Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Cybersecurity

- **Cybercrime** is today’s **fastest-growing** form of criminal activity.
- Cyber security protects important data and information from strangers and hackers.
- Cyber security **professionals** are responsible for protecting servers, networks, and computer systems.
- With the confidentiality of this information in mind, these experts make sure that only authorized people can access the information.

Information security

- Information security (data security specialist) protects from any unauthorized use, access, alteration or removal of information based on protection.
- helps to protect against data corruption or theft.
- Every information is a property.
- Once the information is processed, the companies make any mistakes, it requires information security to protect against use and tampering.

Cybercrime and Business

- Cybercrime is nowadays fastest-growing from of criminal activity.
- According to **Accenture**, the cost of cybercrimes to businesses will reach $5.2 trillion within the next five years.

https://www.accenture.com/

- The world has shifted, and CY is shifting with it (though not always fast enough)
- Survey report (2023*): 3000 responses-15 industries,- 14 countriess
  - CY is Part of core transformation team (53%)
  - CY is required before any solution is deployed(53%)

- *https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf#zoom=40

Cybercrime and Business

- According to **Hiscox,** an insurance carrier, the average cost of cyberattacks to small businesses is $200,000 on average

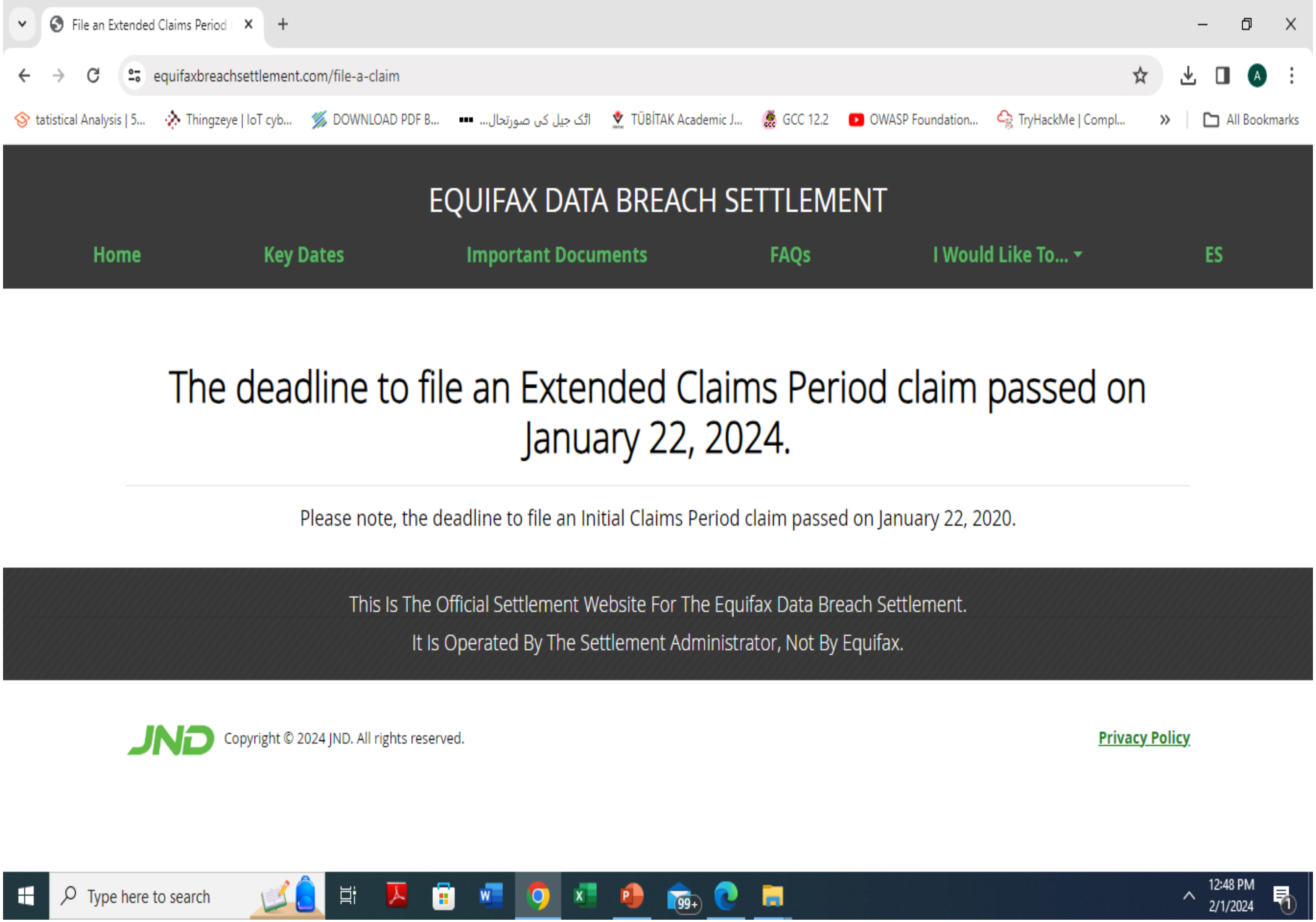
- **McAfee**, an anti-virus provider, reports that 480 new high- tech threats are introduced every minute

