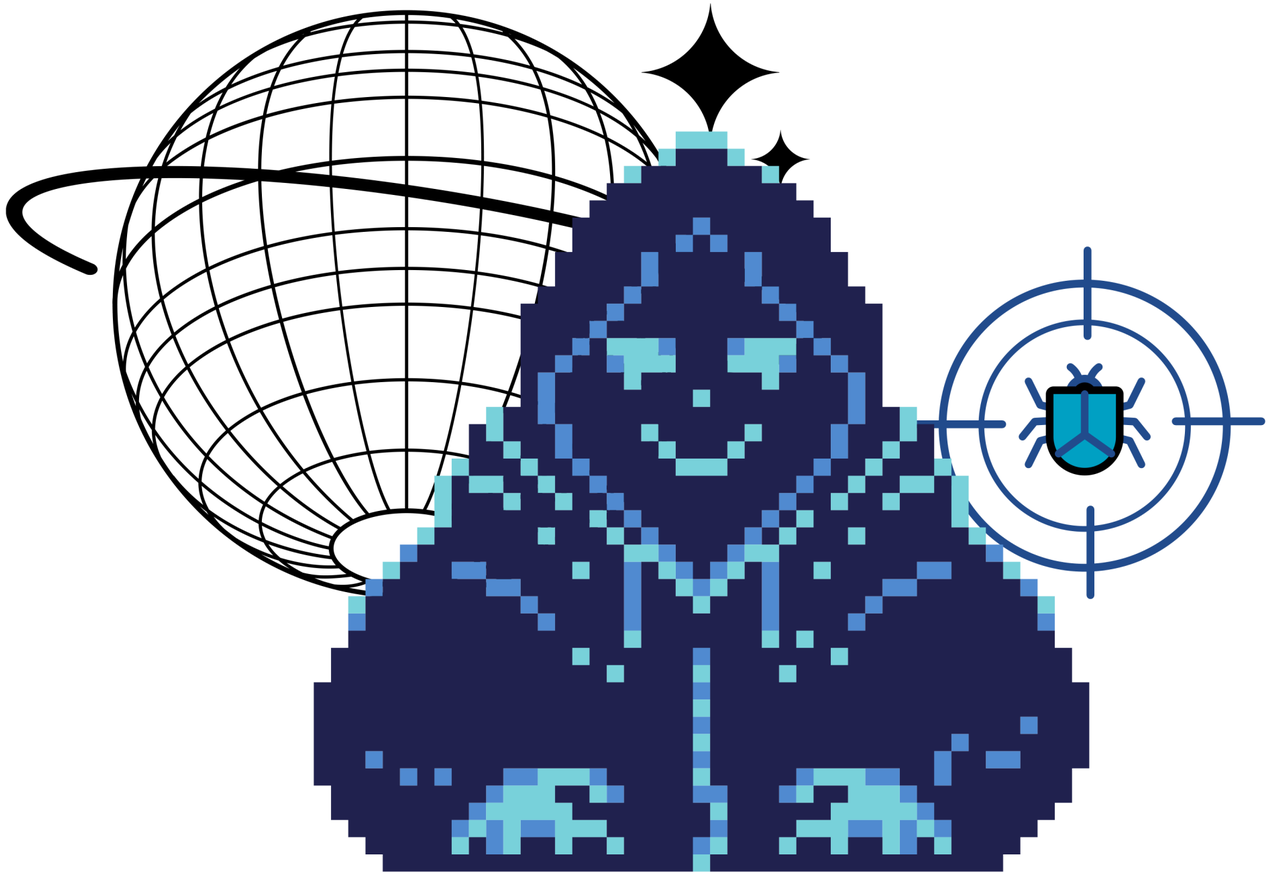
Oussama A. Belaiche present :

