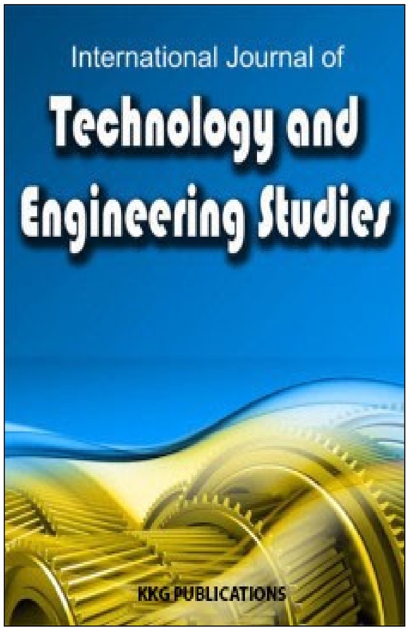


Key Knowledge Generation
Publication details, including instructions for author and subscription information:
http://kkgpublications.com/technology/

# The Degree of Occurrence of Phishing in Indonesia

IWAN BINANTO [1], ATANASIUS RONALD EKO JATMIKO [2]

[1, 2] Department of Informatics, Faculty of Science & Technology, Sanata Dharma University, Yogyakarta, Indonesia

Published online: 24 October 2016

**To cite this article:** I. Binanto and A. R. E. Jatmiko, "The degree of occurrence of phishing in Indonesia," *International Journal of Technology and Engineering Studies,* vol. 2, no. 5, pp. 149-153, 2016.
DOI: https://dx.doi.org/10.20469/ijtes.2.40004-5

**To link to this article:** http://kkgpublications.com/wp-content/uploads/2016/2/Volume2/IJTES-40004-5.pdf

PLEASE SCROLL DOWN FOR ARTICLE

KKG Publications makes every effort to ascertain the precision of all the information (the "Content") contained in the publications on our platform. However, KKG Publications, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the content. All opinions and views stated in this publication are not endorsed by KKG Publications. These are purely the opinions and views of authors. The accuracy of the content should not be relied upon and primary sources of information should be considered for any verification. KKG Publications shall not be liable for any costs, expenses, proceedings, loss, actions, demands, damages, expenses and other liabilities directly or indirectly caused in connection with given content.

International Journal of Technology and Engineering Studies
vol, 2, no. 5, pp. 149-153, 2016

IJTES

# THE DEGREE OF OCCURRENCE OF PHISHING IN INDONESIA

IWAN BINANTO [1]*, ATANASIUS RONALD EKO JATMIKO [2]

[1, 2] Department of Informatics, Faculty of Science & Technology, Sanata Dharma University, Yogyakarta, Indonesia

**Keywords:**
Phishing
Cybercrime
Email
Bookmark

**Abstract.** The aim of this research is to find out the degree of occurrence of Phishing in Indonesia. Phishing is a technique to get a username, password, pin (personal identification number), users' biographical information, bank account information, or others. This research utilizes 2 (two) techniques, which are sending email and bookmarking. This research collected data in period February 23$^{th}$, 2015 until April 10$^{th}$, 2015. The results show that the Indonesian people, especially students, who are potentially exposed to phishing and the highest time to access a fake Facebook website is in working hours, which are 08.00 AM  12.00 PM and 01.00 PM  05.00 PM.

**Received:** 28 July 2016
**Accepted:** 29 August 2016
**Published:** 24 October 2016

## INTRODUCTION

Facebook is a popular social networking site that is used by every society in the world. It is one of the free of charge online social networking services that allow the account's owner to connect with their friends, colleagues, and others who share similar interests or have the same general experiences.

More than 60% of students in Indonesia are Facebook users and 75% from them will access this site every day [1]. According to Socialbakers' data in 2013, Indonesia is at the fourth rank in the world with a total of 50,583,320 users [2].

Nowadays, Facebook is not only used for interaction but also a lot of crimes have been done on this site. One of these crimes is theft of personal data which are crucial and confidential, and usage of all of these data to conduct a campaign on behalf of the account owner that can defame him/her. This is done by fishing the account owner to enter his/her personal data into a special constructed website. This activity is known as phishing. Phishing is a technique to get confidential information which is owned by a personal internet user with the purpose of obtaining a username, password, pin (personal identification number), users' biographical information, bank account information, or others [3]. Alkazimy, as ID CERT (Indonesia Computer Emergency Response Team) manager, said the number of spoofing/phishing that occurs in Indonesia is as many as 1,495 times during July and August. It is based on the results of their study in 2014 [4]. Motivated by these facts, we are interested to find out the degree of occurrence of phishing in Indonesia in the start of 2015, especially those which happen on Facebook.

