 doi:10.20944/preprints202003.0139.v1

Review

A Review of Gamification Applied to Phishing

Franklin Tchakounté[1,*], Leonel Kanmogne Wabo[1,*] and Marcellin Atemkeng [2]

[1] Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundéré; tchafros@gmail.com
[1] Department of Mathematics and Computer Science, Faculty of Science, University of Ngaoundéré; waboleonel@gmail.com
[2] Department of Mathematics, Rhodes University, 6140 Grahamstown, South Africa, M.Atemkeng@ru.ac.za

* Correspondence: tchafros@gmail.com (F.T.), waboleonel@gmail.com (L.K.W.)

Abstract: Phishing is a set of devastating techniques which lure target users to provide critical resources. They are successful because they rely on human weaknesses. Gamification which is a recent and non-traditional learning method with purpose to motivate and engage user to carry out activities, is more and more applied to prevent such cyber threats. This paper provides the first survey of gamified solutions dedicated to educate against phishing from 2007 to 2019. The investigation is conducted on eight proposals in terms of core concepts, game mechanics and learning process. We provide three taxonomies of dimensions to systematically characterize researches on gamified solutions, discuss lacks of surveyed works and opens further orientations to enhance this research area. Some key results are: solutions do not consider elementary level of knowledge and do no offer basic notions; solutions are not adapted to general audience and therefore not reliably applicable in different contexts; platforms partially educate about phishing; learners are evaluated predictably and within a short period. This study constitutes a cornerstone to understand and enhance research on phishing education.

Keywords: education; cyber threats; gamification; phishing; survey; taxonomies

1. Introduction

Phishing is defined as "*a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.*" [1]. Phishing is one of the serious threats within cybersecurity [2]. Anti-Phishing Work Group (APWG) reported that the first quarter of 2018 had recorded an increasing number of phishing attack up to 46% compared to the last quarter of 2017. Phishing exploit users' weaknesses and computer or technology weaknesses [3,4]. Phishing attacks can be delivered through three main media which are Internet, Short Message service (SMS), and voice with the help of social engineering tips. Financial gain, fame and notoriety are the main motivations behind phishing [5]. One mechanism in literature to decelerate phishing is to provide up-to-date surveys to readers for examining gaps and open issues. Authors survey attacker strategies and solutions to detect and prevent phishing ([5–8]). They also propose solution taxonomies and elaborated challenges issues to which research should be orientate to mitigate this flaw. Preventive solutions consist to increase awareness and educate users by designing educative platforms. A new interesting potential in the 21st century to build such learning tools is called gamification [9]. It provides an immediate end-user's behavior change [10]. Gamification is an interactive mood for education on specific topic, engaging and keeping learner focuses on activities with fun, compared to the traditional methods like instructor-based, or email based message

methods. Cybersecurity has just started dedicating gamification to make user aware about threats and adopt safety behaviors [11]. There are considerable solutions relying on gamification to fight against phishing ([3,4], [12–17]). A review of these preventive approaches does not exist in literature at this moment. We propose three taxonomies of dimensions in which surveyed solutions are classified and open issues for further research. This paper proposes three contributions.

- This paper is the first contribution in terms of reviewing anti-phishing proposals based on gamification, in terms of core objectives, game mechanics and learning processes.
- This study provides three taxonomies of dimensions to systematically characterize researches on gamified solutions.
- This research identifies key orientations that require further exploration and research for enhancing gamification in phishing education.

The rest of the paper is organized as follows. Section 2 surveys research works investigating gamification on phishing. Section 2 presents concepts about gamification and phishing. Section 3 describes the research methodology. Section 4 designs the taxonomy to characterize surveyed papers. Section 5 describes existing works and classifies them into proposed taxonomies. Section 6 discusses weaknesses and strengths and proposes new orientations for improving this research area. The last section concludes the study.

2. Related Surveys

There are several surveys in literature concerning phishing threats: those which review detective anti-phishing techniques and those related to gaming but in cybersecurity in general. They are described in the following.

2.1. General Survey about Phishing

Khonji et al. [6] present mechanisms of protection against phishing such as detection, offensive mitigations, correction, and prevention. Tewari et al. [7] investigate approaches anti-phishing, and discuss their strengths and weaknesses. Gupta et al. [5] review background of phishing attacks, provide taxonomies of existing solutions against and provide open issues and challenges to face for upcoming attacks. Aleroud et al. [8] survey phishing attacks and phishing countermeasures in modern and traditional environments. They provide taxonomies of attack approaches, anti-threats, host environments and channels of communication. Chiew et al. [2] investigate deeply characteristics of phishing attacks in terms of vectors and mediums.

2.2. Gaming for cybersecurity

Some authors investigate gaming technologies to raise awareness broadly in cyber security. Alotaibi et al. [10] review gaming applications and their efficiency to educate on cybersecurity. Tioh et al. [9] review serious games approaches applied in cyber security. Both works are too broad studying cyber security and they rely on different aspects of gaming.

The aforementioned works relate that educative solutions are essential to raise awareness and to complement detective solutions. These reviews investigate artificial intelligence and classical gaming mechanisms. But none of them surveyed specifically gamification approaches for phishing education.

3. Preliminaries

 doi:10.20944/preprints202003.0139.v1

3.1. Phishing

Phishing is a cybersecurity threat recognized online as identity theft, which records significant evolution since the first attack on users' accounts of America On-Line (AOL) in 1996 [5]. Attacking strategies fall always into one of the three groups: mimicking attack, here attackers lure their victims with visual illusory tips [2]. The two others are forwards and pop-up attacks where attacker uses mainly Man-in-the-middle techniques and tools. Among the well-known phishing attacks encountered in the literature, there are:

Spear Phishing

Spear phishing is recognized to be a targeted attack compared to traditional approach where attacker sent massive emails to random email addresses. With spear phishing, attack is designed for specific group of person or organization.

Social Engineering

This type of attack is frequently delivered through emails, websites, and social media, among others. The purpose is to lure potential victims that they are making a rational action, while it is an emotional action.

Drive-by-download

This attack affects the victims' computers with a malicious program (malware), virus or shell-code. The malicious program can infect through an email attached document or when user visits some malicious websites.

Whaling

The whaling attack like spear phishing is a targeted attack. It targets important responsible of organizations or enterprises with high privileges. This kind of attack requires more effort and time to phishers because they need to study and spy their potential victims, to design and deliver accurate phishing attack.

Smishing

Smishing is a form of phishing attack through Short Message Service (SMS).

Vishing

Vishing is a form of phishing attack through voice call, conducted mainly via VoIP.

These are only few forms of phishing attack among a wide range of possible scenario of attack. Nevertheless, refer to [2] for a landscape overview of phishing attacks and possible combination of them.

3.2. Gamification

This section presents concepts around gamification.

3.2.1 Definitions

Literature adopted the definition of Deterding and colleagues stating that gamification is "the use of game design elements in non-game context" [18]. The concept of gamification has gained many domains of activities and according to those domains, this definition can differ slightly. For instance, concerning education and training, it is defined as "the use of game-based mechanics, aesthetics, and thinking to engage people, motivate action, promote learning, and solve problems" [19]. Gamification is encountered into fields like marketing and business, health, public governance,

 doi:10.20944/preprints202003.0139.v1

and learning to name just few. Indeed, game-based learning is recognized to enhance learner motivation, outcomes, and participation to activities [20].

3.2.2 Categories

There are two categories or types of gamification: structural gamification and content gamification [21]. A structural gamification is the process of applying game elements to drive learning through content without altering this content. So, the learning content does not become game-like, but structures around do. While, with game-like content and game thinking elements alter learning contents and make it more game-like, like using a story or challenges to present lessons.

3.2.3 Mechanics

Game mechanics used for a gamification project differ from one project to another. But there are Points used to reinforce and rewards good action or behavior, badges which are generally digital token and used to support achievements and provide some kind of recognition, leaderboards are used mainly for ranking and can be viewed as public recognition of work done. These three elements represent the core gamification's elements encountered into the literature ([12,22,23]). We can add levels, challenges or quests to these elements. However, Kim et al. [24] propose a taxonomy with fifteen elements for education domain.