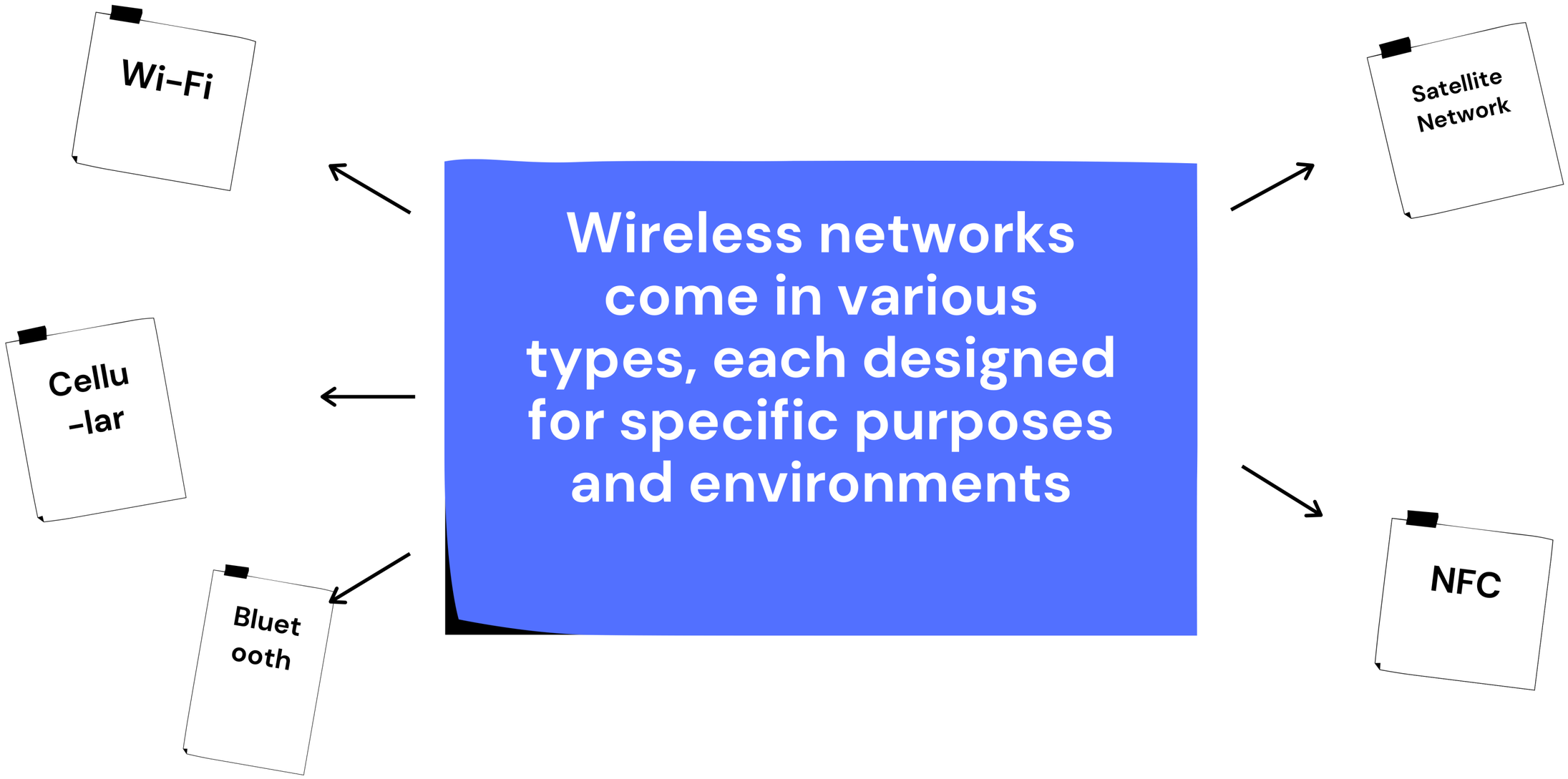
Wireless network attacks & Testing



Cybersecurity

Wireless Network

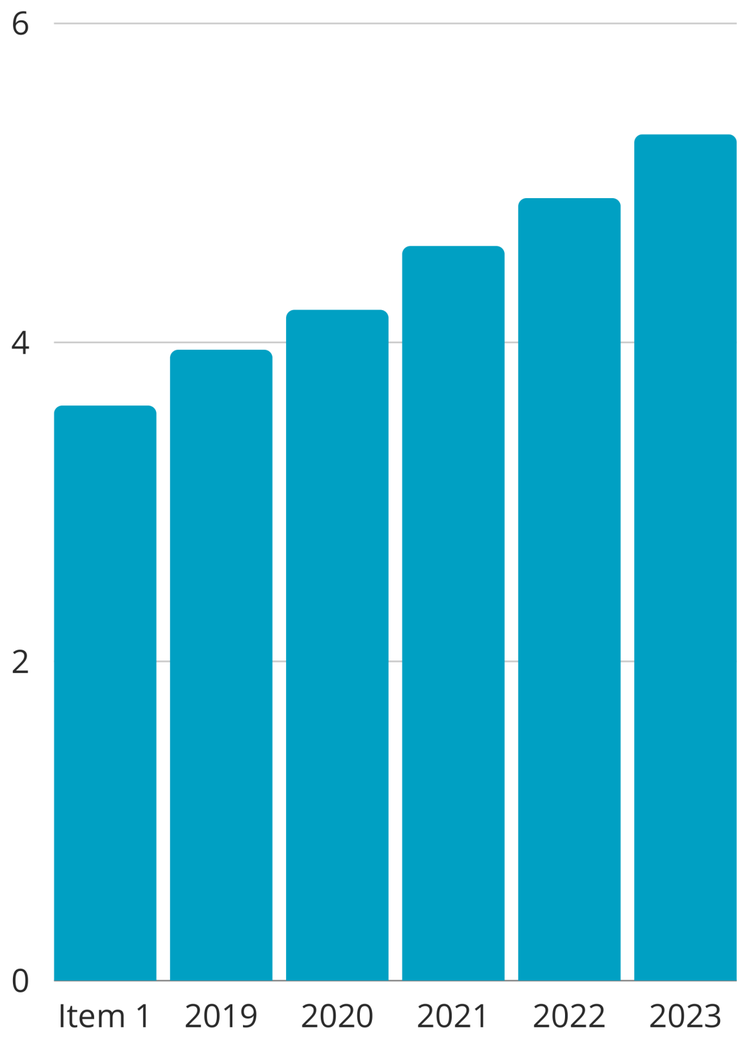
A wireless network is a type of computer network that uses wireless data connections between network nodes. It enables devices to communicate and connect to the internet without using physical wired connections.



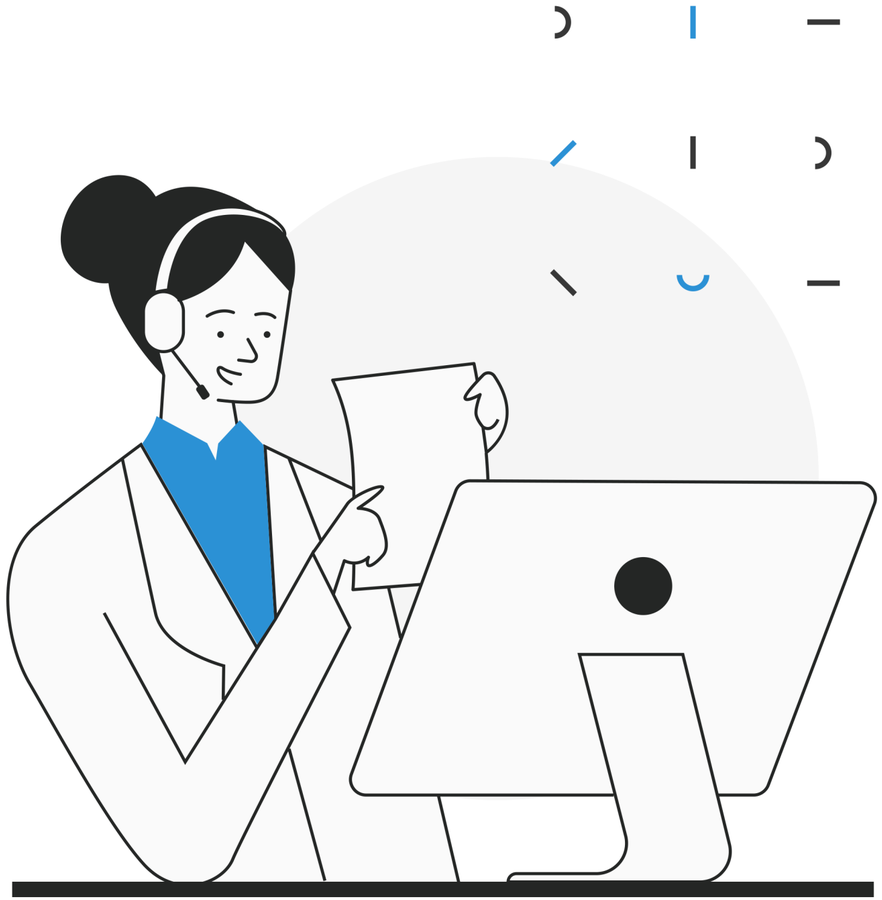
NFC allows for communication between devices in close proximity (usually a few centimeters)

5.3 Billions people in the world use the WN !

65 % of the population in the earth !



Uses of Wireless Network



COMMUNICATION

The Internet facilitates instant messaging, email, video calls, and social media, connecting individuals worldwide.

