

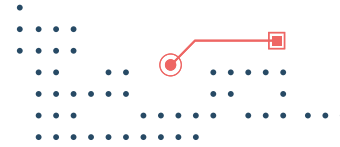


المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

UNLOCK

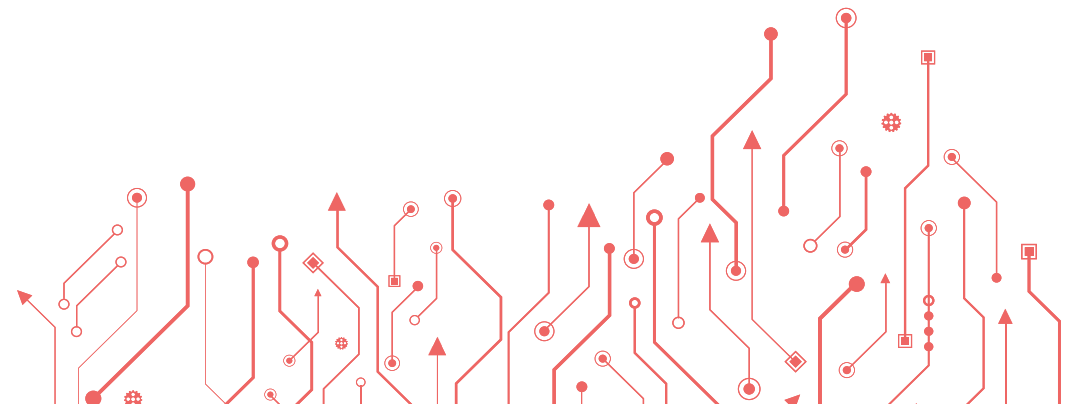
YOUR CAREER IN CYBER SECURITY





Hello

Your Cybersecurity Career
starts here!



Welcome to the World of Cybersecurity Careers!

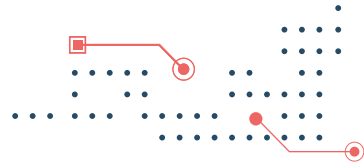
"In our digital era, cybersecurity is crucial, offering diverse opportunities to protect against online threats. This field combines technology skills, problem-solving, and creativity to safeguard individuals, organizations, and nations. This booklet introduces you to various terminologies, cybersecurity specializations, and a potential concept that will help you explore your role and the impact you can make in securing our digital world."



**Dream of being a
Cybersecurity expert?**






**Learn how to transform this
into your professional reality!**

Discover Cybersecurity

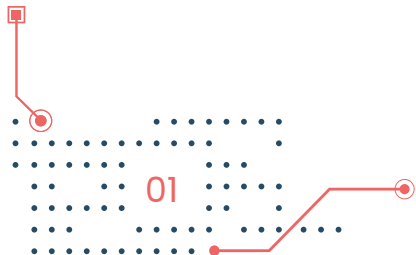


Are you interested in exploring the world of cybersecurity and making it your career?

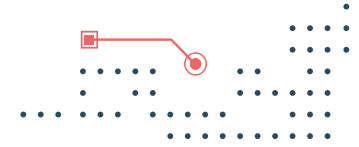
If yes, then you might want to ask yourself these questions:

- | | | | | |
|---|--|-----|----|----|
|  | Do you love working with new technology? | Yes | or | No |
|  | Do you enjoy finding creative solutions to problems? | Yes | or | No |
|  | Did you know that almost everything we use today is connected to the internet in some way? | Yes | or | No |
|  | Do we have enough cybersecurity experts to protect us from cyber threats? | Yes | or | No |
|  | Are you interested in being a defender of Cyberspace? | Yes | or | No |

Cybersecurity is the practice of protecting digital infrastructure and defending networks, communications, devices, and data in cyberspace from dangers, threats, and criminal hackers.



Start Your Cybersecurity Career!



Hey Students!