3.2.4 Gamification designs

There are four frameworks relevant for designing gamified solutions in literature.

a) User-Centered Design: User-Centered approach focuses therefore on user. User needs and goals are central objectives of this design and its development process. According to Nicholson et al. [25], "this framework places the user at the center of the experience and designing process with their needs and desires in the mind".

b) MDA framework: MDA gamification framework was proposed by Hunicke et al. [26]. This theoretical framework stands for Mechanics, Dynamics, and Aesthetics. It is mainly used for pure game design purpose. This framework breaks game design process into three steps which are: rule, system and fun. These steps are translated respectively into mechanics, dynamics and aesthetics: Mechanics describes the particular component of the game at the level of data representation and algorithms; Dynamics describes the run-time behavior of the mechanics; and finally, Aesthetics describes the emotional response when the player interacts with the game system.

c) Schell's framework: Schell's gamification [27] considers four game elements such as story, mechanism, technology, and aesthetic. Story represents the path of event that player can experiment while playing the game. Mechanism describes rules and procedures for the game, and it affects the evolution of the story. Technology includes materials, hardware for game creation. Aesthetic deals with look and feeling that player can get within the game through audio and visual elements which directly influence player experience.

d) Werbach and Hunter's framework: This framework was proposed by Werbach and Hunter

[28], commonly known as 6D framework and encompasses the following steps: definition of business objectives and then proceeding to target the outcome behaviors; description of players; devising the activity loops without losing the fun; the last step is to deploy the gamified solution with the necessary tools. Mora et al. [29] propose to classify different frameworks into three categories: user-centered, game-centered, and technology-centered, with self-determination theory (SDT) as a predominant approach to support intrinsic motivation.

3.2.5 Games vs. Rewards vs. Gamification

There are more or less relations between games, rewards and gamification which share similar mechanics [21]. Rewards programs are programs which use game mechanics to engage user at transactional level, mainly used into business domain to keep user into a consumption loop. Games

 doi:10.20944/preprints202003.0139.v1

are more related to entertainment, with characteristics like fun as the primary currency. Its activities are chosen for their light-hearted character. They are governed by rules and uncertain since the outcome could be other than what player expect. Games also used fiction to immerse player into an imaginary word [29]. Gamification has different purposes in contrast with games and rewards programs. There is no entertainment but fun, the objective is to motivate people to carry out by the funny way some boring task [29]. It engages users at the emotional level for attitudes and behavior change, as well as knowledge acquisition [30]. Nevertheless, there are not clear boundaries between these concepts of games, rewards programs and gamification [19].

4. Methodology

The research methodology follows basically seven main steps:

- The first step defines the research questions required to set the scope of the paper and identifies the relevant information to collect the literature.
- The second step consists to select different search keywords able to retrieve the largest possible set of relevant publications.
- The third step is a keyword-based search on Google scholar.
- In the fourth step, exclusion criteria are used to filter results.
- The sets of results from both search strategies are merged to produce the overall list of publications to review.
- A pre-processing from the selected papers is made with the aim to identify criteria to categorize them. A systematic literature review taxonomy based on those criteria is built.
- Reviewed results are analyzed to identify gaps and future directions within "malware detection based on system calls" research area.

4.1 Research Questions

This paper aims to address three research questions:

RQ1: How to classify current research on gamification solutions for phishing?

RQ2: What is the current state of gamification for phishing with respect to the proposed taxonomies?

RQ3: What are the weaknesses in the current research and what enhancement can be performed?

4.2 Search Strategy

Some keywords have been exploited to perform the search. The search terms include keywords that are related to (1) gamification, (2) phishing, (3) phishing education, (4) learning and (5) awareness. Table 1 shows keywords used in a manual investigation in Google scholar.

Table 1. Keywords

Line 1	Keywords
1	gamification; phishing
2	gamification; phishing; awareness
3	gamification; phishing; learning
4	gamification; phishing; education
5	phishing; awareness

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

A search string includes a disjunction of the six lines of keywords, i.e. R =: line 1 OR line 2 OR line 3 OR line 4 OR line 5 OR line 6 where each line is the conjunction of its keywords.
For instance, e.g., line 6 = phishing AND learning

4.3 Inclusion and Exclusion Criteria

Google scholar was exclusively the collection repository of retrieved papers. The search done using the terms in Table 1, provides a dataset of 110 papers. The dataset has been filtered based on exclusion and inclusion criteria.
Papers excluded are those:

- dealing with educational solutions other than gamification, such as gaming;
- dealing with cyber security in general;
- which apply gamification to areas other than phishing.

Papers retained are those dealing with gamification applied specifically to phishing and its related forms such as spear-phishing, vishing etc.. Thirty (24) papers remained after applying the above criteria. A careful manual filtering was performed to purge irrelevant publications related to this area. This activity allows keeping eight (08) papers. Figure 1 shows these papers by publication years.

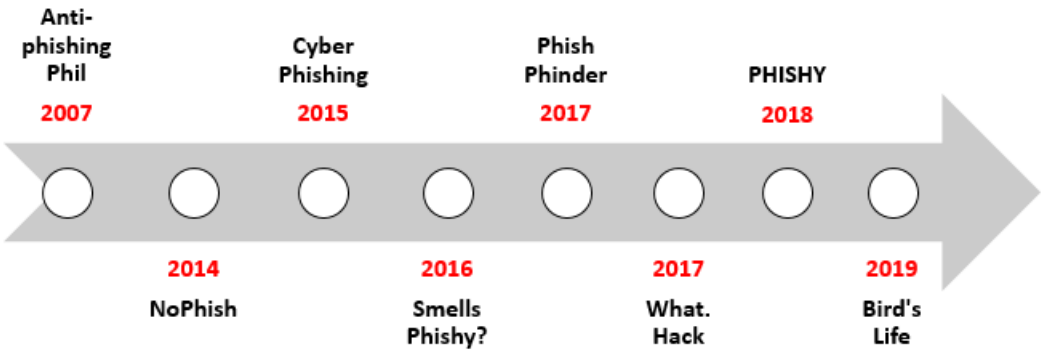


Figure 1. Timeline of solutions

Table 2 presents where they are published (journal, conference or preprint) and their names. It is noticed that only one research has been published in a journal. Most authors presented solutions in this area in conferences and symposiums. They sought to interest large people while exposing their works.

Table 2. Paper sources

	Journal (J) or conference (C)	Name of journal or conference	Year
Anti-phishing Phil[12]	C	Third symposium on usable privacy and security	2007
NoPhish[13]	C	International Workshop on Security and Trust Management	2014
CyberPhishing[14]	C	Hawaii International	2015

		Conference on System Sciences	
Smells Phishy?[15]	C	APWG Symposium on Electronic Crime Research (eCrime)	2016
Phish Phinder[3]	C	Eleventh International Symposium on Human Aspects of Information Security & Assurance	2017
What.Hack[16]	C	CHI Conference on Human Factors in Computing Systems	2017
PHISHY[4]	C	2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts	2018
Bird's Life [17]	J	Journal of Cybersecurity Education, Research and Practice	

