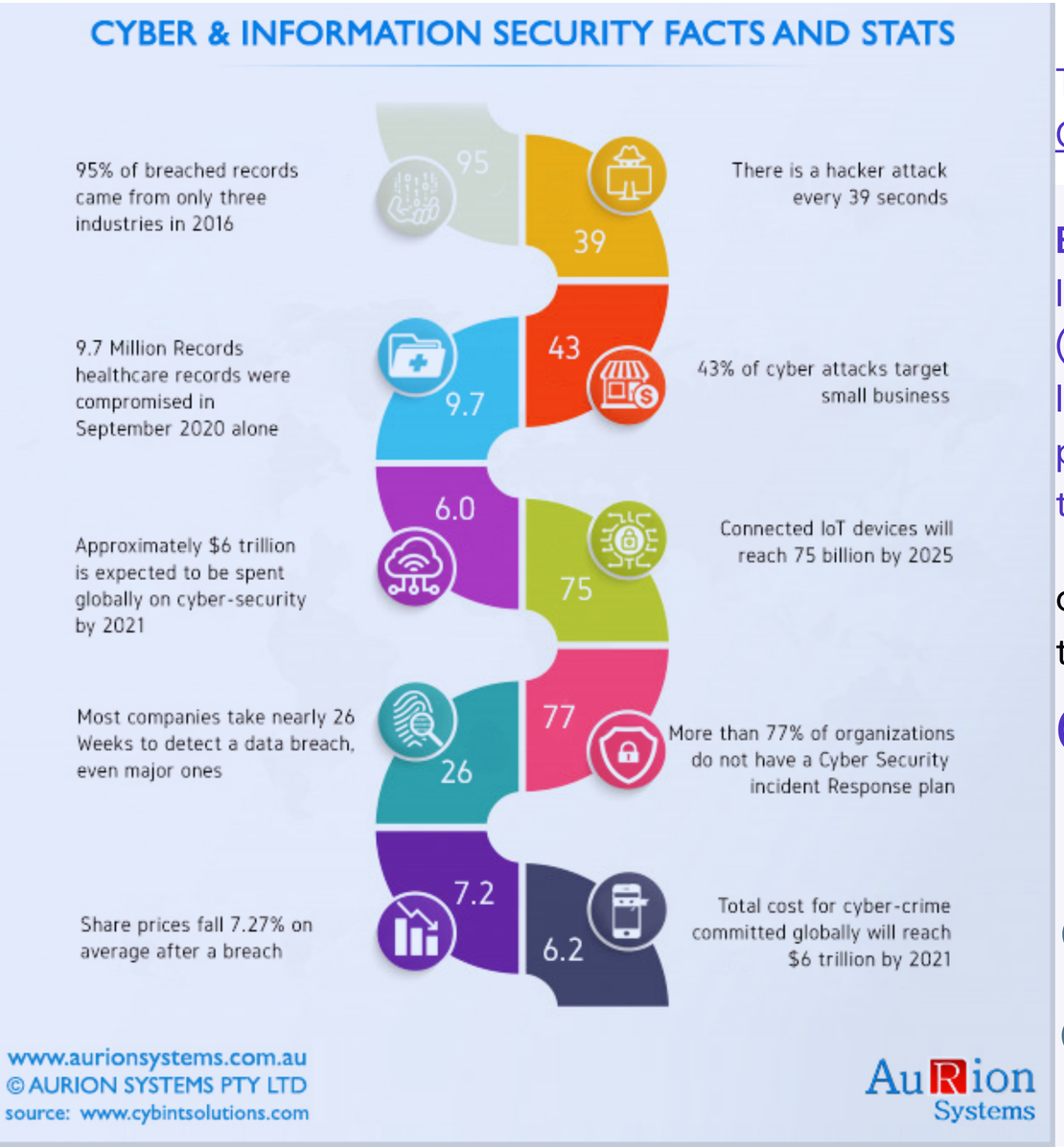
# An introduction to CyberSecurity and Cyberthreats

*Presented by: Fatma LARIBI*

# What's Cybersecurity ?

Cybersecurity is The protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems (access, alter, delete, destroy...)

