# Lab9: Wi-Fi Phishing 1

## Pre-Requisite Knowledge and Skills

1. Understand basic knowledge of Computer network.
2. Be able to configure and use Linux and its applications.
3. Be able to configure and run Wireless Router or Access point
4. Understand basic knowledge of MySQL.
5. Understand basic knowledge of PHP.

## Learning Objective:

1. Understand characteristics and vulnerabilities of Wi-Fi network.
2. Understand usage of Captive Portal in Wi-Fi network.
3. Understand Phishing attack in data communication.
4. Explain countermeasures of Phishing attack in data communication.

## Recommended Running Environment and Software:

1. Raspberry Pi with accessories

## Instructional Material:

1. One Raspberry Pi 3B+
2. One Wireless router (with Internet connection if possible) or Ethernet for Internet connection
3. One PC, Mobile device, Laptop, or Raspberry Pi with Wi-Fi capability
4. Instructions of this activity

## Video Demonstration:

1. to be developed

## Lab Assessment:

1. Exercises
2. Quiz

## Note before starting the lab

This lab is designed for advanced student, who has a basic knowledge of Computer Network and Data Communication. Depending on the knowledge level of student, Instructor should adjust the amount of lab work. For novice students, it is recommended to use pre-built Image for this lab and allocate more time on discussion.

## Lab Instructions

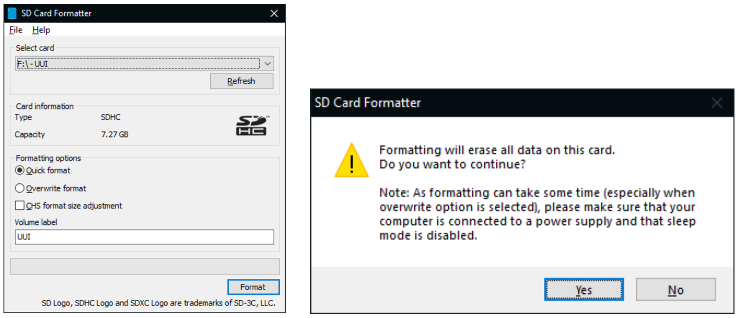
This lab requires one (1) Raspberry Pi, running Raspbian or Linux OS with two Wi-Fi adapters, one (1) Wi-Fi router or access point connected to Internet, and one (1) PC, Laptop, Mobile device, or Raspberry Pi with Wi-Fi capability.

## Getting start with Raspberry Pi

Raspberry Pi requires Monitor, SD card, SD card reader, USB keyboard and mouse. Raspberry Pi is diskless computer and OS should be installed in SD card. You can use any size of SD card that can contain and run Linux OS.

Download Raspbian OS IMG first from the link below.
https://www.raspberrypi.org/downloads/raspbian/

Now, SD card should be formatted and copy the IMG to SD card using SD card formatter. Simple insert the SD card to the reader and plug the reader into the PC. Then, open formatter application and format SD card as shown in Figure 1. Click the "Format" button and then, select "yes" to execute format command.



SD Card Formatter

Select card: F:\ - UUI

Card information
Type: SDHC
Capacity: 7.27 GB

Formatting options
● Quick format
○ Overwrite format
□ CHS format size adjustment
Volume label: UUI

SD Logo, SDHC Logo and SDXC Logo are trademarks of SD-3C, LLC.

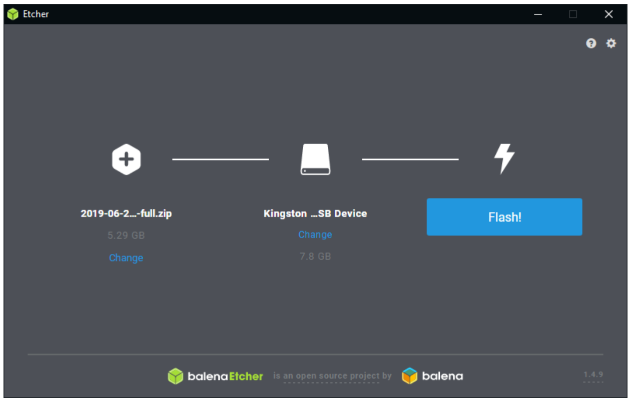
SD Card Formatter

Formatting will erase all data on this card.
Do you want to continue?

Note: As formatting can take some time (especially when overwrite option is selected), please make sure that your computer is connected to a power supply and that sleep mode is disabled.

**Figure 1.** SD Card Formatter

Now, we need to copy OS IMG to SD card using application called "balenaEtcher". Figure 2 shows the UI of application. First, select the IMG file, generally its extension is .iso, .zip, or .img. Select the IMG file and choose the SD card. Then, click "Flash" to upload the OS into SD card.