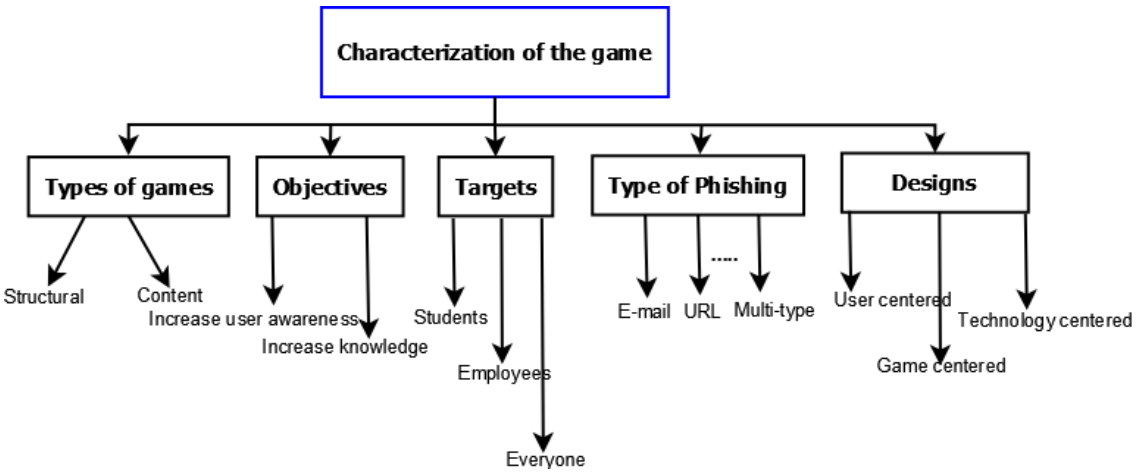
5. Taxonomies

This paper provides different dimensions and properties found in existing surveys. The proposed taxonomy is designed in three sub-taxonomies relying on the surveyed works. The hierarchy of that taxonomy categorizes research following three questions:

1. What are the contextual characteristics of the gamification solutions?
2. What are the structure components of the gamified systems?
3. How do authors evaluate and validate their solutions?

5.1 Taxonomy 1

The first part of the taxonomy concerns the characterization of the game. It includes five dimensions, as shown in Figure 2.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

Figure 2. Taxonomy 1: characterization of the game

Type of games: This dimension indicates types of games meaning that on which elements does the game focus on? The first possibility is that educative solutions can be built around structures and the second possibility is that they can be built around contents.

Objectives: Raising awareness about phishing does not mean that user has knowledge about phishing. This dimension is about categorizing researches aiming to increase awareness and to increase knowledge to recognize and avoid phishing.

Targets: The designed solutions target three categories of people. The first category includes students, the second employees and the third everyone. Researches are originally built for specific nationalities.

Types of phishing: Authors deal with different categories of phishing: email phishing, URL phishing and fake attachments.

Designs: There are four different frameworks: User-Centered, MDA, Schell's, Werbach and Hunter's. They can be summarized in User-Centered, Game-centered, and Technology-centered.

5.2 Taxonomy 2

The second taxonomy concerns different elements constituting the gaming platform. It includes six dimensions, as shown in Figure 3.

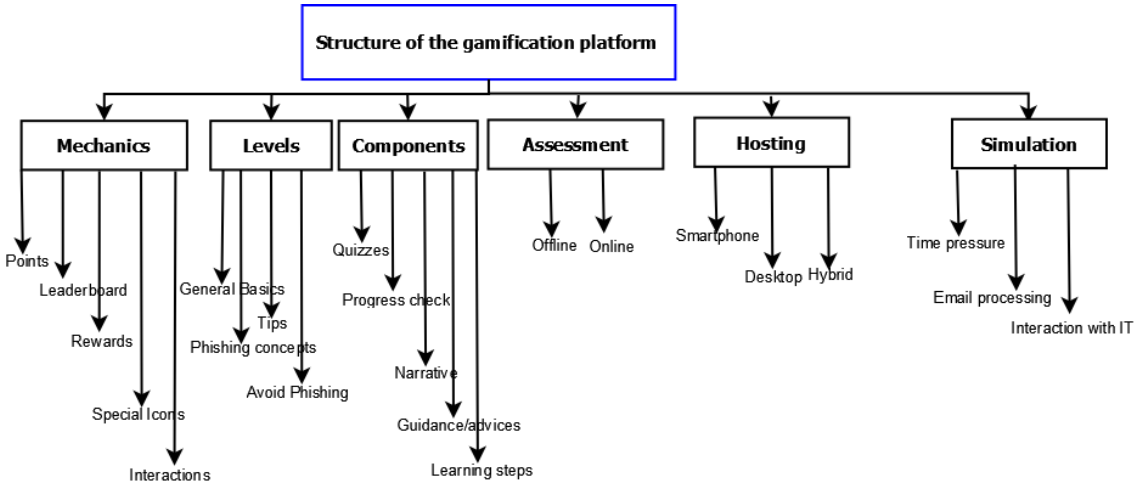


Figure 3. Taxonomy 2: structure of gaming platform

Mechanics: Mechanics aim to build satisfying experience to users by involving engaging and interacting methods. For instance, points to evaluate players, badges for recognition of accomplishments, leaderboards to present order of merit, challenges to assess knowledge, levels to indicate progress and rewards to encourage players.

Levels: Every gamified platform includes different level of learning. First, it starts from general concepts in relation directly or indirectly to phishing such as URL, email, etc. Second, people learn about phishing concepts from basics to advanced scale. Third, people learn about how to identify phishing aspects and four, some tips to prevent such scams.

Components: This dimension includes core elements built within the framework. They are

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

- Narrative that explains to the player what has been realized so far, the actual state of the game and the remaining steps;
- Learning steps as described in the previous dimension;
- Guidance that is referred if the player is not able to decide about the nature of URL or email;
- Progress check which controls the evolution of the game;
- Quizzes which assess the level of knowledge gathered in each step.

Assessment: This dimension is grouped in two categories: inline if players are evaluated within the platform and offline if players are evaluated outside the platform may be through emails.

Hosting: This dimension presents the device where people can install the gamified platform: Desktop or smartphone or hybrid.

Simulation: Platforms simulate real scenarios of phishing to bring players closer to reality. They simulate urgency, how an email is processed by attacker, and what vulnerabilities, the potential victim, derives while interacting with technologies.

5.3 Taxonomy 3

The third taxonomy specifies components considered by authors to evaluate gamified solutions. It includes five dimensions, as shown in Figure 4.

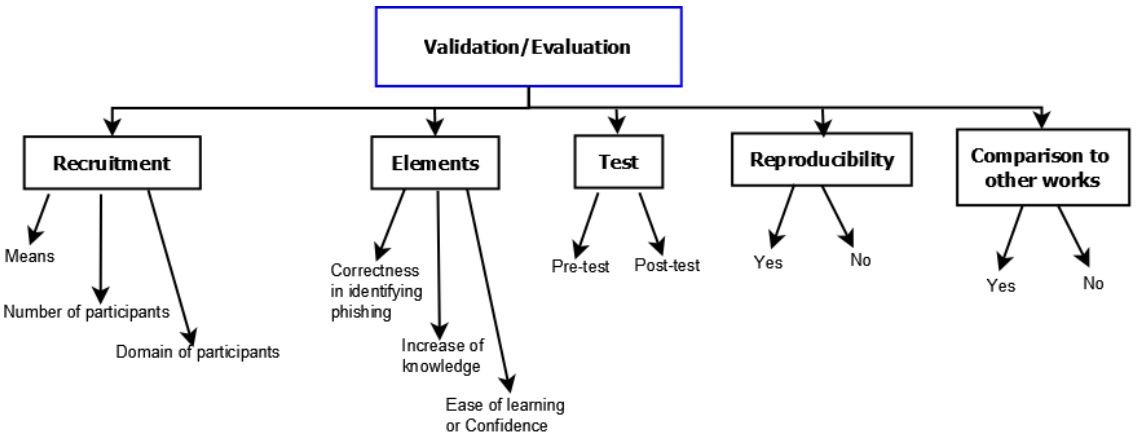


Figure 4. Taxonomy 3: Validation/Evaluation

Recruitment: This dimension includes different components of the recruitment process such as means to recruit participants, and number and domain of participants.

Elements: Research works evaluate correctness about gamified tools concerning identifying phishing as well as the level of increase of knowledge and the ease offered by the platform.

Test: Researches build a test before using the platform (pre-test) to measure the level of recognition and awareness concerning phishing. They let users exploit the developed solutions and make another test (post-test) to measure if there is any positive impact inferred by the platform.

Reproducibility: Any research should publish artifacts to be reproduced by any other researchers. This property is determined in this dimension.

Comparison to other works: Some authors compare similar works among others to validate their works and to show contributions and improvements.

