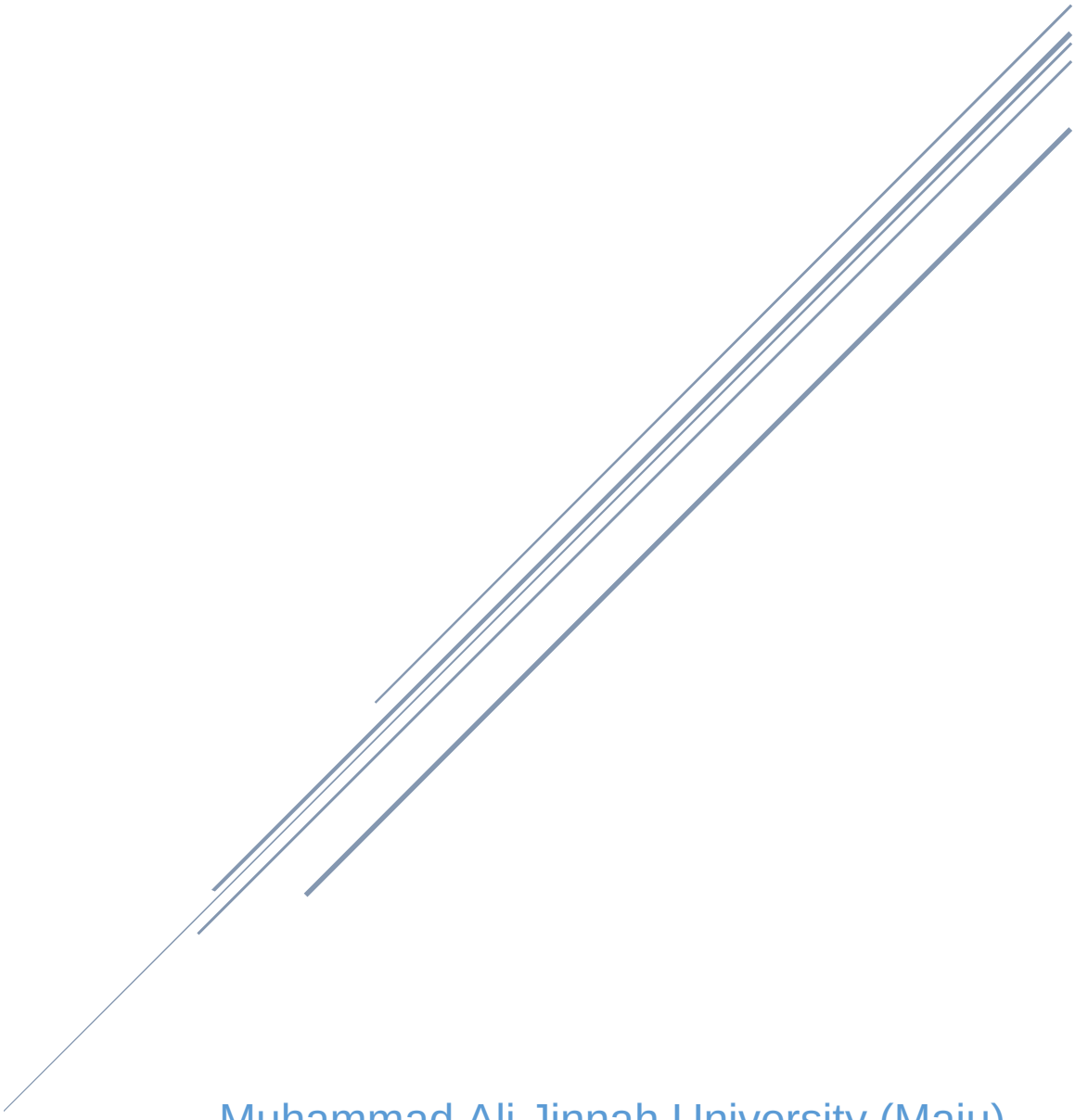
CYBER SECURITY

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 backbone of information technology. Securing the information from the authorized Organization/people has become a challenge nowadays. When someone wants cybersecurity it means they want to prevent themself from the '**cyber crimes**' which are increasing day by day. Governments and Other private companies are taking many actions to control cybercrimes. This report mainly focuses on challenges faced in Cyber Security and the latest technologies. The report also focuses on the techniques of Cyber Security.

