Kalpa Publications in Computing

Volume XXX, 2022, Pages 37–39

Proceedings of V XoveTIC Conference. XoveTIC 2022

Developing a Cybersecurity Awareness Web Application for Non-Technical Users

Daniel Feito-Pin[1*], Rubén Pérez-Jove[123†], and José M. Vázquez-Naya[123‡]

[1] Facultade de Informática, Universidade da Coruña, Elviña, 15071 A Coruña, Spain
[2] Grupo RNASA-IMEDIR, Departamento de Ciencias de la Computación y Tecnologías de la Información, Facultade de Informática, Universidade da Coruña, Elviña, 15071 A Coruña, Spain
[3] Centro de Investigación CITIC, Universidade da Coruña, Elviña, 15071 A Coruña, Spain

Abstract

In a world where technology is becoming more and more a part of our lives, the danger posed by cyberthreats to which we could be exposed is growing. Knowing how to prevent and act against them is crucial to avoid becoming the victim of cybercriminals. Good practices and general knowledge on how to act in cyberspace should be more widely disseminated to the population, especially to those who do not have sufficient technical knowledge of Information and Communications Technology (ICT). This work aims to provide a tool to raise awareness by providing them with concepts, good practices and practical scenarios to reflect on. For this, a tool was developed consisting of an application aimed at all types of users, and accessible on different devices so that it can be used by as many people as possible.

1 Introduction

The boom in the digitization of companies and teleworking due to the pandemic caused by Covid-19 has been accompanied by an increase in the number of cyberattacks and computer scams. In Spain alone, there have been an average of 40,000 cyberattacks every day during 2021 [1]. It is remarkable how, as a result of this situation, the cases of computer fraud increased. According to the crime statistics portal of the Ministry of the Interior [2], in 2020 there were 257,907 known facts of criminal offenses related to cybercrime, in the criminal group "computer fraud".

Another event that generated an increase in cyberattacks worldwide was the beginning of the conflict between Ukraine and Russia after the beginning of the Russian invasion on February 24, 2022. Among the targets of the attacks derived from this political situation, there are public administrations, essential services, and critical infrastructures of various countries, including NATO members.

*Developed the aplication
†Provided support in the realization and revision of this work carried out
‡Provided support in the realization and revision of this work carried out.

Although there are multiple protection measures at the hardware and software level, such as firewalls or intrusion detection systems (IDS), the security level of a system is determined by its weakest part: the user. At the business level, antivirus, firewalls, and other security tools available can be implemented to improve the cybersecurity of a company. Internal policies can also be established to have backups and to configure and manage the systems in a secure way. Nevertheless, the tools and policies lose their usefulness if the employees do not follow a series of good practices [3].

This increase in cyberthreats implies the need to increase the awareness of cyberspace users, preparing them to know how to detect and act against this type of danger. There are various approaches to training in cybersecurity on the Web. Learning platforms host online courses, and cybersecurity companies offer resources for their users to gain hands-on experience. There are also national organizations that have their courses and awareness kits, as is the case with INCIBE. On the other hand, different communities of cybersecurity professionals and enthusiasts provide content on their blogs and social networks. However, there is a lack of free tools, aimed at the novice user without technical computer knowledge, that offer both theoretical content and practical scenarios on which they can apply what they have learned.

This work aims to provide a tool to raise awareness among citizens by providing them with knowledge about the dangers of the Internet and good practices and methods to improve their safety in the face of these, to reduce the number of incidents. For this, an application was developed that offers concepts and good practices as well as practical scenarios that make users reflect on what they have learned. Also, this application is aimed at all types of users, regardless of their computer skills. Since the app was meant to be accessible on various devices, both mobile and desktop, a completely web-based approach was followed. Even so, it was designed from the ground up with possible future migrations to specific platforms in mind and to avoid dependencies on third-party software.

2 Materials & Methods

For the development of this project, it has been chosen to follow the iterative and incremental development methodology. For each iteration of development, the following phases were followed: analysis, design, implementation, and testing.