Etcher

2019-06-2...-full.zip
5.29 GB

Kingston ...SB Device
7.8 GB

balenaEtcher is an open source project by balena
1.4.9

**Figure 2.** Copying IMG file to SD card

Insert SD card to the Raspberry Pi and it is ready to start. In order to run Raspberry Pi, one monitor and USB keyboard and mouse for each Raspberry Pi is recommended. However, you can switch and use them for multiple Raspberry Pi if you need.

Once Raspbian is running at the first time, it will ask to set the password for the user. Default login user should be set as “pi”. But you can create new user. Remember the user login ID and password. We need them for the rest of activities. Once log in the system, you will need to set up the network connection. Raspbian is based on Debian Linux OS and setting up network is similar to the Linux system. If you are familiar with Linux system, now set up the network. If not, please watch and follow the Demo video. If Wireless router is used, correct through Wi-Fi or Ethernet cable. If Wireless router is correctly configured, IP address will be automatically assigned and read to connect Internet. Raspbian may ask for the update if you are connected to Internet. If you want, you can update, but it is not necessary. If you choose to update, wait until it finishes the update and restart the system.

Now, Raspberry Pi should be ready to configure for this lab.

## Discussion 1: Open Discussions before starting the lab

At this moment, it is a good time to check if student understand background information and attack scenario. Depending on student knowledge level, Instructor may adjust the level of discuss.

- **What is Wi-Fi? Where do you find them?**
  Wi-Fi is a wireless networking technology that allows computing devices (e.g., laptop, smartphone, printer, and etc.) to access the Internet. In general, Internet access is allowed through wireless router or access point. People may have their own Wi-Fi at home and business. Most of business place such as Starbucks, Panera, Target, and etc. provides free Wi-Fi service. Student may already know and use Wi-Fi.

- **What are the vulnerabilities of wireless communication?**
  This question is little technical. Allow student to think and discuss freely.
  Wireless communication uses air to transmit the data. Since there is no guided media or cable, there is not specified link and transmitting signal does not follow cable, but it goes everywhere. Due to this fact, the nature of wireless communication is Broadcasting (i.e., one to all). Example is AM or FM radio broadcasting. When one transmits, signal goes everyone in the range. Since the medium (air) is wide open, wireless communication suffers from interference and noise. Due to these, it also suffers from high error rate in transmission. Since transmission power should be controlled to reduce the interference between each other, communication distance is limited. Major vulnerability of wireless communication is Broadcasting. Since it goes everyone in the range, anyone can hear the communication.

- **Do you think Free Wi-Fi is secure?**
  As mentioned above, wireless is vulnerable to sniffing attack due to its Broadcasting nature. Therefore, we have to use password protected Wi-Fi, which encrypts the data in the packet. If Wi-Fi does not provide password protection, you should use it carefully. You should use application with secure communication protocol such as SSH, HTTPS, and etc. These application uses encryption to protect the data. However, we cannot say it is 100% secure. We will explore it in this lab.

After the discussion, students understand more about Wi-Fi and should be ready to move on the rest of this lab.

### Wi-Fi Phishing attack Scenario

Free Wi-Fi is available everywhere in these days and people are enjoying free Wi-Fi for their online activities such as web surfing, online shopping, and etc. without hesitation. Wi-Fi Phishing attack takes advantage of general behavior of people about free Wi-Fi usage to steal credential information. The architecture of Wi-Fi Phishing attack is illustrated in Figure 3.