Current State of Cybercrime

- In 2017, **Equifax**, one of the largest consumer credit agency, was attacked.
  - Hackers stole sensitive information of 147 million people (data breach).
- Company agreed to Global settlement
  - with the Federal Trade Commission,
  - the Consumer Financial Protection Bureau, and
  - 50 U.S. states and territories
- The incident cost Equifax $600 million.
  - settlement includes up to $425 million to help people affected by the data breach

- https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Current State of Cybercrime



EQUIFAX DATA BREACH SETTLEMENT

The deadline to file an Extended Claims Period claim passed on January 22, 2024.

Please note, the deadline to file an Initial Claims Period claim passed on January 22, 2020.

This Is The Official Settlement Website For The Equifax Data Breach Settlement.

It Is Operated By The Settlement Administrator, Not By Equifax.

Current State of Cybercrime

- In 2017, **Uber** reported a data breach including personal information of 57 million customers and drivers

- The names and driver's license numbers of around 600,000 drivers in the US.

- Uber paid $148 million in regulatory fines.

- https://lifelock.norton.com/learn/data-breaches/uber-data-breach-affects-57-million-rider-and-driver-accounts

Current State of Cybercrime

- In 2018, Marriot reported that data of up to 500 million guests were exposed (including duplicate records).
  - including credit card and passport numbers
- Marriot paid $200 million in fines
- Marriott's stocks dropped by 5% (loss of 1B revenue (https://coverlink.com/case-study/marriott-data-breach/)
- One of its reservation systems was compromised
- * involvement of state owned chinses hackers?
  - From code and attack patterns
  - No sale on dark web

