An Approach to Phishing Attacks Modeling for Network Gamified Educational Projects*

Konstantin Safonov[1][0000-0003-0405-3065], Vyacheslav Zolotarev[1] [0000-0002-8054-8564], Nikita A. Romme[2] [0000-0002-2729-5713], Nikolay Parotkin[1] [0000-0002-3486-0602], and Ekaterina Maro[3] [0000-0001-5136-7804]

[1] Siberian State University of Science and Technology, Krasnoyarsky Rabochy Av., 31, 660037 Krasnoyarsk, Russia
[2] Siberian Federal University, Svobodny av., 79, 660041, Krasnoyarsk, Russia
[3] Southern Federal University, Bolshaya Sadovaya Str., 105/42, 344006 Rostov-on-Don, Russia
safonovkv@rambler.ru, amida.2@yandex.ru, abakanromme@mail.ru, NYParotkin@yandex.ru, eamaro@sfedu.ru

Abstract. The article presents an overview of the current state of phishing attacks on network gamified projects for undergraduate and graduate IT-education courses. Issues are considered related to secure interaction within a gamified educational environment, in particular in the field of game cases used for information security training. The algorithm of actions for modeling the vulnerability of participants in network gamified projects to phishing attacks is presented. Also, experimental results of modeling phishing attacks on a simulation model of a social network are shown. The results can be useful in developing and applying interaction methods in online educational projects.

Keywords: IT-education, Training, Gamification, Phishing Attack, Social Network

1 Introduction

In modern education trends, especially with the extensive integration of distance (namely online) education processes into areas where it was rarely used before, the number of security threats to participants in online educational projects has sharply increased. Security threats both related to participant's actions (phishing, spam, substitution and theft of payment card data) and with the disadvantages of known learning environments are relevant. In the field of information security education there are many ways to involve participants through gamification approaches [1-5].

In all above cases, the main goal of the training gamified project is to improving professional skills withal ensuring security in network interaction is responsibility of the participants themselves and their common sense.

* Supported by the Russian Science Foundation, grant No. 19-013-00711A.

Proceedings of the 4th International Conference on Informatization of Education and E-learning Methodology: Digital Technologies in Education (IEELM-DTE 2020), Krasnoyarsk, Russia, October 6-9, 2020.

1.1 Phishing Attacks on Online Educational Projects

The phishing attacks explored in this article are based on various ways to recipient spoofing in a network interaction. The main types of phishing attacks are presented in [6-8].

A phishing attack on the educational process can have devastating consequences both in terms of violating its security (participants lose personal data, credit card numbers, accounts, etc.) and reputational consequences (as example, termination of using a current educational service). At the same time, even a successful response to such attack by information security tools also rejects participants from educational (especially gamified) processes, because in consequence of interacting with information security tools the dynamics and logic of the education game can be destroyed and participant's accounts are blocked. In view of the above issues predicting and preventing such attacks seems to be the best tactic.

2 Modeling phishing attacks on educational resources

It is known that the social network as a tool for interaction brings many additional issues to any network project. Among these issues are: unauthorized cooperation of participants, including phishing; substitution and deletion (destruction) of accounts of participants in a network project as a way of introducing third parties into the project or disrupting its functioning; suppression by the flow of external information of project participants, decrease in involvement, intensity of information exchange; use of project resources for actions unrelated to its main tasks, etc. [9].

Therefore, adding a social network to the list of interaction tools in a networked gamified educational project, it is necessary to take these issues into account by modeling phishing attacks on educational resources. Moreover, gamification obviously requires more disclosure; consequently, during modeling it is necessary to take into account the specifics of gamification process, such as the use of common resources and interest groups, nodes and connections that unite project's participants, and the use of open problems in teaching methods.

2.1 Interaction Metrics in a Network Educational Project and a Phishing Attack Model

If we consider gamification in a network communication form as a certain level of interaction, collaboration of various groups interacting through a social network, then the metrics of the participant's interaction will be the number and complexity of connections between them, the intensity of interaction, as well as formal assessments of the impact on the social graph [10]: average vertex degree, intermediateness, eigenvector and relative importance. If we take into account the limitations associated with phishing attacks, then it is advisable to add the ability to assess the resistance to primary and repeated attacks.

