JOEICT(Jurnal of Education and Information Communication Technology)
Volume 1, Nomor 1, Tahun 2017: 1 - 5

ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME

Mia Haryati Wibowo[1)],Nur Fatimah[2)]
[1, 2)]prodi teknologi informasiSTKIP PGRI Tulungagung
Jl. Mayor Sujadi Timur No. 7 Tulungagung 66221
e-mail: mia.wibowo96@gmail.com[1)], nurfatimah2627@gmail.com[2)]

ABSTRAK

*Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Phishing termasuk dalam kejahatan siber. Dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer.Sosial media merupakan tempat dimana orang-orang dapat berhubungan dari jarak jauh, juga tempat untuk mendapatkan informasi secara cepat. Hampir semua orang di penjuru dunia menggunakan sosial media. Sehingga para aktivis kejahatan siber sangat memanfaatkan kesempatan itu untuk melakukan aksinya terhadap pengguna sosial media. Kemudian mereka melakukan serangan dengan berbagai cara yang salah satunya adalah phishing itu sendiri.Dalam sosial media, phishing bisa di lakukan dengan cara menjebak sang pengguna melalui link yang begitu meyakinkan, juga bisa dengan mengirimkan via email. Saat pengguna sedang lengah dan tidak sengaja meng-*klik *alamat tersebut, maka seluruh data yang ada di akunnya akan terbaca dan di curi. Selain itu juga phishing mengancam para pengguna nasabah bank.Setiap ancaman, pasti ada jalan keluarnya. Banyak sekali antisipasi-antisipasi untuk mencegah serangan phishing. Pada jurnal ini nantinya akan dibahas beberapa cara menanggulangi phishing pada sosial media yang paling umum digunakan.Berdasarkan hasil survey dari beberapa jurnal, website merupakan sumber ancaman phishing yang sering terjadi dan cara pencegahannya dengan cara self-efficacy.*

***Kata Kunci**: Cyber Crime, Phishing, Sosial Media*

ABSTRACT

Phishing is a form of activity that is threatening or trap someone with concept fishing of the person. It's mean deceiving someone so that the person indirectly provides all the information needed by the trapper. Phishing included in cyber crime. Where it is bustling happen crime through computer networks. Along with the times, crime is also rapidly evolving around the world. So that the threat is a lot going on today through the computer.Social media is a place where people can relate from a distance, is also the place to get information quickly. Almost all people around the world using social media. So that cyber-crime activists took the opportunity to perform an action against users of social media. Then they carried out attacks in various ways, one of which is a phishing itself.In social media, phishing can be done by trapping the user through links are so reassure, also can send via email. When the user is careless and accidentally clicking that address, then all the data available in their account will be read and stolen. In addition, phishing scams threaten users of bank customers.Every threat, there must be a way out. Lots anticipations to prevent phishing attacks. On this journal will discuss some ways to cope phishing on social media most commonly used.Based on survey results from journals that we already read, the website is a source of phishing threat that always occurred and its prevention by means of self-efficacy.

***Keywords**: Cyber Crime, Phishing, Social Media*

I. PENDAHULUAN

Di era modern sekarang, orang-orang tidak bisa lepas dari yang namanya internet dan *gadget*. Di tambah, saat ini orang-orang berlomba memperbanyak akun jejaring sosial mereka untuk mencari kepopuleran seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Untuk mendapat berita ter-*update*orang-orang juga bisa menjumpai berbagai macam artikel baik dalam maupun luar negeri melalui sebuah laman *web* ataupun di jejaring sosial juga. Pastinya orang-orang membuka *web browser* dulu agar bisa pergi ke berbagai jejaring sosial semacam itu. Setiap orang pasti memiliki akun jejaring sosial lebih dari satu. Selain itu, sosial media juga digunakan untuk lahan berbisnis misalnya *online shop*. Kegiatan ini sangat mudah dan menguntungkan karena tidak membutuhkan modal dan hanya tinggal memposting barang jualan. Untuk pembayarannya bisa lewat rekening, *COD*, *market*, dll.

