International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

Development of Mobile Application that Detects Phishing Messages to Decrease the Percentage of Data Theft during the COVID-19 Pandemic

Enrique Lee Huamaní[1], Brian Meneses-Claudio[2], Jehovanni Fabricio Velarde-Molina[3], Dr. Hema Mirji[4], Dhananjay Narayan Bhavsar[5]
[1]Image Processing Research Laboratory, Universidad de Ciencias y Humanidades, Lima Peru
[2]Facultad de negocios, Universidad Tecnológica del Perú, Lima-Perú
[3]Escuela de posgrado Newman, Tacna-Perú
[4]Assistant Professor Bharati Vidyapeeth Deemed to be University, Pune
[5]Assistant Professor,Dr. D.Y. Patil Institute of Technology, Pune

Summary— The COVID-19 pandemic has established not only a health emergency, but has generated an emergency in the control of personal data of all those people who make use of technological means, which increased the activity of phishing which consists of the theft of personal data through the circulation of false information through the different social networks, in addition, the circulation with messages related to the cure of this disease only for the theft of data. This research develops a mobile application that detects malicious URLs found within the content of textmessages. The developed application performs an analysis of the URLs according to the database that is updated with each attack detected, performing a blocking of the content and notifies the user of the actions that canbetaken, with this the theft of the personal data of the users is avoided. This application is very useful for all those people who use mobile equipment (mobile) and have no knowledge of these types of attacks, since they are likely to perform the actions that the perpetrators foresee for the obtaining of their personal data, so this application provides a means of security against these types of phishing attacks.

Keywords— Attack, Kanban, phishing, Scrum, URL, data theft.

I. INTRODUCTION

Peru, like other countries in the world, is immersed in the COVID-19 pandemic, which has caused a health emergency not only at the national level but also at the global level[1]. This led to a change in the consumption of resources by people, the same ones who stopped giving the same priority to food, clothing and footwear, which were relegated by the increase in the consumption of technological goods such as desktops, laptops, tablets and mobile phones[2]. In this sense, it has been noticed an increase in the data that are shared through these different technological devices, however, there is no authentication which guarantees that personal information is not lost on the way to its destination[3]. There are people who are engaged in the illicit act of stealing valuable personal information by sending text messages with fraudulent information, this activity is called phishing[1].

It is not surprising that large companies such as Facebook are concerned about the type of fraudulent information that is transmitted through their services, since it takes as a point of trust the prestige that this company has[3]. However, although this company tries to carry out actions such as checking the content that is shared, this would attack the privacy of users[3]. Another solution that arises is to be able to create a means in this case an application through which you can analyze the characteristics of websites with functions that verify the content of the URL or DNS. [1] This comes to be a research topic related to phishing activity[1].

In the midst of this COVID-19 pandemic phishing attacks have increased by sending mass emails detected by cybersecurity companies, these same have used the information of supposed medical reports in which the cure to this disease can be found which is totally false as reported by BBC News. [4] This type of scam "bait" users with this type of information which aims to collect private data through these false circumstances[1]. Attackers establish a system through which text messages containing phishing URLs are distributed, this taking the name of several well-known companies. The user enters this URL without knowing that this leads to the execution of the theft of their personal information, which will be used in illicit acts by the attacker[5]. The data that these attacks mostly seek are those belonging to credit card numbers and other data that serve to prove the use of them, although this does not ensure

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

that the illicit act is carried out since many of the pages of virtual stores establish other means to ensure the legitimacy of their transactions, this is mentioned by the newspaper El Comercio[6].

What this research seeks is to create a mobile application system that helps reduce the percentage of people who are victims of this type of information theft. Since with this information the people who use it carry out illicit actions such as the use of credit card data which can be offered on social networks such as Facebook[7].

In our research work we will address in detail what this type of activity consists of through the description of the methodology used by these fraudsters; the approach and definition of the mobile application system that would be responsible for the detection of these fraudulent messages; and the results that this would generate in the number of people who are victims of such illegal acts.

