Jurnal Komputer dan Teknik Informatika (KOMTI)
Vol. 1, No. 1, Desember 2024, hlm. 17-27 p-ISSN: 0-0
DOI: 10./… e-ISSN: 0-0

PERANCANGAN SISTEM DETEKSI SOCIAL ENGINEERING UNTUK KEAMANAN SIBER MENGGUNAKAN MACHINE LEARNING

Firmansah Muh Jakarya*[1], Muhamad Malik Mutoffar[2]

[1,2]Fakultas Industri Kreativ, Departemen Teknik Informatika, Universitas Teknologi.Bandung
Email: [1]firmansyahmuhamadzakaria@gmail.com, [2*]malik@utb-univ.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 1 Desember 2024, diterima untuk diterbitkan: 17 Desember 2024)

Abstrak

Serangan *social engineering* telah menjadi salah satu serangan rekayasa sosial paling banyak yang dihadapi oleh pengguna internet publik, pemerintah, bisnis, sekolah, dll. Menanggapi ancaman ini, jurnal ini mengusulkan untuk memberikan visi apa itu machine learning, apa yang penipu gunakan untuk mengelabui pengguna yang mudah tertipu dengan berbagai jenis teknik serangan social engineering atau bisa disebut phishing dan berdasarkan survei. email phishing adalah yang paling efektif untuk dijadikan target. Oleh karena itu, diperlukan teknologi pendeteksi social engineering atau phishing yang lebih efektif untuk mengurangi ancaman email phishing yang tumbuh pada tingkat yang mengkhawatirkan dalam beberapa tahun terakhir, sehingga akan membahas teknik mitigasi phishing oleh algoritma machine learning dan solusi teknik yang telah diusulkan untuk mengurangi masalah phishing dan berharap kesadaran pengetahuan pengguna harus sadar untuk mendeteksi dan mencegah agar tidak tertipu oleh penipuan phishing. Dalam pekerjaan ini, peneliti mengusulkan model deteksi menggunakan teknik machine learning dengan memisahkan kelompok data untuk melatih model deteksi dan memvalidasi hasil menggunakan data uji , untuk menangkap karakteristik yang melekat pada teks email, dan fitur lain yang akan diklasifikasikan sebagai phishing atau non-phishing menggunakan tiga dataset yang berbeda, Setelah membuat perbandingan di antar data, peneliti memperoleh bahwa jumlah fitur yang paling banyak digunakan hasil yang paling akurat dan efisien menggunakan algoritma machine learning decision tree dengan hasil akurasi 0.88, 1.00, dan 0.97.

Kata kunci: keamanan siber, *social engineering, machine learning, algoritma, klasifikasi,*

SOCIAL ENGINEERING DETECTION SYSTEM DESIGN FOR CYBER SECURITY USING MACHINE LEARNING

Abstract

Recently, social engineering attacks have become one of the most social engineering attacks faced by public internet users, governments, businesses, schools, etc. In response to this threat, this journal proposes to provide a vision of what machine learning is, what phishers use to trick gullible users with various types of social engineering attack techniques or can be called phishing and based on surveys. Phishing emails are the most effective to target. Therefore, a more effective social engineering or phishing detection technology is needed to reduce the threat of phishing emails which is growing at an alarming rate in recent years, so we will discuss phishing mitigation techniques by machine learning algorithms and engineering solutions that have been proposed to reduce phishing problems. and hope that the knowledge awareness of users must be aware to detect and prevent from being deceived by phishing scams. In this work, the researcher proposes a detection model using machine learning techniques by separating data groups to train the detection model and validate the results using test data, to capture the inherent characteristics of the email text, and other features to be classified as phishing or non-phishing using three different data sets. After making comparisons between the data, the researcher found that the number of features that were used the most were the most accurate and efficient using a machine learning decision tree algorithm with accuracy results of 0.88, 1.00, and 0.97

Keywords *cyber security, social engineering, machine learning, algorithm, classifier*

1. PENDAHULUAN

Kejahatan dunia maya mengacu pada kejahatan yang menargetkan komputer atau jaringan. Kejahatan komputer yang dilapisi dengan berbagai kegiatan kriminal yang berpotensi. Social Engineering adalah serangan yang paling umum digunakan pada rekayasa sosial. Melalui serangan tersebut, penipu mencoba untuk mendapatkan informasi rahasia dari pengguna, dengan tujuan menggunakannya secara curang terhadap pengguna. Dalam dunia digital saat ini, semakin banyak orang memanfaatkan peluang dunia maya yang terus berkembang. Dikarenakan perkembangan teknologi internet di keseharian kita terutama akibat dampak covid-19 yang memaksa semua pengguna untuk lebih banyak aktifitas dirumah menggunakan internet. Situs web phishing terlihat sangat mirip dengan situs resminya yang sesuai untuk menarik banyak pengguna Internet. Perkembangan terbaru dalam pendeteksian phishing telah menyebabkan pertumbuhan banyak pendekatan baru berdasarkan kesamaan visual.