Di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya yaitu dengan *phishing*. *Phishing* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung

memberikan semua informasi yang di butuhkan oleh sang penjebak. *Phishing* termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam *phishing*. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh *fake link* pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran *online*.

Untuk pengantisipasian serangan *phishing* semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada *link* yang masuk melalui akun sosial media maupun *email* yang di gunakan untuk akun sosial media. Karena *link* yang tidak di kenal patut di curigai sebagai serangan *phishing* yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain.

Sebenarnya tujuan di buatnya jurnal ini yang pertama yaitu agar orang-orang mulai mengubah pemikirannya terlebih dahulu terhadap serangan *phishing*. Kemudian orang-orang harus mengetahui hal-hal yang mencurigakan pada akun jejaring sosial maupun situs *web* yang lain. Bila benar ada serangan *phishing*, maka mereka harus meninggalkan laman palsu itu sesegera mungkin. Jangan hanya pergi begitu saja, kita juga harus mencari jalan keluar untuk menyelamatkan akun kita. Tentu kita harus mencari anti*phishing* untuk mencegahnya. Karena sekali kita terkena serangan, maka ancaman *phishing* juga akan menyerang pengguna yang lain. Dan serangan akan terus menyebar dan menyebar ke seluruh penjuru dunia. Bila dalam jejaring sosial pengguna yang terserang tidak tau apa-apa, di pihak lain akan marah-marah karena pengguna yang terserang tadi akan terus mengirim pesan spam pada seluruh akun yang berteman dengannya.

Tidak tau sampai kapan serangan *phishing* akan di lancarkan sebagai kejahatan siber. Karena para *hacker-hacker* itu terus memunculkan ide-ide baru untuk merusak kegiatan di internet.Dan sayangnya di setiap tahunnya kasus seperti ini semakin bertambah banyak dan korban yang terjaring juga tidak bisa hanya di hitung dengan jari. Mereka mencari uang dengan cara yang mudah. Namun tak selamanya mereka melakukan itu karena uang. Biasanya mereka hanya ingin bersenang-senang atau ingin mengintip kegiatan sang pemilik akun. Jika beruntung, mereka juga bisa mendapat uang sekaligus melihat-lihat isi akun pengguna yang mereka serang untuk bersenang-senang. Bila hanya orang biasa yang mereka serang mungkin masalah tidak akan terlalu besar. Bagaimana jika yang mereka serang adalah orang yang penting atau pun orang yang berpengaruh di dunia ini.Kasus itu pasti sudah sering terjadi. Orang-orang yang memiliki kuasa tertinggi beberapa juga melakukan kejahatan tetapi ia hanya menjadi bagian penyuruh untuk sang hacker. Selanjutnya hacker-hacker itu yang melaksanakan perintah untuk menyerang. Hal-hal itu sudah wajar terjadi apalagi saat masa-masa kampanye berpolitik ataupun contohnya pada saat dua perusahaan yang awalnya menjalin hubungan yang baik tiba-tiba salah satu perusahaan merasa kecewa karena saat pembagian hasil tidak memenuhi sepakat yang tercantum sebelumnya. Maka muncul lah ide-ide berbuat kecurangan. Mereka akan memanfaatkan *hacker* sebagai sarana penghancur sang lawan. Mereka menyuruh sang hacker untuk diam-diam mencuri data keuangan perusahaan musuh dan kemudian memanipulasi data tersebut sebaik mungkin. Lalu pada akhirnya semua uang hasil kerja sama mereka menjadi milik perusahaan yang menyewa hacker tadi semua. Pastinya si *hacker* tadi mendapat keuntungan beberapa persen. Untuk itulah masih ada banyak orang baik di dunia ini yang mau menciptakan alat pendeteksi atau aplikasi untuk mencegahnya. Para peneliti maupun pembuat aplikasi itu biasanya merupakan orang-orang yang pernah mengalami serangan *phishing*. Mereka tidak terima dan kemudian memutuskan untuk membalaskan dendamnya dengan sebuah aplikasi anti *phishing*. Maka dari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan *phishing*. Bila enggan melakukan sesuatu yang menurutnya terlalu merepotkan, mereka juga bisa menjaga akunnya sebaik mungkin dengan pengamanan yang tepat. Hanya dengan cara itu akun tidak akan di serang dan pengguna bisa nyaman bersosialisasi di dunia maya tanpa hambatan.