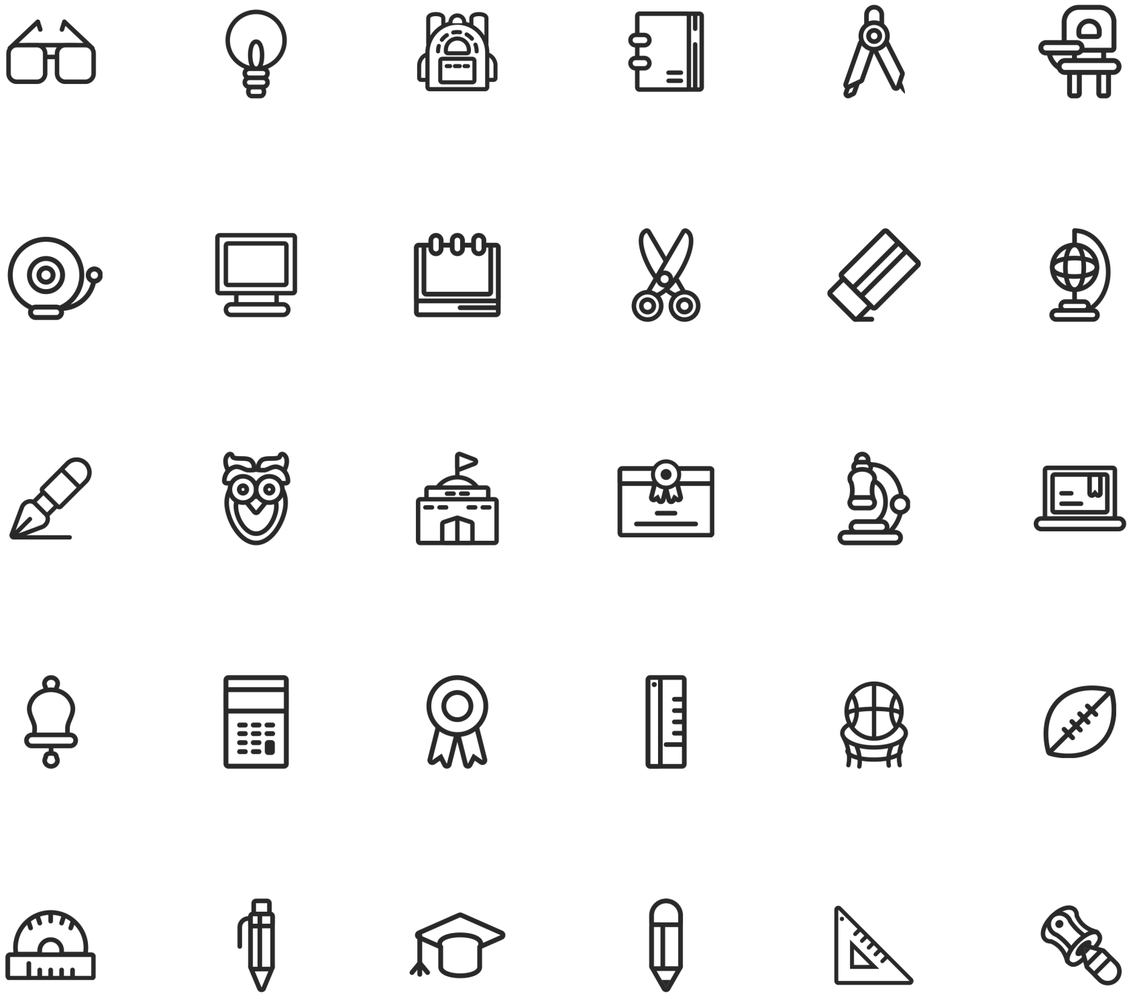
EDUCATION

The Internet provides a platform for online learning, courses, and resources, enabling self-education and skill development.

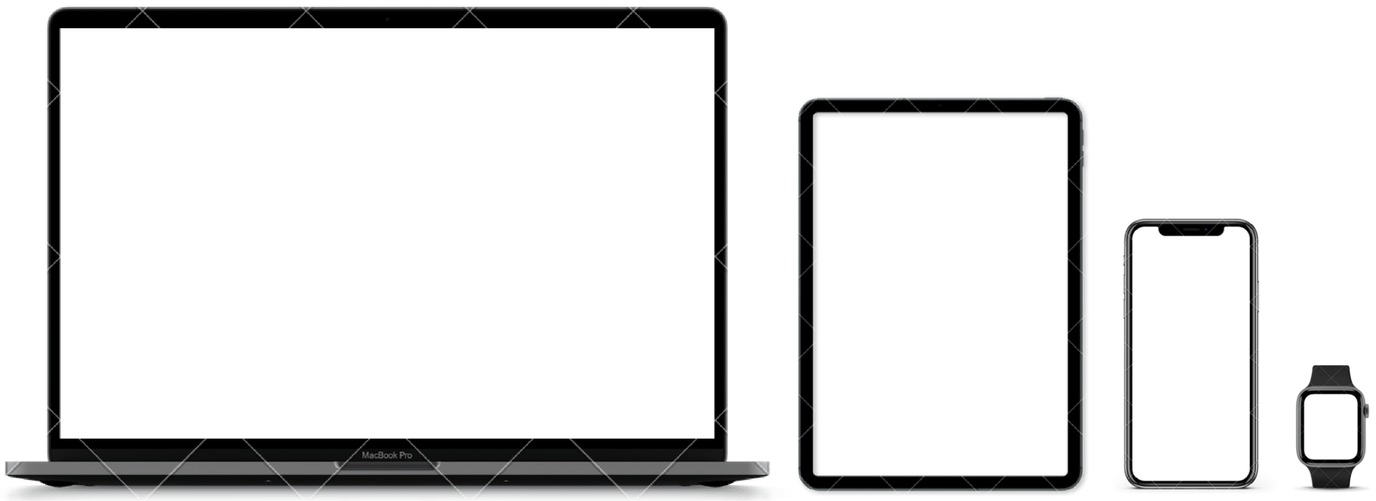
BUSINESS

It is a powerful tool for commerce, enabling businesses to reach a global audience, conduct transactions, and market products or services online