II. METHODOLOGY

More than a methodology, SCRUM is a framework through which projects and applications can be developed. These are developed in Sprints which have a certain development time and a specific set of tasks. This methodology is characterized by constant communication with both the interested party (client) and the development team through daily meetings where progress and solution to possible errors are exposed [8].

A. beginning

As an initial phase, the main roles and the work teams that the development of the project will have are delimited. In this sense, se performs the identification of who will be the Scrum Master and the Stakeholders; in the same way, the members of the work teams are defined. The skills of each of the team members will be taken into account to create an environment of fluid communication both between the different members and between the work teams [9].

B. Planning and estimation

In thisphase, all the functionalities that the project will have to create the user stories are taken into account, the same ones that will be placed in the Backlog of the product. The latter contains the user stories ordered according to the priority that has been delimited by the team and work, likewise, this dictates everything that the work team can do during the duration of the realization of the project [8].

C. implementation

In this phase we proceed to implement each of the user stories that are in the backlog list, it is possible to hold meetings to discuss what are the difficulties encountered during the development of the same [9].

D. hindsight

In this phase the respective review of the Sprint is carried out by the team, in an activity that allows the inspection and adaptation of the product the most important thing is the conversation by the team to understand the situation and receive feedback.

III. CASE STUDY

Cell phones do not have a filter specialized in identifying the content of text messages that reach you. These when receiving a new message comply with the functional cycle that has been programmed, in this sense, they make the notification to the user of new messages whether these are trusted or not. Users after opening these messages have in their hands the decision whether or not to open the URL with which these messages have. Once opened they find very similar pages (cloned) of the official pages of different entities, whether social networks or banks, the same ones that request the filling out of forms with personal data of the victims. This data is stored somewhere where the attacker can later access it. The data that is collected is used for the performance of illegal activities in Figure I regarding the flow that follows a phishingattack.

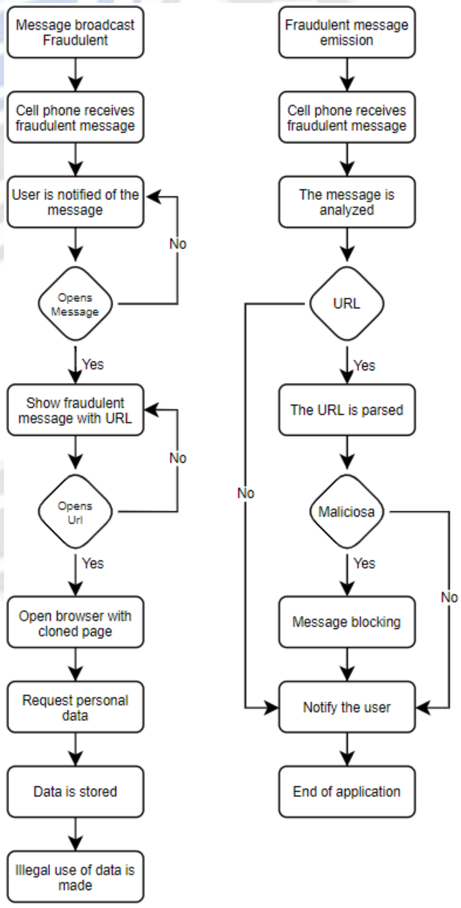

Fig. I Flowchart of Phishing Scam and Mobile App Flowchart

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

The application that will be developed is designed to serve as an intermediary between the user's actions and the functionality of the software of the cellular equipment. This can be seen in Figure I regarding the work of the application,where the flow of actions changes to prevent the user from entering one of these pages and therefore seeks to prevent the theft of personal information.

The team then proceeds to start with the phases of the SCRUM framework for the development of this research project.

A. beginning

Taking into account the skills of each of the members of the development team, the roles were determined as shown in Table I where the rolis and the descriptionof whois the make it upare shown.