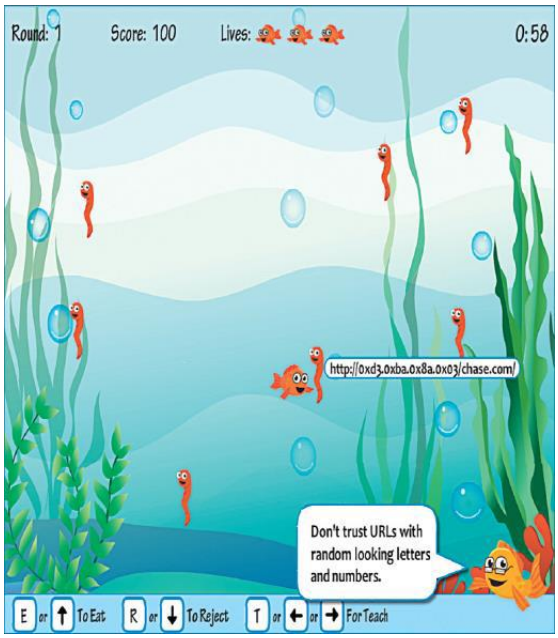
Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

6. Survey Results

This section has two orientations. The first shows a landscape of existing gamified solutions devoted to educate people about phishing attack, in terms of their core concept, game mechanics, as well as the learning process. The second orientation characterizes those works into different taxonomies.

6.1 First Step – Description of Existing Gamified Solutions

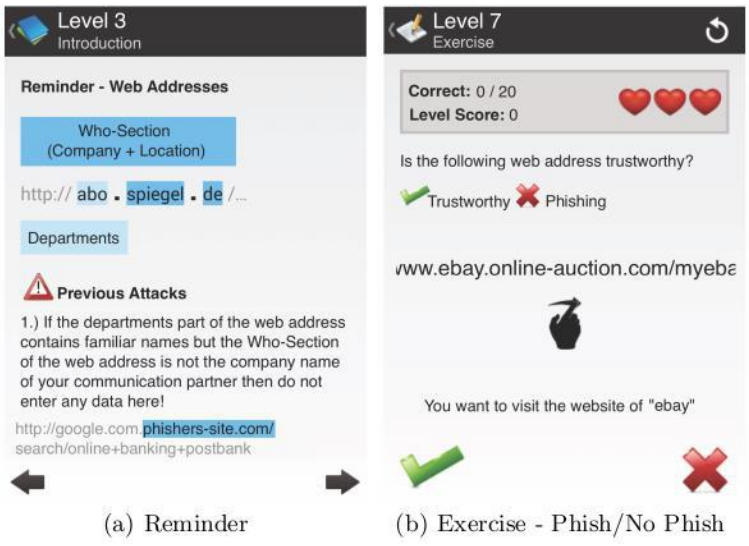
Anti-phishing Phil: Anti-phishing Phil (Figure 5) is a web-based anti-phishing solution devoted to teach users good habits useful to avoid phishing attacks [12]. Authors postulate that end users should be guided in automated system for detecting phishing attacks. It is justified because those systems are not 100% accurate especially when it requires some contextual knowledge information. So, it is important that user acquires some knowledge. This solution has three objectives: first, helping user to identify phishing websites by teaching user how phisher can manipulate the URLs to deliver malicious actions. Second, teaching user where to look into the web browser frame to appreciate the trustworthy and untrustworthy of a website. And third, teaching user to always use search engine with purpose to evaluate the legitimacy of a website. Authors deal with following learning contents organized into three categories: long URLs with subdomains, IP-based phishing URLs, finally similar and deceptive domains topic. The whole game turns around a small fish named Phil and its father. The game's entire story is around Phil living into a pond named 'Interweb bay'. Phil must eat worms present in the pond to become a big fish. Each worm is attached to some URLs of two statuses: benign and malicious. So, player through Phil has to be careful about which worm to eat. Players are rewarded with a certain amount of points (100 points) when players eat worm related to a benign link or reject bad worm. They lose one life when Phil eats worm with bad URL. Phil player can refer to Phil's father in case of doubt. Phil's father is an experienced and knowledgeable fish in the sea which provides advices and guidance to Phil when it requests him. Anti-phishing Phil is serious game based on learning science theory which savvy points, time pressure, life, and story as the main game mechanics. This game is split into four rounds, and each round takes two minutes long, and during this period Phil has to deal with eight worms.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

Figure 5. Anti-phishing Phil, https://goo.gl/mZHDAX

NoPhish: NoPhish (Figure 6) is an Android application dedicated to educate people about phishing by assessing, parsing and checking URLs [13]. They assume that smartphone users are more likely to access phishing websites than desktop users. This anti-phishing application was designed by following a user-centered design approach. NoPhish has two introductory parts. The first part referring to the game part includes several gamification's elements such as ten levels, with lives, levels, leaderboards and achievements. The first part is dedicated to raise awareness of spoofed messages. The second part presents to user how to access the address bar and view the entire URL within the mobile phone screen size constraints. They recommend that user to scroll entirely the address bar to view the complete URL. The core game part is split into ten levels with increasing difficulties. Each level has an introductory block and an exercise block. With NoPhish, there are not game characters like those encountered into Anti-phishing Phil solution. The player interacts directly with the learning content, and receives direct feedback based on their action made. Each user starts with three lives (represented by hearts), for a good answer, user receives a certain amount of points. The player should obtain a certain predefined amount of point to move from one level to another. In the first level, NoPhish provides learning about the structure of URLs, with purpose to equip user with the capability to properly parse URLs, before learning spoofing techniques. From level two to eight, user is presented with various URL spoofing tricks. Level nine deals only with HTTPS topic, since legitimate and phishing websites can both use it [13]. The last level shows remarks and advices.



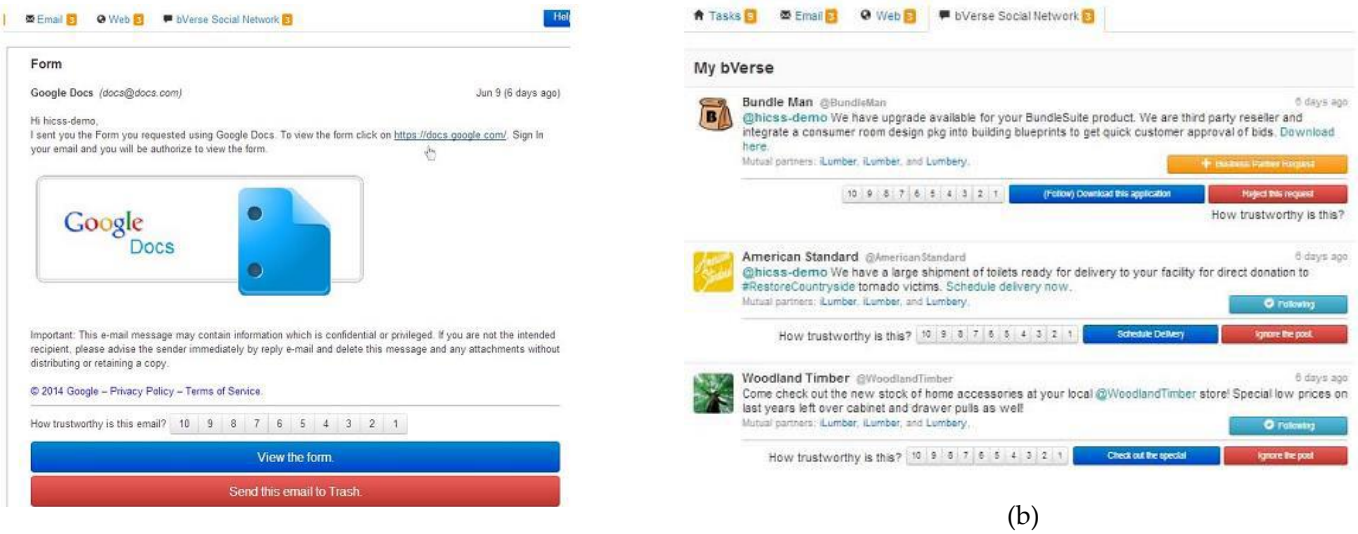
(a) Reminder (b) Exercise - Phish/No Phish