II. SUMBER-SUMBER ANCAMAN PHISHING

Untuk mengetahui sumber-sumber ancaman phishing kami telah melakukan *survey* literatur *phishing* dengan membaca beberapa jurnal. Berikut adalah garis besar dari beberapa sumber ancaman phishing berdasarkan *survey* yang telah kami lakukan :

A.Email

Berdasarkan survey yang telah dilakukan pada tahun 2014 ada lebih dari 120.000 serangan *phishing* yang berpuncak pada miliaran transmisi *email*[1]. 65% dari serangan *phishing* mulai dengan mengunjungi *link* yang diterima dalm sebuah *email*[2]. Pada Maret 2016, 229.265 laporan *emailphishing* diterima oleh Kelompok Kerja Anti-*Phishing* dari konsumen[8]. 18,3% penduduk Australia menjadi korban dari *phishing* melalui *email*[8].

B.Website

Phishing pada *website* meliputi iklan dan sosial media (Facebook, Twitter, Instagram). Berdasarkan *survey* yang telah dilakukan Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 bukan milik pengguna yang sebenarnya dan perkiraan sekitar 1,5% (14.320.000) adalah akun yang secara tidak sengaja menyebarkan isi berbahaya tanpa diketahui oleh pengguna, seperti pesan *spam* dan *link* yang mencurigakan [3]. Sebagian besar serangan phishing dilakukan melalui *web server* yang sudah di*hack*dan 73% situs telah menjadi korban[11]. Pada Maret 2016 123.555 situs phishing terdeteksi oleh Kelompok Kerja Anti-*Phishing*[8]. 15,7% penduduk Australia menjadi korban *phishing* melalui situs belanja *online* dan 6,9% melalui sosial media[8].

C.Malware

Phishing yang dilakukan melalui penyebaran *malware*salah satunya adalah *malware* Koobface yang telah membuat 81% pengguna menjadi korbannya [3]

III. CARA KERJA PHISHING

Berikut merupakan cara kerja *phishing* berdasarkan sumber-sumber ancaman phishing yang telah kami *survey* dari beberapa jurnal :

A. Email

Serangan ini di mulai dengan mengirimkan *email* yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian *email* tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti *link URL* yang terdapat dalam *email* tersebut [2]. Pada dasarnya, *phishing* menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima *email* [9]. Penyerang akan mengirimkan jutaan *email* ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut [13]. Pastinya serangan-serangan tersebut menggunakan *email* palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi [15].

B. Website

Pada situs *web* mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti *password* dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas [7].*Phiser* juga menggunakan *tool* untuk mencuri kode sumber laman *web* yang sah dan menggantinya dengan *web* palsu [6]. Selain itu, *phiser* menciptakan *embedding link* untuk mendapatkan informasi sensitif milik korban [3].

C. Malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu *file* yang di kirim oleh *phiser* sebagai penetralisir *malware* di komputer nantinya [8].

IV. CARA MENCEGAH PHISHING

Berikut adalah hasil survey kami mengenai cara pencegahan atau antisipasi terhadap serangan *phishing* melalui *website* dari beberapaliteratur :

