



UKRAINE TEAM



United Nations Educational, Scientific and Cultural Organization



Junior Academy of Sciences of Ukraine

Danyil Mamentovych SIMULATING A PHISHING ATTACK ON A WIRELESS NETWORK USERS

INTRODUCTION

Wi-Fi wireless networks have long become an integral part of everyday life. Public networks are available in places with large concentrations of people: public transport, airports, hotels, catering establishments, education, etc. This creates an attractive space for phishing attacks because the user is not always aware of the risks of using an unfamiliar network or understands which applications on his mobile device are sending certain data in the background.

TASKS

- analyze the nature and general features of phishing attacks;
- compare available devices for simulating phishing attacks;
- form requirements for your own device;
- choose and configure a hardware platform;
- configure the software;
- simulate a phishing attack and analyze the results of the experiment.

HYPOTHESIS

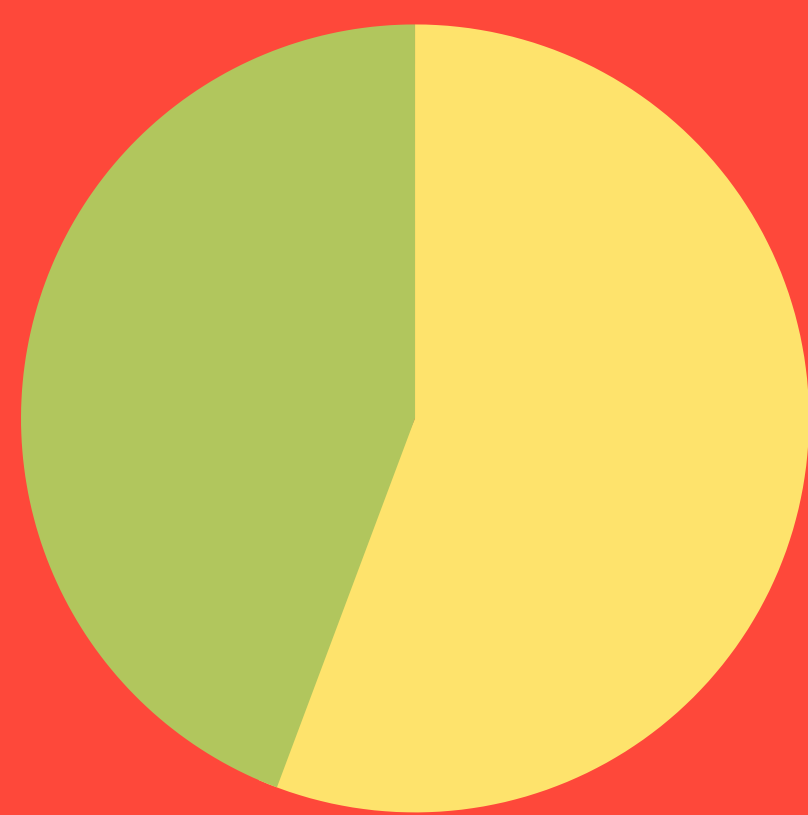
A single board computer may be used to build an affordable pentesting device to simulate phishing attacks in Wi-Fi networks.



METHODS

- survey;
- simulation;
- observation;
- experiment.

Don't know
44.3%



Know
55.7%

How many percent of people know what phishing attack is?

SOLUTION

The result of the investigation was an affordable and open-source pen-testing device prototype. It was based on a single board computer with custom scripts and acted like a Wi-Fi access point that stole users' credentials secretly. We used it to simulate an attack at our lyceum with the permission of the principal and without actual passwords stored for ethical reasons. As a result of the experiment, we were able to detect vulnerable devices and ignorant users.

CONCLUSIONS

- The survey showed insufficient awareness of users regarding phishing attacks;
- devices available on the market are quite expensive;
- the main result is a prototype device for phishing attacks using a captive portal;
- testing demonstrated the effectiveness of attacks on devices with different versions of Android.