Figure 6. NoPhish [13]

CyberPhishing: CyberPhishing (Figure 7a and 7b) is a web simulation platform allowing researchers to dynamically build content and then, customizable experience related to phishing [14] . The idea behind this tool is that realism should pervade user experience and immerse user within the context. To achieve this vision, the application includes three primary interfaces which show real world experiences. The first one is a story dashboard used as landing page. The second

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

one is an email inbox simulation interface which presents emails (phishing and normal) to user as standard real mail client do, like Gmail. The third one is a real simulation of web browser with security elements like https lock icon, certificate information for simulated site, shows simulated URLs, and capabilities of encountered within an email interface. Game mechanics used are point (score), badges and titles. Among the simulated scenario of this platform there are: people posing as friends on social media, suspicious links and pop-ups within the content of the web browser, information on item prices too good to be true (appealing offer online), call for some emotions like urgency and greed, usage of some greeting and catching phrase by phisher, instances of poor spelling within an email or web page for instance, to name just few scenarios. Realism is the vital characteristic of this anti-phishing solution, as well as the learning content. But the experimentation process seems a bit complex as it walks through different phases.



(a) (b)

Figure 7. (a) CyberPhishing – Email simulation [14] (b) CyberPhishing – Social media simulation [14]

Smells Phishy?: Smells Phishy? (Figure 8) is a game designed by Baslyman and Chiasson, to raise users' awareness about online phishing scams [15]. The game's scenario used to educate user is based on real life activity which is online shopping. This game is under three purposes. The first purpose is to teach user about phishing scams, how to protect themselves, as well as the importance to remain vigilant online. The second purpose is to entertain learner by promoting fun. This purpose is used to encourage player to continue the learning process and acquire knowledge without feeling bored. The third purpose is to provoke discussion and debate among player on phishing related topics. This purpose will help to link the cybersecurity learning content to their real-life activities. Players start the game virtually with certain amount of money (pre-paid credit card) and a list of items that they should buy. Each action yields a positive or negative outcome which will affect the game process. Authors used cartoon to depict the game by using cards (task cards, police cards, credit cards, hint cards, and shopping lists). Police cards are used to show consequences of player's action. If the player falls for phishing scam, two outputs are possible: redirection in jail for a turn and loss of money. But, when an appropriate action is taken, the player is congratulated and may receive a certain amount of money. The game can be played by 2 to 4 players simultaneously and the winner

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

is the first who completed tasks on the purchase list and has the most remaining money. Authors have tested their solution on 21 participants and receive globally a positive feedback. The phishing scenarios tested were URLs and website content, phishing related and identity theft, use anti-phishing tools, attention to security indicators.

Figure 8. Smells Phishy? [15]

Phish Phinder: Phish Phinder (Figure 9) is a serious game prototype designed by Gaurav and colleagues to boost the user's confidence. It mitigates phishing attacks by providing both conceptual and procedural knowledge on phishing [3]. Users are trained through a series of gamified challenges, designed to educate about most relevant phishing related concepts, all this within an interactive User Interface (UI). The key aspect of this solution is 'self-efficiency or self-confidence', as users make better decision when they are confident and sure on their skills and ability to deal with not difficult situations [31]. Unlike the two first solutions, Phish Phinder deals with the phishing email topic rather than only URLs topic. Indeed, this solution introduces phishing email's concepts like: subject line, reply-to, HTML in the body of the email, and spoofed email' sender name. Nevertheless, Phish Phinder is too similar to Anti-phishing Phil. Indeed, the core game story turns also around a small fish and its father, an experienced big fish. The young fish is named 'Johnny' rather than 'Phil' and the second a knowledgeable big fish is named 'Shifu'. There are also worms that the small fish should eat to become a big fish. Johnny has to take care as each worm as it is attached to the content. This content could be a URL or an email message. There are obviously good and bad worm. However, authors argue that their solution is different to [12] in the way that it integrates self-efficiency to the game processes. An interesting concept of this solution as technology evolves is that authors present URLs obfuscation techniques like URL's shorteners. But they lack to show its malicious utilization to deliver phishing attacks. Although Phish Phinder is still a prototype project, it presents and deals with very important phishing topics.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

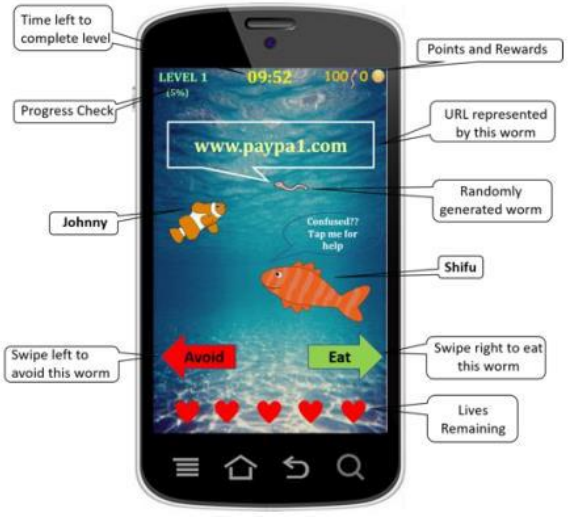


Figure 9. Phish Phinder [3]

What.Hack: What.Hack (Figure 10) is an anti-phishing game built to teach defense methods and information security for social engineering threats. The player walks through a sequence of puzzle [16]. Each puzzle requires that the player respects some set of rules recorded into a rulebook. The rulebook determines which emails are safe and unsafe and which grows in complexity. The educational objective of this game is twofold. The first teaches user how to safely handle URLs, social media and attachments. The second learns how social engineering attacks can lead to significant security breaches, through a narrative and engaging approaches. Authors argue that Antiphishing Phil is the most popular interactive, game devoted to teach users how to spot out phishing URLs. What.Hack simulates email client software, used by the player as a worker of a big enterprise (Big Red Bank) within the game story. The player should assess business emails and indicate if it is safe or unsafe to conclude a deal. The player provides a yes or no decision based on the simulated email transferred to the client software. When the player starts, there is only one rule, but along the game, others rules are added and the game become complex. Authors added non-player assistance named Cherise to support the gamified process of teaching conceptual knowledge before stating each challenge. This assistance tells the player which new features make an email malicious. However, the player can also ask Cherise for help. Cherise pop-ups and introduces elements to help the player to deal with the next email but at the end of a party.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

Fig. 10. What.Hack [16]

PHISHY: PHISHY (Figure 11) is a serious game dedicated to train enterprise users by raising phishing awareness. The user is educated on various aspects of phishing URLs and how to spot them out [4]. The main objective of this solution is to provide phishing awareness training to enterprise users through three main points: identifying phishing URLs, getting familiar with short URLs, and searching online for brand names to get the legitimate URLs. PHISHY is a story-based game and single-player with the central character of the game story named 'Sam'. At the beginning of the game, the story is introduced using a comic format, summarized as follow: Sam received a message on its phone telling that he won a lot of money and all-expense trip for a paradisiac island. He must confirm banking details by clicking on the link provided with the message to accept that opportunity. Sam is excited about the offer, and proceeds without extra verifications. When Sam realized that it was a scam, it was too late and criminals have taken all his money and leave him on the boat with a hungry tiger, in the middle of the ocean. Therefore, Sam has to struggle to survive and back to the shore, while Sam fails to feed fish, the hungry tiger moves one step forwards on Sam's direction. As the main challenge, player navigates the boat to safely reach the shore through three levels each focusing on specific type of phishing URLs. The first level hooks fish for the hungry tiger. The second level correctly answers questions per hook, by applying the onscreen tips. The third level avoids dangerous fishes like sharks and tentacles. The main game mechanics are points, life, levels, and no timer. The game survey shows in general valuable outcomes, and sustains the fact that game-based learning can positively help to train users.

