EyeBit: eye-tracking approach for enforcing phishing prevention habits

Daisuke Miyamoto, Takuji Iimura, Gregory Blanc, Hajime Tazaki, Youki Kadobayashi

EyeBit: Eye-Tracking Approach for Enforcing Phishing Prevention Habits

Daisuke Miyamoto*, Takuji Iimura*, Gregory Blanc†, Hajime Tazaki*, Youki Kadobayashi‡
*Information Technology Center
The University of Tokyo
2-11-16 Yayoi, Bunkyo-ku, Tokyo, 113-8658 JAPAN
{daisu-mi, iimura, tazaki}@nc.u-tokyo.ac.jp

†Institut Mines-Télécom/Télécom SudParis
CNRS UMR 5157 SAMOVAR
9 rue Charles Fourier, 91011 Évry, FRANCE
gregory.blanc@telecom-sudparis.eu

†Graduate School of Information Science
Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, Nara, 630-0192 JAPAN
youki-k@is.aist-nara.ac.jp

***Abstract*—This paper proposes a cognitive method with the goal to get end users into the habit of checking the address bar of the web browser. Earlier surveys of end user behavior emphasized that users become victims to phishing due to the lack of knowledge about the structure of URLs, domain names, and security information. Therefore, there exist many approaches to improve the knowledge of end users. However, the knowledge gained will not be applied unless end users are aware of the importance and develop a habit to check the browser's address bar for the URL structure and relevant security information.**

We assume that the habit of checking the bar will improve educational effect, user awareness of secure information, and detection accuracy even in the case of sophisticated phishing attacks. To assess this assumption, this paper conducts a participant-based experiment where 23 participants' eye movement records are analyzed, and observes that novices do not tend to have the said habit. We then consider a way for them to acquire these habits, and develop a system which requires them to look at the address bar before entering some information into web input forms. Our prototype named EyeBit is developed as a browser extension, which interacts with an eye-tracking device to check if the user looks at the browser's address bar. The system deactivates all input forms of the websites, and reactivates them only if the user has looked at the bar. This paper shows the preliminary results of our participant-based experiments, and discusses the effectiveness of our proposal, while considering the potential inconvenience caused by EyeBit.

Keywords*—*Phishing, Cognitive Psychology, Eye-Tracking

I. Introduction

Phishing is a fraudulent activity defined as the acquisition of personal information by tricking an individual into believing the attacker is a trustworthy entity [1]. Phishing attackers lure people through the use of a phishing email, as if it were sent by a legitimate corporation. The attackers also attract the email recipients to a phishing site, which is the replica of an existing web page, to fool them into submitting personal, financial, and/or password data.

There have been many participants-based studies to understand decision patterns of end users while the fundamental problem in phishing is the fact that they are deceived. According to Dhamija [2], some participants do not look at browser-based information such as the address bar, the status bar or the security indicators, leading to incorrect choices 40% of the time. Instead, they consider various other criteria while assessing a website's credibility.

In our previous work [3], we asked 309 participants the reason of their decision. The participants browsed 14 simulated phishing sites and six legitimate sites, judging whether or not the site appeared to be a phishing site, and answered the reason for their decision via a questionnaire. The results showed that experts tended to evaluate a site's URL and/or browser's SSL indicator rather than the contents of a web page to judge the credibility of the sites. Conversely, novices, who often failed to decide rightly, received strong signals from web contents only while. Due to the nature of phishing, the web contents are quite similar to what is displayed by a legitimate site, leading novices to fall victims to the phishing trap.

It can be naturally assumed that checking the browser's address bar is beneficial for end users to be aware of phishing. The reader should note that modern web browsers do show the website's URL and security information in the address bar. Even the knowledge of URL and security are also important for phishing prevention and are the strong motivation for seeing there, the both of them could not work before the users did not see the bar. This

paper assesses this assumption with a participant-based experiment in which 23 participants are shown with 20 websites, and asked to determine which ones are phishing while having their eye movement monitored. Based on our experiment, it might be reasonable to consider that novices do not have the habit of visually checking the address bar.

According to these results, this paper then explores new mechanisms for the users to acquire the habits of checking the address bar while assessing the credibility of a website. Our idea is to enforce them to look there first, before entering any information to web input forms. Our proposed system, named *EyeBit*, is implemented as a browser's extension, and interacts with an eye-tracking device. EyeBit deactivates all input forms at the beginning of browsing, and activates the forms when it confirmed that the user gazed the address bar. For our preliminary evaluation of EyeBit, we called ten participants to test if they got a habit in checking the address bar.

To this end, this paper makes the following contributions:

- We present an approach to counter phishing tactics, that we argue significant benefit for getting into the habit of secure web browsing.
- We propose EyeBit which forms the habit of checking the address bar for safe browsing in section III-A. To the best of our knowledge, this is the first attempt at making end users to acquire habits for phishing prevention.
- We assess our assumption (*"checking the browser's address bar is beneficial to end users in making them aware of phishing"*) through a participant-based experiment in section III-B.
- We design EyeBit in consideration of cognitive aspects, and then implement a prototype of EyeBit as an extension for Chrome web browser in section III-C.
- We evaluate the effectiveness of seeing the address bar with an eye-tracking camera in a within-subject experiment. The implementation is demonstrated to show the effectiveness of getting the habit in section III-D.
- We observe that the inconvenience caused by EyeBit is negligible in section IV-A.

II. Related work

A. Behavior of end users

The targets of phishing attacks are end users, so there were various contributions to analyze end users and their activities. According to an analysis report of 2,684 people by Fogg et al. [4], 46.1% checked the design look and feel of a website and 28.5 % used website structure of information, when people assessed a real web site's credibility. Ye et al. [5] also stated that end users would convinced by the content of HTML and URL, regardless of checking SSL padlock icons.