# The increasing number and consequences of cyber attacks




The global cyber threat continues to evolve at a rapid pace
Cybercrime Up 600% Due To COVID-19 Pandemic

**Examples of cyber attack incidents:**
In Tunisia one of the most recent cyber attacks was a phishing attack on BIAT (a Tunisian bank) on february 18th 2021, that infected all the computers.
In 2020, a Twitter breach targeted 130 accounts, including those of past presidents and Elon Musk, resulted in attackers swindling $121,000 in Bitcoin through nearly 300 transactions

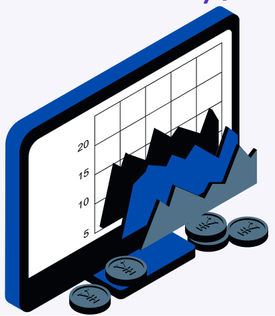
check out: https://cybermap.kaspersky.com/ for a real-time map of cyber threats:

## Consequences on businesses

01 financial loss (arising from theft of corporate information or money)

02 Reputational damage (loss of customers, less profits)

03 Legal consequences due to client data theft



# Types of Cyber attacks

## Malware

malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

## Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information

## Man-in-the-middle attack

occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data. Points of entry: unsecure wifi or malware.


## Denial-of-service attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

## SQL injection

occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

# Causes of data breaches

## Individuals

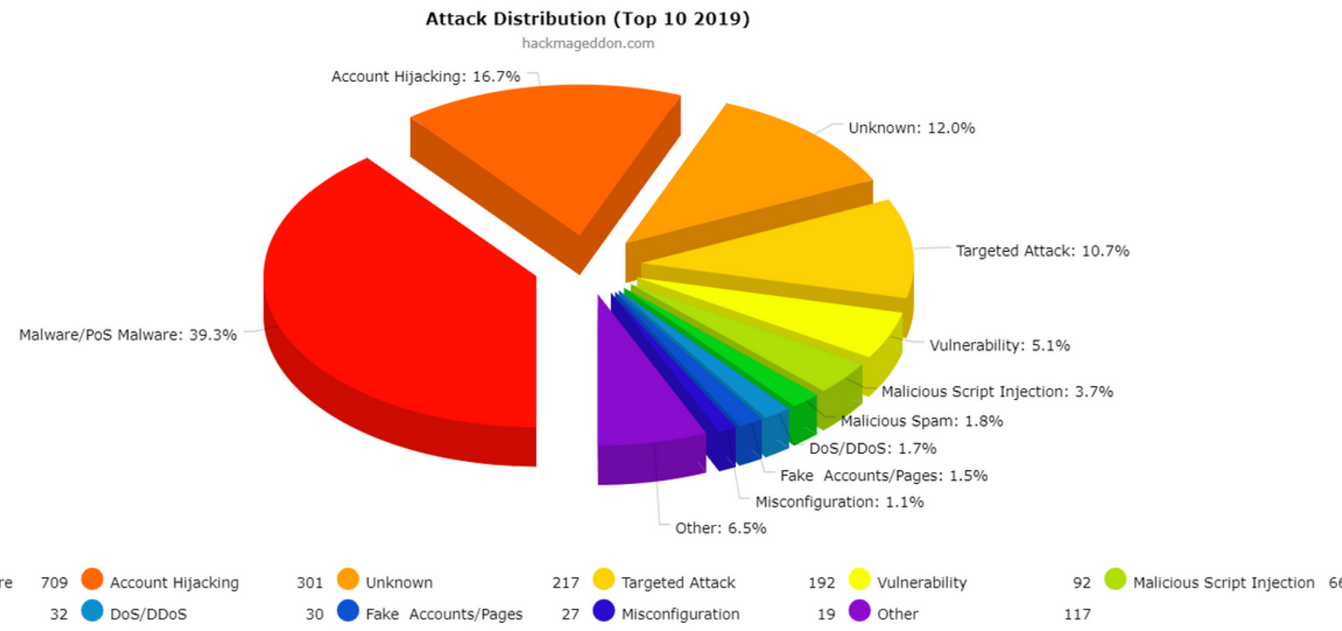
- Password vulnerability: using common, simple and easy to remember passwords.They are very easy to crack through brute-force attacks  or dictionary attacks... In fact Nate Anderson a newbie to password cracking, could decypher half of 16,000 cryptographically hashed passcodes in a couple of hours.
  Source: https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/
  To test your password vulnerability: https://howsecureismypassword.net/