We can use the wireless network in **any thing !!**

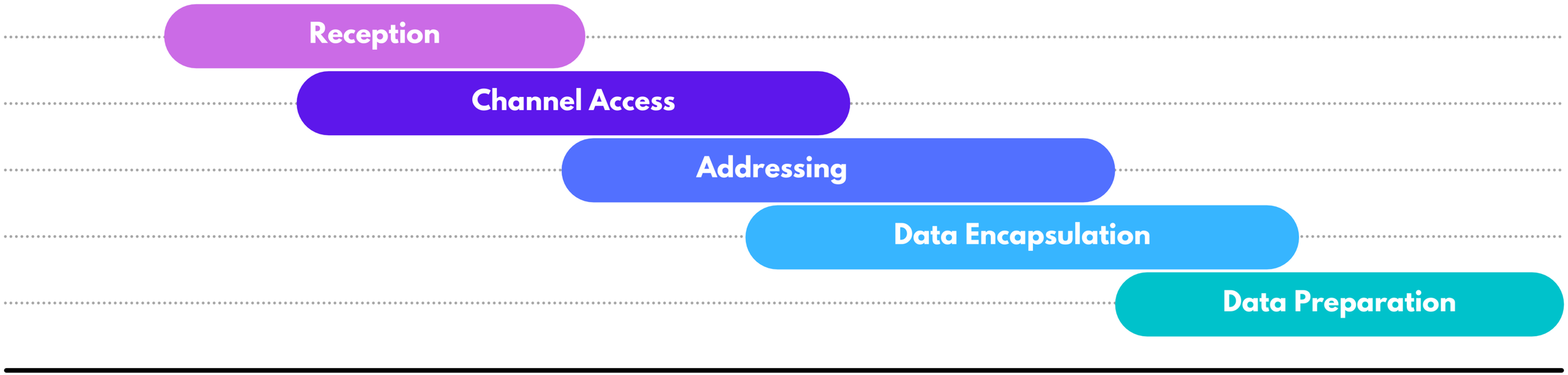


How devices Use WN



RoadMap

for every device to send data



Data Preparation

The device prepares the data for transmission

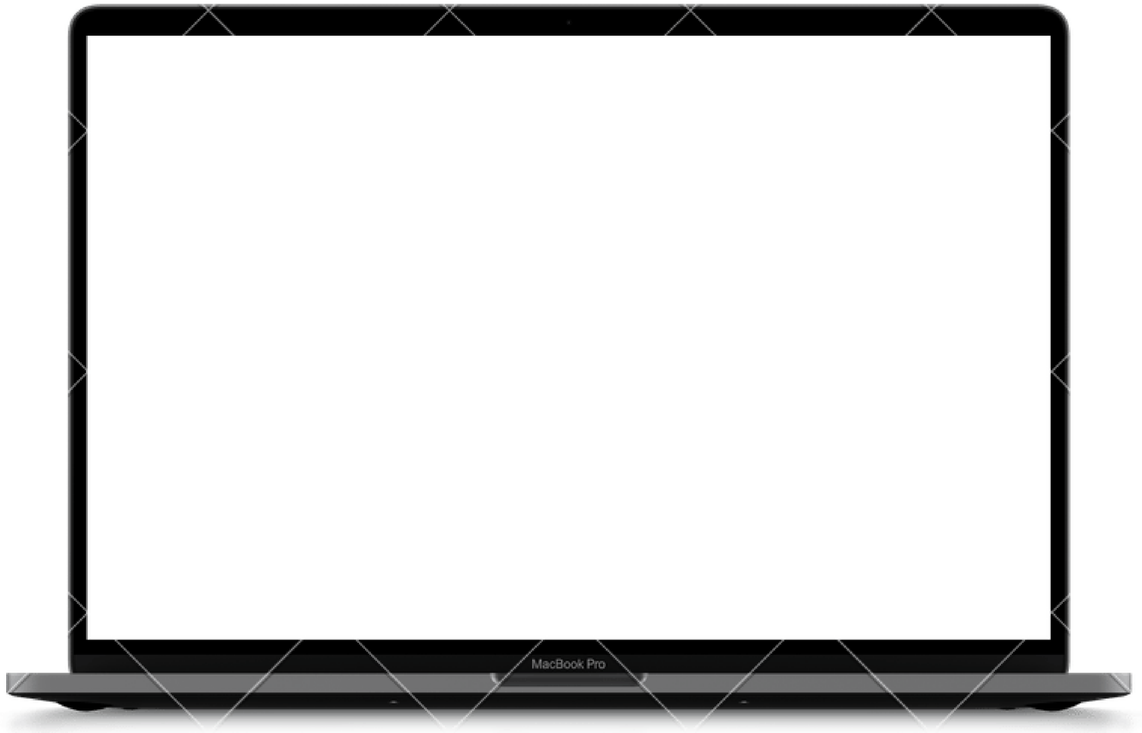
01 text messages

02 images

03 videos

Addressing

The device identifies the destination device's unique address



Channel Access

The device gains access to the wireless medium (such as the Wi-Fi channel)

Encapsulation

The data is broken down into smaller units called packets

01 **Head :** Contains control information like the source and destination addresses, sequence numbers, and error-checking codes.

02 **Payload:** This is the actual data being sent

03 **Trailer:** Contains error-checking information to ensure the packet's integrity during transmission.

Reception

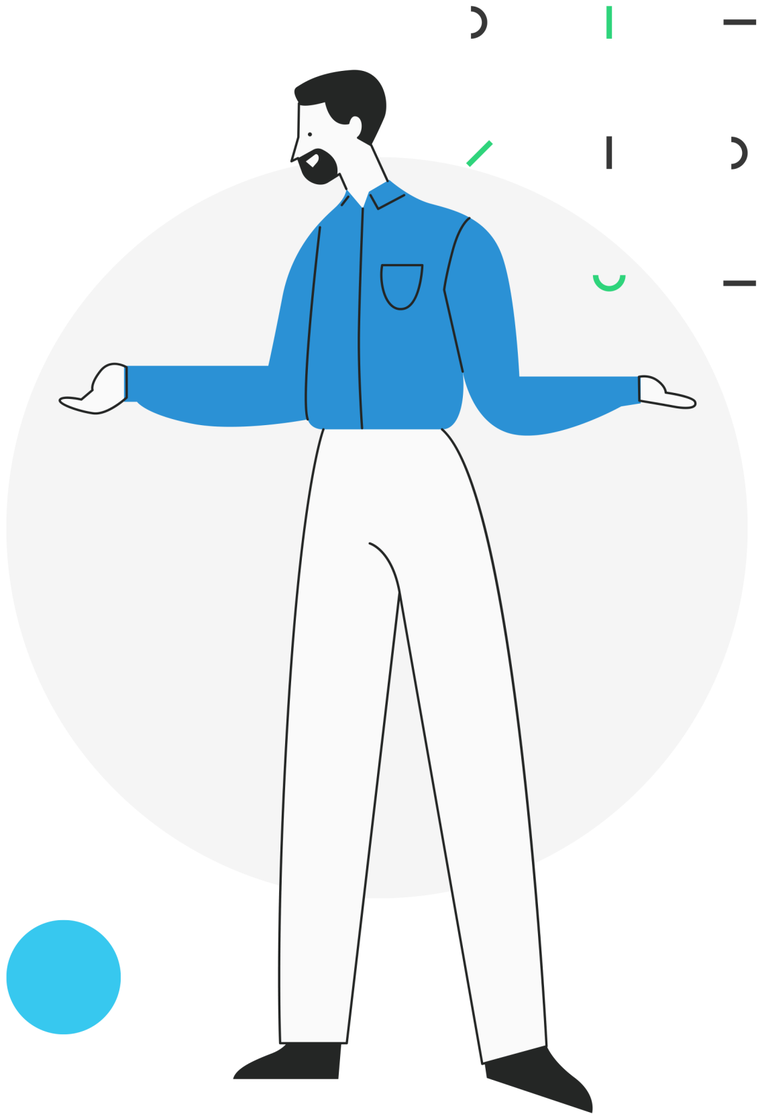
The receiving device's captures the transmitted radio signals.

01 demodulates the radio signals to extract the digital data

02 decodes the packets to retrieve the original information.

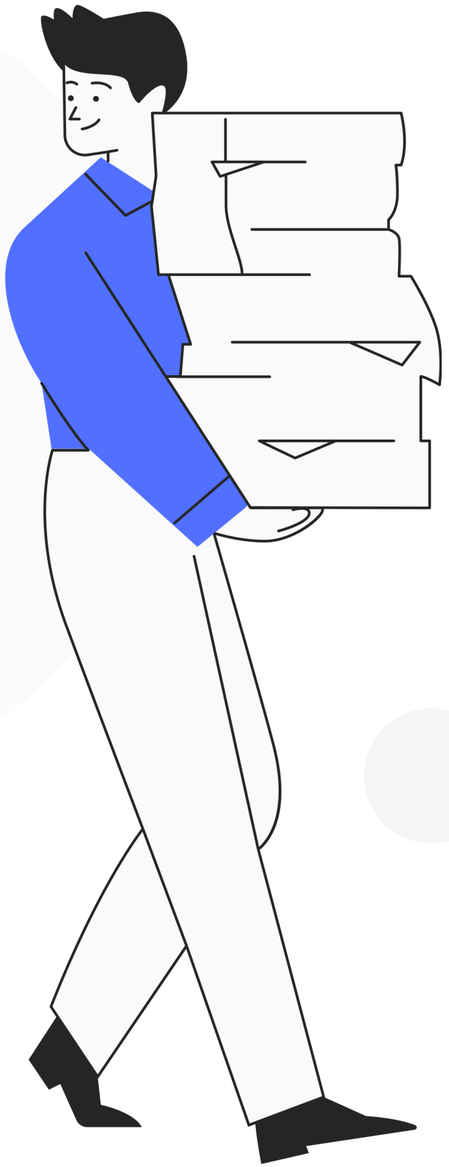
WHITE SIDE

On the white side, the Internet serves as a global platform for positive activities. It facilitates legitimate communication, education, commerce, and collaboration. Social media, e-commerce, and reputable online services contribute to the Internet's constructive aspects, showcasing its potential as a force for good in the modern world.