The app consists of courses grouped by related topics. Each course is made up of different topics which, in turn, are made up of lessons and exercises. Lessons aim to teach a concept or best practice to the user, while exercises consist of forms or questions about a presented scenario that the user will have to solve.

The application is intended to be accessible on different devices, both mobile and desktop. For this, an entirely Web-based approach was used in this first version, following the principles of mobile-first and responsive web design. For the development of the application, we chose a client-server architecture following the Model-View-Template (MVT) design pattern.

To facilitate the execution of the back-end on various platforms, it was decided to use Python as the main programming language and work with one of the frameworks it offers for the development of light web applications, in this case, Flask.

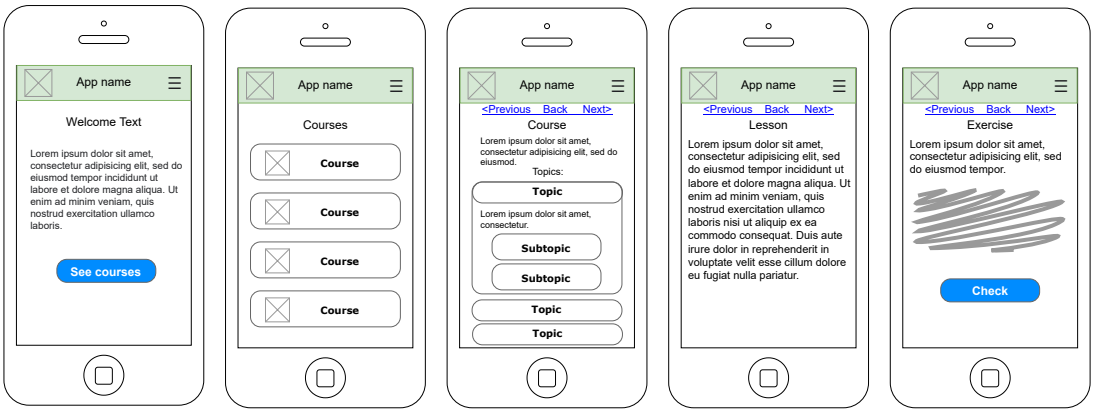
For the design of the front-end, special care was taken in the features that could affect the user experience. Furthermore, the front-end not only displays content but also includes logic that is executed to provide further interaction with the application. Visual aspects were taken into account that would benefit usability in several of its aspects: learning, efficiency, memory... This focused the style of the application towards a simple and intuitive design, but without abandoning the aesthetic factor. For this, an attempt was made to include the least amount

of logic possible, taking into account the possible load that it could have on the resources and battery of the client machines.

3 Results & Discussion

The work carried out resulted in a user-friendly application available on different devices and sizes. Also, it was developed in such a way that the server sends the response with everything already structured, being ready to execute its functionalities with a single click or touch of the user.

It has a few screens and a simple navigation system between them to facilitate its use. These can be seen in Figure 1, where to simplify the images, the wireframes for the mobile views used during development are shown.



(a) Splash Screen. (b) Courses Screen. (c) Course Screen. (d) Lesson Screen. (e) Exercise Screen.

Figure 1: Wireframes of the different views of the application.

The user can see the characteristics of each course and its topics with their subtopics and easily navigate between them. The lessons lead to a reading screen that provides knowledge to the user. On the other hand, the exercises lead to a screen with a form that the user must answer regarding a given situation.

In future lines of work, a user profile system could be added to show progress in the different courses. An achievement system could also be added on top of the previous one to improve user interest and participation.

References

[1] PIXEL. El año de los grandes ciberataques en españa. [online], 2021. Available at https://www.elmundo.es/tecnologia/2021/12/01/61a63b4ae4d4d8db5a8b4577.html.

[2] Gobierno de España. Portal estadístico de criminalidad. [online], 2019. Available at https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/.

[3] INCIBE. ¡Actualízate en ciberseguridad con el nuevo kit de concienciación! [online]. Available at https://www.incibe.es/protege-tu-empresa/blog/actualizate-ciberseguridad-el-nuevo-kit-concienciacion.