## METHOD AND MATERIALS

This research collected data in period February 23$^{th}$, 2015 until April 10$^{th}$, 2015 by utilizing two phishing techniques and two attack techniques:

### Phising Technique

### Sending Email Technique

This is the most frequent technique employed [5]. It was done in period from March 3rd, 2015 until April 9$^{th}$, 2015 according to the following steps:

i. Collecting email addresses by using google to find them (Fig. 1a & Fig. 1b).
ii. Sending phishing message (Fig. 2) to the collected email addresses.
iii. Sending phishing messages using email address admin@sys-facebook.com which are expected to be trusted by recipients because of its similarities with the genuine domain name.
iv. Analyzing the following data:

- Time stamp
- Type of browser
- Type of operating system
- Type of device
- Location

### Bookmark Technique

This was done in the lecture time from February 23rd, 2015 until April 10th, 2015 by the following steps:

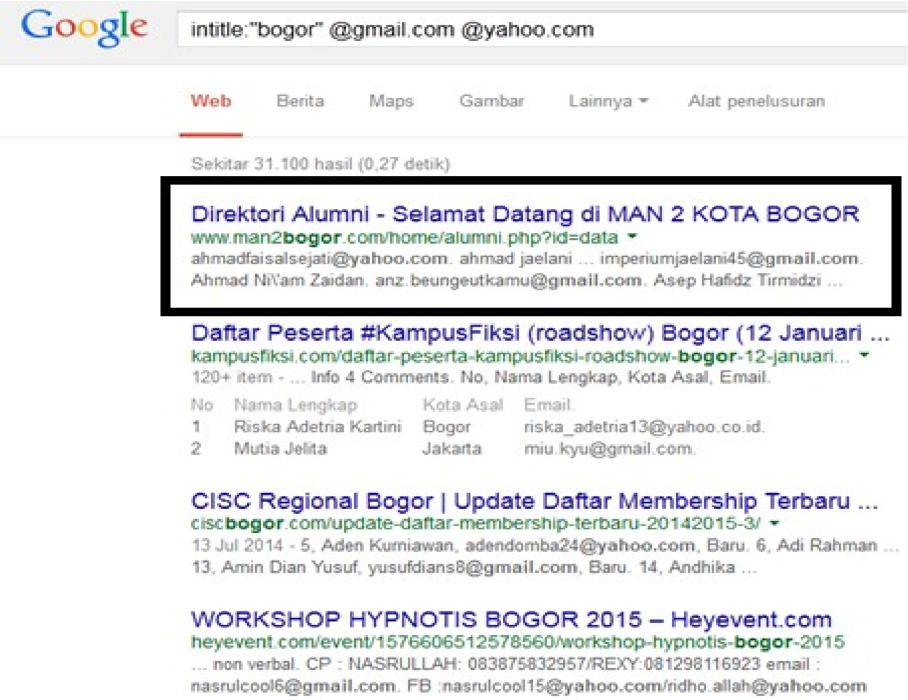
i. Access a phishing web page that has been prepared on a

*Corresponding author: Iwan Binanto
†Email: Iwan@Usd.Ac.Id

browser on computer.

ii. Do a bookmark to a phising website on the browser.

Bring out the phising bookmark on the browser in three (3) Basic Computer Laboratory (LKD) at the University of ABCD.



intitle:"bogor" @gmail.com @yahoo.com

Sekitar 31.100 hasil (0,27 detik)

Direktori Alumni - Selamat Datang di MAN 2 KOTA BOGOR
www.man2**bogor**.com/home/alumni.php?id=data
ahmadfaisalsejati@yahoo.com. ahmad jaelani ... imperiumjaelani45@gmail.com. Ahmad Ni\'am Zaidan. anz.beungeutkamu@gmail.com. Asep Hafidz Tirmidzi ...