DARK SIDE

The dark side of the Internet involves clandestine activities on the hidden corners of the web, including the notorious Dark Web. Cybercriminals engage in illegal trades, hacking, and other nefarious activities, exploiting the anonymity provided by online tools and cryptocurrencies.



Objectives of the Presentation

RAISE AWARENESS ABOUT WIRELESS SECURITY RISKS

Clearly articulate the potential risks and vulnerabilities associated with wireless networks

PROMOTE BEST PRACTICES FOR WIRELESS SECURITY TESTING

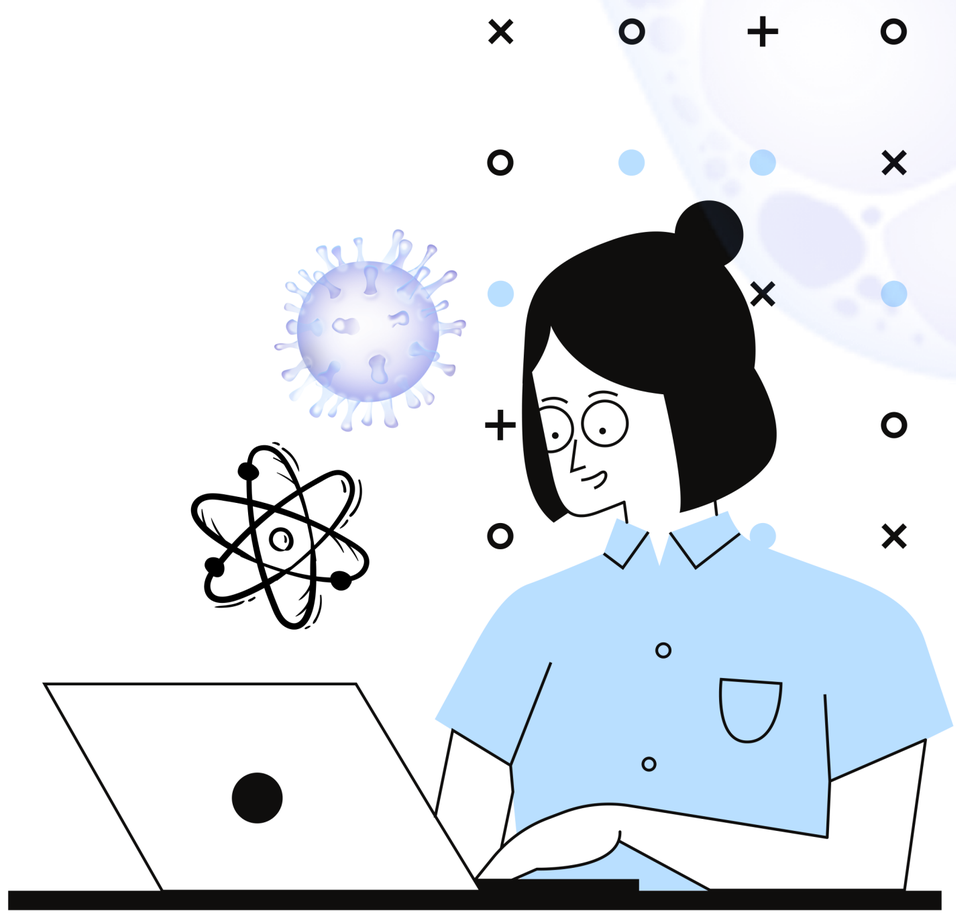
Educate the audience on effective methods and tools used in wireless security testing

EMPOWER THE AUDIENCE WITH PRACTICAL SKILLS:

Offer hands-on demonstrations or simulations of common wireless attacks and testing techniques.

WIRELESS NETWORK ATTACKS

A wireless network attack is an unauthorized attempt to exploit vulnerabilities in a wireless communication system.

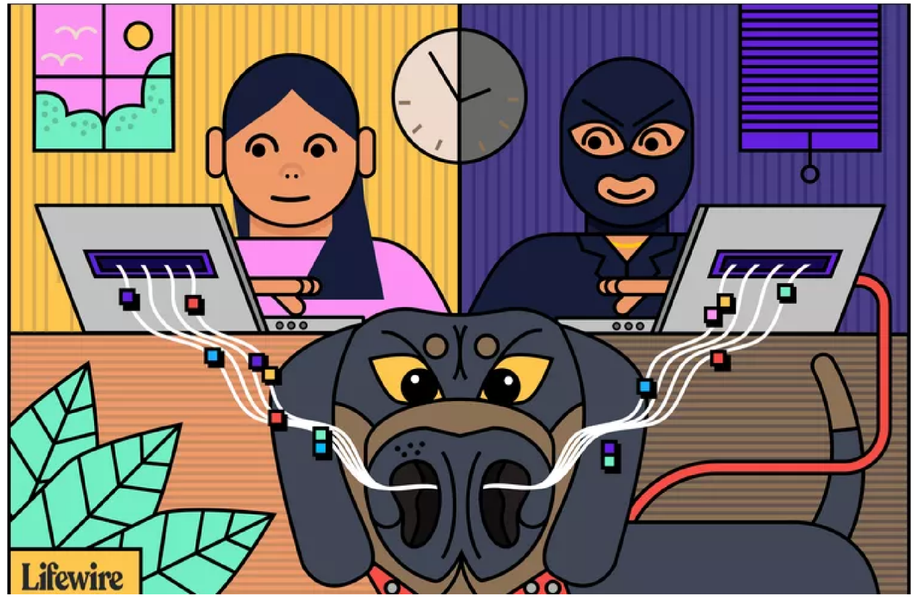


The most common attacks in wireless networks

There are numerous wireless network (WN) attacks that can significantly impact the security and functionality of wireless systems.