According to Kumaraguru et al. [6], there were the difference in the model for making trust decision between novices and experts. In comparison to experts, novices were sensitive to superficial signals when they made trust decision. Novices also ignored some signals such as SSL, address bar, and so on, where experts received these signals. Dhamija et al. [2] reported their participant within tests for identifying phishing sites. They found that phishing caused of lack of knowledge. For example, participants thought www.ebay-members-security.com belongs to www.ebay.com due to the lack of system knowledge. Also, many participants did not understand security indicators. They did not know that a closed padlock icon in the browser indicates that the page they are viewing was delivered securely by SSL. Even if they understand the meaning of that icon, users can be fooled by its placement within the body of a web page. They also found that the best phishing websites fooled 90% of participants. The URL of the site is "www.bankofthevvest.com", with two "v"s instead of a "w" in the domain name.

Wu et al. also measured the effectiveness of security toolbars, which informs end users that they are visiting phishing sites [7]. They tested three types of security toolbars, namely, Neutral-information toolbar such as NetCraft Toolbar [8], SSL-Verification toolbar such as TrustBar [9], System-Decision toolbar such as SpoofGuard [10]. Each of the three security toolbars was tested with ten participants, and they browsed both phishing sites and legitimate sites with one security toolbar, and they also classified the site was phishing or not. Wu et al. concluded that all toolbars failed to prevent users from being spoofed by high-quality phishing attacks. Users failed to continuously check the browser's security indicators, since maintaining security was not the user's primary goal. Although users sometimes noticed suspicious signs coming from the indicators, they either did not know how to interpret the signs or they explained them away.

B. Failure analysis

The root cause of social engineering is human errors; the targets failed to behave or understand against attacks. Failure analysis is the process of investigating the reason of failure. Its process also collects and analyzes data, and develops methods and/or algorithms to eliminate the root causes of the failure. Zahran et al. [11] summarized the categorization techniques for such analysis and introduced the component-based categorization; the failure can be caused of the components of information systems, namely, hardware, software, communications networks, people, data resources and organization. The analysis of human error is also important part in cyber security. Especially, the interface studies investigated the reasons of users' misjudgments [12]. Based on their subjects experiments, they clarified the mental model of users and indicated the way for improving the user interfaces.

In the context of the people in enterprise, human factors were analyzed to mitigate risks in the organization. According to Hawkey et al. [13], [14], challenges of IT security managements were classified into technical, organizational, and human factors. To understand human

behavioral model, Parkin et al. [15] showed five behavioral foundation, namely cultural, ethical, temporal, mindset, and capability difference. Based on the foundation, they developed ontology which aims at maintaining compliance with ISO27002 standard [16] while considering the security behaviors of individuals within the organization.

Alfawaz et al. [17] classified the characteristics of organizational subjects involved in these information security practices. They analyzed the participants' activities and categorized individual security behaviors into four modes, (i) Knowing-Doing mode, (ii) Knowing-Not doing mode, (iii) Not knowing-Doing mode and (iv) Not knowing-Not doing mode. Term "Knowing" means that the participants know the organization's requirements for information security of behavior and have security knowledge. "Doing" also means that they are doing the right behavior. The cases of (i) and (iv) said that the participants (do not) know the requirements and (do not) have the knowledge, therefore, they are (not) doing the right behavior. The example of the mode (ii) is that the participant is unaware of the requirements, but asks someone before taking certain actions. The mode (iii) is serious, that the participants do not perform the right behavior even they know the requirements. The root causes of the mode (iii) is regarded as stressful events. Basically, people have a limited capacity for information processing and routinely multitasks [18]. They tends to conserve mental resources; full attention is for few tasks and decisions.

The earlier researches can be summarized that understanding both the personal knowledge and his/her internal mental processes are necessary for thwarting the impact of human error. There are many approaches to reduce the human errors, and this paper focuses on habits of security. Trustworthy computing habits can maximize opportunities that the knowledge works efficiently. It must be noted that the habitual action is often performed under unconscious. Regardless of the stress, habits have possibilities to improve the chance to exert the knowledge for end users.

C. Cognitive analysis

Cognitive psychology is the study of relationship between internal mental processes and observable behavior. To address the problem in the observation, this paper refers to the evaluation of cognitive methods for supporting operators studied by Groojten [19] in which the following criteria were formulated.

- **Sensitiveness to workload changes.**
  We need to employ the behavioral observation methods that can estimate the internal mental model. The methods might also leverage the collected information regardless of the Fear of Negative Evaluation (FNE) [20]; observations are often affected by FNE, in which some of people will conceal their human errors. In fact, disclosing mistakes often damage their own self-image and professional standing.
- **Obtrusiveness for the operator.**
  The observation should not take much effort to start collecting data or disturb the handling of people during the tasks performance. Furthermore, people will not carry implants or needles or other devices which may hurt them in any way.
- **Availability of equipment.**
  The observation should employ the method which is easily applicable to people. Within the context of phishing prevention, the methods should be available while users are browsing. Non-contact devices might be preferred.

Based on the requirements, this paper explores the suitable methods. Brain activity [21], heart measure, and blood pressure [22] are feasible due to the sensitivity to workload changes, but they tend to require much obtrusiveness for people. Contrastively, Facial expression [23] and Gesture recognition [24] were often affected by FNE.

We speculate that the following research domains that might be helpful for the observation.

- **Eye Movements.**
  Research on experimental psychology has evidenced a strong link between eye movements and mental disorders [25], [26]. Leigh et al. [27] classified the eye movements into four categories, namely Saccades, Fixations, Smooth pursuit movements, and Vestibulo-ocular reflexes. In the context of mental model, Irwin et al. showed that the mental rotation is suppressed during the movements [28], and Tokuda [29] showed that mental workload, the indicator of how mentally/cognitively busy a person is, can be estimated from saccadic intrusions. In addition to that, recent eye-tracking devices also support non-mounting monitoring as well as head-mount monitoring.
- **Facial Skin Temperature.**
  Variation of facial skin temperature has received some attention as a physiological measure of mental status [30]–[32]. According to Genno et al. [33], their experiments showed that temperature change in nose area when subjects experienced sensations like stress and fatigue. Furthermore, the thermography, when combined with other modes of measurement provides a highly automated and flexible means to objectively evaluate workload [30].

In this paper, we decided to employ eye movements-based observations by following reasons. At first, our motivation is to let end users to get the habits of investigating the browser's address bar; an eye-tracking is a straight forward way for observing users' behavior. The second is that monitoring eye movement will not significantly penalize users' convenience according to the above consideration. We also expect the eye-tracking for recognizing mental anomalies to reduce impact of human failure.