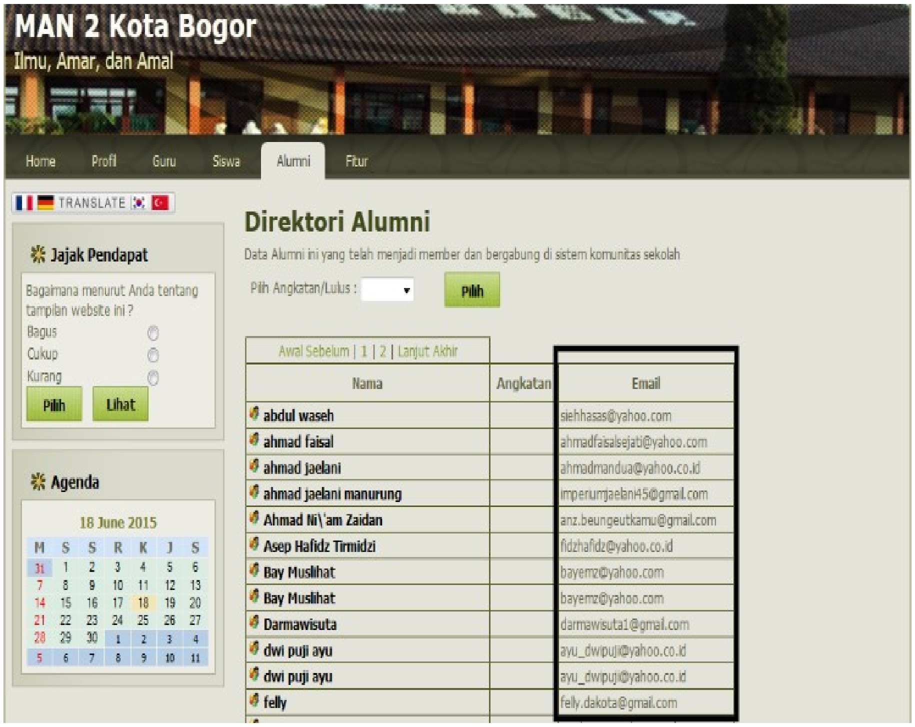
Daftar Peserta #KampusFiksi (roadshow) Bogor (12 Januari ...
kampusfiksi.com/daftar-peserta-kampusfiksi-roadshow-**bogor**-12-januari...
120+ item - ... Info 4 Comments. No, Nama Lengkap, Kota Asal, Email.

| No | Nama Lengkap | Kota Asal | Email. |
|---|---|---|---|
| 1 | Riska Adetria Kartini | Bogor | riska_adetria13@yahoo.co.id. |
| 2 | Mutia Jelita | Jakarta | miu.kyu@gmail.com. |

CISC Regional Bogor | Update Daftar Membership Terbaru ...
cisc**bogor**.com/update-daftar-membership-terbaru-20142015-3/
13 Jul 2014 - 5, Aden Kurniawan, adendomba24@yahoo.com, Baru. 6, Adi Rahman ... 13, Amin Dian Yusuf, yusufdians8@gmail.com, Baru. 14, Andhika ...

WORKSHOP HYPNOTIS BOGOR 2015 – Heyevent.com
heyevent.com/event/1576606512578560/workshop-hypnotis-**bogor**-2015
... non verbal. CP : NASRULLAH: 083875832957/REXY:081298116923 email : nasrulcool6@gmail.com. FB :nasrulcool15@yahoo.com/ridho.allah@yahoo.com

Fig. 1 (a). Utilizing Google to find email addresses



Jajak Pendapat

Bagaimana menurut Anda tentang tampilan website ini ?
Bagus ○
Cukup ○
Kurang ○

Agenda

18 June 2015

| M | S | S | R | K | J | S |
|---|---|---|---|---|---|---|
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