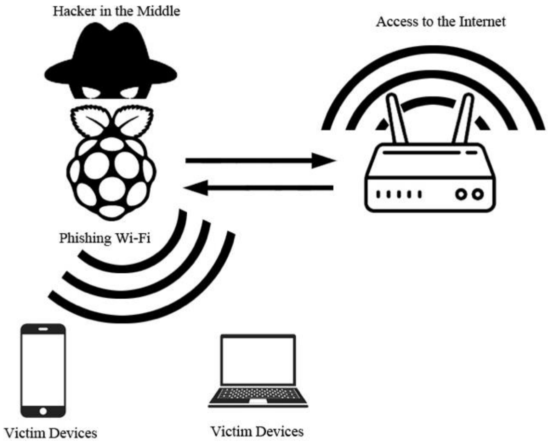


**Figure 3.** Architecture of Wi-Fi Phishing attack

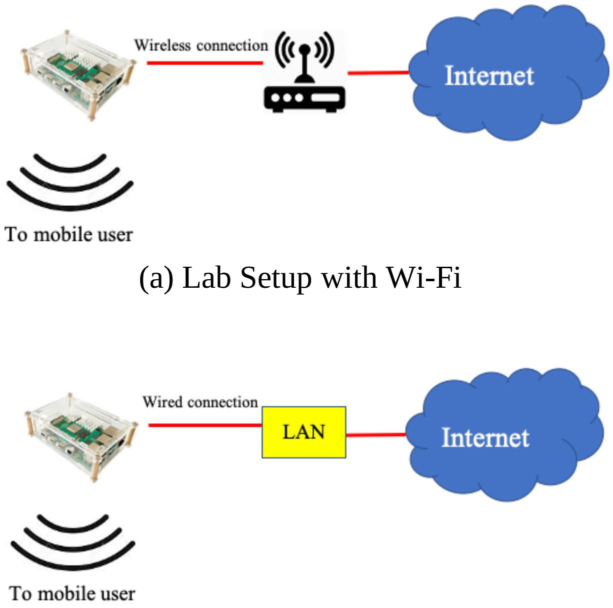
This attack is a Man-in-the-middle type attack. The basic idea of Wi-Fi Phishing is placing the Phishing device (i.e., Raspberry Pi) between Public Wi-Fi and users and provide an Internet access service just like Free Public Wi-Fi. As shown in Figure 3, Phishing device (Raspberry Pi) is normally connecting to Public Wi-Fi and also advertise itself as a Public Free Wi-Fi to attract users. When user select Phishing device to access the Free Wi-Fi, user becomes a victim. This lab will introduce how easily user credential can be stolen.

This lab utilizes “captive portal”, which is a web page that interacts with user before access is granted. Captive portal is generally used when it requires to control the user access to the Public Wi-Fi, which allows only authorized people. In the past, authentication process requires username and password, however, it becomes much easier now using third-party. Recently, third-party such as email, phone, and social media, is used for login or sign-up and a lot of people enjoy it for their convenience. This lab introduces how these services can be used to steal user credentials.

### Lab Setup and Configurations

General basic required installations and setups (i.e., Apache, PHP, and Wireless Access point) are available in Basic Configuration document. Please refer it if you want let student do these configurations. Otherwise, use pre-built image. The required in detail configurations for this lab is in “Lab9-Configuration Instruction”. Use this instruction for advance students to build.

Practically, we need two wireless adapters for Raspberry Pi, one to provide the Wi-Fi service and the other to access Free Wi-Fi for Internet access. If you do not have two Wi-Fi adapter or Wi-Fi is not available, you can use Ethernet connection (i.e., Ethernet cable) to connect Internet instead of Public Wi-Fi for the convenience as shown Figure 4.



(a) Lab Setup with Wi-Fi

(b) Lab Setup without Wi-Fi

**Figure 4.** Two possible Wi-Fi Phishing Lab Setups

There are three major parts of configuration in the Raspberry Pi besides basic setups and configurations. One is IP redirection using Iptables, another is creating Database using MySQL, and the other is creating captive portal using PHP.

## Lab Setup

### Step1: Setup Attacker’s device (Raspberry Pi)

Follow the basic setup instruction or use pre-built image to configure Raspberry Pi first. The next step is to place the attacker’s device between user and Free Wi-Fi. If two Wi-Fi adaptors and Wi-Fi network are available, use one adaptor to connect Wi-Fi network. As mentioned above, you can use Ethernet cable to connect the Internet instead for the convenience. Once connect to the Internet in either way, make sure your device has an IP address and connection is active. You can check your Internet connection by accessing any websites or ping know website such as google.com. If not, you should check your Internet connection. However, Internet access is optional. If Internet access is not available, you can skip this step and proceed to next step.

### Step 2: Setup Free Wi-Fi for Phishing

The other Wi-Fi adaptor will be using to deploy Free Wi-Fi network for users to login. Follow the basic setup to deploy Wi-Fi access point service with required services including DHCP, IP routing, and etc. or use pre-built image. Make sure your wireless adaptor has IP address of 192.168.4.1 255.255.255.0. If you want to use other IP address, you should modify IP address correspondingly in every configuration. In order to check your Wi-Fi access point, use any wireless capable device to connect this Wi-Fi.

**Discussion 2:** Ask students how we can implement this attack. They do not need to use technical term here. Let them have enough time to discuss freely with their own idea to make it possible. Following is an idea of this lab and use it to help students in their discussion.

- First, check if incoming user is new user or already login user first.
- For new use, Captive portal page should be brought up and ask for login with his/her email or social media account. Once user login, save the information and grant the Internet access.

