International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 63-66 www.ijaem.net ISSN: 2395-5252

Concept of cyber security

Eng.Abdalgader Egreira Ali Abuhamra1 , Eng Nassreedin Mustafa Abdullah Ali2 , Eng Ashraf Mahfoudh Abdannabi Ali 3

Technology College of Civil Aviation & Meterology,aspaia, Libya.)
(Faculty of Science and Medical Technology Tripoli)2
(Higher Institute of Science and Technology Tripoli)3

Date of Submission: 25-03-2024 Date of Acceptance: 05-04-2024

ABSTRACT
Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security

I. INTRODUCTION

New threats emerge every hour of every day in today's technological environment. When you connect to the Internet, you leave yourself up to the prospect of a hacker targeting your company. Cybercrime is becoming huge business, and corporations and governments around the world are focusing on cyber risk. People nowadays utilize the Internet to advertise and sell a variety of products, communicate with their customers and retailers, and conduct financial activities. Hackers and cybercriminals take advantage of this by using the internet to disseminate malware and carry out cyber attacks. So to control this, we need to know about cyber security.

The term "cyber" refers to the study of cybernetics. The term "cyber" is a prefix or adjective that refers to or describes information technology (IT), computers, and virtual reality. The study of communication and automatic control devices or machines, as well as living organisms, is known as cybernetics. In the early 1980s, the term "cyber" was invented as a shorthand for "cybernetics."

Cyber security refers to the protection of computers, servers, mobile devices, electronic systems, networks, and data from attack, damage, or unauthorized access. It's also known as information technology security or electronic information security. Individuals and businesses utilise the method to prevent illegal access to data centres and other digital systems.

A strong cyber security strategy can help protect an organization or user against hostile attacks aimed at obtaining access to, modifying, deleting, destroying, or extorting important data from their systems. Cyber security is also important in preventing attacks that try to disable or impair the function of a system or device.

The necessity of cyber security continues to expand as the number of people, devices, and programmers in the modern company grows, along with the rising deluge of data, most of it is sensitive or confidential. There will be benefits to cyber security, but there will also be drawbacks.

The basics of cyber security

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

Use passwords for all laptops, tablets, and Smartphone. Don't leave these devices unattended in public places. Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, Smartphone, removable drives, backup tapes, a

Types of cyber security

It is helpful to understand the ten most commonly referenced types of cyber security.

- Application security. ...
- Cloud security. ...
- Critical infrastructure security. ...
- Data security. ...
- Endpoint security. ...
- IoT (Internet of Things) security. ...
- Mobile security. ...
- Network security.
- hat is the definition of cyber security?

- Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransom ware; or interrupting normal business processes.

II. CYBER CRIMES

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it.

Types of Cyber Crimes

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it.

Cybercriminals usually try to profit off of their crimes using a variety of tactics, including:

- Denial of Service, or DOS

Where a hacker consumes all of a server's resources, so there's nothing for legitimate users to access

- Malware

Where victims are hit with a worm or virus that renders their devices useless

- Man in the Middle

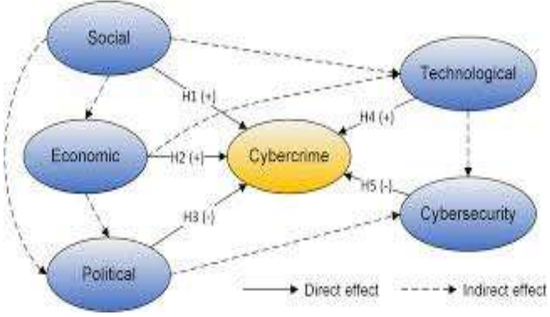
Where a hacker puts himself between a victim's machine and a router to sniff data packets

- Phishing

Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information

Other types of cyber attacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.

Motivates Cyber Criminals?



The main motive behind the cybercrime is to disrupt regular business activity and critical infrastructure. Cybercriminals also commonly manipulate stolen data to benefit financially, cause financial loss, damage a reputation, achieve military objectives, and propagate religious or political beliefs. Some don't even need a motive and might hack for fun or simply to showcase their skills.