Did you know that the world needs about **1.8 million qualified Cybersecurity professionals** to keep computers and networks safe from unauthorized access and attacks? If you're interested in cybersecurity, here are five things you can do right now:



01

Explore and research about Cybersecurity career profiles to learn about different jobs in this field.



02

Join or start an IT/Cybersecurity club at your school.



03

Ask your teachers about Cybersecurity concepts in your classes.



04

Sign up for courses in advanced math, science, or creative subjects like writing and art.



05

Ask your guidance counselor about Cybersecurity career opportunities.



Get Started!

Classes to take in high school

- ☐ Advanced Math Science.
- ☐ Creative Writing (English/Arabic and Communication).
- ☐ Technology Ethics.
- ☐ IT-related subjects.

Majors to pursue in college

- ☐ Computer Science.
- ☐ Information Technology.
- ☐ Cybersecurity.
- ☐ Artificial Intelligence and Cybersecurity.
- ☐ Computer Engineering.
- ☐ Data Science and Cloud Technologies.

Additional ways to get a head

- ☐ Participate in local Cybersecurity contests, clubs, and camps.
- ☐ Consult your guidance counselors about career paths in Cybersecurity.
- ☐ Ask your teachers to incorporate Cybersecurity concepts into the lessons.

My Notes

.....

.....

.....

Career Options

Explore the following specializations and write a brief description:

Cryptographer / Cryptanalyst aka Encryption Expert.

☐

.....

.....

Cyber Forensics Expert.

☐

.....

.....

Cyber Defense Incident Responder.

☐

.....

.....

Cyber Legal Advisor.

☐

.....

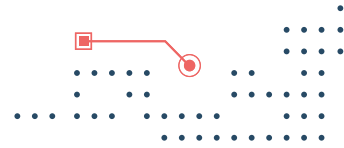
.....

Cyber Security Engineer.

☐

.....

.....



Information Systems Security Manager.



Software Developer.



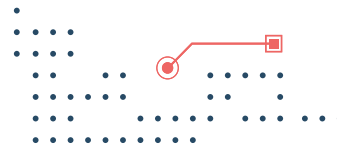
IT Project Manager.



Multi-Disciplined Language Analyst.



Vulnerability Assessment Analyst.



Cyber Crime Investigator.



Cyber Operator.



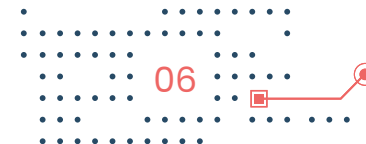
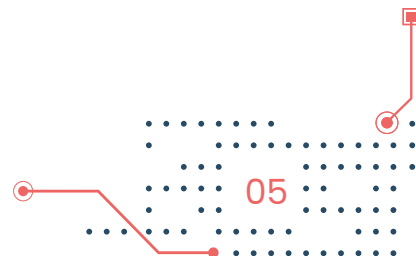
Technical Support Specialist.

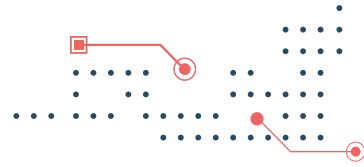


System Testing & Evaluation Specialist.



Systems Administrator.





Cyber OPS Planner.



Information Assurance Analyst.



Knowledge Manager.



Pen Tester.

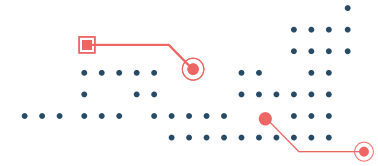


Threat & Warning Analyst.



Cyber-tionary

Cyber-tionary



Below are 27 essential Cybersecurity terms along with their definitions that you can learn to start your Cybersecurity knowledge:



01 Cybersecurity

The protection of networks, information technology systems, operational technology systems, and their components, including hardware and software, the services they provide, and the data they contain, from any unauthorized access, disruption, modification, or exploitation. The concept of cybersecurity encompasses information security, electronic security, digital security, and more.