Table of contents

✓ INTRODUCTION:

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

Cybersecurity has become a need in this era of technology but it starts in the early 1970's mid. In the 1970s the concept of cybersecurity was introduced and in 1976 some security software becomes part of the operating system as support of security and reliability. In 1979, a 16-year-old Kevin Mitnick hacked

most of the software company's data and get copies of the software and later on he was arrested but Today he is running his own Mitnick Security Consulting. But then in 1987, the official concept of cybersecurity was introduced because at that time there were some threads that some files are being attacked with the viruses with the extension of .com files at that time the cybersecurity concepts develop more and more and the antivirus concept has started at that time, And finally in 1988 many antivirus companies officially introduced themselves including AVAST too. Today if we see that AVAST has a team of more than 1700 worldwide and stops around 1.5 billion attacks every single month which is a lot. But at the early stages, antivirus companies have a simple scanner that can only scan simply and perform context search and detect unique virus code sequence and these most of the scanners include *immunizers* that modified the programs to make virus think the computer was already infected but nowadays not only antivirus detect the virus but also resolve it more efficiently and fast and get malware out of the devices we have.

b. Cyber Crime.

Cybercrime is a criminal movement that either targets or employments a computer, a computer arrange 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 cyber extortion).
- 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:

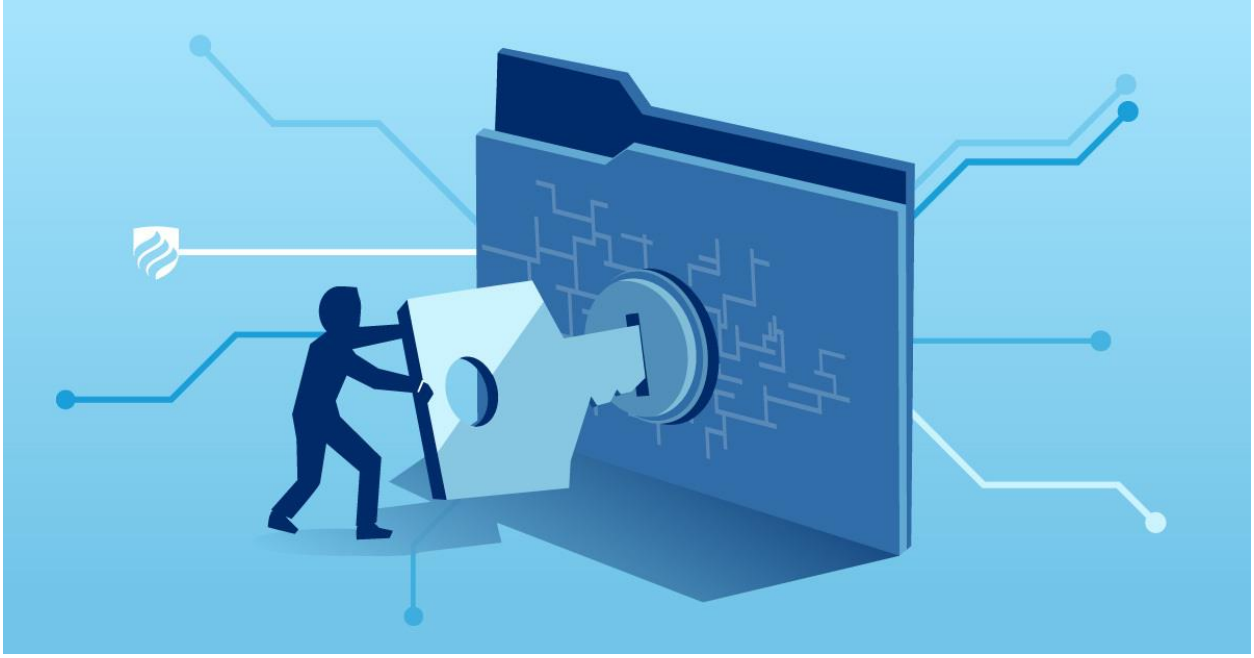
- Criminal activity that *targets*
- Criminal activity that *uses* computers to commit other crimes.

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 from 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 cyber defense 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 infrastructures 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 cyber threat 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.

✓ CYBERSECURITY TECHNIQUES

- **Access control and password security:**

  The concept of user names and passwords has been the fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity.

- **Authentication of data:**

  The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating 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 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. Anti-virus software is a must and a basic necessity for every system.

✓ CYBER ETHICS

Cyberethics is the study of ethics about 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 is it is important to instill appropriate cyber etiquette at an early age but if you haven't there is still time to tell your child.

- **Responsible Behaviors on the Internet**
  Cyberethics concerns 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 for 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 and need to resolve.

1. Copyrighting or Downloading

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search for 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 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 the best way to show children the costly consequences of their internet actions.

3. Internet Hacking

Hacking is 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 hackers must be stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling them 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 is carried by devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, websites, and chat.

When a child encounters cyberbullying that they should:

- Tell a trusted adult, and keep telling them until they take action.
- Avoid opening, read or respond to messages from cyberbullies.
- 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.