https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

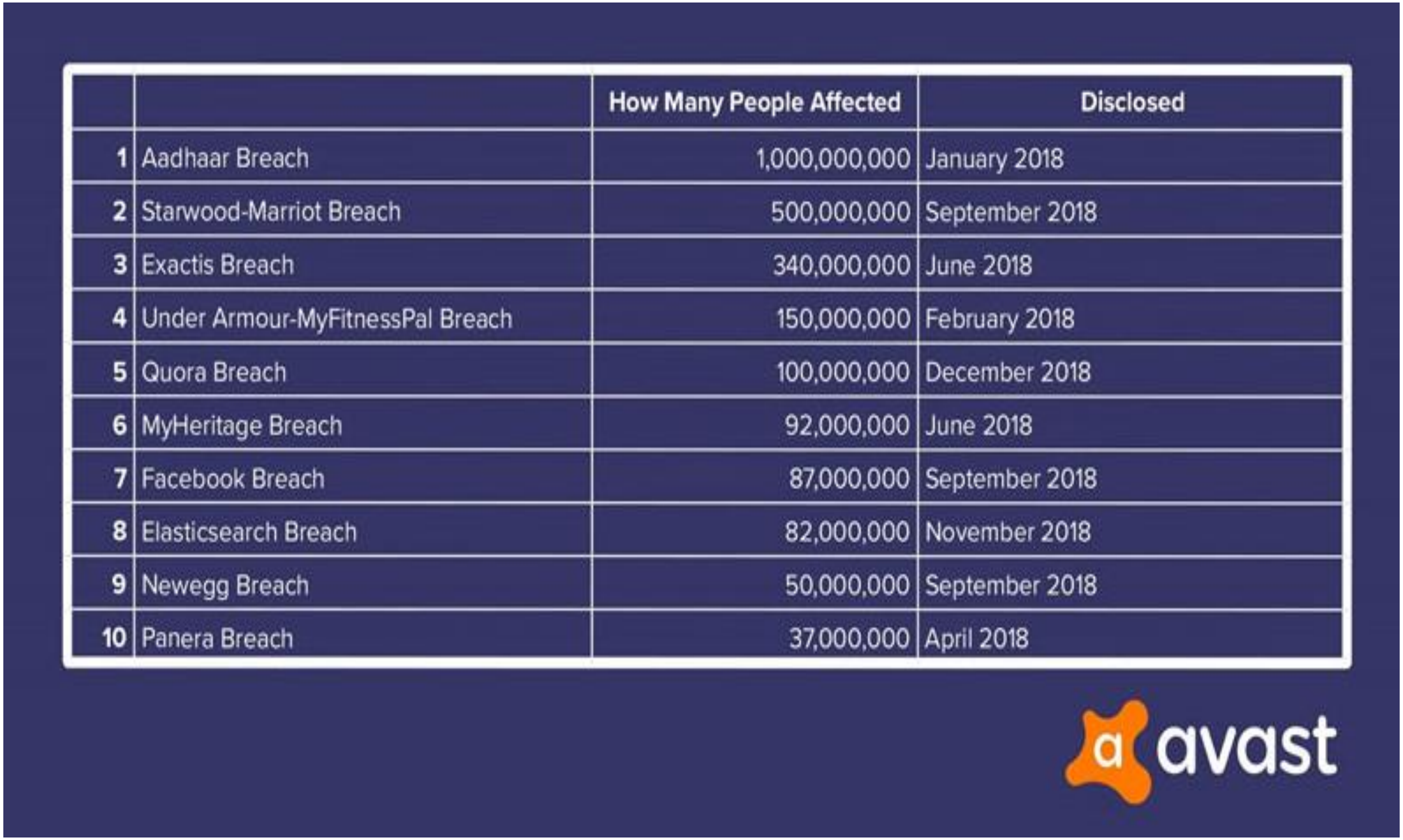
Current State of Cybercrime

- In 2018, **Aadhaar** administered by UIDAI, the world’s largest government database was breached and personal information about **1 billion** people was exposed
  - sold online for £6, report claims