Sniffing Attacks

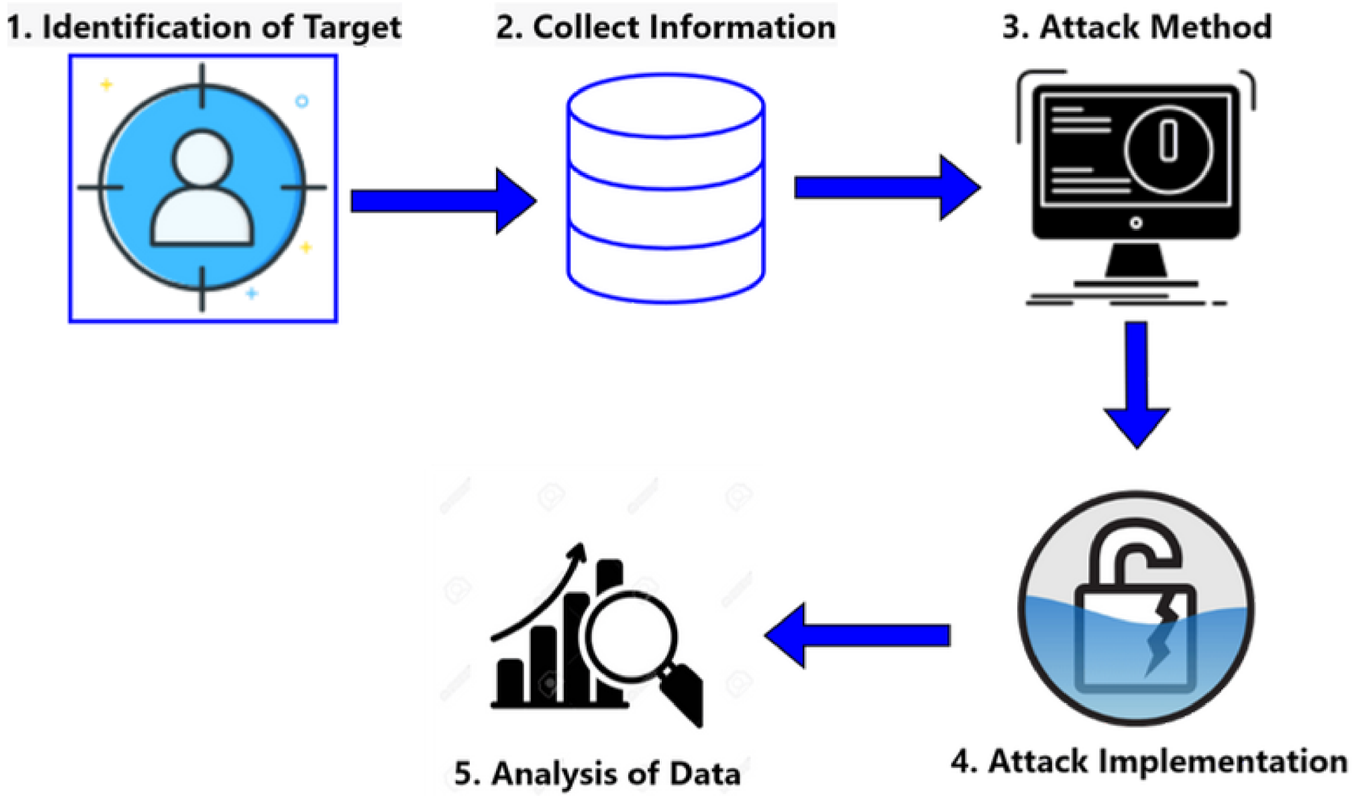
In the realm of wireless network security, one of the most insidious threats is the sniffing attack. This form of cyber intrusion involves **the unauthorized interception of wireless transmissions, allowing attackers to eavesdrop on sensitive data exchanges.**
(we use malwares or any malicious program to do it)



Attack Stages

Packets Sniffing Attacks

PACKETS SNIFFING ATTACK STAGES



IDENTIFYING A TARGET

The first step is identifying a target for the attack, such as a specific individual or organization. As soon as the attacker identifies the target

COLLECT INFORMATIONS :

The attacker picks a specific person, group, or organization as their target. They then gather information about the target, like how they communicate and any **weaknesses** in their systems that could be exploited.

METHOD SELECTION

Once they have the information, the attacker chooses a method to carry out the attack. This could involve things like tapping into unsecured networks, **using malicious software (malware)** to access devices, or utilizing specialized hardware.

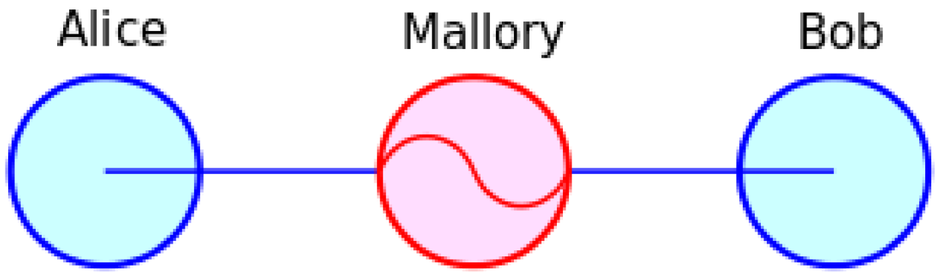
EXECUTING THE ATTACK

With the method chosen, the attacker launches the attack on the target's system, gaining access to their communication or data.

Attack Implementation

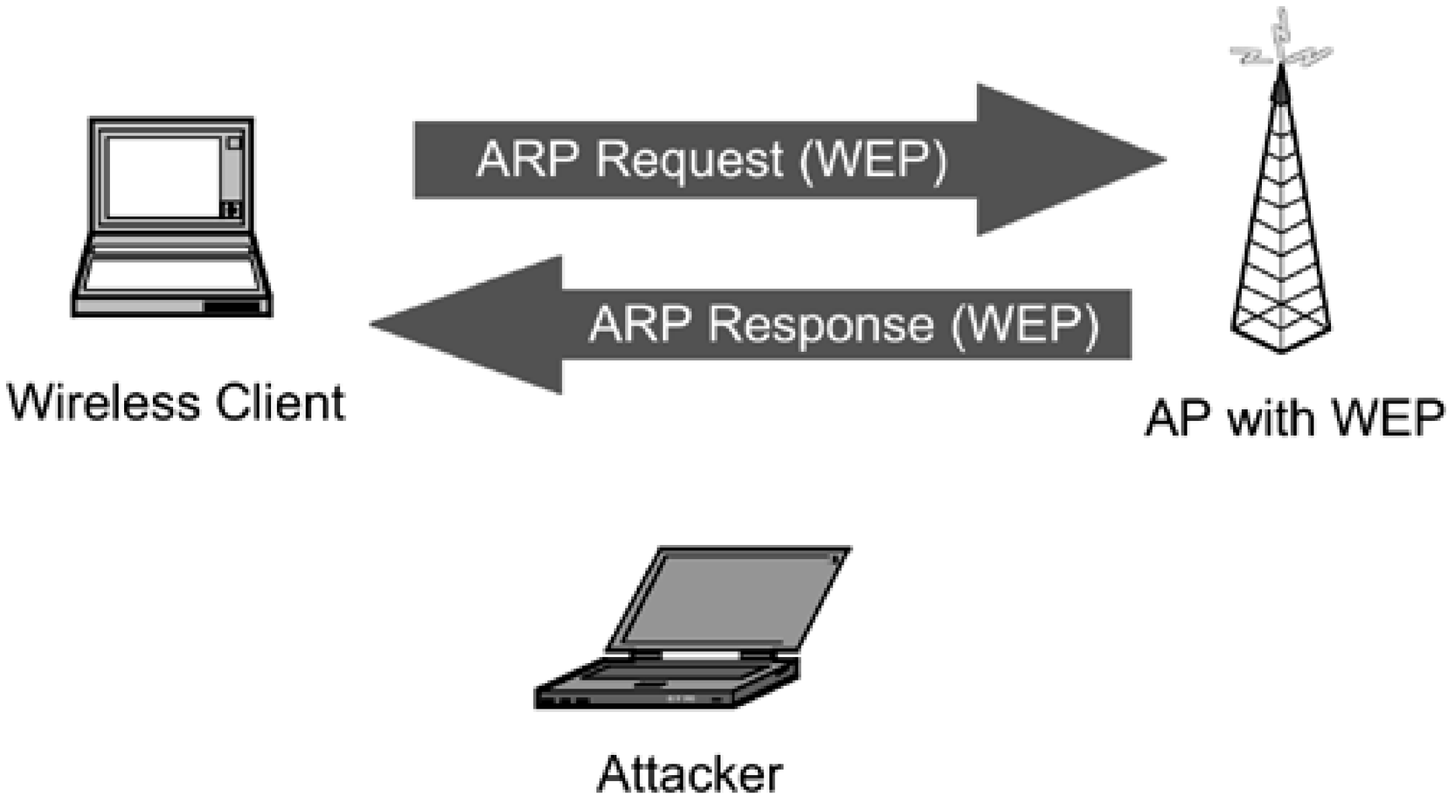
Man-in-the-Middle (MitM)