TABLE I ROLES OF SCRUM AND ITS MEMBERS

Roles	description
Product Owner	System owner
Scrum Master	Project members
Team	Project members

B. Planning and estimation

Through a meeting, the team defined which are the epics that meet the requirements for the fulfillment of the functions of the application. Once the epics are defined, we proceed to make the user stories that would become the tasks to be performed by the work team.

Then, through the use of estimation methods such as Planing Poker and Analogous Estimation, the group members provided a score based on their experience and knowledge in the development of each of these stories. The result of this estimate and the user stories are reflected in Table II in relation to the Backlog which contains the stories, their score and their estimate.

As the last step of this phase is made the determination of the number of sprints with which it was counted for the development of the project in Table II where it is detailed with the number of user stories its value and the sprint points that each of them entails, in the first we see a score of 9 because stories were made to provide a first deliverable, in the second sprint it was determined to perform a greater number of tasks that is why a score of 73 was obtained, and in the last part knowing what our performance was, less demanding tasks were performed but of equal importance.

C. implementation

In this phase, the work team proceeded with the development of each of the activities established in the Backlog, this following the order of prioritization that was determined for each of the tasks.

In this sense, we proceeded with the creation of the database that the application used for the registration of fraudulent numbers and URLs that are found during its execution on the different devices on which it is installed.

TABLE II THE BACKLOG OF THE APPLICATION, USER STORIES AND ESTIMATION

User Story	Q1	Q2	Q3	estimate
I as an administrator want the system to be activated when you enter a new message.	13	13	13	13
I as an administrator want the system to parse URLs not registered in the database.	13	13	13	13
I as an administrator want the system to analyze the content of messages in search of URLs.	13	13	13	13
I as an administrator want the system to verify the URL in the database.	8	8	8	8
I as an administrator want the system to record malicious URLs in the database.	8	8	8	8
I as an administrator want the system to perform the blocking of dangerous text messages.	8	8	8	8
I as an administrator want the system to notify about the dangerous URL found.	5	5	5	5
I as an administrator want the system to store the phone numbers that send dangerous messages.	5	5	5	5
I as an administrator want the system to record the name of the sender of the message.	5	5	5	5

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

I as an administrator want the system to notify about message blocking.	3	3	3	3
I as an administrator want an interface where the user can see all messages with a malicious URL.	3	3	3	3
I as an administrator want an interface, where the user can see all the details of the message.	3	3	3	3
I as an administrator want an interface where the user can see notifications.	3	3	3	3
As an administrator, I want the application to be able to show me the weekly, monthly and annual report of messages with dangerous content.	2	2	2	2

For the creation of this database was made use of the relational database managerMySQL, because it is recognized worldwide as one of the best in its branch, in addition to executing queries in a faster way as well as its speed in reading data [10].

TABLE III SPRINT PLANNING

Sprint No.	User Story	value	Sprint Points
1	H12	3	9 points
	H11	3	
	H13	3	
2	H03	13	73 points
	H02	13	
	H01	13	
	H04	8	
	H05	8	
	H06	8	
	H08	5	
	H09	5	
3	H07	3	10 points
	H10	3	
	H14	3	

Then, following the preset tasks proceeded with the development of the main interface which interacts with the inbox of the text messages of the mobile (cellular) equipment, provides the user options, the list of messages and messages blocked so far, as shown in Fig. II where the prototype of the main interface is shown.

Fig. II Main Application Interface

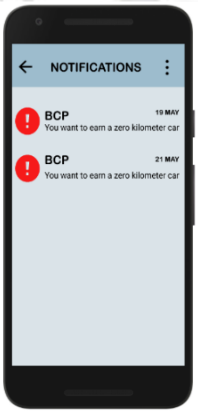

Fig.III Interface for notification of fraudulent messages

As part of the execution of our project a notification center was implemented so that the user can have knowledge that they have entered messages that are registered as fraudulent or that after being analyzed they have a fraudulent URL for which it is registered in the database and proceeds to its notification in Fig. III we are shown the notification interface of the application after finding fraudulent messages.