UIDAI: Unique Identification Authority of India

- https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar

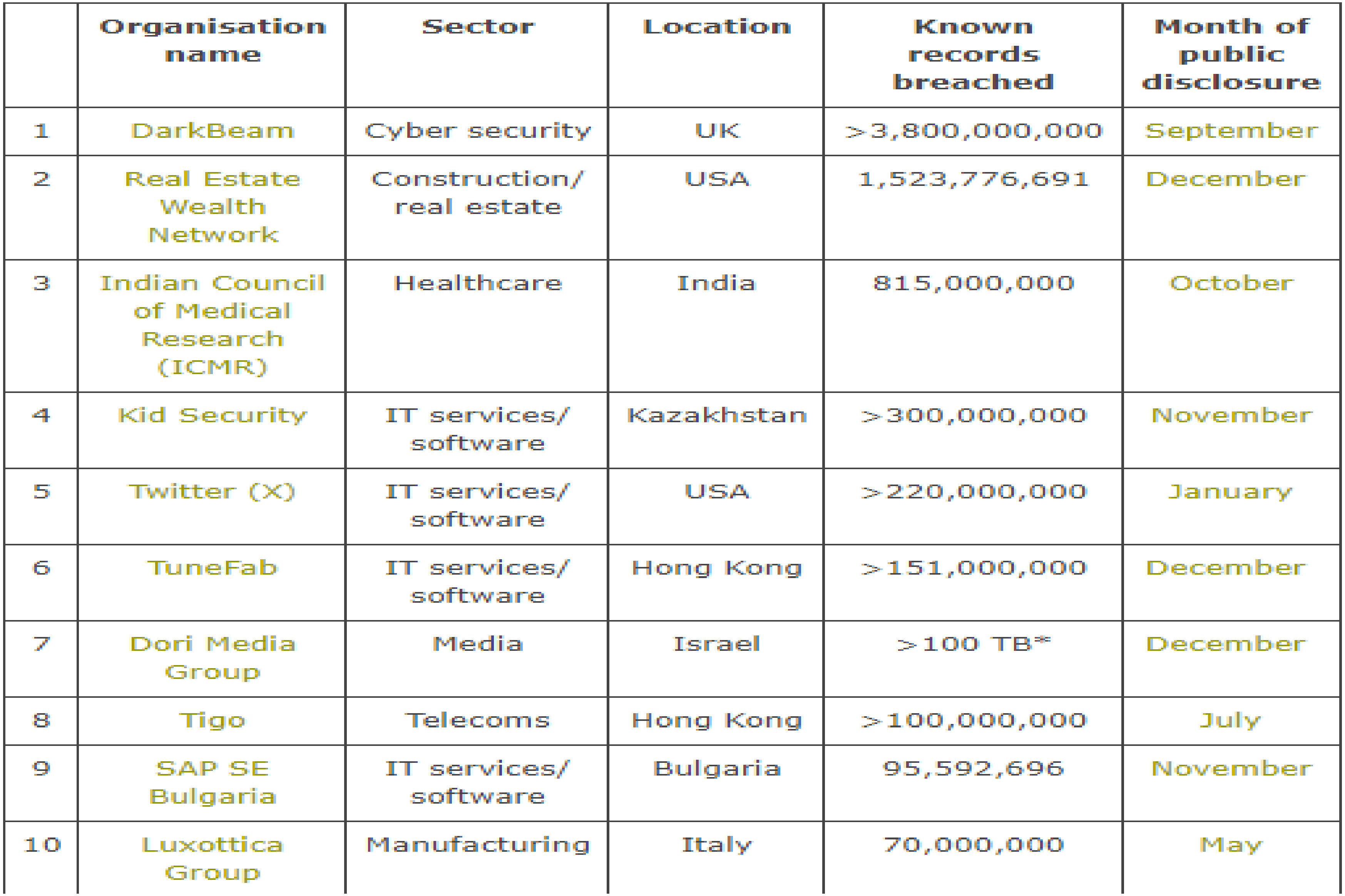
Current State of Cybercrime



		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

- https://www.moneylife.in/article/aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html
- https://blog.avast.com/biggest-data-breaches

Top 10 Data Breaches in 2023



	Organisation name	Sector	Location	Known records breached	Month of public disclosure
1	DarkBeam	Cyber security	UK	>3,800,000,000	September
2	Real Estate Wealth Network	Construction/ real estate	USA	1,523,776,691	December
3	Indian Council of Medical Research (ICMR)	Healthcare	India	815,000,000	October
4	Kid Security	IT services/ software	Kazakhstan	>300,000,000	November
5	Twitter (X)	IT services/ software	USA	>220,000,000	January
6	TuneFab	IT services/ software	Hong Kong	>151,000,000	December
7	Dori Media Group	Media	Israel	>100 TB*	December
8	Tigo	Telecoms	Hong Kong	>100,000,000	July
9	SAP SE Bulgaria	IT services/ software	Bulgaria	95,592,696	November
10	Luxottica Group	Manufacturing	Italy	70,000,000	May

- https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

Top 10 Data Breaches in 2023

- Number of incidents in 2023: 2,814.
- Number of breached records in 2023: 8,214,886,660.

- Number of incidents in December 2023: 1,351.
- Number of breached records in December 2023: 2,241,916,765.