**Note:** From Step 3 to Step 5, you can find the corresponding steps in Lab9-Configuration Instruction. Use them to configure if you want to create your own. If you use pre-built image, you do not need any configuration. In each Step, discuss implemented techniques to make this attack possible.

**Step 3: Redirect incoming traffic**
In order to check all incoming packets from users, we need to lead them to front page to process it properly. For this purpose, we have to use user utility program in Linus, Iptables, to redirect the traffic. Iptables is an IP packet filter rules in Linux system, which can control the incoming and outgoing traffics on specified network interface.

**Step 4: Build the storage**
When user login, we need to store the user information in the system. In this lab, we use database because we need to identify the user in order to avoid overlapping. MySQL is an open source database management system. We use this to create the database with three columns. First two columns are for user ID and password. The last column is for MAC address.

**Discussion 3:** When user login, we will have to store user information such as login ID and password. However, we do not want to store same information over and over. If user information is already in the storage, we do not need to store it. Discuss how to check if user information is already in the database.

- Start discussion with asking what type of information we can utilize in the packet. In the packet, which information indicates the source? Basically, there are two addresses available in the packet, IP address and MAC address.
- Ask students about the difference between IP address and MAC address.
- IP address is like mailing address while MAC address is like Social Security Number. Therefore, IP address specifies the location of the source where MAC address identifies the host.
- MAC address should be used to identify the user and also to check if user information is in the database.

**Step 5: Redirected page with login**
Next step is to setup the first webpage user will see when connected. When user accesses the web server, in general the first webpage user will see is the one, called “index.html” or

“index.php”. Therefore, we will have to code Captive portal in “index.php”. In this page, we should check if it is new user or not. If new user, ask for login, otherwise skip it.

**Step 6: Access the Phishing Wi-Fi**
User PC or other type of device with Wi-Fi capability to connect Phishing Wi-Fi. Then, open web-browser and go to any website. It should bring up the captive portal and asking login as shown in Figure5. Then, sign in. **DO NOT USE** your real user ID and Password!

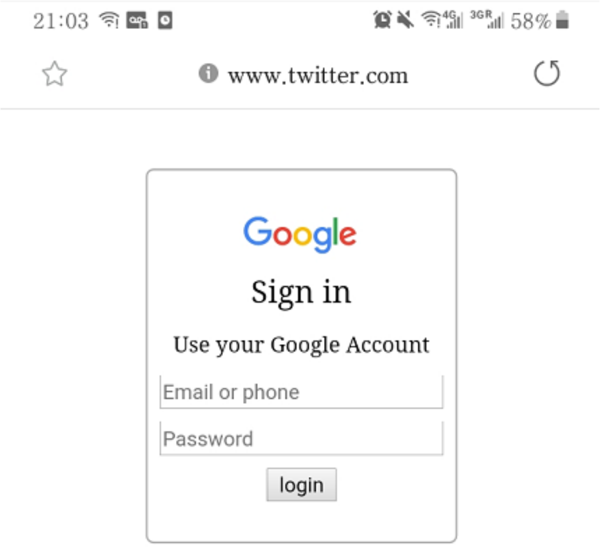
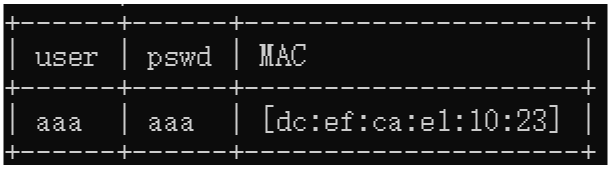


**Figure 5.** Captive Portal in Phishing Wi-Fi

**Step 7: Collecting user credentials**
In order to obtain collected user credential information, use terminal application at Raspberry Pi. Use following commands to observe the collected information from the database. The example of database command output is shown in Figure 6.

```
#mysql – u root -p
#user portal
#select * from portal
```



```
+------+------+---------------------+
| user | pswd | MAC                 |
+------+------+---------------------+
| aaa  | aaa  | [dc:ef:ca:e1:10:23] |
+------+------+---------------------+
```

**Figure 6.** output of database command

As you see, user credential information is stored in database.

**Discussion 4:** Discuss about the countermeasure of this attack. How we can avoid this attack?

- Let students have enough time to discuss how to avoid this type of attack.
- Technically, this type of attack is not easy to detect and avoid.
- Whenever use Public Wi-Fi asking for login, ask network owner (e.g., Starbuck, Panera,

Target, etc.) if it is their login page.

- Whenever you use Public or Free Wi-Fi or Internet service, you have to be very careful and make sure it is safe to use.

**Discussion 5:** Discuss other types of Phishing attack. Ask student what other Phishing attacks in cyberworld and let them discuss freely.