focuses on challenges faced in Cyber Security and latest technologies. Report is also focuses on the techniques of in Cyber Security.

Table of contents

➤	Introduction.....	4
	a. History	
	b. Cyber Crime	
	c. Cyber Security	
➤	CYBER SECURITY TECHNIQUES.....	7
	a. Access control and password security.	
	b. Authentication of data.	
	c. Malware scanners	
	d. Firewalls	
	e. Anti-virus software	
➤	CYBER ETHICS.....	8
	a. Responsible Behaviors on the Internet	
	i. Copyrighting or Downloading	
	ii. Crime and Punishment	
	iii. Internet Hacking	
	iv. Cyberbullying	
➤	TRENDS CHANGING CYBER SECURITY.....	9
➤	Conclusion	16

✓ INTRODUCTION:

Nowadays man is able to send and get any form of information may be a mail or a sound or video just by the press of a button but did he ever think how safely his information id being transmitted or sent to the other individual securely without any leakage of data?? The reply lies in cyber security. Nowadays the Web is the fastest growing foundation in each day life. In today's specialized environment numerous latest technologies are changing the confront of the mankind. But due to these rising technologies we are incapable to defend our private information in an awfully compelling way and hence these days cyber violations are expanding day by day. Nowadays, more than 60 percent of total commercial exchanges is done online, so this field required a tall quality of security for transparent and best exchanges. Thus cyber security has gotten to be a most recent issue. The scope of cyber security isn't fair constrained to securing the information in IT industry but too to various other areas like cyber space etc.



Privacy and security of the information will continuously be top security measures that any organization takes care. We are by and by living in a world where all the data is kept up in a digital or a cyber shape. Social organizing sites provide a space where clients feel secure as they interact with companions and family. Within the case of home clients, cyber-criminals would proceed to target social media locales to take individual data. Not as it were social organizing but too amid bank transactions an individual must take all the required security measures.

a. History.

b. Cyber Crime.

Cybercrime is criminal movement that either targets or employs a computer, a computer arrangement or an organized device. Most, but not all, cybercrime is committed by cybercriminals or programmers who need to create cash. Cybercrime is carried out by people or organizations. Some cybercriminals are organized, utilize progressed strategies and are profoundly actually gifted. Others are amateur hackers. Rarely, cybercrime points to harm computers for reasons other than benefit. These may well be political or personal.

➤ Types of cybercrime

Here are some specific examples of the different types of cybercrime:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).



Most cybercrime falls under two main categories:

- Criminal activity that *targets*
 - Criminal activity that *uses* computers to commit other crimes.
- Cybercrime that *targets* computers often involves viruses and other types of malware.

Cybercriminals may infect computers with viruses and malware to damage devices or stop them working. They may also use malware to delete or steal data.

c. Cyber Security.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks. A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.



In today's connected world, everyone benefits from advanced cyberdefense programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyber attack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open source tools. Their work makes the Internet safer for everyone.

✓ CYBER SECURITY TECHNIQUES

➤ Access control and password security:

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.



➤ Authentication of data:

The documents that we receive must always be authenticated before downloading that it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

➤ Malware scanners:

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.



➤ Firewalls:

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.





Anti-virus software:

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.



✓ CYBER ETHICS

Cyber ethics is the study of ethics pertaining to computers, covering user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics.



With the increase of young children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think they have it all sorts out. That is why it is important to instill appropriate cyber etiquette at an early age but if you haven't there is still time to tell to your child.

➤ Responsible Behaviors on the Internet

Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life. The responsible behavior on the internet in many ways aligns with all the right behavior in everyday life, but the results can be significantly different.

Some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep logs of their activities which can be used to spot illegal or inappropriate behavior.

Following some issues are increasing daily due to children using the internet improperly and we have to take care of it.

1. Copyrighting or Downloading

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search what they need from the web and download it for their purpose. Their thinking is like "if everybody is doing it therefore it's ok", but an understandable and an age appropriate lesson on Cyber Ethics could help children to learn the risks involved in Internet downloading.

2. Crime and Punishment

Children do not believe that they will get into any real problem from neglecting the use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

3. Internet Hacking

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance.

4. Cyberbullying

Cyberbullying is increasing and people are becoming aware of its effects on children. Cyberbullying is bullying that takes place carrying electronic technology. Electronic technology carried by devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, website and chat.

When a child encounters cyber bullying that they should:

- Tell a trusted adult, and keep telling them until they take action.
- Avoid to open, read or respond to messages from cyber bullies.
- Always keep messages from bullies. They may be needed to take corrective action
- Use software to block bullies if they encounter them through chat or IM.

Use of technology by students is globally accepted as it facilitates the searching and retrieval of information needed for their academics and consequently the successful completion of their education programs. They need to be aware and knowledgeable about the ethics surrounding the use of ICT is therefore, important. Students must be aware and possess the knowledge about cyber ethics. Therefore, cyber ethics education must be provided to students by the school and colleges.

✓ TRENDS CHANGING CYBER SECURITY:

✓ **Conclusion:**