Direktori Alumni

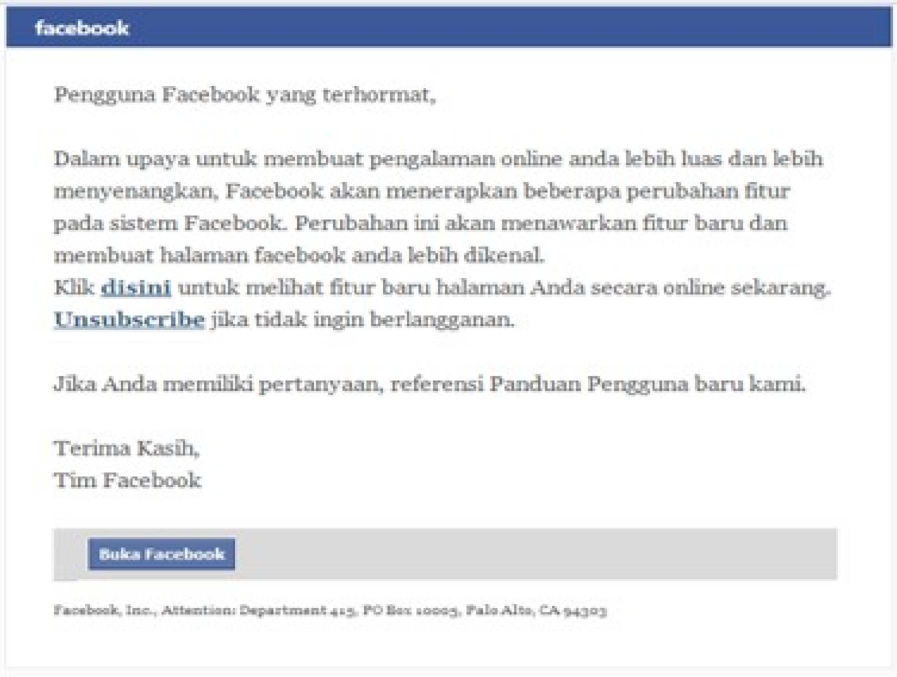
Data Alumni ini yang telah menjadi member dan bergabung di sistem komunitas sekolah

Pilih Angkatan/Lulus :

Awal Sebelum | 1 | 2 | Lanjut Akhir

| Nama | Angkatan | Email |
|---|---|---|
| abdul waseh | | siehhasas@yahoo.com |
| ahmad faisal | | ahmadfaisalsejati@yahoo.com |
| ahmad jaelani | | ahmadmandua@yahoo.co.id |
| ahmad jaelani manurung | | imperumjaelani45@gmail.com |
| Ahmad Ni\'am Zaidan | | anz.beungeutkamu@gmail.com |
| Asep Hafidz Tirmidzi | | fidzhafidz@yahoo.co.id |
| Bay Muslihat | | bayemz@yahoo.com |
| Bay Muslihat | | bayemz@yahoo.com |
| Darmawisuta | | darmawisuta1@gmail.com |
| dwi puji ayu | | ayu_dwipuji@yahoo.co.id |
| dwi puji ayu | | ayu_dwipuji@yahoo.co.id |
| felly | | felly.dakota@gmail.com |

Fig. 1 (b). Utilizing Google to find email addresses (Cont.)



Pengguna Facebook yang terhormat,

Dalam upaya untuk membuat pengalaman online anda lebih luas dan lebih menyenangkan, Facebook akan menerapkan beberapa perubahan fitur pada sistem Facebook. Perubahan ini akan menawarkan fitur baru dan membuat halaman facebook anda lebih dikenal.
Klik disini untuk melihat fitur baru halaman Anda secara online sekarang.
Unsubscribe jika tidak ingin berlangganan.

Jika Anda memiliki pertanyaan, referensi Panduan Pengguna baru kami.

Terima Kasih,
Tim Facebook

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

Fig. 2 . Content of a phishing email

**Attack Technique**

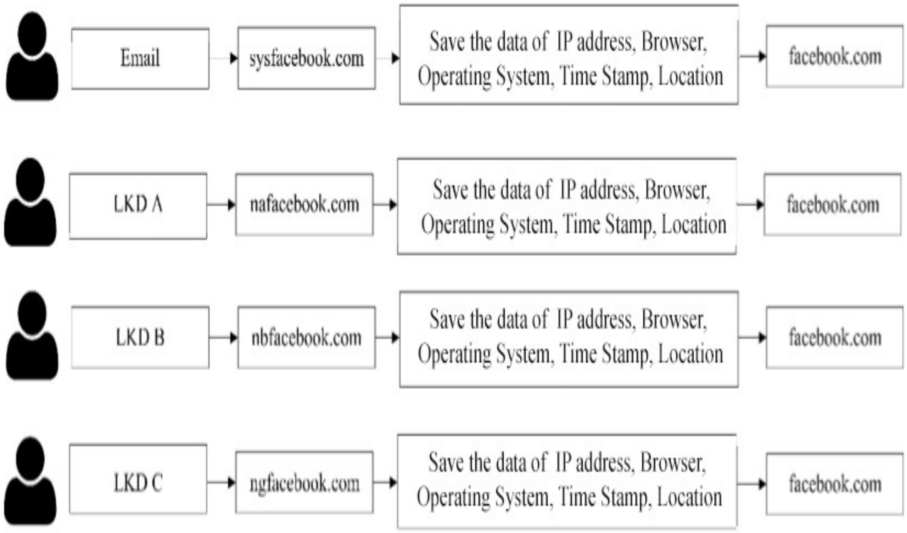
1. Using the following domain names which are similar to Facebook: i. sysfacebook.com
ii. nafacebook.com
iii. nbfacebook.com
iv. ngfacebook.com