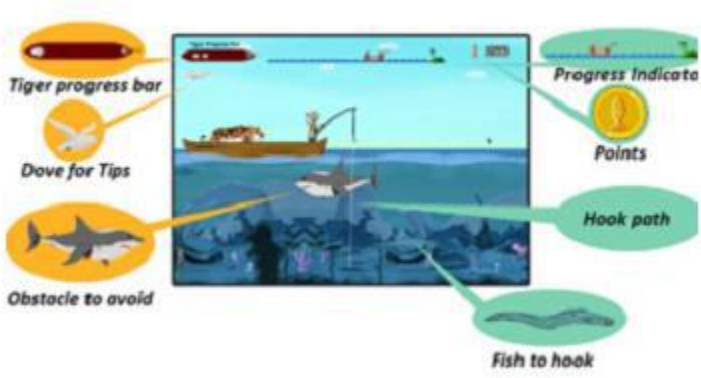


Figure 11. PHISHY [4]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

Bird's Life: Bird's Life (Figure 12) is a 2D educational game aiming to teach college students about cybersecurity [17]. Players learn phishing attacks and anti-phishing techniques through real-world scenarios by using a fun gaming context. Bird's Life is a decision-making game, where the main character is controlled using arrow keys on PC and motion controls on mobile devices. It is structured in three main levels: level one introduces the game story, in which designers encourage player to dive into the game. Level two gathers phishing prevention tips. The player starts with five lives, the learning currencies are worms in this level. Red worms represent phishing email and scam whereas grey worms represent tips that user should collect (five grey worms collected consecutively give a tip). Rewards earned can be used to purchase health. At the end of this level, player is expected to know exactly what to do during a phishing attack before diving into the last level. During the last level, player uses knowledge acquired during the previous level to spot out phishing emails. The player needs to answer four correct on five questions to pass the level.

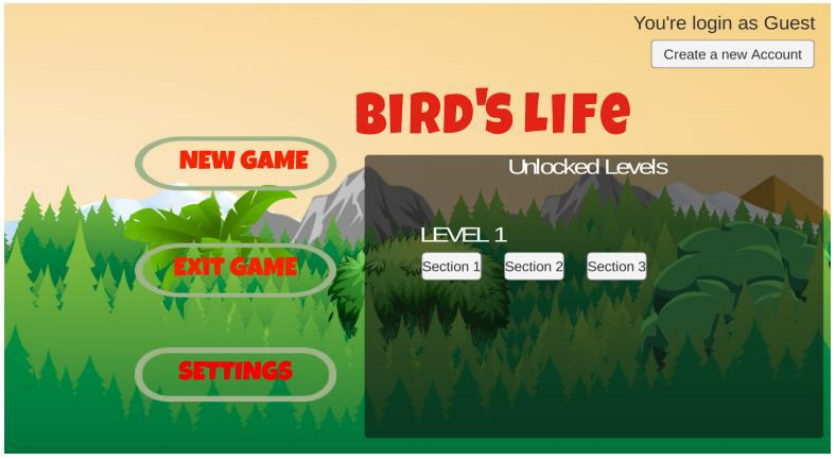


Figure 12. Bird's Life [17]

6.2 Second Step –Classification of Proposals in Taxonomies

1) Classification according to characterization of the game: Table 3 classifies different approaches into dimensions related to game characteristics. Seventy-five of solutions focus on mixed elements for a game-like education. Two of them (PHISHY and Bird's Life) as well as the two others (What.Hack and Cyber Phishing) also focus on structuring narrative that supports the overall learning. The studied solutions aim to increase knowledge to identify phishing scams (at 75%). Some authors (the half) also dedicated their solutions to make users aware of phishing before providing learning materials for detecting malicious traces. Author developers target every end-user even if learning contents are specific to some languages and habits. The type of phishing that is mainly learned is URL phishing which lures users with fake domain names (87.5%). It is followed by phishing exploiting fake attachments into emails (75%). The half of solutions provides email learning phishing contents. Authors have designed their tools to put users in the center of learning with gaming elements which provides a friendly environment. None of these solutions focuses on improving used technologies exploited to design the platform. It is noticed that NoPhish has no design basis.

 doi:10.20944/preprints202003.0139.v1

2) Classification according to the structure of gamified platform: Table 4 classifies different approaches into dimensions related to structure of gamified platform. Authors insert mechanics such as points (75%), rewards (75%), interaction mechanisms between learning materials and the platform (50%), and leaderboards (12.5%). We see that those mechanics exist to engage and motivate the player along the game. They help to gamify nongaming educative environments. Most of gamified solutions start to describe phishing concepts, then ways to avoid phishing and tips to prevent phishing traps. No basic concepts related to phishing such as email structure or browser security indicators. To achieve learning objectives, authors define a story of learning which guides different steps involved in the learning process. Half of proposals are supported by a structure including steps. Each step is evaluated and validated and progresses are reported in seventy-five cases. Some advices are elaborated to assist in case users require more knowledge for decision making. Quizzes are designed to evaluate each step and the overall learning to measure user's understandings. Evaluations are made within the platform (87.5%). Most of proposals propose simulations of fake emails or URL and let the users recognize them as such. They also simulate urgency derived in fake email, email processing between the potential victim and the attacker, and behaviors of users with IT. Solutions are implemented to be deployed is desktop and some of them both in smartphone and desktop. Only one solution (Smells Phishy?) integrates several players compared to others with only one player.

3) Classification according to game evaluation**:** Table 5 classifies different gamified solutions into game evaluation dimensions. This part studies how authors validate the proposed solutions. Authors recruit people to test their solutions. This recruitment is done through flyers, interactions, email or website announcements and direct invitations. What.Hack and Anti-phishing Phil rely on flyers. The number of participants varies from 6 to 8071. The latter concerns people with diverse countries and different demography. Most participants are young students with age from 18 to 44 years old with no IT knowledge. These participants are submitted to a test before using the educative platform to measure the level of knowledge and awareness. This test evaluates their level of knowledge and awareness of phishing scams. Then they are submitted to the learning environment. They are finally tested with samples of emails and URLs and they are evaluated about correct recognition of phishing situations, and correct identification of the nature of email or URL (fake or real). Surprisingly, only two works publicize their platforms to enable exploitation by a third-party. In so doing, they make their research reproducible and scalable. The remaining six researches lack to do it. One research (What.Hack) provides a comparison with related solutions to show its contribution to others. This evaluation phase has not been done by others.

Table 3. Taxonomy on game characteristics

Dimensions	Sub-dimensions	Approaches	Percentage
Type of games	Structural	What.Hack, PHISHY, Bird's Life, Cyber Phishing	50%
	Content	Anti-phishing Phil, PhishPhinder, PHISHY, Cyber Phishing, Smells	75%

 doi:10.20944/preprints202003.0139.v1

		Phishy?, NoPhish	
Objectives	Increase user awareness	Smells Phishy?, PHISHY, Cyber Phishing, NoPhish	50%
	Increase knowledge	Anti-phishing Phil, Phish Phinder, Bird's Life, Cyber Phishing, Smells Phishy?, NoPhish	75%
Targets	Students	Bird's Life	12,5%
	Employees	What.Hack, PHISHY	25%
	Everyone	Anti-phishing Phil, Phish Phinder, Smells Phishy?, Bird's Life, NoPhish, CyberPhishing	75%
Types of phishing	E-mail / spear phishing	What.Hack, Phish Phinder, CyberPhishing, Bird's Life	50%
	URL / domain phishing	Anti-phishing Phil, Phish Phinder, What.Hack, NoPhish, Smells Phishy?, CyberPhishing, PHISHY	87,5%
	Fake attachment	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Smells Phishy?, NoPhish	75%
Designs	User-centered	What.Hack, Phish Phinder, Smells Phishy?, NoPhish,	50%
	Game-centered	Anti-phishing Phil, Cyber Phishing, Bird's Life,	37.5%

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 March 2020 doi:10.20944/preprints202003.0139.v1