attackers position themselves between two communicating parties, intercepting and potentially altering the flow of information. This breach of communication confidentiality poses a serious risk to data integrity and privacy



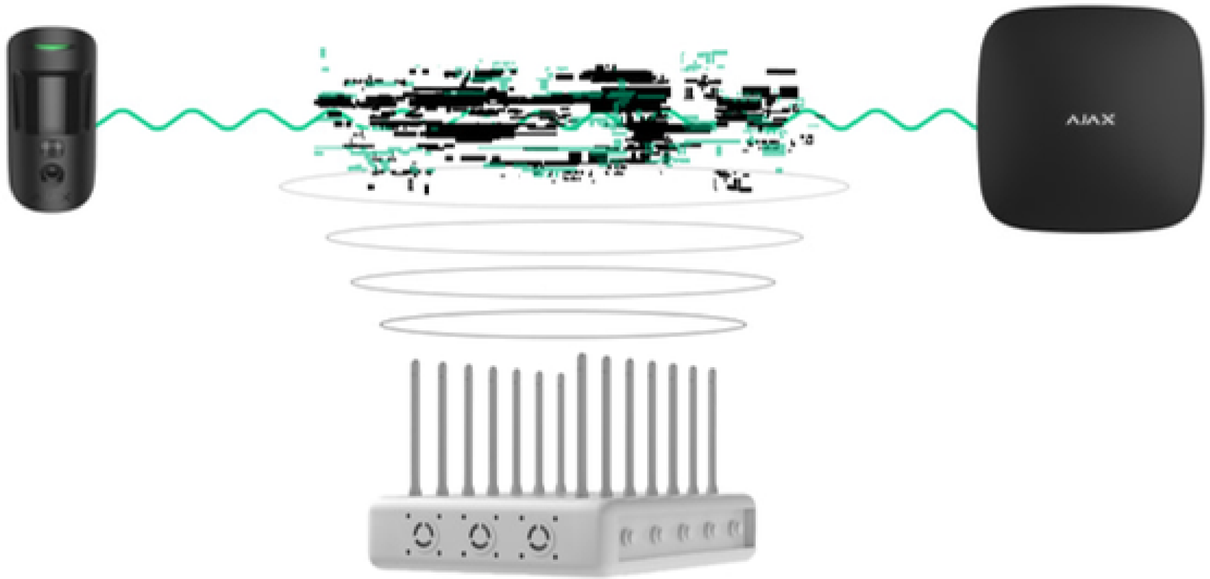
WEP/WPA/WPA2 Cracking

cyber adversaries employ various techniques to exploit weaknesses in these encryption methods. Understanding the intricacies of these attacks is paramount for fortifying wireless networks against potential breaches and ensuring the robustness of data protection mechanisms.



Wireless Jamming

Wireless Jamming" refers to the deliberate interference with radio frequency signals, causing disruption or denial of service. This disruptive technique involves flooding the targeted wireless environment with excessive and often random radio frequency noise, hindering the normal operation of wireless communication



Attack Targets

ORGANIZATIONS SYSTEMS

Schools and universities are targets for data breaches, intellectual property theft, and disruption of educational services

INDIVIDUAL PC’S

Residential Wi-Fi networks are targeted for unauthorized access, leading to potential privacy invasion and data theft.

GOVERNMENT ENTITIES

Military networks and defense systems are high-priority targets for espionage, disruption, and the theft of classified information.

WEBSITES

Website attacks, ranging from data breaches to service disruptions, pose significant challenges to the integrity and security of online platform

MORE TARGETS

IMPACTS OF SNIFFING ATTACK

DATA EXPLOITATION

The attacker might use the information for various purposes, such as identity theft, financial fraud, corporate espionage, or to gain a competitive edge in business.

FURTHER ATTACKS:

If the initial attack was successful, the attacker might continue to exploit the compromised system or launch additional attacks, potentially targeting other systems or entities.

IMPACTS OF SNIFFING ATTACK

DATA SALE OR RANSOM

In some cases, attackers may sell the stolen data on the dark web or use it as leverage for ransom demands, threatening to release sensitive information unless a ransom is paid.

DETECTION :

Unusual Network Behavior such as slow internet speeds

Unexplained Data Loss: Sudden data loss or unauthorized access to confidential information might suggest a breach.

Login Anomalies: logins from unfamiliar locations on their accounts

PREVENTION :

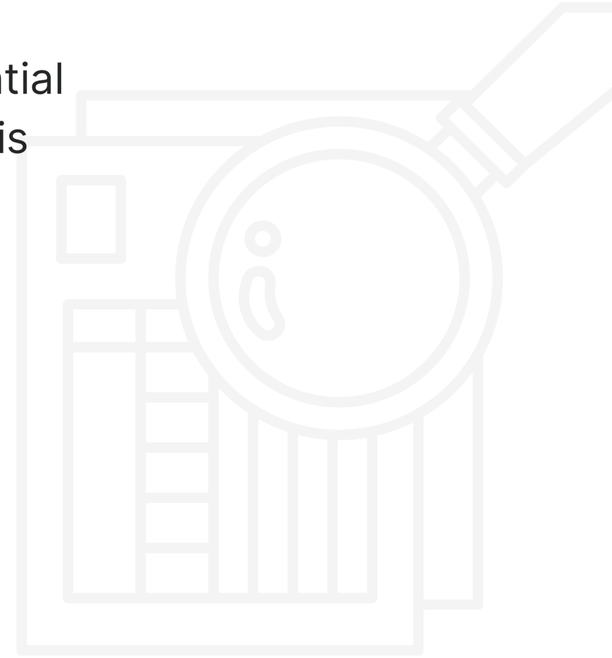
End-to-End Encryption : Employ robust encryption protocols

Virtual Private Networks (VPNs): VPNs create secure tunnels for data transmission

ACLs: Use ACLs to control network traffic and prevent unauthorized access to sensitive areas.