02 Cyberspace

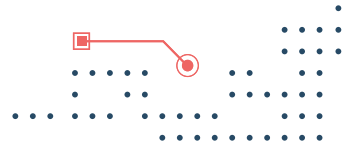
The interconnected network of information technology infrastructure, including the Internet, communication networks, computer systems, and Internet-connected devices; along with the associated hardware and control devices.



03 Critical National Infrastructure

The interconnected network of information technology infrastructure, including the Internet, communication networks, computer systems, and Internet-connected devices; along with the associated hardware and control devices.

- A significant negative impact on the availability, integrity, or delivery of essential services, including services that could lead to loss of property and/or life and/or injuries in the event of their compromise taking into account the economic and/or social impacts at the national level.
- A significant impact on national security and/or national defense and/or the state's economy or national assets.



04 Availability



Ensuring access and use on demand by an authorized user, process, or system in a reliable manner.



05 Integrity



Protection against unauthorized modification or destruction of information, and also includes ensuring non-repudiation of information and authenticity.



06 Confidentiality



The property of non-disclosure of information to an unauthorized user, process, or system except in the event of authorization to access it.



07 Information Assurance



The measures that protect information and information systems by ensuring their availability, integrity, authenticity, non-repudiation, and confidentiality.

My Notes



.....

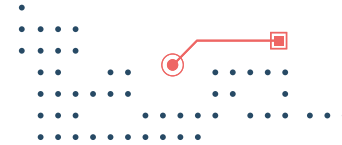
.....

.....

.....

.....

.....



08 Accountability



The ability to trace the path of a specific activity or event back to the responsible party, the originator of the activity. This supports non-repudiation, fault diagnosis, intrusion detection and prevention, and post-detection actions such as recovery and legal proceedings.



09 Authentication



Verifying the identity of a user, process, or device, and is often a prerequisite for granting access to technical resources. It is not related to determining access rights to technical resources and assets.



10 Multi-Factor Authentication



A security system that verifies the identity of a user; it requires the use of multiple independent elements of authentication mechanisms. Authentication mechanisms include several elements:

- Knowledge: something the user knows (such as a password).
- Possession: something the user possesses (such as a token or a temporary SMS for login) and is called a one-time password.
- Inherence: a biometric characteristic related to the user himself (such as a fingerprint).

My Notes

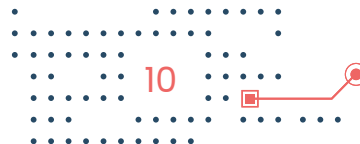


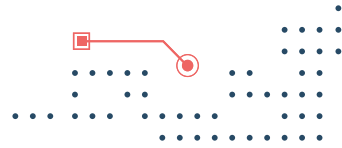
.....

.....

.....

.....





11 Authorization

Defining the rights/licenses to access information and technical resources for the entity in general, and controlling and verifying access levels in particular.



12 Assets

Tangible or intangible resources that are valuable to the organization. Including employees, technologies, facilities, patents, software and services, information and characteristics (such as the organization's reputation, identity, and cognitive or professional capabilities).



13 Cryptography

Rules that include principles, means, and methods for storing and transmitting data or information in a specific form in order to hide its semantic content and prevent unauthorized use and undetected modification, so that unauthorized persons cannot read or process it.



14 Cybersecurity Resilience

An organization's overall ability to withstand, absorb, and recover from cyber incidents in a timely manner.

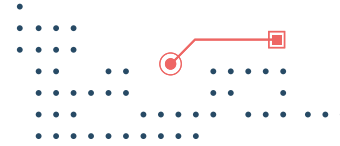
My Notes

.....

.....

.....

.....



15 Defense-in-Depth

A concept that means clearly defining multiple defensive layers of security controls through integration between people, technology, and operational capabilities.



