



En cybersécurité aussi, le savoir n'a de valeur
que si il est partagé.

In Cybersecurity too, knowledge only
increases in value once shared.

Wi-Fi Captive Portal

Disclaimer

Disclaimer

The following demonstration is for educational purposes only.

We do not promote or encourage illegal activities.

Knowing your enemy is a half-won battle

La connaissance n'est réellement profitable que lorsqu'elle est partagée

Wi-Fi Captive Portal

Agenda

1. What is a Captive Portal Wi-Fi?
2. How works a Captive Portal Wi-Fi?
3. What are the weaknesses of a Captive Portal?
4. How to protect a Captive Portal?



An abstract network diagram on the left side of the slide, featuring a series of interconnected nodes and lines forming a complex, web-like structure. The nodes are represented by small dots, and the lines represent connections between them. The overall shape is roughly circular, with many lines radiating from the center to the periphery.

What is a Captive Portal Wi-Fi?

Wi-Fi Captive Portal

What is a Captive Portal Wi-Fi?

- Public Wi-Fi in places like airports, cafes, and hotels.
- Secure enterprise networks where authentication is required before granting access.
- Networks that monetize internet access (e.g., by charging a fee).

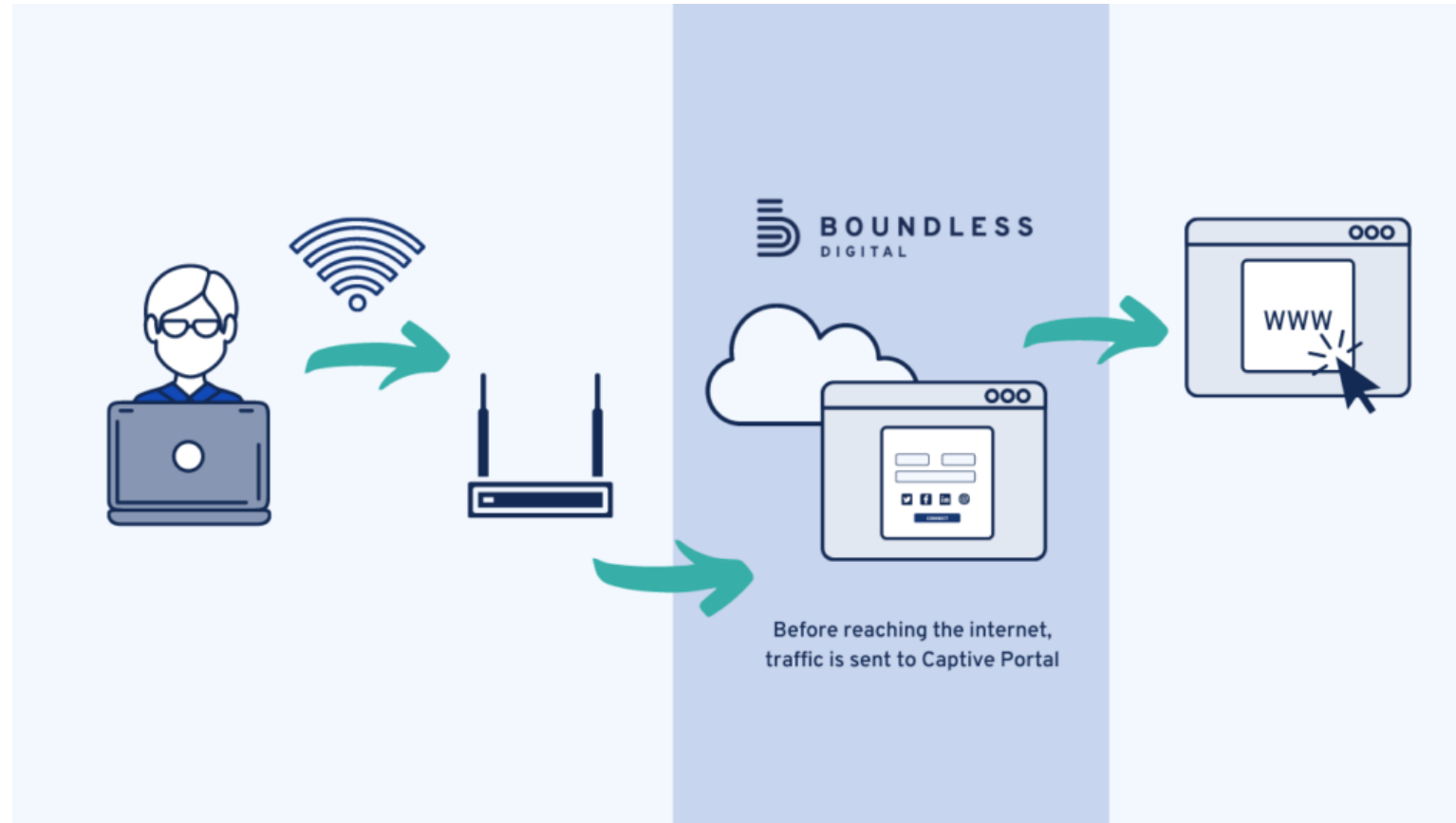
The screenshot shows a mobile interface for a Wi-Fi captive portal. At the top, the status bar shows the time 1:31 and signal icons. The browser address bar displays 'bloomwifi.com'. The main content area features a large red and blue diamond logo with two white dots. Below the logo, the text 'Free Wi-Fi' is prominently displayed. A blue button with a Facebook icon and the text 'Log in with Facebook' is visible. Below this, a white input field is labeled 'Enter email to Connect to Wi-Fi (Required)' with a red asterisk indicating it is mandatory. Further down, there is a section for 'ENTER BIRTHDATE:' with a white input field showing '04/24/2021'. Below that, a section for 'ENTER GENDER:' has three radio button options: 'Female', 'Male', and 'Other'. A line of text states 'By connecting to this Wi-Fi network, you are agreeing to our' followed by a blue link 'Terms of service'. A large green button with a right-pointing arrow and the text 'ACCEPT & CONNECT' is positioned below the terms. At the bottom, it says 'From our friends at Bloom Wi-Fi' next to a logo. The footer contains two links: 'Privacy Policy' and 'Contact Support'.