III. EyeBit: eye-tracking for phishing prevention

This section introduces EyeBit, a system for end users to get into the habit of checking the surrounding area

of the browser's address bar while assessing a website's credibility. Section III-A summarizes the overview, and Section III-B assesses our assumption, that is, checking the browser's address bar is beneficial for end users. Section III-C presents the design and implementation of EyeBit , which is evaluated in Section III-D.

A. Overview

In this paper, we speculate that the habit of checking the address bar plays an important role in safe browsing. The key idea is to require end users to look at the browser's address bar before entering anything into the web input forms.

According to Dhamija [2] who studied the reason why novices fall victims to phishing, phishing is often successful when there is a lack of knowledge about domain names (in order to differentiate between URLs), about security information, or lack of attention to this information. However, modern social engineering attacks attempt at affecting victims' composure. For example, a phishing email states *"your account was locked because you violated the terms of service"* which will prompt the victim to immediately click an URL placed below and presented as a way of recovery. From a psychological aspect, the victims' primary concern is about their locked account, and not security, leading the authors to invalidate security education as not sufficient, in that case, to prevent phishing.

To improve the acquisition of security education and knowledge, the habit of looking at the bar might be reasonable. The advantage is that this habitual action is often performed unconsciously. Even if the primary concern of the end user is not security, the habit would work like a conditioned reflex action. The habit also improves the chance of being aware of security information. Since modern web browsers show the website's URL and related security information in the address bar, the surrounding area of the browser's address bar shows good signals for phishing detection.

We therefore develop EyeBit, a system for enforcing phishing prevention habits. Based on eye-tracking technologies, EyeBit monitors if users see a particular portion of the screen. Failing to look at the address bar will deactivate parts of web contents in which users can input their personal information.

B. Assumption

In this section, we want to examine the assumption that checking the browser's address bar is beneficial to end users in making them aware of phishing. In order to assess if gazing the address bar improves the accuracy, we performed a participant-based experiment to monitor an end-user's eye activity. It must be noted that our experiments must not collect and/or analyze personally identifiable information. The experimental design, concept and methodologies for recruiting participants are also explained below.

1) Recruitment of participants through a poster advertisement at a college campus.
2) Explanation of our experiment to the participant.
   - Our purpose is to observe the user's activity, in particular with respects to assessing the credibility of websites.
   - Our goal is to develop security mechanisms for protecting users from phishing.
   - Before the experiments, each participant will be asked his/her age and sex.
   - During the experiments, each participant will be monitored by an eye-tracking device, and be shown 20 websites. Their activity will be monitored, and they will be asked if each website seems to be phishing or not. They will also be asked the reason of their decision.
   - Collected data consists of the participants' age, sex, decision result, decision criteria, and eye-tracking data.
   - Collected data is shared with both European and Japanese research members.
3) Display of 20 website screenshots, including legitimate websites and pseudo phishing sites.
   In the experiment, the phishing sites are not real phishing sites to avoid information leakage. Instead, our participants are presented with 20 screenshots of a browser that rendered the websites. These screenshots were taken on Windows 7 equipped with IE 10.0.

As shown in Table I, we prepared twelve phishing sites and eight legitimate ones for the test. In comparison, a typical phishing IQ test [2] presented participants with 13 phishing sites and seven legitimate ones, so the ratio of phishing sites over legitimate ones is quite similar to ours.

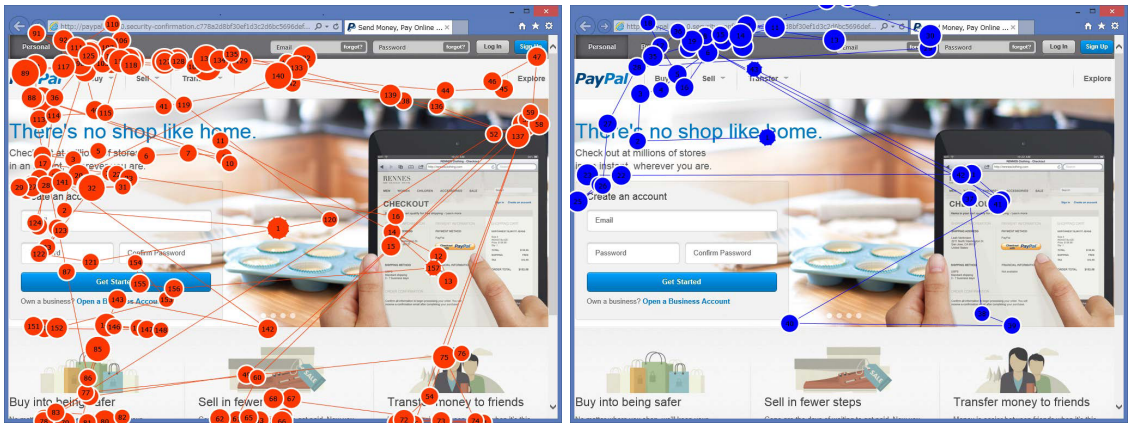
In this experiment, we recruited 23 participants to observe their eye movement. The volunteers were mainly males in their twenties. With their consent, their eye movements were recorded by our prepared eye-tracking device, Tobii TX300 [34]. It needed calibration procedure for each participant.

We observed that the participants who rely on the URL of the website would fail to flag websites 5, 14 and 17, since these sites had almost the same URL as the legitimate sites, except for one letter. The URLs of the websites 7, 12, and 19 contained a legitimate-sounding domain name. Website 20 was legitimate but the domain name of this site had no indication of its brand names. For participants who tended to rely on security information of browsers, websites 11 and 20 might be difficult to assess because although they were phishing sites, they presented participants with a valid SSL certificate. Conversely, websites 6 and 9 were legitimate but did not employ valid SSL certificates though they required users to login. Of course, since our prepared phishing websites were lookalikes of the legitimate ones, it might have been more difficult for the participants who relied on web contents.