1) Medeteksi dengan toolsdetect

Sekarang ini internet sudah dianggap sebagai makanan sehari-hari, bahkan ada beberapa orang yang berangga-pan tanpa internet mereka tidak bisa hidup. Ada banyak hal yang bisa kita lakukan dengan internet, mulai dari mencari informasi, berbagi informasi, dsb. Namun, pasti kita pernah menjumpai situs-situs yang muncul tanpa kita inginkan dan mengandung informasi berhadiah yang menggiurkan. Tentu saja hal tersebut akan menarik kita untuk mengisinya dengan data penting tanpa tau bahwa itu hanyalah situs *phishing*. Untuk mencegah hal tersebut kita dapat menggunakan *toolsdetect* yang mana dapat membedakan mana situs yang asli dan palsu (*phishing*). Berikut *toolsdetect* yang dapat digunakan :

a) PhishShield

PhishShield merupakan aplikasi *desktop* yang berkonsentrasi pada *URL* dan konten situs *web phishing* [13]. Cara kerjanya dengan mengambil *UR*L sebagai masukan dan outputnya berupa status yang mengkonfirmasi *URL* [13] termasuk *phishing* atau situs asli [13]. Tingkat akurasi yang diperoleh untuk PhishShield adalah 96,57% dan mencakup berbagai situs *phishing* yang dihasilkan tingkat kepalsuan negatif dan positif [13].

b) LinkGuard Algoritma

LinkGuard Algoritma digunakan untuk menganalisis dua *URL* dan akhirnya tergantung pada hasil yang dihasilkan oleh algoritma [15]. *URL* tersebut adalah *URL* yang melibatkan ekstraksi *URL* yang sebenarnya dan *URL* visual (yang dilihat pengguna) [15].

c) PhishDetector

PhishDetector adalah ekstensi *browser* yang digunakan untuk mendeteksi serangan *phishing* yang mana menggunakan algoritma pencocokan string perkiraan untuk menentukan hubungan antara konten dan *URL* dari suatu halaman *web*[11].

2) Menggunakan add ons web browser anti tabnabbing

Setiap tahunnya para *phisher* melancarkan aksi-aksinya dengan membuat serangan-serangan baru. Dan salah satu serangan baru tersebut yaitu bernama tabnabbing. Serangan *phishing* tersebut dapat menyerang pada *web*. Dimana cara penyerangannya ketika pengguna membuka banyak *tab*, *phishing* tersebut akan terbuka di sela-sela *tab* yang lain. Saat pengguna lengah, maka *tab* tersebut akan di buka dan serangan di mulai. *Tab* palsu itu di samarkan menjadi salah satu *tab* yang di buka oleh pengguna dan *tab* asli yang sebelumnya lenyap. Untuk itulah serangan ini di anggap serangan yang pintar karena tidak lagi menggunakan *link* yang di klik dulu agar pengguna masuk perangkap *phisher*. Namun sepintar apapun suatu serangan, pasti ada jalan keluar. Beberapa cara pencegahan serangan tabnabbing: a) Ketika pengguna membuka firefox dan terjadi serangan, pengguna bisa mengatasi serangan dengan *account manager*. *Account manager* dapat mengamankan pengguna karena pengguna di sarankan menyimpan login dan saat itu juga pengguna di berikan *password* acak setiap kali *login* [14]. b) Tidak hanya pada firefox saja, pada crome juga di berikan pengamanan terhadap phishing tabnabbing. Yaitu menggunakan AgenTab. AgenTab melakukan tindakan ketika pengguna mulai membuka situs *web* [14]. AgenTab akan menyalakan peringatan ketika serangan terdeteksi. Peringatan tersebut akan muncul ketika *tab* tiba-tiba berubah tempat [14]. c) Dan yang terakhir dalam pencegahan tabnabbing dapat di lakukan dengan NoTabNab4. Add-on tersebut di usulkan oleh *web browser* Unlu dan Bicakci, dimana serangan phishing dapat diketahui saat suatu tab palsu meniru tab asli lalu *add-on* tersebut bekerja dengan cara memperingati dengan memberi tanda warna kuning atau merah sesuai tingkat serangan pada highlightned [14].