- https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

3 Biggest Data Breaches in Dec 2023

- **Unprotected Real Estate Wealth Network: more than 1.5 billion records exposed** (property ownership data)
  - **Data breached: 1,523,776,691 records**
- **TuneFab: more than 151 million records exposed**
- **TuneFab** converts music from popular streaming platforms, including Spotify, Apple Music, YouTube and Audible, to other formats
  - **Data breached: >151,000,000 records.**
- **Dori Media Group** (international): **allegedly more than 100 TB of data exfiltrated**
  - **Data breached: >100 TB of data**
  - https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023

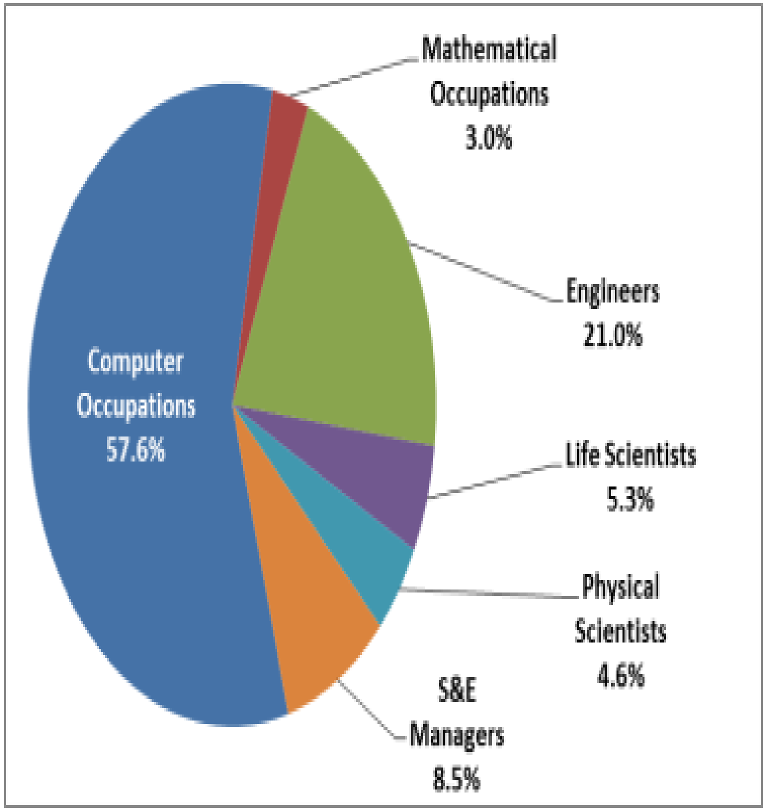
The demand for cyber and information security professionals is growing

In the current situation, the demand for security professionals is huge.

with extensive use of the Internet, more cases of abuse

Bureau of Labor Statistics.