So who are these cybercriminals? Here's a breakdown of the most common types:

- Black-Hat Hackers

Black-hat hackers use fake identities to conduct malicious activities for a profit

- Gray-Hat Hackers

They work both with malicious intent and as legitimate security analysts

- White-Hat Hackers

White-hat hackers work as security analysts to detect and fix flaws and protect against malicious hackers

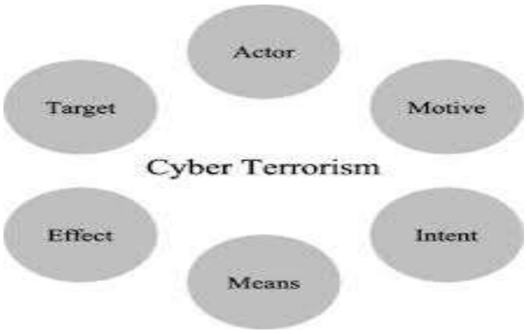
- Suicide Hackers

They aim to openly bring down the critical infrastructure for a social cause

- Script Kiddies

They are unskilled hackers who run scripts and software created by more experienced hackers

III. CYBER TERRORISM



Cyber terrorism refers to the use of cyberspace to conduct terrorist activities. It involves the deliberate use of computer systems, networks, and information technology to create fear, disruption, and damage for ideological or political purposes.

They create fear by disrupting large-scale computer networks; motivated by religious or political beliefs

Cyber Security experts employ different tactics to secure computer systems and networks. Some of the best practices include:

- Using two-way authentication
- Securing passwords
- Installing regular updates
- Running antivirus software
- Using firewalls to disable unwanted services
- Avoiding phishing scams
- Employing cryptography, or encryption
- Securing domain name servers, or DN

IV. CONCLUSION

To summaries, cyber security is one of the most critical parts of today's rapidly evolving digital world. Its threats are difficult to dismiss, therefore learning how to guard against them and teaching others how to do so is critical.

Widespread security flaws, as well as speedier and more sophisticated cyber attacks, make it incredibly difficult for security specialists to avert such dangers. As a result, a comprehensive cyber security strategy should be implemented to prevent cyber attacks from inflicting harm. Understanding cyber security techniques and methods is critical for effectively defending against digital threats.

It is entirely up to you whether you take safeguards or ignore this increasingly significant problem when it comes to your cyber security. We must be careful in using anything by supplying enough knowledge so that there is no problem like account being hacked. Do not dismiss this cyber threat as a little issue, since this problem has the potential to destroy your life.

We need to think about the consequences that will come before doing something. For example, do not post pictures of our happiness on the internet because this may affect people who are jealous of our happiness which can cause the account to be hacked and so on. So please be aware to the issue of cyber security.

Lastly, cyber security has an advantages and disadvantages. But if everyone will not handle problem of cyber security effectively this may lead lot problem to people and themselves. That is why cyber security requires the greatest amount of focus, research, inventiveness, and action.

REFERENCES

[1]. Adams, Anne, Martina Angela Sasse, and Peter Lunt. (1997). Making passwords secure and usable. In: People and Computers XII - Proc. of the 7th International Conference on Human-Computer Interaction (HCI'97), Springer.

[2]. Balfanz, Dirk, Glenn Durfee, Diana K. Smetters, and R. E. Grinter. (2004). In search of usable security: Five lessons from the field. Security & Privacy, IEEE, Vol. 2(5), 19-24.

[3]. Barth, Bradley. (2018). Monero bug that doubled coin transfer amounts allowed attackers to steal from Altex.exchange. SC magazine, 3 August 2018.

[4]. Borodkin, Michelle. (2001). Computer Incident Response Team.

[5]. Bursztein, Elie, Jonathan Aigrain, Angelika Moscicki, and John C. Mitchell. (2014). The end is nigh: Generic solving of text-based CAPTCHAs. In: Proceedings of the 8th USENIX Workshop on Offensive Technologies.

[6]. bran, Alain, Moore, James W., Bourque, Pierre, & Tripp, Leonard L., eds. Guide to the Software Engineering Body of Knowledge. IEEE Computer Society. 2004. www.computer.org/web/swebok/index.

[7]. Eloff, M. M. and J. H. P. Eloff. (2002). Human Computer Interaction: An Information Security Perspectives. In: M. Adeeb Ghonaimy, Mahmoud T. El-Hadidi and Heba K. Aslan. Security in the Information Society: Visions and perspectives. Springer.

[8]. Furnell, Steven. (2005). Why users cannot use security. Computers & Security, Vol. 24(4), 274-279.