The modeling of a phishing attack in this article was based on the following idea: visualization of the situation, namely, the availability of freely available information on the user's page, the number and quality of connections affect the choice of an account as a distributor of a phishing attack, as well as the success of this attack both on the user himself and on his friends and subscribers.

The procedure for the experiment was as follows:

1. Collecting user data (initial modeling involved 31 accounts actually used in gamified networking tasks through the SEQuest project team in 2020).
2. Setting up the creation of links between user's accounts.
3. Create n users for imitating social network users.
4. Configure a simulated phishing attack.
5. Run an experiment.

Technically, the project was carried out using Selenium WebDriver, a headless version of the Chromium browser and the PyQt5 library. All experiments on user's data were carried out on a simulation model of a social network of a networked educational project.

2.2 Algorithm for Modeling Connections and Accounts of Participants

In order to create a user in a simulation model of a social network of a networked educational project a general algorithm is used. The procedure for creating a user is as follows:

1. Suppose that the project database contains the data of n users; as the information was collected, m different types of data connecting this information were identified. Therefore, the original matrix has dimension nxm. The matrix consists only of 0 and 1 (the type of data connecting users, such as common interests, place of residence, etc., coincides or not), the number of values equal to 1 is estimated, then on the basis of this estimation we calculate a satisfying value of probability p_a for the attack.
2. When re-entering matrix data types are made, the previous change to the matrix is taken into account; thus, it is possible for the second and subsequent elements to have a higher p_a by increasing the number of matches. This parameter can be adjusted.

The algorithm creates random data sets that simulate user connections and the probability of choosing a value for an attack. Initial data - anonymized statistics of 1000 users of the VKontakte social network system (official link is https://vk.com).

Further, the average number of user connections and the average deviation from this value are estimated. It is advisable to evaluate them on the basis of real statistics of the simulated group of the educational project. In groups of educational projects, in comparison with the social network in general, there are fewer participants and they are interconnected, so it is necessary to assess the probability of a connection between simulated accounts. The calculation is performed for each account, which allows us to normalize the number of links, the probability of following a link depending on the number of matches for the types of these accounts and the links already created.

Then, the account's resistance to phishing attacks was assessed. Three types of resistance to phishing attack are considered, since the attack itself can come from a friend, from a subscriber, from a random account. The assessment of the primary indicator is presented at [11].

Individual resistance is calculated when simulating an attack, depending on the attack settings and account indicators by formula:

$$100 - \frac{Yz\ + \frac{J}{MaxJ} * 100}{2} \tag{1}$$

where Yz - account vulnerability, which is calculated as: 100 - Set. (1, 2, or 3);

J - the number of data types for the current account;

MaxJ - the maximum number of account data types.

Therefore, it becomes an ability to lower the user's stability depending on the amount of information available to the user account and important to the attacker. During an attack, user resistance indicators will increase by a resistance step if the attack against the user is successful (depending on the setting). If all resistance indicators exceed the value of 100, the user gains attack immunity.

3 Experimental Results

Consider the results of 12 attacks carried out with the same settings, on one simulation of a social network, but with a return to the initial state of the results after each attack. For 1000 accounts on a simulation model of a social network of a networked educational project with 35 types of data connecting users and an average of 151 users exposed to the primary attack:

1. The number of attacked accounts ranges from 170 to 254.
2. The number of successfully attacked accounts ranges from 16.6% to 24.8%.
3. At the same time, the number of accounts that will not be attacked in the future (become immune to attack) is only from 0.1% to 2.2%;
4. For users with missing matches on the original dataset, the probability of a successful attack is only 0.3% (it is necessary to understand that in one group of the educational project there will be a minimum or no such users); for users with matching datatype sets (even with replay resistance) there is a 24% chance of a successful attack.

Increasing the resilience step, that is (by ability to educate users to counter phishing attacks) dramatically increased the possibility of a re-attack failing. For example, when entering a training condition, the number of attack-resistant accounts of the simulation model during the first iteration of attacks was 44.1%.

In addition, the difference between mass attacks and attacks across a small number of accounts was assessed. In the case of an attack using 2.5% of nodes as attackers, the number of successfully attacked accounts for three attacks increased to 48.1%, even taking into account the resistance to repeated attack.