	Technology-centered	-	0%

Table 4. Taxonomy on structure of gaming platform

Dimensions	Sub-dimensions	Approaches	Proportions
Mechanics	Points	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Bird's Life, Smells Phishy?	75%
	Leaderboard	Nophish	12,5%
	Rewards	Anti-phishing Phil, Phish Phinder, PHISHY, Cyber Phishing, Bird's Life, Smells Phishy?	75%
	Special icons	Phish Phinder, PHISHY, Cyber Phishing, Smells Phishy?	50%
	Interactions/competitions	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Smells Phishy?, Nophish,	75%
Levels	General basics	-	0%
	Phishing concepts	Anti-phishing Phil, Phish Phinder, Bird's Life, Smells Phishy?	50%
	Avoid phishing	What.Hack, Anti-phishing Phil, Bird's Life, Smells Phishy?	50%
	Tips	Bird's Life, Smells Phishy?	25%
Components	Narrative	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY	50%
	Learning steps	What.Hack, Phish Phinder,	75%

 doi:10.20944/preprints202003.0139.v1

		PHISHY, Bird's Life, Smells Phishy?, NoPhish	
	Progress check	What.Hack, Phish Phinder, PHISHY, Bird's Life, Smells Phishy?, NoPhish	75%
	Guidance/advices	What.Hack, Anti-phishing Phil, Phish Phinder, NoPhish	50%
	Quizzes	PHISHY, Bird's Life	25%
	Offline	-	0%
Assessment	Inline	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Smells Phishy?, NoPhish	87,5%
	Desktop	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Smells Phishy?, Bird's Life	87,5%
Hosting	Smartphone	Phish Phinder, Bird's Life, NoPhish,	37,5%
	Hybrid	Bird's Life	12,5%
	Time pressure	What.Hack, Cyber Phishing	25%
	Email processing	What.Hack, PHISHY, Cyber Phishing	37,5%
Simulation	Interaction with IT	What.Hack, Cyber Phishing	25%
	Fake email / URL	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY,	87,5%

		Bird's Life, Cyber Phishing	
Type of players	Mono-player	What.Hack, PhishPhinder, Antiphishing Phil, PHISHY, CyberPhishing	62,5%
	Multi-players	Smells Phishy?	12,5%

Table 5. Taxonomy on game evaluation

Dimensions	Sub-dimensions	Approaches	Proportion
Recruitment	Means	What.Hack(FL), Anti-phishing Phil(FL, EA), Phish Phinder(IV), PHISHY(EA)	50%
	Number of participants	What.Hack(39), Anti-phishing Phil (14), Phish Phinder(6), PHISHY(8071), CyberPhishing(14), Bird's Life (100), Smells Phishy? (21)	87,5%
	Domain of participants	What.Hack (students), Phish Phinder (students + academics), PHISHY (students + associates)	37,5%
	Age of participants	What.Hack(18), Phish Phinder(26-34), PHISHY(21-30), Cyber Phishing(28.3), Smells Phishy? (24 -44)	62,5%
Elements	Correctness in identifying phishing	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Smells Phishy?	62.5%
	Increase of knowledge	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Bird's Life, Cyber Phishing, Smells Phishy?	87.5%
	Ease of learning or confidence	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Cyber	75%

Test	Pre-test	Phishing, Bird's Life What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Bird's Life, Smells Phishy?	75%
	Post-test	What.Hack, Anti-phishing Phil, Phish Phinder, PHISHY, Bird's Life, Smells Phishy?	75%
Reproducibility	Yes	Anti-phishing Phil, NoPhish	25%
	No	What.Hack, Phish Phinder, PHISHY, Cyber Phishing, Bird's Life, Smells Phishy?	75%
Comparison to other works	Yes	What.Hack	12,5%
	No	Anti-phishing Phil, Phish Phinder, PHISHY, Cyber Phishing, Bird's Life, Smells Phishy?, Nophish	87,5%

FL: flyers, FI: Face-to-face interactions, EA: Email/Website announcements, IV: Invitation

7. Discussions and Open Issues

Some points are relevant to discuss and to explore.

7.1 Discussions

We first notice that almost all of these solutions deal with URLs obfuscation techniques used by attacker to trick people, but only few deals properly with email as the vector of phishing. Authors should concentrate on e-mail as starting point, and then bring the learner to fake URL or fake attachments. What.Hack shows an interesting point of view on this subject of emails assessment with their set of constraint rules, compared to Phish Phinder which remains a prototype. Nevertheless, these solutions globally yield positive outcome for phishing education, based on gamification approach. It is important to underline that all solutions presented above do not embody that learners may not have enough IT knowledge for understanding the learning content. Because when talking about URLs obfuscation techniques, it is necessary that learner already know at least what is a URL and its utility, etc. rather to directly present phishing techniques using URLs. NoPhish has attempted to show the structure of URLs, but they have performed it by using alias manner (the who-domain rather than 'the domain name' for instance). In the same way, for email assessment, it could happen that learner does not really know which part of an email concerns the sender, the subject line etc. The solutions are targeted to broad audience which requires to be circumscribed to obtain efficient results. We believe that developers should build solutions for specific persons of a

certain age or a class of society. A phishing process includes three phases: preparation, attack and exploitation. During the preparation phase, attacker starts by setting up a fake website which looks legitimate like well-known brand or organization. During the attack phase, the attacker sends a large number of emails including social engineering elements designed in the preparation phase, to convince potential victims. During exploitation phase, people are deceived on the fake website believing that it is a real and legitimate. The attacker can exploit information retrieved from victims to conduct other illegal activities. It is found that solutions educate only on the attack phase. It is therefore a partial education. Participants are evaluated within a short period and they know that they are evaluated. This fashion is predictable and predisposes learners to guess responses.

7.2 Further Research

Some open issues for further research are the following.

- Game theory: Game theory is useful to design a game and interactions between different players. We believe that research should look into building games predicting future phisher or defender intents based on simulated scenarios. This information is interesting because it helps to think as the attacker.
- Extracting similarities: There are similar and different features in gamified solutions. Applying techniques of software product lines could give a good support from which new products can be mounted. Research could therefore provide anti-phishing gamified products for different class of customers: students or company employers.
- Association with intelligent detective solutions: Attackers develop sophisticated phishing attacks with the evolution of technology. This requires also adapted solutions which sometimes include artificial and computational intelligence. Gamified and up-to-date modules should be inserted in such solutions to learn administrators about new phishing vacuums when they deploy solutions for detection in the network.
- Crowd-gamification: Authors should design gamified solutions involving collaborative intelligence. It means that people across the cloud could participate in educating about phishing experiences and countermeasures.
- Multiple players: We believe that solutions with multiple players are closer to the reality and can participate to strengthen learning situations.
- Multi-steps education: Authors of gamified platforms should educate users about each phase of phishing.
- Unpredictable game: Developers should insert the game into normal communication activities of the learner such that they ignore that incoming messages or mails are related to the game. Therefore the evaluation could in a long period and repeated. To achieve this, various sets of simulated phishing scenarios must be designed and updated over time.

8. Conclusion

This paper investigated gamified solutions applied for phishing education. While many researches using gamification approach have been conducted in cybersecurity in general, none of them were dedicated to phishing. Therefore, we presented eight main anti-phishing solutions which use game mechanics to motivate players to remain engaged through the learning process. These solutions are not equivalent according to the game mechanics, the type of gamification structure and the level of

understanding provided by anti-phishing educational solutions. We have made comparative discussions revealing that educative solutions based on gamification should increasingly propose basic level where learners get in touch with elementary notions. Gamified solutions should evaluate learners unpredictably and should cover every step of phishing. This work provides some open issues to investigate to improve this research area.

Author Contributions

Franklin Tchakounté performed formal analysis, proposed the research design and taxonomies, Leonel Kanmogne Wabo collected data and proposed a summary of the papers. Marcellin Atemkeng provided technical review, and edited the manuscript.