Finally, the application, having already registered the data in the system database, proceeds to notify the user of the options

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

that the user can make with respect to the fraudulent messages found. The system allows the user to view the messages without the user being able to interact with the content of the same. The options available to the userare: the first option is the message blocking which allows the system to separate the messages from the inbox to the application where they can only be viewed but have no interaction with them; the second option is the deletion of messages worth redundancy allows the user to delete the messages from both the inbox and the application which completely discards the interaction of this with the user's data. Fig. IV shows the message detail interface with the options of locking utensils and message deletion.

Fig. II Detailed interface of system actions with fraudulent messages

IV. RESULTS AND DISCUSSIONS

In this section the results and discussions that have been obtained through the development of this research work are exposed, in this sense, in the section of the results a description of the work carried out in each of the Sprints was made, and in the section of the discussions the SCRUM and KANBAN methodology was analyzed defining the similarities and the most notable differences that were found between both.

A. From the case study

In the project 3 Sprints have been developed which have been made taking into account the skills of the development team, hence, in the first Sprint you have 9 story points with 3modules; in the second Sprint you have 72 history points and a total of 8 modules feel the Sprint with the highest number of nodules; and in the third Sprint with a total of 10 Sprint points. This distribution can be seen in Table III which details the path that the project has followed for its correct development. The following describes each of the Sprints that have been performed.

1. *For Sprint 1:* In the present Sprint the prototypes *were*delivered *with respect to the* interface mordulo each one of them with a user-friendly design, the same one that maintains a readable text format to avoid confusion at the time of its reading both in the content of the messages and in the notifications that will be made by the system. As can be seen in Fig. V in the graph of bursts of the first Sprint, for its development have taken 9 days on the X axis and on the Y axis have been considered the 9 points of respective history, which represent the expected time with the time re*to the development of the*present Sprint.

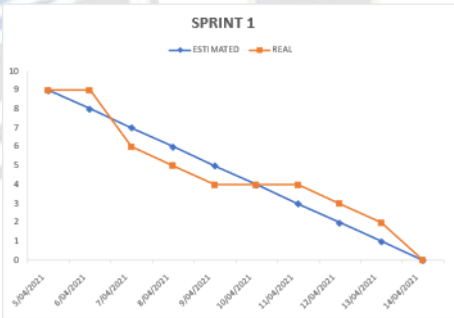

Fig. III Development route for the First Sprint

2. *For Sprint 2:* In this Sprint the prototypes were delivered of several of the modules such as URL, blocking, notification, storage and message; because the development team has been getting to know the skills that are available, the decision was made to perform several of the main functions for the operation of the system. This allowed the system to be activated when receiving a message by proceeding to perform the respective analysis of the content and the registration of the same in the storage system. As can be seen in Fig. VI in the burst graph of the second Sprint, for its development have taken 36 days on the X axis and on the Y axis have been considered the 73 points of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 10
DOI: https://doi.org/10.17762/ijritcc.v10i10.5733
***Article Received**: 28 July 2022 **Revised**: 05 September 2022 **Accepted**: 12 September 2022*

respective history, which represent the expected time with the real time of the development of this Sprint.