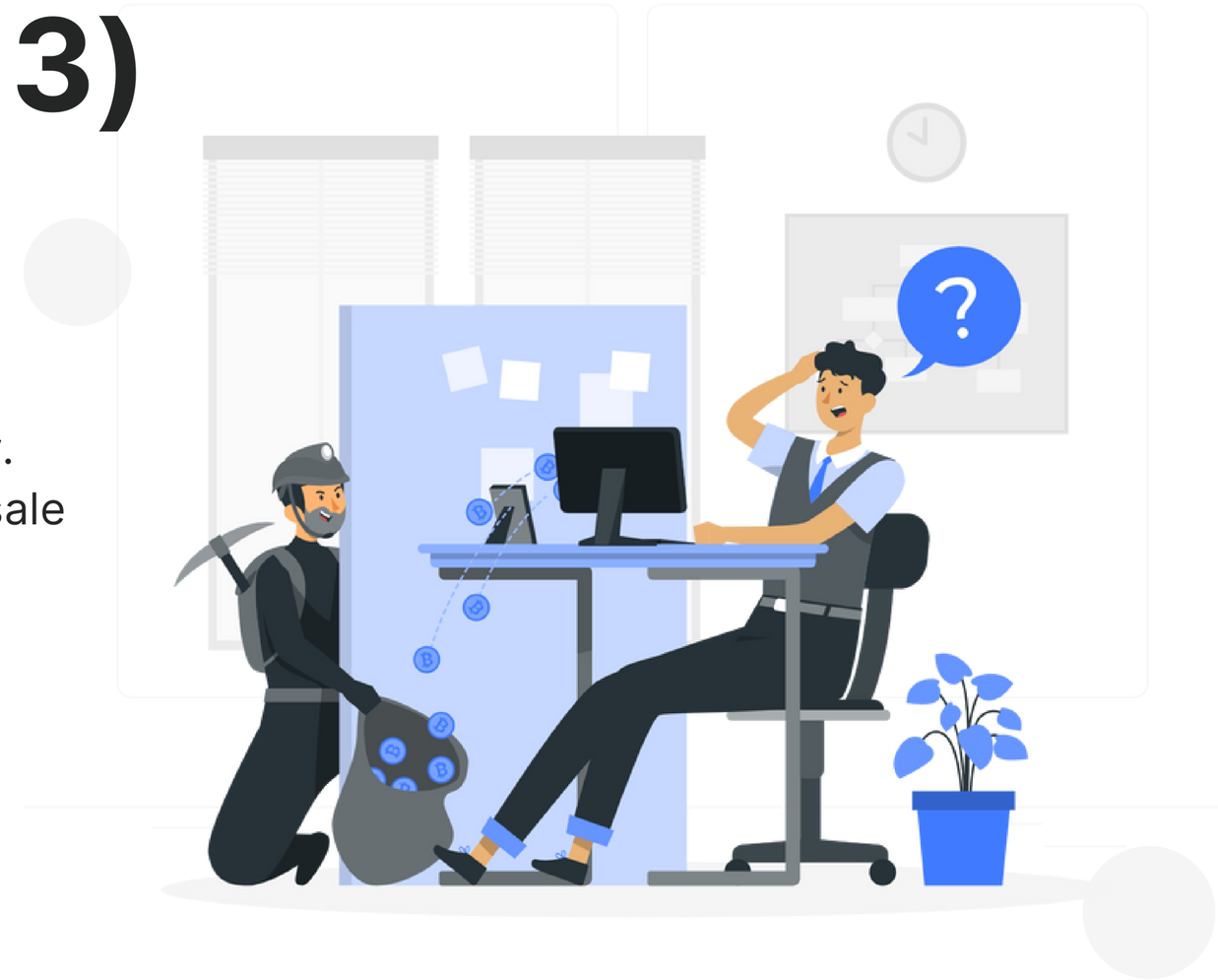
SNIFFING ATTACK Case Studies

The vast landscape of wireless networks encompasses numerous potential threats, making it challenging to cover them all comprehensively. In this presentation, we'll narrow our focus to delve into a specific type of attack:**Sniffing Attacks**



🎯 Target Data Breach (2013)

Attackers gained unauthorized access to Target's network using credentials from a third-party vendor. They installed malware on the company's point-of-sale (POS) systems, which included packet sniffing capabilities. This malware intercepted credit card information and personal data of millions of Target customers during transactions.

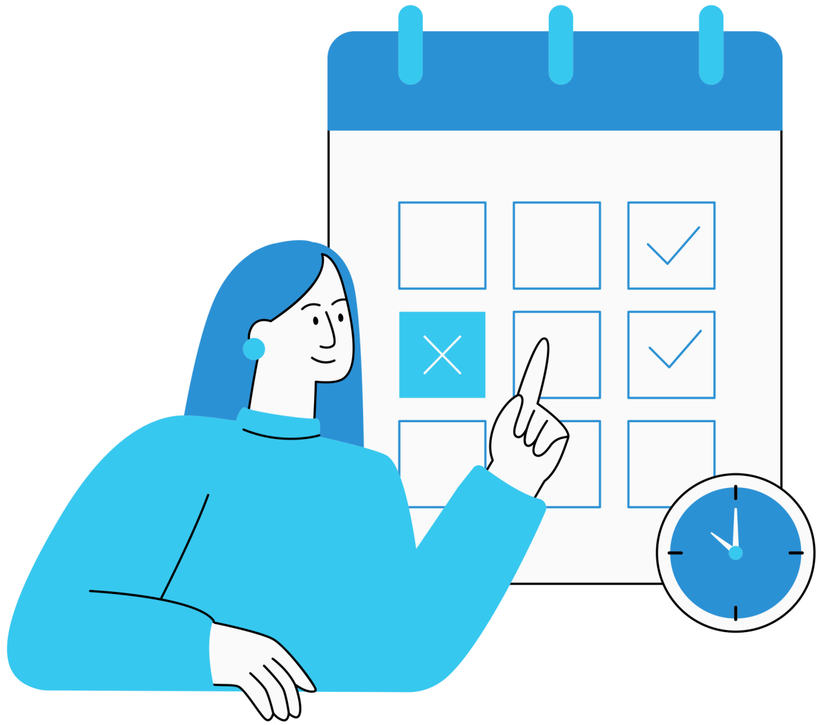


Scope of the Breach:

he breach affected around 41 million customer payment card accounts. Additionally, personal information of approximately 70 million customers, including names, addresses, email addresses, and phone numbers, was also compromised.

Duration of the Breach:

The attack occurred during the busy holiday shopping season, starting in late November and continuing until mid-December 2013. The breach went undetected for several weeks.



Response

Target publicly disclosed the breach in December 2013 after becoming aware of the issue. The fallout included a significant impact on Target's reputation, customer trust, and financial repercussions, including legal settlements, regulatory investigations, and costs associated with security enhancements.

ATTACK SIMULATION

WHAT WE NEED ? :

AN WIFI ADAPTER

TARGET