An abstract network diagram on the left side of the slide, featuring a dense web of interconnected nodes and lines, resembling a globe or a complex network structure.

How works a Captive Portal Wi-Fi?

Wi-Fi Captive Portal

How works a Captive Portal Wi-Fi?



An abstract graphic on the left side of the slide, featuring a globe-like shape composed of numerous small dots connected by thin, light-colored lines, creating a network or web-like structure.

What are the weaknesses of a Captive Portal?

Wi-Fi Captive Portal

What are the weaknesses of a Captive Portal?

1. Lack of Security in Open Networks:

- Most captive portals operate on open Wi-Fi networks with no encryption



```
root@kali:/var/www/html# ./wifi.sh wlan0 eth0 Free-WiFi
#####
##Back up/Creating hostapd.conf
##Back up/Creating dnsmasq.conf
##Adding routes to iptables
net.ipv4.ip_forward = 1
##Starting apache
##Configuring wlan0
##Turning on dnsmasq
##Starting hostapd
```

2. Bypass Techniques:

- Users can sometimes bypass captive portals by manually configuring their DNS settings or accessing specific IP addresses.
- Tools like VPNs or proxies may allow users to bypass restrictions.

3. Vulnerabilities to Attacks:

- Captive portals can be targeted for attacks like phishing, where attackers clone the login page to steal user credentials.
- Weaknesses in portal software or configurations can expose the system to exploits, allowing unauthorized access or data theft.

4. Session Hijacking:

- Since captive portals often use IP or MAC address-based session management, an attacker may hijack a user's session by spoofing their MAC address or IP address.



How to protect a Captive Portal?

Wi-Fi Captive Portal

How to protect a Captive Portal?

- Block all incoming connections and allow HTTPS to your router before granted user permissions
- Choose carefully which public Wi-Fi you want to connect and use a VPN



WOCSA

Join Us!



www.wocsa.org



[@wocsa](#)



contact@wocsa.org



[@wocsa_asso](#)



[@WOCSA-rx2mn](#)



[@wocsa](#)



<https://discord.gg/pDunje3tpb>



Join us to change the digital world:
<https://www.helloasso.com/associations/wocsa/adhesions/bulletin-d-adhesion-2>



Please provide your feedback for our quality check process:
<https://www.wocsa.org/qcheck.php>