3) Menggunakan mekanisme pre-filter

Pencegahan *phishing*juga dapat di lakukan dengan penggunaan anti-*phishing* pre-filter ini. Di dalam pre-filter terdapat tiga bagian pencegahan yakni *Site Identifier*, *Login Form Finder*, dan *Webpage Feature Generator*. Ketiganya tersebut melakukan pencegahan secara berurutan. *Site Identifier* digunakan untuk mengurangi jumlah perhitungan situs yang tidak perlu dan hanya mendeteksi halaman yang sah [6]. Kemudian *Login Form Finder* di gunakan untuk menyaring halaman tanpa bentuk login lalu menghentikan mereka dari proses lebih lanjut karena *form login* merupakan satu-satunya cara untuk menyadarkan pengguna bila informasi pribadinya dicuri oleh *phiser* [6]. Sistem ini dapat mengurangi kesalahan positif dari sistem tanpa harus mencurigai jumlah kesalahan negatif [6]. Yang terakhir adalah *Webpage Feature Generator*, dimana fungsinya adalah mengidentifikasi halaman *web phishing* dengan melacak karakteristik *phishing* yang di pamerkan dalam halaman tersebut [6]. Seseorang dapat menggunakan cara ini ketika merasa bila halaman *web*nya sudah terserang *phishing*.

4) Pendeteksian dengan streaming analytics 'PhishStrom'

Sekarang ini banyak sekali orang-orang yang berlomba-lomba melakukan penelitian untuk menciptakan suatu alat maupun aplikasi. Namun bukan hanya itu saja. Orang-orang juga mulai melakukan pendeteksian dengan berbagai cara. Dan anti *phishing* kali ini yaitu melakukan pendeteksian berupa streaming analisa menggunakan *PhisStrom*. *PhisStrom* sendiri di gunakan untuk mendeteksi *URL* yang terserang *phishing*. Dalam percobaannya, pendeteksian dengan cara ini dapat menghasilkan akurasi klasifikasi 94, 91% dengan tingkat positif palsu yakni 1,44% [10]. Untuk risiko pada pengujian *dataset* menunjukkan pengidentifikasian 99,22% pada *web* yang sah dan *phishing* 83,97% [10]. Untuk selanjutnya, *PhisStrom* dapat di gunakan sebagai alat *add-on* pada Mozila Firefox agar mempermudah dalam pendeteksian serangan *phishing* pada *web*.

5) Self-efficacy

Untuk mencegah terjadinya phishing tidak hanya membutuhkan suatu aplikasi atau *software* anti-*phishing* melainkan juga membutuhkan *self-efficacy*. *Self-efficacy* adalah keyakinan individu dalam mengambil tindakan pengamanan[4]. Dengan memiliki sikap tersebut dapat menunjukkan kepercayaan individu dalam pemecahan masalah dan penyelesaian tugas sesuai kemampuan mereka sendiri[17]. Sangat penting bagi kita melatih sikap tersebut dari dini karena di era modern ini kita tidak bisa jauh dari teknologi dan mau tidak mau kita akan menjumpai bahkan terjerat dalam serangan *phishing*. Caranya adalah dengan mencari tau tentang *phishing* mulai dari definisi, cara kerja, contohnya, dll. Pada beberapa jurnal menunjukkan bahwa peserta yang secara khusus mengikuti studi *phishing* lebih berhati-hati dalam membedakan *web* asli dan palsu(*phishing*) dari pada peserta yang tidak mengikuti studi *phishing*[12]. *Phisher* biasanya menyerang perusahan karena untuk mengambil keuntungan (uang) dengan melalui karyawan-karyawannya. Ada dua temuan utama alasan *phisher* menyerang karyawan perusahaan: a) karyawan mudah tertipu dan rentan menjadi korban pada *SNS* yang mana unsur-unsur konseptual memberikan pemicu psikologis untuk penyerang; b) organisasi tidak memiliki *mekanisme* untuk mengontrol ancaman keamanan pada *SNS online*[16]. Untuk itu sangat perlu pembinaan terhadap karyawan-karyawan tentang *phishing* guna untuk melindungi informasi perusahaan.