Fig. 1 and 2 show typical eye-movement records on both phishing and legitimate website, for a novice and an expert respectively. Circles denote fixations, and the numbers in the circles denote the order of the fixation. In the phishing case, the novice looked at the web content but ignored the

TABLE I: Conditions of each site used for recording eye movement

#	Website	Phish	Lang	Description
1	Google	no	JP	SSL
2	Amazon	yes	JP	`tigratami.com.br`, once reported as a compromised host
3	Sumishin Net Bank	no	JP	EV-SSL
4	Yahoo	yes	JP	`kazuki-j.com`, once reported as a compromised host
5	Square Enix	yes	JP	`secure.square-enlix.com`, similar to legitimate URL `secure.square-enix.com`
6	Ameba	no	JP	non-SSL
7	Tokyo Mitsubishi UFJ Bank	yes	JP	`bk.mufg.jp.iki.cn.com`, similar to legitimate URL `bk.mufg.jp`
8	All Nippon Airways	yes	JP	IP address
9	Gree	no	JP	non-SSL
10	eBay	no	EN	EV-SSL
11	Japan Post Holdings	yes	JP	`direct.yucho.org`, SSL
12	Apple	yes	EN	`apple.com.uk.sign.in...`
13	DMM	no	JP	SSL
14	Twitter	yes	JP	`twittelr.com`
15	Facebook	yes	JP	IP address
16	Rakuten Bank	yes	JP	`vrsimulations.com`, once reported as a compromised host
17	Sumitomo Mitsui Card	yes	JP	`www.smcb-card.com`, SSL
18	Jetstar Airways	no	JP	SSL, non pad-lock icon by accessing non-SSL content
19	PayPal	yes	EN	`paypal.com.0.security-c...`
20	Tokyo-Tomin Bank	no	JP	3rd party URL `www2.answer.or.jp`, EV-SSL



(a) Novice (b) Expert

Fig. 1: Eye-tracking in phishing website

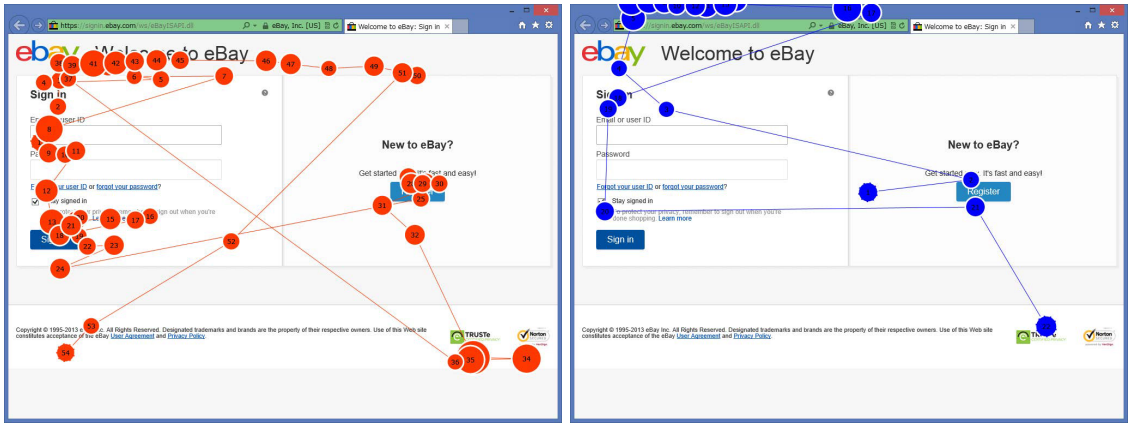
browser's address bar while assessing credibility, as shown in Fig. 1a. Since the text and visual in phishing sites are quite similar to the ones in legitimate sites, he failed to label the phishing site correctly. In the legitimate case, he also only paid attention to the web content as shown in Fig. 2a. In contrast, an expert tends to evaluate the site's URL and/or the browser's SSL indicator rather than the contents of the web page to judge the credibility of the sites, as shown in Fig. 1b and 2b.

We then analyzed the detection accuracy of participants who looked at the address bar and those who did not look, respectively. The results were shown in Fig. 3, where he blue bar denotes the average rates for the participants looked at the address bar of the browser, and the orange bar denotes that for the participants did not look at the bar.

Out of the 331 times the bar was gazed, 89 (26.9%) misjudgments were observed. In the phishing websites case, the participants looked at the bar 200 times in total, which occurred 61 (30.5%) false negatives, i.e., labeling phishing as legitimate. In the legitimate websites case, they looked at the bar 131 times in total, which occurred 28 (21.4%) false positives, i.e., labeling legitimate as phishing. In contrast, the average error rate was 41.1% (53 out of 129), the false negative rate was 56.6% (43 out of 76), and the false positive rate was 18.9% (10 out of 53), when participants would ignore the address bar. The average error rate and false negative rate indeed decreased when the address bar was checked, although experimental errors might have occurred due to some possible offsets caused by the eye-tracking calibration procedure. The increase of the false positive rate seems to be marginal. We therefore considered that our assumption, i.e., *checking the browser's address bar is beneficial to end users in making them aware of phishing*, is reasonable.

C. Design and implementation

Based on the assumption described in Section III-B, we implemented EyeBit, a system which enables novices to get into the habit of checking the address bar. The requirements of EyeBit are as follows.



(a) Novice (b) Expert

Fig. 2: Eye-tracking in legitimate website

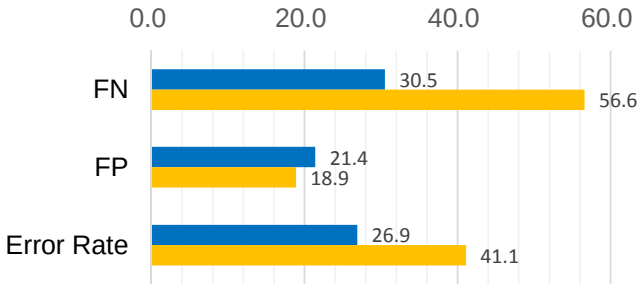


Fig. 3: The average false positive, false negative and error rate for users that looked (blue) and did not look (orange) at the address bar

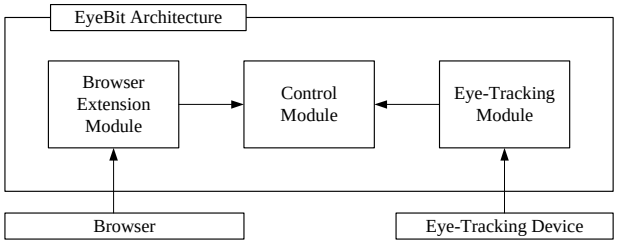


Fig. 4: The architecture of EyeBit

- **Web inputs control.**
  It must have functions to activate/deactivate web input forms. EyeBit deactivates all input forms, at first. When it detects that the user has checked the browser's address bar, all input forms are then activated.
- **Eye-tracking capabilities.**
  It must interact with eye-tracking devices, and identify that the user has looked at a particular portion in the web browser with certainty. It also should provide interfaces to obtain an end user's eye position from third-party developed application.
- **Address bar localization.**
  It should be able to locate the address bar within the screen.