- According to Rob Sobers from Inside out Security Blog, 95% of cybersecurity breaches are caused by human error

## Enterprises

- System vulnerabilities
- No good security mechanisims: use of outdated encryption algorithms like md5...

Most attacks are  Malware (ransomware)

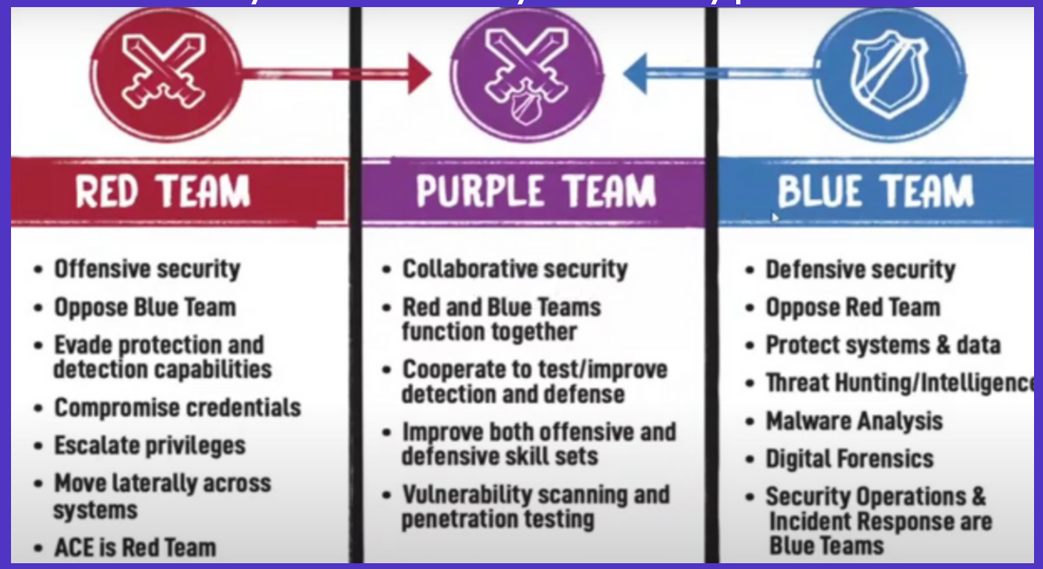


# How to prevent cyber attacks

-Bug bounty programs like hackerone or bugcrowd

-A good cybersecurity team

cybersecurity team types




-Dummy computer systems called honey pots : used to attract attackers

-Firewalls: filter the incoming and outgoing traffic from your device to safeguard your network

-Randomize passwords and use a password manager

-Beware of public wifis

-Use an antivirus software

# Thank you for your attention !

## The Importance of Cybersecurity and Security Technology


**Safety is key in protecting personal information, intellectual property, and data**

Without a supreme investment in cybersecurity, the stability, the hard-earned progress, and precious company information will be all for nothing.

## Some of the not mentioned resources

https://www.hackmageddon.com/2020/01/23/2019-cyber-attacks-statistics/
https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
https://www.universnews.tn/eco-business/exclusif-la-biat-victime-aujourdhui-dune-mega-cyber-attaque/
https://purplesec.us/resources/cyber-security-statistics/