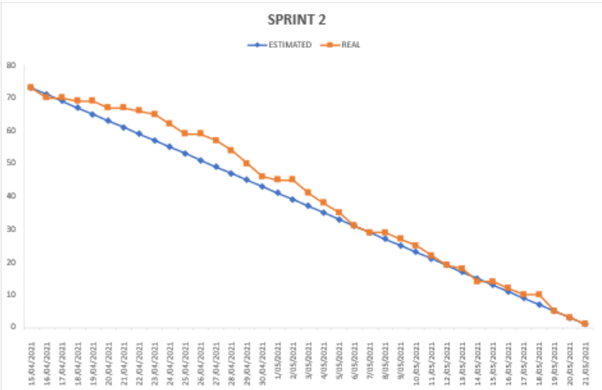

Fig. IV Development route of the Second Sprint

3. *For Sprint 3: In this Sprint the delivery of the* latest prototypes was made *with respect to the* reporting, notification and storage module, *in this Sprint the system* finishes analyzing the messages in search of the sender to be registered in the database in order to be recognized in future phishing attacks, in addition, as part of the project a section was made in which the system can provide a report of the record of the different attacks in a range of time such as days or months. As can be seen in Fig. VII in the graph of bursts of the third Sprint, for its development have taken 10 days on the X axis and on the Y axis have been considered the 10 points of respective history, which represent the expected time with the real time of the development of this Sprint.

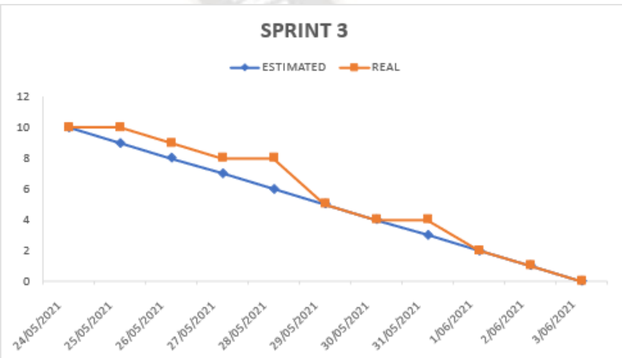

Fig. V Development route of the Second Sprint

B. Methodology

Among the most used project development methodologies we have Scrum and Kanban, each with its respective characteristics. Scrum is a methodology structured in development teams with multiple functions in both design, coding and etc., but this type of methodology has the myth of being mostly efficient in the development of large applications [11]. In this sense, in our project we came to correctly implement this structure defining the functional requirements which have been divided into the different Sprint. However, here there is a bottleneck inconvenience when performing the delimited tasks which can be observed in Table III in the second Sprint with a total of 8 tasks to perform and 73 history points. Also, the time that takes between the completion of tasks from one Sprint to another could sometimes be used to finish some additional tasks which would have served to conclude the project earlier.

On the other hand, in the Kanban methodology the tasks are placed on a board which can be physical or digital which is something very convenient considering the pandemic situation that is lived in front of COVID-19 [12]. For the development of their tasks are performed one by one as they are completed, this in order to avoid bottleneck problems by not having many tasks to perform, in addition, you have a saving in development time since the tasks are performed as soon as the previous one is completed [11].

Table IV provides a comparison of some of the advantages and disadvantages of these methodologies.

TABLE IV SCRUM AND KANBAN ADVANTAGES AND DISADVANTAGES

	ADVANTAGES	DISADVANTAGES
SCRUM	• Involve the customer. • Multifunctional equipment. • Iterative and incremental. • Continuous meetings. • Troubleshooting.	• Suitable for large projects. • It does not detect bottlenecks. • The postponed tasks. • It requires specific knowledge about the methodology.
KANBAN	• Avoid bottlenecks. • Tasks performed one after the other. • Time saving. • Easy to handle.	• It is not specific for software development. • If the deadlines are not met, the production schedule varies. • Faced with a large number of labels the members can be confused.

V. CONCLUSIONS

In conclusion, with the implementation of the application developed in this research project it is avoided that the user performs any type of action with the URLs attached within the content of the phishing text messages that reach his mobile computer in Fig. II it is seen how the system executes the pertinent actions according to the situation helping the user with a notification of the operations that can be performed with the phishing message which serves as a help to those who do not know what actions to take against this type of data theftattacks.

The use of the Scrum methodology ensures a work structure in which the development team can be guided for the elaboration of the project, however, as shown in Table III there is a bottleneck in the determination of the tasks necessary for the second Sprint to be delivered overloading the work of the development team so that the Kanban work method could be implemented to avoid this type of situation.