E.S. conducted formal analysis and drafted the manuscript, S.K. developed the concept of the study, directed the analysis, provided technical review, and edited the manuscript, and P.T. collected data and performed descriptive analysis of this study.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. APWG APWG: Phishing Activity Trends Report Q4 2018. *Comput. Fraud Secur.* **2019**, *2019*, 4.
2. Chiew, K.L.; Yong, K.S.C.; Tan, C.L. A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches. *Expert Syst. Appl.* **2018**, *106*, 1–20.
3. Misra, G.; Arachchilage, N.A.G.; Berkovsky, S. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. In Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017); Steven Furnell, N.L.C., Ed.; Adelaide, Australia, 2017; pp. 41–51.
4. CJ, G.; Pandit, S.; Vaddepalli, S.; Tupsamudre, H.; Banahatti, V.; Lodha, S. PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness. In Proceedings of the Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts - CHI PLAY '18 Extended Abstracts; ACM Press: New York, New York, USA, 2018; pp. 169–181.
5. Gupta, B.B.; Tewari, A.; Jain, A.K.; Agrawal, D.P. Fighting against phishing attacks: state of the art and future challenges. *Neural Comput. Appl.* **2016**, 1–26.
6. Khonji, M.; Iraqi, Y.; Jones, A. Phishing Detection: A Literature Survey. *IEEE Commun. Surv. Tutorials* **2013**, *15*, 2091–2121.
7. Tewari, A.; Jain, A.K.; Gupta, B.B. Recent survey of various defense mechanisms against phishing attacks. *J. Inf. Priv. Secur.* **2016**, *12*, 3–13.
8. Aleroud, A.; Zhou, L. Phishing Environments, Techniques, and Countermeasures: A Survey. *Comput. Secur.* **2017**, *68*, 160–196.
9. Tioh, J.-N.; Mina, M.; Jacobson, D.W. Cyber security Training a Survey of Serious Games in Cyber Security. In Proceedings of the 2017 IEEE Frontiers in Education Conference (FIE); IEEE, 2017; pp. 1–5.
10. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A Review of Using Gaming Technology for Cyber-Security Awareness. *Int. J. Inf. Secur. Res.* **2016**, *6*.
11. Hendrix, M.; Al-Sherbaz, A.; Bloom, V. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? *Int. J. Serious Games* **2016**, *3*.

12. Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Anti-Phishing Phil: the Design and Evaluation of a Game that Teaches People Not to Fall for Phish. In Proceedings of the Proceedings of the 3rd Symposium on Usable Privacy and Security - SOUPS '07; ACM Press: New York, New York, USA, 2007; p. 88.
13. Canova, G.; Volkamer, M.; Bergmann, C.; Borza, R. NoPhish: An Anti-Phishing Education App. In; Springer, Cham, 2014; pp. 188–192.
14. Hale, M.L.; Gamble, R.F.; Gamble, P. CyberPhishing: A Game-Based Platform for Phishing Awareness Testing. In Proceedings of the 2015 48th Hawaii International Conference on System Sciences; IEEE, 2015; pp. 5260–5269.
15. Baslyman, M.; Chiasson, S. "Smells Phishy?": An Educational Game about Online Phishing Scams. In Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime); IEEE, 2016; pp. 1–11.
16. Wen, Z.A.; Li, Y.; Wade, R.; Huang, J.; Wang, A. What.Hack: Learn Phishing Email Defence the Fun Way. In Proceedings of the Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '17; ACM Press: New York, New York, USA, 2017; pp. 234–237.
17. Weanquoi, P.; Johnson, J.; Zhang, J. *Using a Game to Improve Phishing Awareness*; 2018; Vol. 2018;.
18. Deterding, S.; Dixon, D.; Khaled, R.; Nacke, L. From Game Design Elements to Gamefulness: Defining "Gamification" In Proceedings of the Proceedings of the 15th International Academic MindTrek Conference on Envisioning Future Media Environments - MindTrek '11; ACM Press: New York, New York, USA, 2011; p. 9.
19. Burke, B. *Gamify : How Gamification Motivates People to Do Extraordinary Things*; Routledge, Ed.; 2014; ISBN 1937134857.
20. Tseng, S.-S.; Yang, T.-Y.; Wang, Y.-J.; Lu, A.-C. Designing a Cybersecurity Board Game Based on Design Thinking Approach. In; Springer, Cham, 2019; pp. 642–650.
21. Kapp, K.M. *The Gamification of Learning and Instruction : Game-based Methods and Strategies for Training and Education*; John Wiley & Sons, Ed.; 2012; ISBN 1118096347.
22. Landers, R.N.; Auer, E.M.; Collmus, A.B.; Armstrong, M.B. Gamification Science, Its History and Future: Definitions and a Research Agenda. *Simul. Gaming* **2018**, *49*, 315–337.
23. Arachchilage, N.A.G.; Love, S. A Game Design Framework for Avoiding Phishing Attacks. *Comput. Human Behav.* **2013**, *29*, 706–714.
24. Kim, S.; Song, K.; Lockee, B.; Burton, J. Gamification Framework. In *Gamification in Learning and Education*; Springer International Publishing: Cham, 2018; pp. 59–90.
25. Nicholson, S. A User-Centered Theoretical Framework for Meaningful Gamification. In Proceedings of the Games+Learning+Society 8.0; Madison, WI, 2012.
26. Hunicke, R.; Leblanc, M.; Zubek, R. MDA : A Formal Approach to Game Design and Game Research. In Proceedings of the Nineteenth National Conference of Artificial Intelligence; San Jose, CA, 2004.
27. Schell, J. *The Art of Game Design : a Book of Lenses*; CRC Press, 2008; ISBN 0123694965.
28. Werbach, K.; Hunter, D. *For the Win : How Game Thinking can Revolutionize your Business*; Wharton Digital Press, Ed.; 2012; ISBN 1613630239.
29. Mora, A.; Riera, D.; Gonzalez, C.; Arnedo-Moreno, J. A Literature Review of Gamification Design Frameworks. In Proceedings of the 2015 7th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games); IEEE, 2015; pp. 1–8.

30. Caporarello, L.; Magni, M.; Pennarola, F. One Game Does not Fit All. Gamification and Learning: Overview and Future Directions. In; Springer, Cham, 2019; pp. 179–188.
31. Morschheuser, B.; Hassan, L.; Werder, K.; Hamari, J. How to Design Gamification? A Method for Engineering Gamified Software. *Inf. Softw. Technol.* **2018**, *95*, 219–237.

In the text, reference numbers should be placed in square brackets [ ], and placed before the punctuation; for example [1], [1–3] or [1,3]. For embedded citations in the text with pagination, use both parentheses and brackets to indicate the reference number and page numbers; for example [5] (p. 10), or [6] (pp. 101–105).

1. Author 1, A.B.; Author 2, C.D. Title of the article. *Abbreviated Journal Name* **Year**, *Volume*, page range.
2. Author 1, A.; Author 2, B. Title of the chapter. In *Book Title*, 2nd ed.; Editor 1, A., Editor 2, B., Eds.; Publisher: Publisher Location, Country, 2007; Volume 3, pp. 154–196.
3. Author 1, A.; Author 2, B. *Book Title*, 3rd ed.; Publisher: Publisher Location, Country, 2008; pp. 154–196.
4. Author 1, A.B.; Author 2, C. Title of Unpublished Work. *Abbreviated Journal Name* stage of publication (under review; accepted; in press).
5. Author 1, A.B. (University, City, State, Country); Author 2, C. (Institute, City, State, Country). Personal communication, 2012.
6. Author 1, A.B.; Author 2, C.D.; Author 3, E.F. Title of Presentation. In Title of the Collected Work (if available), Proceedings of the Name of the Conference, Location of Conference, Country, Date of Conference; Editor 1, Editor 2, Eds. (if available); Publisher: City, Country, Year (if available); Abstract Number (optional), Pagination (optional).
7. Author 1, A.B. Title of Thesis. Level of Thesis, Degree-Granting University, Location of University, Date of Completion.
8. Title of Site. Available online: URL (accessed on Day Month Year).