The architecture of EyeBit is shown in Fig. 4. It consists of (i) an eye-tracking module, (ii) a browser extension module, and (iii) a control module. In order to meet the requirements, we implemented EyeBit as a browser extension. The module deactivates all input forms at first, and then activates them after the eye-tracking module has confirmed that the user looked at the address bar. The task of the eye-tracking module is to interact with an eye-tracking device. We selected an eye-tracking camera which could provide an interface to obtain an end user's eye position from our implementation.

Our prototype was implemented as an extension of Google Chrome, therefore written in JavaScript, and consisted of roughly 100 lines of code. We also selected EyeTribe-Tracker [35] as the eye-tracking device. Its software development kit (SDK) embeds the function of web server and provides the user's eye position in JavaScript Object Notation (JSON) format messages.

Due to the performance difference, this device could not correctly deal with eye-fixation, however, our implementation checked if the user looked at the area of the address bar and 50 pixels of margins on each side. It stores the 30 seconds of eye-tracking records, and inspected his/her gaze position in one second intervals, and reactivated the forms when the position of the gaze was in the area for at least one time interval.

The limitation of our prototype was the localization of the address bar. Instead, it measured the absolute position within the screen. Assuming the browser's window is maximized, the position of the bar can be easily estimated. We will discuss about methods for locating the bar in Section IV-D.

TABLE II: Conditions of each site used for evaluating EyeBit

#	Website	Phish	Lang	Description
1	Yahoo	yes	JP	`dmiurdrgs.cher-ish.net`, once reported as a phishing site
2	PayPal	no	EN	EV-SSL
3	eBay	yes	EN	`signin-ebay.com`, similar to legitimate URL `signin.ebay.com`
4	DMM	no	JP	SSL
5	Amazon	yes	EN	`www.importen.se`, once reported as a phishing site
6	Bank of America	no	EN	EV-SSL
7	Facebook	no	JP	SSL
8	Square Enix	yes	JP	`hiroba.dqx.jp...`, similar to legitimate URL `hiroba.dqx.jp`
9	Twitter	yes	JP	`twittelr.com`
10	Google	no	JP	SSL
11	Battle.net	no	EN	EV-SSL
12	Sumitomo Mitsui Card	yes	JP	`www.smcb.card.com....`, similar to legitimate URL `www.smbc-card.com`

TABLE III: Decision results of participants

#	A_1	A_2	A_3	A_4	A_5	B_1	B_2	B_3	B_4	B_5
1	F				F		F	F		
2										
3	F				F		F	F	F	
4	F		F					F		
5									F	
6										
7			F							
8										
9					F	F				
10		F	F							
11	F	F	F					F		
12										

D. Evaluation

This section evaluates the effectiveness of EyeBit. As our pilot study, in May 2014, we invited ten participants and performed a within-subject experiment. The participants browsed six emulated phishing sites and the same number of legitimate sites, as listed in Table II. They checked whether the site appeared to be a phishing site or not. Among the ten participants, nine belonged to Nara Institute of Science and Technology, and the rest belonged to the University of Tokyo. All of them were male, two of them completed their M.Eng degree in the last five years, while the remaining were master's degree students. We explained to them our purpose, goal, and usage of the collected data as stated in Section III-B.

The experiment is composed of the following steps.

1) **First stage: labeling websites 1–4**
   All participants were shown four websites 1 – 4 in Table II and checked whether the sites were phishing or not. When the participant deemed the site legitimate, he/she would input the word "john" as a pseudo persona for the website's username input field.
2) **Educational break**
   Before employing EyeBit, we would explain about what the address bar indicates. The participants would be shown with our educational material. With reference to typical material [36], we convinced them to carefully check the website's URL, the presence of an SSL padlock icon, and the EV-SSL information.
3) **Second stage: labeling websites 5–8**
   After the educational break, five of the ten participants would equip with EyeBit and be explained about EyeBit; input forms would be deactivated until the browser's address bar was gazed upon. The rest of the participants were not equipped with EyeBit. This differentiation was made to comparatively study the effectiveness of EyeBit.
   All participants were shown four websites 5 – 8 in Table II and checked whether the sites were phishing or not. Similarly to the first stage, the participants inputted the word "john" to the website's input form when deeming a site legitimate. The five participants equipped with EyeBit would need to activate the forms by checking the address bar before labeling a website as legitimate.
4) **Interval for sanitizing**
   Basically, people tend to be sensitive to phishing after the education. We wait one hour for interval between the second and last stage.
5) **Last stage: labeling websites 9–12**
   Finally, we let all participants show the last four websites 9 – 12 in Table II. We intended to analyze the behavioral differences between five participants who used EyeBit and the rest participants who did not use EyeBit. We also planned to observe remaining effect of education, therefore, all participants did not equip EyeBit.

The detection results were shown in Table III, where $A_1 \cdots A_5$ denote the participant who used EyeBit, $B_1 \cdots B_5$ denote the participant who did not use EyeBit, the letter "F" denotes that a participant failed to judge the website, and the empty block denotes that a participant succeeded in judging correctly.

We assumed that participants A_1 and A_5 were novices. Since they had no criteria for making decisions, they often received strong signals from web content and hence, they answered all of websites in the first stage as legitimate. After the education, they were seemed to have criteria, so they could perfectly answered to the websites 5 – 8. During one hour, the effect would not be significantly attenuated. In the case of websites 9 – 12, they saw the browser' address bar at least ten seconds, even if they did not equip EyeBit.