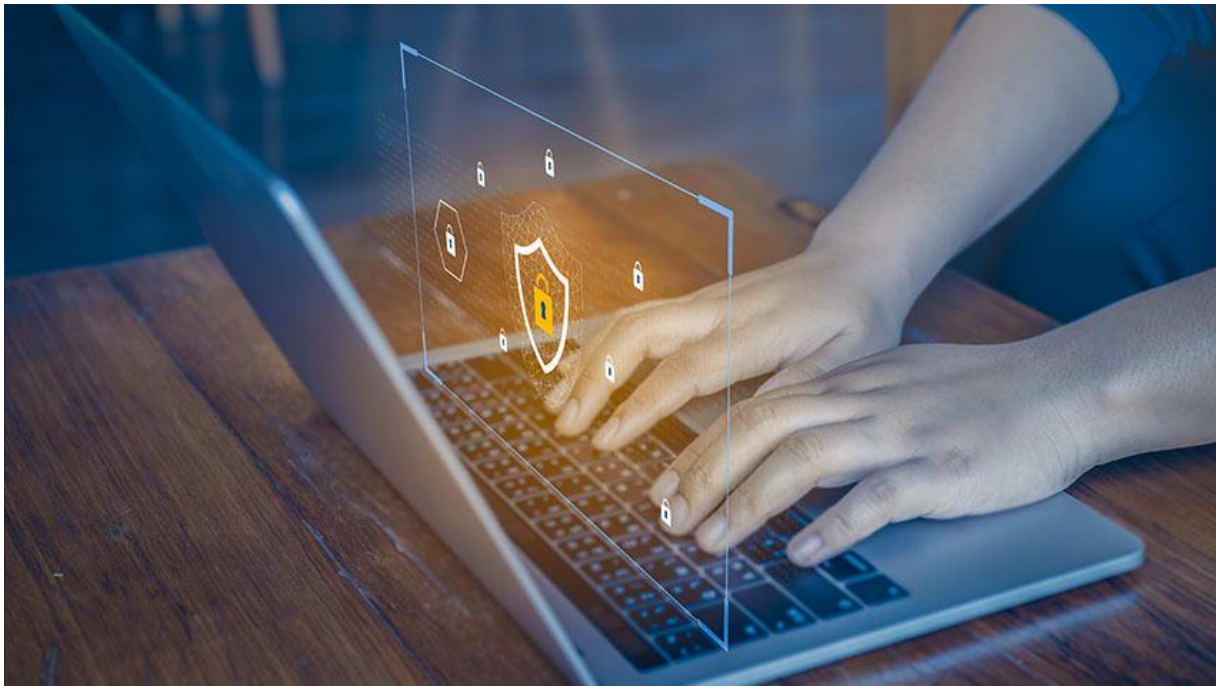
The use of technology by students is globally accepted as it facilitates the searching and retrieval of information needed for their academics and consequently the successful completion of their education programs. They need to be aware and knowledgeable about the ethics surrounding the use of ICT is,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

✓ TRENDS CHANGING CYBER SECURITY:

The trend is always changing also in the field of cybersecurity because the technology is growing strong and unique more and more, some of the latest trends in the field of cybersecurity are

- **Automotive Hacking**

  Automotive hacking is one of the big problems in cybersecurity and it is one of the latest trends in cybersecurity in this method the methods and software are created to do the hacking automatically and getting control over the drivers of a device making it fully controlled by the hacker cybersecurity teams are looking at these things to prevent it.



- **Integrity with AI**

  The AI is one of the best cybersecurity tools because the face detection tool, fingerprint scanner, and many other tools are introduced and combined with a security system that can secure the system up to 90% and no one can get into it and it became more challenging for the hackers to break a system with more and more security layers

- **Cloud is not safe too**

  The Cloud technology seems a lot more interesting and a secure way to back up your data but on the other hand it is much more in trouble because hackers think to get the data directly from someone's cloud data. The cloud data is also secured a lot and the security measurements have been made on it but the problem is that for hackers now it's becoming a trend to hack directly into the cloud and cyber teams are also looking at these things to prevent it.

✓ Conclusion:

In the end, we want to conclude that the world is now has also a kind of war which is a cyber war not only normal hackers get involved in it but also different countries government war each other by technology which is in the form of cyberwar so cybersecurity has become a major thing that should be improved more and more and that's why it is called the backbone of information technology because not only it is securing the system but also preventing everyone to get that thing and because of the reason the cybercrimes are increasing the only hope to stop them is the cybersecurity which should improve that much that it should be more than enough to secure a system.

Moreover, if in this fast-growing world of technology if a country doesn't focus on getting themselves secure not only by wars but also cyber wars there is a lot of chance that they can lose most of their precious data which will eventually lead them to lose by every means. That means that it is that much important that it should be improved more and more and should be focused more and more to secure everyone's data which can be sell out misused or can lead to many problems to not only that person but also for others, So that's why cybersecurity is also a major priority in our normal routine of life too to secure us from different threads of cyberattacks.