V. KESIMPULAN

Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Sumber-sumber ancaman *phishing* yaitu *email*, *website*, dan *malware*. Berdasarkan hasil *survey* yang telah dilakukan *website* merupakan sumber ancaman *phishing* paling banyak dan cara pencegahan yang sering dilakukan adalah *self-efficacy* (keyakinan individu dalam mengambil suatu tindakan).

DAFTAR PUSTAKA

[1]Abdelhamid, N. (2015). Multi-label rules for phishing classification. *Applied Computing and Informatics*, *11*(1), 29–46. http://doi.org/10.1016/j.aci.2014.07.002

[2]Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Expert Systems with Applications Phishing detection based Associative Classification data mining. *Expert Systems With Applications*, *41*(13), 5948–5959. http://doi.org/10.1016/j.eswa.2014.03.019

[3]Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., & Razak, A. (2016). Author ' s Accepted Manuscript Malicious accounts : Dark of the social networks Reference : http://doi.org/10.1016/j.jnca.2016.11.030

[4]Asanka, N., Arachchilage, G., & Love, S. (2014). Computers in Human Behavior Security awareness of computer users : A phishing threat avoidance perspective. *COMPUTERS IN HUMAN BEHAVIOR*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

[5]Gavahane, M., Sequeira, D., Pandey, A., & Shetty, A. (2015). A nti-Phishing U sing H adoop- F ramework, 4–7.

[6]Gowtham, R., & Krishnamurthi, I. (2013). ScienceDirect A comprehensive and efficacious architecture for detecting phishing webpages. *Computers & Security*, *40*, 23–37. http://doi.org/10.1016/j.cose.2013.10.004

[7]Hamid, I. R. A., & Abawajy, J. H. (2014). An Approach for Profiling Phishing Activities. *Computers & Security*. http://doi.org/10.1016/j.cose.2014.04.002

[8]Junger, M., Montoya, L., & Overink, F. (2017). Computers in Human Behavior Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. http://doi.org/10.1016/j.chb.2016.09.012

[9]Lacey, D., Salmon, P., & Glancy, P. (2015). Taking the bait : a systems analysis of phishing attacks. *Procedia Manufacturing*, *3*(Ahfe), 1109–1116. http://doi.org/10.1016/j.promfg.2015.07.185

[10]Marchal, S., State, R., & Engel, T. (2014). PhishStorm : Detecting Phishing With Streaming Analytics, *11*(4), 458–471.

[11]Moghimi, M., & Varjani, A. Y. (2016). PT. *Expert Systems With Applications*. http://doi.org/10.1016/j.eswa.2016.01.028

[12]Parsons, K., Mccormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). ScienceDirect The design of phishing studies : Challenges for researchers. *Computers & Security*, 1–13. http://doi.org/10.1016/j.cose.2015.02.008

[13]Rao, R. S., & Ali, S. T. (2015). PhishShield : A Desktop Application to Detect Phishing Webpages through Heuristic Approach. *Procedia - Procedia Computer Science*, *54*, 147–156. http://doi.org/10.1016/j.procs.2015.06.017

[14]Sarika, S., & Paul, V. (2015). AgentTab : An Agent Based Approach to Detect Tabnabbing Attack. *Procedia - Procedia Computer Science*, *46*(Icict 2014), 574–581. http://doi.org/10.1016/j.procs.2015.02.094

[15]Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). AN IDEAL APPROACH FOR DETECTION AND PREVENTION OF PHISHING ATTACKS. *Procedia - Procedia Computer Science*, *49*, 82–91. http://doi.org/10.1016/j.procs.2015.04.230

[16]Silic, M., & Back, A. (2016). Computers in Human Behavior The dark side of social networking sites : Understanding phishing risks. *Computers in Human Behavior*, *60*, 35–43. http://doi.org/10.1016/j.chb.2016.02.050

[17]Sun, J. C., & Chen, A. Y. (2016). Computers & Education Effects of integrating dynamic concept maps with Interactive Response System on elementary school students ' motivation and learning outcome : The case of anti-phishing education. *Computers & Education*, *102*, 117–127. http://doi.org/10.1016/j.compedu.2016.08.002