The participants $B_1 \cdots B_5$ did not employ EyeBit, and we speculated that the participant B_2 and B_3 were also novices; they could not correctly identify phishing websites in the first stage. However, their eye movement were formed to see the address bar after the education.

There were some reasons that EyeBit worsened in the participants $A_1 \cdots A_5$ compared to when it was not used $B_1 \cdots B_5$. We assumed that the most predominant reason

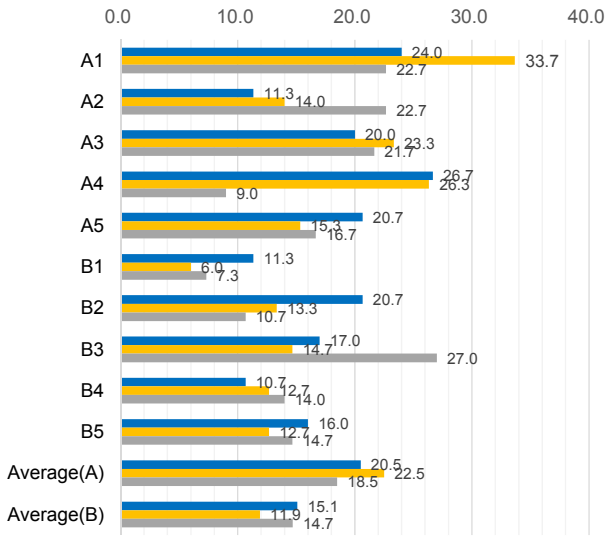


Fig. 5: The average time required for making decision for websites 1-3 (blue), websites 5-7 (orange), and websites 9-11 (gray), in respectively

was the small sample size. In the cases of the participant A_2 and A_3, EyeBit had a potential for making them paranoid, since websites 9 and 10 were legitimate but were labeled as phishing. The another reason was that the educational effect did not dissolve in one hour, and hence, the participants $B_1 \cdots B_5$ performed better.

We then conducted a follow-up study in June 2014. The study was focused on four novices, namely the participants A_1, A_5, B_2, and B_3, and we observed the difference of the educational effect remains in four participant after one month. The participants were shown websites 1 to 20 in the table II. We observed that the participants A_1, A_5, and B_2 often looked the browser's address bar, although the participant B_3 did not. In regard to a difference from the pilot study in May 2014, the participants A_5 and B_2 could judge correctly the websites $1-4$. Through the follow-up study, no false negative error was observed in the case of the participant A_1 since he often looked at the bar. In the case of the participant B_3, the false negatives increased in comparison of the pilot study. In particular, he answered that the websites $1-4$ seemed to be legitimate, as same as the first stage of the pilot study.

Due to the small number of the participants, it is difficult to accurately determine that EyeBit could exert the educational materials in long time period. However, based on the observations of the pilot and follow-up study, we assumed that EyeBit is helpful for getting the habit of seeing address bar while making trust decisions.

IV. Discussion

A. Potential inconvenience caused by EyeBit

The primary motivation for our experiment was to assess the effectiveness of EyeBit in influencing users' behavior to check the address bar. Essentially, it must be investigated the address bar to correctly judge, therefore, time increase for seeing the address bar must be acceptable.

However, the significant time increase might penalize users' convenience. In general, there is a tradeoff between usability and security, and hence EyeBit would penalize the user's experience to the benefit of security. There are various methodologies for estimating the convenience, and here we tentatively employed the overhead of time spent on the site as a measure.

Fig. 5 shows the average time for making decision, where x axis denotes the number of seconds, y axis denotes each participant, Average(A) is the average time of $A_1 \cdots A_5$ and Average(B) is the average time of $B_1 \cdots B_5$. The blue bar denotes the average time for the first stage (websites $1-3$), the orange bar denotes the second stage (websites $5-7$), and the gray bar denotes the last stage (websites $9-11$). Note that we could not obtain the time on the last websites in each stage due to the limitation of our experiment system, the time spent in the website 4, 8, and 12 were not measured.

In comparison to the results, we could not observe significant increase of time raised from EyeBit. We confirmed that it took 22.5 seconds at the second stage for the participants with EyeBit, whereas 11.9 seconds for the participants without EyeBit. However, once the user gets in habits of seeing the address bar, the average time was deceased to 18.5 seconds, whereas it took 14.7 seconds. In regard to the differences among individuals from the first stage, we assumed that the inconvenience caused of EyeBit would be negligible.

B. Educational approach

Education is one of the straightforward ways to counter phishing since phishing problems are caused of human errors. There were much number of educational materials. For example, Merve et al. [37] proposed educational materials and a strategy on preparing to avoid phishing attacks.

Despite claims by security and usability experts that user education about security does not work [38], there are some evidence that well designed user security education can be effective. Kumaraguru et al. proposed to employ a comic as an educational material [39]. They tested the educational effectiveness of 30 subjects with three types of educational materials. Their results suggested that typical security notices were ineffective. Their results also indicated that that their comic strip format was more effective than the text and graphics. Sheng et al. [40] found that the game is a novel educational material. The main character of the game was Phil, a young fish living in the Interweb Bay. Phil wanted to eat worms so he can grow up to be a big fish, but has to be careful of phishers that try to trick him with fake worms (representing phishing attacks). They conducted the total correctness of subjects' classification before and after the education. By using this game, the correctness increased from 69%, before the education, to 87%. In the case of using existing training materials, the correctness increased from 66% to 74%.

In contrast with past studies [37], [39], [40], our approach focused on getting habits, rather than development of educational materials. Since educational materials are often ignored by users, our EyeBit was designed for getting end users to pay attention to the address bar.

An alternative approach employed learning science principles in which phishing education is made part of a primary task for users [41]. This intended to extend their past research [39], and analyzed the individual user characteristics for improving their educational materials. Our EyeBit gave further evidence to their observations [41] on personalization of phishing prevention.

C. Evaluation of effectiveness

All at first, getting habitual actions usually takes time. EyeBit selected a methodology which enforces end users to see the address bar before using input forms, and there are many alternative methodologies for getting habits. Comparative study among methodologies should be considered in future works.

