Cyber Security

Name: Ahmed Kasteer

Roll Number: 20F-0336

Section: 5C

Cyber Security is a process that’s designed to protect networks and devices from external threats. Businesses typically employ [Cyber Security professionals](https://www.simplilearn.com/tutorials/cyber-security-tutorial/how-to-become-cyber-security-engineer) to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or [CIA](https://www.forcepoint.com/cyber-edu/cia-triad). Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

Types of Cyber Crimes

[Cybercrime](https://www.simplilearn.com/bad-guys-of-cybercrime-and-the-need-for-good-guys-to-fight-back-article) 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 cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.

## **What 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.

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](https://www.simplilearn.com/white-hat-hacker-article) 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

### **Cyber Terrorists**

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

### **State-Sponsored Hackers**

They penetrate government networks, gain top-secret information, and damage information systems; paid by a hostile government

### **Hacktivists**

Promote political agendas by secretly defacing and disabling websites

Who Are Cyber Security Experts?

As [data breaches](https://www.simplilearn.com/2-billion-bits-of-info-exposed-inside-a-record-breaking-data-leak-article), hacking, and cybercrime reach new heights, companies are increasingly relying on [Cyber Security specialists](https://www.simplilearn.com/what-is-a-cyber-security-analyst-article) to identify potential threats and protect valuable data. It makes sense, then, that the[Cyber Security market](https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=Cj0KCQjwiILsBRCGARIsAHKQWLOjWyA6WwWgHuBBPEVEmPlcsMUCjbxdv0ZY2wmrOJR9InUlk4ytBxgaAi9VEALw_wcB) is expected to grow from $152 billion in 2018 to $248 billion by 2023.

Cyber Security experts usually:

* Find, test, and repair weaknesses within a company’s infrastructure
* Monitor systems for malicious content
* Identify network breaches
* Install regular software updates, firewalls, and antivirus protection
* Strengthen areas where attacks may have occurred

They work in one or more of these common Cyber Security domains to keep data safe:

* Asset security: Analyze networks, computers, routers, and wireless access points
* Security architecture and engineering: Standardize security policies and procedures
* Communication and network security: Regulate cloud storage and data transfer
* Identity and access management: Track user authentication and accountability
* Security operations: Monitor security to identify attacks
* Security assessment and testing: Test security policies to ensure compliance with industry standards
* Software development security: Create and repeatedly test code
* Security and risk management: Identify potential risks and implement appropriate security controls

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 DNS