16 Cyber Attack

The unauthorized exploitation of computer systems, networks, and organizations that rely on information and communications technology for the purpose of causing harm. It includes any type of malicious activity that attempts to gain unauthorized access to, disable, prevent, or destroy information system resources or the information itself.



17 Distributed Denial-of-Service (DDoS) Attack

Attempts to disable the system and make its services unavailable by sending a large number of requests from multiple sources at the same time.



18 Phishing Emails

Masquerading as trusted entities through email messages to obtain sensitive information, such as usernames, passwords, or credit card details, for malicious and harmful purposes.

My Notes

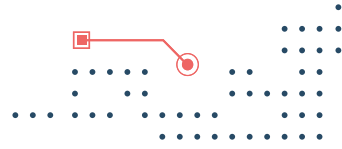
.....

.....

.....

.....





19 Threat Intelligence

Organized information that has been analyzed about recent, current, and potential attacks that could pose a cyber threat to the organization.



20 Information Sharing

The exchange of data and information, or knowledge – or both – for use in managing risks and threats or responding to cyber events.



21 Malware

Short for “malicious software,” it refers to any software designed to harm or exploit any programmable device, service, or network.



22 Ransomware

A type of malicious software designed to block access to a computer system or data until a sum of money is paid.



23 Disaster Recovery

Activities, programs, and plans designed to restore an organization’s critical business functions and services to their normal state after a cyber-attack or disruption of these services and functions.

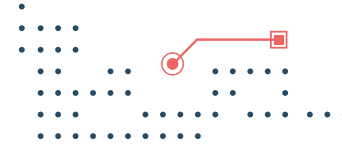
My Notes

.....

.....

.....

.....



24 Firewall

Hardware or software that restricts network data traffic according to a set of access control rules that govern what is allowed and what is not.



25 Vulnerability

Any type of weakness in a computer system, its programs or applications, or in a set of procedures, that makes cybersecurity vulnerable to threats.



26 Vulnerability Assessment

A systematic process of examining information systems or applications to identify the level of security controls, identify their shortcomings, and provide data that can be used to predict the effectiveness of security controls and ensure their effectiveness after implementation.



27 Penetration Testing

The process of testing a system, network, website, or mobile app to identify vulnerabilities that could be exploited to carry out a cyber attack.

My Notes

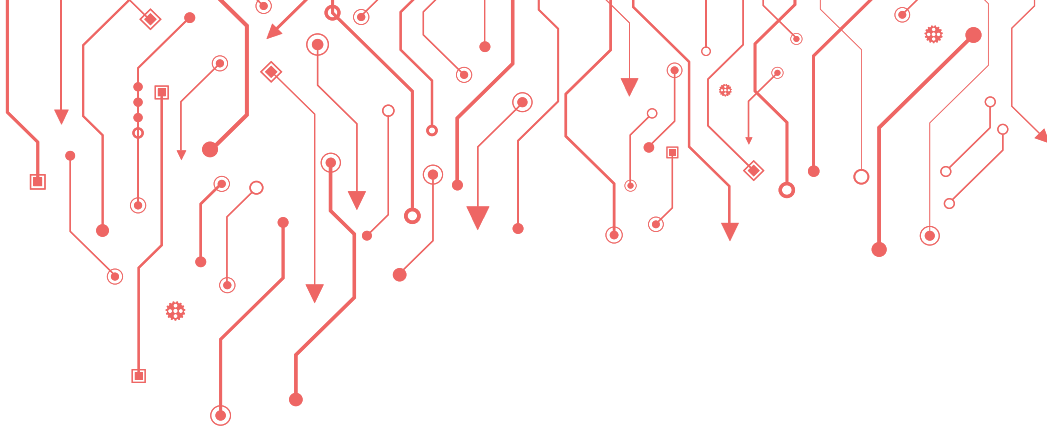
.....

.....

.....

.....





With Regards
NATIONAL CYBER SECURITY CENTER



www.ncsc.gov.bh
[#CyberWiser](https://twitter.com/CyberWiser)