In order to confirm these effectiveness gained by EyeBit, we will evaluate the effectiveness for long-term retention. Nevertheless there are few research focused on observing the effectiveness in long time periods, Kumaraguru et al. [42] conducted the evaluation of various educational materials. In the case of EyeBit, we should evaluate the effectiveness to end users in different mental modes; the results might be different if the users feel stressed. It may be difficult due to the potential violation of the ethics whenever we intentionally make stressful events to participants.

Furthermore, we will conduct our evaluation of modularity for EyeBit in regard to cognitive aspects. Aside from anti-phishing, understanding users' mental state with eye-tracking may be feasible solution to personalize cyber defense systems. Since recent social engineering employs psychological manipulation techniques, the anomalies in mental state might be recognized by observable behavior. To assess this hypothesis, we will analyze end users' behavior, find its characteristics, and develop personalized defense mechanisms in consideration of the attributes of each end user. As shown in section II-C, eye movement will give much insights while estimating the users' behavior and its foundation.

For evaluating the effectiveness, elimination of bias might be discussed. In our experiments, there were some bias due to the number of samples and/or biased samples. In order to thwart the bias, we will present our prototype of EyeBit at shared code repository [43]. It is possible by distributing the work as browser-extension with some feedback and getting a large population of users to agree to use it.

D. Limitation of implementation

In this study, we used two eye-tracking devices that are designed for non-mounting monitoring. They are usually affected by sudden movements of head, neck and/or face. In order to suppress it, the head-mount eye-tracking device might be available. Our experiments were intended to thwart participants' inconvenience caused by equipment of the head-mounted device. However, it might be worthwhile to evaluate EyeBit in the case of using this type of devices.

As we mentioned in section III-C, the limitation of our prototype was recognition of the address bar. EyeBit should identify a browser window on the screen at first, and then recognize the position of its address bar. One possible way is pattern matching in a digitized image. Alternative is estimating from the position of the browser's top-left corner. In both cases, adjusting for each participant will be necessary.

A potential implementation issue is lack of support for smartphone devices. Recently, people use smartphone devices as well as personal computer. However, smartphone users are also faced with cyber crimes, since the user interfaces for smartphones are constrained by their small screens, browsers in the smartphones often lack a function for showing trustworthy indicators. Due to the small size of the smartphone browser's address bar, it is necessary not only checking the users' gaze to the address bar, but also monitoring their additional activities. This might entail the best practice for browsing with smartphones, but it is beyond the scope of this paper.

V. Conclusion

Basically, habits of checking the address bar will exert security education and knowledge, improve a chance to be aware of security information from browsers, and work like a conditioned reflex action regardless of the users' primal concern. This paper therefore focused on enforcing end users to get the habit of checking the address bar. Our key contribution is development of EyeBit, which aims end users acquiring the habit of seeing browser's address bar before entering any data into websites. EyeBit was able to control web input forms, and deactivate all of them until the end users saw the address bar. By interacting with eye-tracking devices, it finally activated the forms when the users saw there.

We confirmed that the effectiveness of seeing the bar, at first. Our participant-based test showed that the decision accuracy increased by checking the address bar. Based on the observation, we designed and implemented EyeBit as a browser extension with eye-tracking camera. In the pilot study, we performed new participant-based test. The effectiveness of the education with EyeBit succeeded to form the behavior of novices. We found the inconvenience caused of EyeBit was negligible. One month later, we performed a follow-up study to observe behavior of novices. The pilot study could not show significant difference in the case of the education without EyeBit, however the follow-up study indicated that EyeBit could decrease false negative errors in which a participant deems a phishing website as legitimate. The eye movements of novices who employed EyeBit in the pilot study often checked the address bar. We therefore considered that EyeBit was helpful for getting the habit of seeing address bar while making trust decisions.

Acknowledgment

This research has been supported by the Strategic International Collaborative R&D Promotion Project of the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533 (NECOMA). The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the Ministry of Internal Affairs and Communications, Japan, or of the European Commission.

References

[1] C. Abad, "The economy of phishing: A survey of the operations of the phishing market," *First Monday*, vol. 10, no. 9, 2005.

[2] R. Dhamija, J. D. Tygar, and M. A. Hearst, "Why Phishing Works." in *Proceedings of Conference On Human Factors In Computing Systems*, Apr. 2006.

[3] D. Miyamoto, H. Hazeyama, Y. Kadobayashi, and T. Takahashi, "Behind HumanBoost: Analysis of Users' Trust Decision Patterns for Identifying Fraudulent Websites," *Journal of Intelligent Learning Systems and Applications*, vol. 4, no. 4, pp. 319–329, 2012.

[4] B. J. Fogg, L. Marable, J. Stanford, and E. R. Tauber, "How Do People Evaluate a Web Site's Credibility? Results from a Large Study," Stanford, Tech. Rep., Nov. 2002.

[5] Z. E. Ye, Y. Yuan, and S. Smith, "Web Spoofing Revisited: SSL and Beyond," Department of Computer Science, Dartmouth College, Tech. Rep. TR2002-417, Feb. 2002.

[6] P. Kumaraguru, A. Acquisti, and L. F. Cranor, "Trust modeling for online transactions: A phishing scenario," in *Proceedings of the 3rd Annual Conference on Privacy, Security, and Trust*, Oct. 2005.

[7] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do Security Toolbars Actually Prevent Phishing Attacks?" in *Proceedings of Conference On Human Factors In Computing Systems*, Apr. 2006.

[8] Netcraft, "Netcraft Anti-Phishing Toolbar," Available at: http://toolbar.netcraft.com/.

[9] A. Herzberg and A. Gbara, "TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks," Cryptology ePrint Archive, Report 2004/155, Tech. Rep., Jul. 2004.

[10] N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell, "Client-side defense against web-based identity theft," in *Proceedings of the 11th Annual Network and Distributed System Security Symposium*, Feb. 2004.

[11] S. M. Zahran and G. H. Galal-Edeen, "A Categorization Technique for Resolving Information System Failures Reasons," *International Journal of Electrical and Computer Science*, vol. 12, no. 5, pp. 67–77, 2012.