With regard to phishing messages you can implement a way to analyze the messages that also arrive through social networks such as Telegram, Whatsapp, Facebook, etc., this because the user can receive attack through these networks allowing the attacker to steal the data of users without any means to prevent it.

REFERENCES

[1]. I. Saha, D. Sarma, R. J. Chakma, M. N. Alam, A. Sultana, and S. Hossain, "Phishing attacks detection using deep learning approach," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 1180–1185, 2020, doi: 10.1109/ICSSIT48917.2020.9214132.

[2]. F. Almeida, J. Duarte Santos, and J. Augusto Monteiro, "The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World," *IEEE Eng. Manag. Rev.* , vol. 48, no. 3, pp. 97–103, 2020, doi: 10.1109/EMR.2020.3013206.

[3]. A. Gupta, P. Prabhat, R. Gupta, S. Pangotra, and S. Bajaj, "Message authentication system for mobile messaging applications," *Proc. - 2017 Int. Conf. Next Gener. Comput. Inf. Syst. ICNGCIS 2017*, pp. 126–130, 2018, doi: 10.1109/ICNGCIS.2017.32.

[4]. J. Tidy, "Coronavirus: how hackers are using the fear of covid-19 disease to spread computer viruses - BBC News World." .

[5]. Oshin Dhiman, & Dr. Anand Sharma. (2022). Incorporation of Booster in Carbon Interconnects for High-Speed Integrated Circuits. Acta Energetica, (03), 22–28. Retrieved from http://actaenergetica.org/index.php/journal/article/view/473

[6]. J. W. Joo, S. Y. Moon, S. Singh, and J. H. Park, "S-Detector: an enhanced security model for detecting Smishing attack for mobile computing," *Telecommun. Syst.* , vol. 66, no. 1, pp. 29–38, 2017, doi: 10.1007/s11235-016-0269-9.

[7]. N. E.C. PERU, "Cybercriminal reveals how he steals money from credit cards in Mexico | world | EL COMERCIO PERÚ."

[8]. D. El Comercio, "Cybercriminal reveals how he steals money from credit cards in Mexico | world | EL COMERCIO PERÚ." .

[9]. B. V. Deemer, By Pete, Gabrielle Benefield, Craig Larman, "The Scrum Primer," *Scrum Train. Inst.* , vol. 1.1, pp. 1–20, 2009.

[10]. P. Chilito, D. Viveros, C. Pardo, and F. J. Pino, "Scrum+: An agile guide for the global software development (GSD) multi-model project management," *2018 IEEE Colomb. Conf. Commun. Comput. COLCOM 2018 - Proc.* , pp. 0–5, 2018, doi: 10.1109/ColComCon.2018.8466710.

[11]. Tadeusz Chmielniak, & Nadica Stojanovic. (2022). Design of Computer Aided Design in the Field of Mechanical Engineering . Acta Energetica, (01), 08–16. Retrieved from http://actaenergetica.org/index.php/journal/article/view/460

[12]. G. Ongo and G. P. Kusuma, "Hybrid Database System of MySQL and MongoDB in Web Application Development," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. September, pp. 256–260, 2018, doi: 10.1109/ICIMTech.2018.8528120.

[13]. A. Mundra, S. Misra, and C. A. Dhawale, "Practical scrum-scrum team: Way to produce successful and quality software," *Proc. 2013 13th Int. Conf. Comput. Sci. Its Appl. ICCSA 2013*, pp. 119–123, 2013, doi: 10.1109/ICCSA.2013.25.

[14]. S. Nakazawa, K. Komatsu, T. Tanaka, and K. Matsumoto, "Development and Evaluation of Large-Screen Digital Kanban with Smartphone Operation," *Proc. - 2017 6th IIAI Int. Congr. Adv. Appl. Informatics, IIAI-AAI 2017*, pp. 295–300, 2017, doi: 10.1109/IIAI-AAI.2017.151.