The aim of using these domain names is to acquire data in a simple way. Every domain name has specific task:
i. sysfacebook.com is used to send phising messages by email
ii. nafacebook.com is used with the bookmark technique in Basic Computer Laboratory A (LKD A)
iii. nbfacebook.com is used with the bookmark technique in Basic Computer Laboratory B (LKD B)
iv. ngfacebook.com is used with the bookmark technique in Basic Computer Laboratory C (LKD C)

Utilizing URL Redirection: It serves to distract users from phishing.

**Acquiring Data**

Figure 3 is the process of acquiring data in three (3) Basic Computer Laboratory.



Email
sysfacebook.com
Save the data of IP address, Browser, Operating System, Time Stamp, Location
facebook.com
LKD A
nafacebook.com
Save the data of IP address, Browser, Operating System, Time Stamp, Location
facebook.com
LKD B
nbfacebook.com
Save the data of IP address, Browser, Operating System, Time Stamp, Location
facebook.com
LKD C
ngfacebook.com
Save the data of IP address, Browser, Operating System, Time Stamp, Location
facebook.com

Fig. 3 . Chart of acquiring data

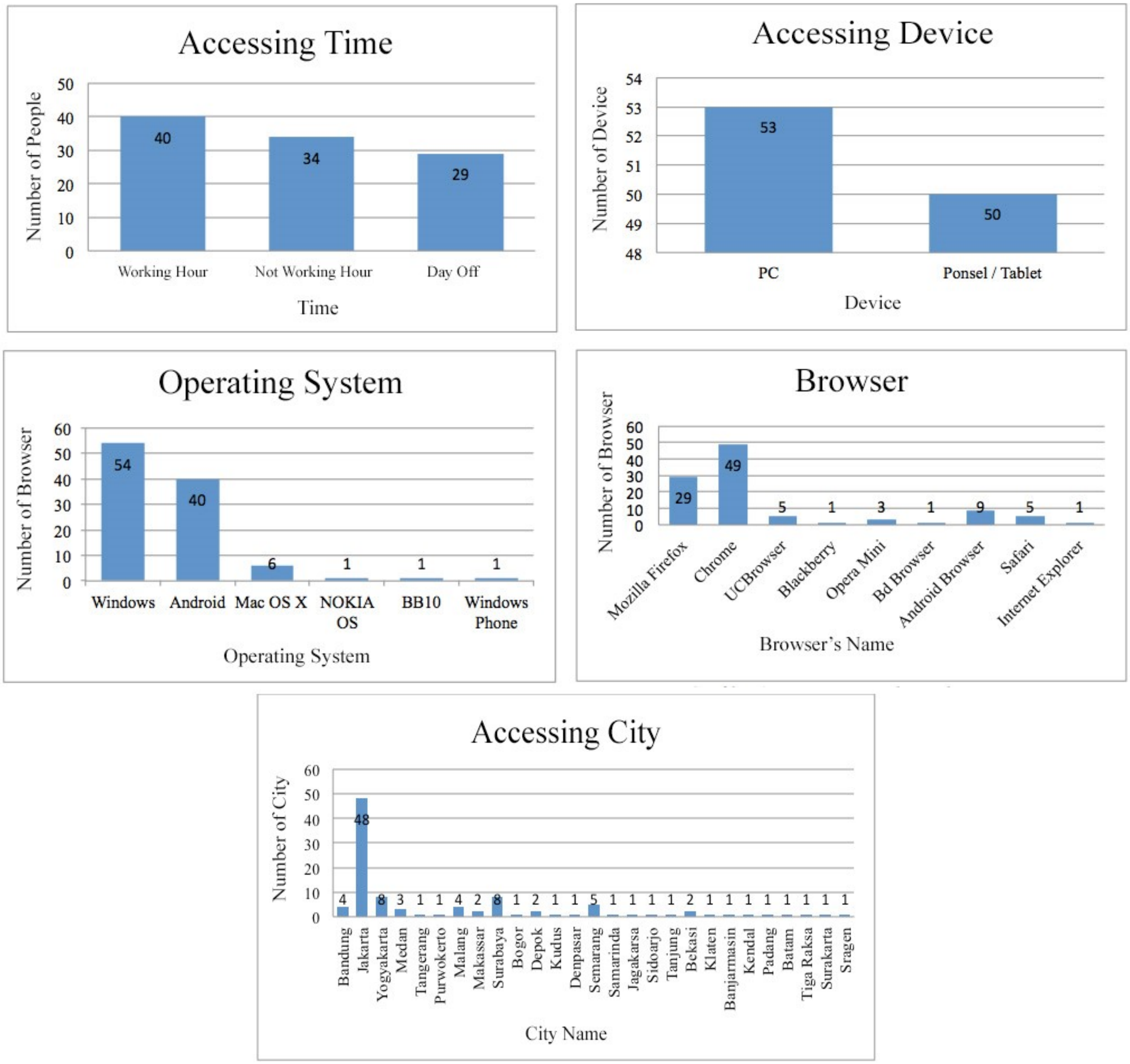


Fig. 4 . The result of acquired data

## RESULTS

### Sending Email Technique

By this technique, we are able to get 103 emails from 3463 emails sent by phishing emails, i.e. 2.9743% of the population.

The data show (Fig. 4) that the highest time to access phishing website is during working hours, those are from 08:00 AM to 12:00 PM and from 1:00 PM to 5:00 PM.

Most devices that are used to access phishing website are Personal Computers with MS Windows and Google Chrome browser. Mostly location is in Jakarta. Furthermore, it can be seen that the victim of phishing's users are mostly located in the western region of Indonesia.

### Bookmark Technique

By using this technique 1,515 students from 4,478 students who attended the lecture hours are affected by phishing. This number means 33.832068% of the population. The bookmark technique differs from sending email technique and hence the outcomes are also different.