Considering further possibilities of using the obtained data or changing the alleged attack vector, it is necessary to take into account the characteristics of the platform used to implement user interaction with the training material and grading.

Moodle is one of such platforms, which are often used in the Russian and world-wide education processes. Like any web-based system, it has a number of vulnerabilities [12]. Let's consider some of vulnerabilities, dividing them into four categories:

- **Informational.** CVE-2019-3810 allows to get information about the full name of users when they hover over the profile picture. CVE-2019-3848 due to incorrectly set permissions before loading information about the edited calendar event in the modal window allows other users (with rights above the guest account) to get read access to this information. CVE-2019-10154 a web service that retrieves messages without being limited to the current user's conversation.
- **Cross-Site Request Forgery** (CSRF). CVE-2019-10186 missing session key token when loading / unloading XML by the administrator.
- **Privilege escalation**. CVE-2019-3849 Users can assign themselves a promoted role in a course or current educational context available through Learning Tools Interoperability (LTI) by changing the request to the LTI publisher site.
- **Interaction with third-party resources**. CVE-2019-3850 Opening links in comments in the same window. CVE-2019-10133 The course subgroup form contained a redirect field unbounded by internal URLs.

The given examples of Moodle vulnerabilities allow obtaining the necessary information for the operation of the considered model based on identifying the context of interaction. Also, using the profiles of the interaction participants most susceptible to phishing attack according to the model, it is possible to access control materials on the platform or gain access to the end nodes of the participants using additional exploits.

4 Conclusion

The main vulnerability of a networked gamified educational project is user’s interactions. From the point of view of pedagogical technology, such an implementation of the principle of open education approach, which implies free use of links in projects and different fragments of information from the "outside world", and lack of control over internal and external relations, may endanger online educational system. Nevertheless, the possibilities for predicting phishing attacks on participants in online gamified educational projects exist and are feasible.

References

1. Yasin, A., Liu, L., Li, T., Fatima, R., and Jianmin, W. Improving Software Security Awareness Using A Serious Game. *IET Software*, vol. 13, no. 2, pp. 159-169, 2019.
2. Yasin, A., Liu, L., Li, T., Wang, J., and Zowghi, D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Information and Software Technology*, 95, 2018, pp. 179–200.
3. Hart, S., Margheri, A., Paci, F., and Sassone, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security*, Vol. 95, 2020, 101827.
4. Seaborn, K., Fels, D. I. Gamification in theory and action: A survey. International Journal of Human-Computer Studies, 74, 14-31, 2015. http://dx.doi.org/10.1016/j.ijhcs.2014.09.006
5. Grandhi, S.R., Galimotu, N.C. Understanding social engineering threats in massively multiplayer online role-playing games: an issue review, GAP Indian Journal of Forensics and Behavioural Sciences, Volume 1, Issue 1, 66-71, 2020.
6. Kang, L., Chek, K., and Choon, L. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106. pp. 1-20.
7. Chaudhry, J.A., Chaudhry, S. A., and Rittenhouse, R. G. Phishing Attacks and Defenses. *International Journal of Security and Its Applications*, Vol. 10, No. 1(2016), pp.247-256. http://dx.doi.org/10.14257/ijsia.2016.10.1.23
8. Sahu, K.R., Dubey, J. Article: A Survey on Phishing Attacks. *International Journal of Computer Applications* 88(10):42-45, February 2014.
9. Safonov, K.V., Zolotarev, V.V. Assessment of vulnerability to phishing of participants in online gamified educational projects in the field of information security [in Russian]. *Bulletin of the Krasnoyarsk State Pedagogical University named after V.P. Astafieva*, 52 (2), 2020, p. 76-84.
10. Basarab, M.A., Ivanov, I.P., Kolesnikov, A.V., and Matveev, V.A. Detection of illegal activity in cyberspace based on the analysis of social networks: algorithms, methods and means (review) [in Russian]. *Issues of Cybersecurity*, vol. 4 (17), 2016, p. 11-19.
11. Kuznetsov, M. V., Simdyanov I. V. Social engineering and social hackers [in Russian]. SPb.: BHV-Petersburg, (2007), 368 p.
12. Moodle: CVE security vulnerabilities, version and detailed reports. https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105