According to the data, in 2012–2022 information security work



Hackers

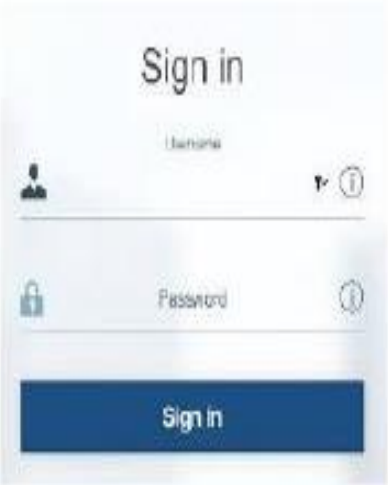
White hat hacker / Ethical hacker

Grey hat hacker

Black hat hacker

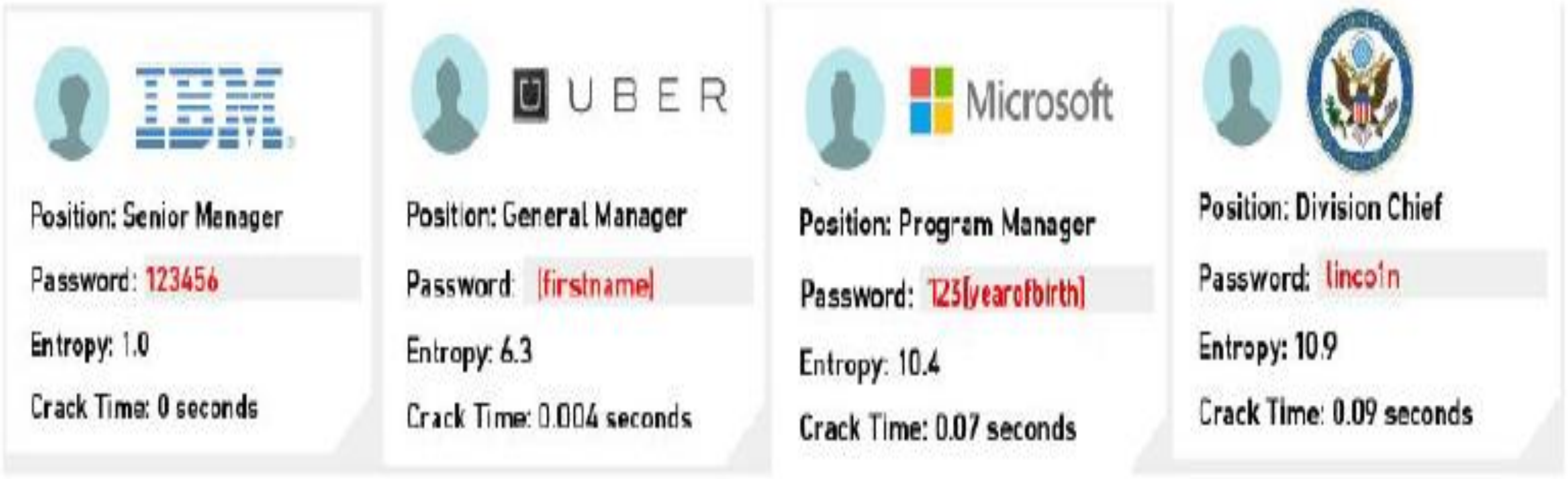
Authentication

The ability to know that a person is who he or she claims to be

			
Password	**Token**	**Smart Card**	**Biometric Authentication**

Why One-factor Authentication Fails

Research on 10,000,000 passwords



Position: Senior Manager

Password: 123456

Entropy: 1.0

Crack Time: 0 seconds

Position: General Manager

Password: [firstname]

Entropy: 6.3

Crack Time: 0.004 seconds

Position: Program Manager

Password: 123[yearofbirth]

Entropy: 10.4

Crack Time: 0.07 seconds

Position: Division Chief

Password: linco1n

Entropy: 10.9

Crack Time: 0.09 seconds

Multi-Factor Authentication

- Multi-factor authentication is a method that grants user access after presenting two or more pieces of evidence proving his/her identity.
  - **Example:** Password + code sent to your mobile
- Many schools, companies, online services use two-factor authentication.
- To withdraw money from ATM, you need correct card and password combination.

Good Browsing habits:

- Chrome: Incognito mode
- Clear DNS Cache: delete all unnecessary IPs, Cmd / ipconfig / Flushdns
- Antivirus
- Password manager
- Ad blocker
- Avoid danger websites, links, files
- Use VPN
- Check app permissions

In what areas do you need to study to work in cybersecurity

- Information security analyst
- Information security coordinator
- **Cybersecurity analyst**
- Information security manager
- Information security officer
- Information security engineer
- **Software security specialist**
- Cryptographer
- **Forensic specialist**
- Chief information security officer

Cybersecurity Breakdown

- A large part of cybercrime is so-called traditional crime, such as fraud, drug-related crime and money laundering, but information networks bring new ways of carrying them out.

Cybercrime classification

- Information technology crime targeting information technology and networks
  - Data breaches
  - Data hijacking by malware
  - Cyber attacks, such as denial-of-service attacks
- Offences committed using information technology and information networks

Cybersecurity Breakdown

Cybercrime classification

- Offences committed using information technology and information networks
  - Fraud
  - Phishing
  - Ransomware
  - Drug-related crime
  - Money laundering
  - Hate crime
  - Sexual violence
  - Terrorism-related offences, including dissemination of terrorist material, recruitment of new members and violent radicalisation
  - Internet gambling

Cybersecurity Breakdown

Cybercrime classification

- Offences committed using information technology and information networks
  - **Fraud**
    - Love betrayals
    - Investment fraud
    - E-commerce scams
    - Means of payment fraud
    - Scam letters
    - The fake police phenomenon
    - Offer letters in the form of an invoice

Cybersecurity Breakdown

- Since the internet and other digital information networks operate independently of physical location,
  - cybercrime is often international in nature.
  - For example, the perpetrators and victim of a crime may be located in different countries.
  - As a result, a significant proportion of cybercrimes are never reported to the police.
  - Therefore, a lot of cybercrime remains unsolved and many victims do not seek help.