This technique shows that students prefer to clicking directly rather than typing in the browser's search field. It is also surprising because in the lecture hours students access Facebook.

## CONCLUSION AND RECOMMENDATIONS

1. Indonesian people are potentially exposed to phishing with a relatively small percentage, about 2.9743%. However, it is much bigger when compared to Get Cyber Safe data (2012) from Canada which is about 0.05128205% [6], [7], [8].

2. The number of students exposed to phishing in Basic Computer Laboratory is quite big, that is about 33,839625%.

3. The highest time to access a fake Facebook website is in working hour, which are 08.00 AM  12.00 PM and 01.00 PM  05.00 PM. This indicates that most companies give permission to their employees to access Facebook in working hours.

4. The Bookmark technique is quite effective to perform a phishing activity.

### Declaration of Conflicting Interests

No conflicts of interest.

## REFERENCES

[1] M. Williyanson, *Hacking Facebook.* Jakarta, Indonesia: PT Elex Media Komputindo, 2010.

[2] A. C. Pratikta, “Effectiveness problem solving training for reduction trends in social networking site addiction learners: Quasi-experimental research of the three students class XI SMAN 4 Bandung school year 2013/2014,” Doctoral dissertation, University of Indonesia, Depok, Indonesia, 2013.

[3] R. E. Latumahina, “Aspects of personal data protection law in cyberspace,” *Jurnal Gema Aktualita,* vol. 3, no. 2, pp. 14-25, 2014.

[4] A. Alkazimy. (2014). *Trend and ID-CERT security warning* [online]. Available: https://goo.gl/QCRP9C

[5] Sto., *Certified Ethical Hacker 400% Illegal.* Jakarta, Indonesia: Jasakom Publishing, 2011.

[6] Get Cyber Safe. (2012). *Phishing: How many take the bait?* [online]. Available: https://goo.gl/o2QcpY

[7] A. C. Singh, K. P. Somase and K. G. Tambre, “Phishing: A computer security threat,” *International Journal of Advance Research in Computer Science and Management Studies,* vol. 1, no. 7, pp. 64-71, 2013.

[8] M. Alsharnouby, F. Alaca and S. Chiasson, “Why phishing still works: User strategies for combating phishing attacks,” *International Journal of Human-Computer Studies,* vol. 82, pp. 69-82, 2015.

— This article does not have any appendix. —