[12] F. Raja, K. Hawkey, and K. Beznosov, "Revealing hidden context: improving mental models of personal firewall users," in *Proceedings of the 5th Symposium On Usable Privacy and Security*, July 2009, pp. 1–12.

[13] K. Hawkey, D. Botta, R. Werlinger, K. Muldner, A. Gagne, and K. Beznosov, "Human, Organizational, and Technological factors of IT security," in *Extended Abstracts on Human Factors in Computing Systems*, April 2008, pp. 3639–3644.

[14] R. Werlinger, K. Hawkey, D. Botta, and K. Beznosov, "Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations," *International Journal of Human-Computer Studies*, vol. 67, pp. 584–606, 2009.

[15] S. E. Parkin, A. van Moorsel, and R. Coles, "An information security ontology incorporating human-behavioural implications," in *Proceedings of the 2nd international conference on Security of information and networks*, October 2009, pp. 46–55.

[16] British Standards Institution, "ISO/IEC 27002:2005 - Information Technology - Security Techniques - Code of Practice and Information Security Management," 2005.

[17] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: a behaviour compliance conceptual framework," in *Proceedings of the 8th Australasian Conference on Information Security*, July 2010, pp. 47–55.

[18] R. West, "The Psychology of Security," *Communications of the ACM*, vol. 51, pp. 34–41, 2008.

[19] M. Grootjen, M. A. Neerincx, and J. C. van Weert, "Task Based Interpretation of Operator State Information for Adaptive Support," ACI/HFES-2006, Tech. Rep., 2006.

[20] D. Watson and R. Friend, "Measurement of social-evaluative anxiety," *Consulting and Clinical Psychology*, vol. 33, pp. 448–457, 1969.

[21] G. F. Wilson, "An analysis of Mental Workload in Pilots during flight using multiple psychophysiological measures," *International Journal of Aviation Psychology*, vol. 12, pp. 3–8, 2002.

[22] S. Miyake, "Multivariate workload evaluation combining physiological and subjective measures," *International Journal of Psychophysiology*, vol. 40, pp. 233–238, 2001.

[23] H. van Kuilenburg, M. Wiering, and M. den Uyl, "A Model Based Method for Automatic Facial Expression Recognition," in *Proceedings of the 16th European Conference on Machine Learning*, Oct. 2005.

[24] A. Haag, S. Goronzy, P. Schaich, and J. Williams, "Emotion Recognition Using Bio-Sensors: First Steps Towards an Automatic System," in *Proceedings of Affective Dialogue Systems, Tutorial and Research Workshop*, June 2004, pp. 36–48.

[25] T. Crawford, S. Higham, T. Renvoize, J. Patel, M. Dale, A. Suriya, and S. Tetley, "Inhibitory control of saccadic eye movements and cognitive impairment in alzheimer's disease," *Biological Psychiatry*, vol. 9, no. 57, pp. 1052–1060, 2005.

[26] B. Noris, K. Benmachiche, J. Meynet, J.-P. Thiran, and A. Billard, "Analysis of Head-Mounted Wireless Camera Videos for Early Diagnosis of Autism," *Advances in Soft Computing*, vol. 45, pp. 663–670, 2007.

[27] R. J. Leigh and D. S. Zee, *The Neurology of Eye Movements*, 4th ed. Oxford University Press, 1991.

[28] D. E. Irwin and J. R. Brockmole, "Mental rotation is suppressed during saccadic eye movements," *Psychonomic Bulletin and Review*, vol. 7, no. 4, pp. 654–661, 2000.

[29] S. Tokuda, G. Obinata, E. Palmer, and A. Chaparro, "Estimation of mental workload using saccadic eye movements in a free-viewing task," *Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 4523–4529, August 2011.

[30] C. K. Ora and V. G. Duffyb, "Development of a facial skin temperature-based methodology for non-intrusive mental workload measurement," *Occupational Ergonomics*, vol. 7, pp. 83–94, 2007.

[31] L.-M. Wang, V. G. Duffy, and Y. Du, "A composite measure for the evaluation of mental workload," in *Proceedings of the 1st International Conference on Digital Human Modeling*, 2007, pp. 460–466.

[32] J. Voskamp and B. Urban, "Measuring Cognitive Workload in Non-military Scenarios Criteria for Sensor Technologies," in *Proceedings of the 5th International Conference on Foundations of Augmented Cognition*, June 2009, pp. 304–310.

[33] H. Genno, K. Ishikawa, O. Kanbara, M. Kikumoto, Y. Fujiwara, R. Suzuki, and M. Osumi, "Using facial skin temperature to objectively evaluate sensations," *International Journal of Industrial Ergonomics*, vol. 19, pp. 161–171, 1997.

[34] Tobii Technology, "Tobii TX300," Available at: http://www.tobii.com.

[35] The EyeTribe, "The Eye Tribe Tracker," Availabel at: https://theeyetribe.com.

[36] Anti Phishing Working Group and CMY-CyLab, "Education Landing Page Program," Available at: http://phish-education.apwg.org/r/about.html.

[37] A. Van der Merwe, M. Loock, and M. Dabrowski, "Characteristics and Responsibilities Involved in a Phishing Attack," in

Proceedings of the 4th International Symposium on Information and Communication Technologies, Jan. 2005.

[38] J. Evers, "Security Expert: User education is pointless," Available at: http://news.com.com/2100-7350_3-6125213.html, Oct. 2007.

[39] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. I. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in *Proceedings of Conference On Human Factors In Computing Systems*, Apr. 2007, pp. 905–914.

[40] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. I. Hong, and E. Nunge, "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 1st Symposium On Usable Privacy and Security*, Jul. 2007.

[41] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J. I. Hong, "Getting users to pay attention to anti-phishing education: evaluation of retention and transfer," in *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, Oct. 2007, pp. 70–81.

[42] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. F. Cranor, J. I. Hong, M. Ann, and T. Pham, "School of Phish: A real-World Evaluation of Anti-Phishing Training," in *Proceedings of the 5th Symposium On Usable Privacy and Security*, Jul. 2009.

[43] NECOMA Project, "necoma - github," Available at: https://github.com/necoma/eyebit, (to appear).