Machine learning dan Artificial intelligence (AI) telah digunakan secara efisien dalam beberapa aplikasi kehidupan manusia, banyak peneliti sebelumnya menggunakan machine learning di bidang keamanan seperti di beberapa perusahaan besar. Serangan keamanan komputer diklasifikasikan menjadi tiga jenis: serangan fisik, serangan sintetik, dan serangan semantik. Social enineering adalah salah satu jenis serangan semantik. Dalam serangan seperti itu, kerentanan pengguna menjadi sasaran; misalnya, cara pengguna menafsirkan pesan komputer, karena sebagian besar pengguna membaca sumber informasi tanpa verifikasi dan menanggapi permintaan mereka. Social engineering adalah jenis serangan rekayasa sosial yang sering digunakan untuk mencuri data pengguna yang digunakan untuk mengakses rekening bank, akun sosial media dan dapat mengakibatkan pencurian identitas. Itu terjadi ketika penyerang, yang menyamar sebagai lembaga sah yang tepercaya, menipu korban melalui saluran komunikasi. Pengguna kemudian dibujuk untuk mengklik tautan berbahaya, yang dapat menyebabkan pemasangan malware, pembekuan sistem sebagai bagian dari serangan ransomeware yang dijalankan, dan pengungkapan informasi sensitif.

Penipu melakukan serangan mereka dengan menggunakan Email yang merupakan saluran paling umum untuk phishing dan reverse social engineering attack, mengirim pesan seperti "anda mendapatkan hadiah 100jt dari blablabla" pesan tersebut sangat popularitas di dalam Teknik social engineering untuk melakukan serangan social engineering dan reverse social engineering attack.

Menurut hasil laporan APWG serangan jumlah phishing yang diamati oleh APWG dan anggotanya tumbuh hingga tahun 2022, berlipat ganda sepanjang tahun. Phishing tersebar melalui e-mail, SMS, jejaring sosial dll, tetapi e-mail adalah cara yang populer untuk melakukan serangan ini. Email phishing dapat menyebabkan kerugian finansial. Penyerang yang selalu mengirim email cenderung membuat pengguna percaya bahwa mereka berkomunikasi dengan entitas tepercaya dan menipu mereka untuk memberikan kredensial pribadi untuk mengakses layanan, seperti nomor kartu kredit, kredensial login akun, atau informasi identitas. Pada 2022, 293,6 miliar email dikirim dan diterima setiap hari. Ini termasuk miliaran email promosi yang dikirim oleh pedagang setiap hari. Sementara banyak pengguna email percaya bahwa konten tersebut termasuk ke dalam folder spam, email pemasaran umumnya tidak berbahaya jika tidak nyaman bagi pengguna. Pesan spam menyumbang 47,3 persen dari lalu lintas email pada September 2021 yang menyebabkan kerugian ekonomi dan masalah sosial yang serius. Email spam Hampir tidak mungkin memikirkan email tanpa mempertimbangkan masalah spam. Varian spam berbahaya yang paling umum di dunia termasuk Trojan horse, spyware, dan ransomware. Ada banyak pendekatan yang telah dikembangkan untuk menangani masalah spam. Saat ini, tiga cara untuk mengurangi serangan tersebut menonjol: Fokus berdasarkan kesadaran, berdasarkan daftar hitam, dan berdasarkan machine learning.

Bagian 1 dari jurnal ini menerapkan machine learning pada tiga dataset berbeda di mana dua dataset pertama bergantung pada multi fitur dan yang ketiga tergantung hanya pada fitur teks. Bagian 2 meninjau Pekerjaan Terkait pengklasifikasi digunakan dalam mendeteksi email phishing. di bagian 3 disebutkan korban yang ditargetkan dalam phishing. Metodologi yang dimiliki telah diikuti

untuk melakukan penelitian ini telah diperkenalkan di bagian 4. Bagian 5 mengemukakan eksperimen untuk mengklasifikasikan Email Phishing Menggunakan machine learning, Bagian 6 hasil dan kesimpulan.

2. TINJAUAN PUSTAKA

Kemudahan berkomunikasi dengan munculnya email menyebabkan masalah email masal yang tidak diinginkan, terutama serangan phishing melalui email. Berbagai teknik anti-phishing telah dikembangkan untuk mengatasi masalah serangan phishing. Jurnal ini berfokus pada pemisahan email penting dari spam. Salah satu faktor utama untuk klasifikasi adalah bagaimana pesan akan direpresentasikan. Secara khusus perlu memutuskan fitur mana yang akan digunakan dan cara menggunakan fitur tersebut ketika mengkategorikan mereka. banyak peneliti telah menggunakan AI didalam sistem intelegen, dan banyak dari mereka menggunakan Machine learning dalam aplikasi keamanan siber.

Proses memfilter email yang disebut PILFER yang menggunakan10 fitur termasuk fitur berbasis URL dan Script untuk mendeteksi serangan phishing. Dengan memfilter email phishing sebelum dibaca oleh pengguna, dapat mengurangi persentase pengguna yang melakukan penipuan. Penipu dapat menyembunyikan URL dan menggunakan alat seperti TinyUrl untuk membuat URL seperti asli. Penipu menjadi semakin canggih dalam melakukan proses mereka dengan menggabungkan teknik penilaian untuk melewati alat anti-phishing yang ada.

Proses yang berasal dari filter spam disebut dengan Beaks. Untuk mengklasifikasikan email ke dalam spam dan bukan spam. Teknik pemrosesan yang dirancang untuk mengidentifikasi kata-kata tandai spam yang relevan dengan pengelompokan data. Menurut para pakar mengusulkan alat anti-phishing yang bergantung pada sembilan fitur yang berasal dari fitur berbasis struktur dan berbasis perilaku. alat pengirim nama domain, kata-kata yang masuk daftar hitam dan konten, alamat IP di URL, titik di URL, simbol di URL, pengirim unik, nama domain unik, hyperlink. Semua fitur yang direkomendasikan dipilih berdasarkan teknik phishing yang biasa digunakan oleh penipu.

Internet diferente telah memperkenalkan sistem tiga langkah yang di rancang untuk metode deteksi spam untuk mengklasifikasikan setiap email baru yang masuk sesuai dengan algoritma yang diberikan sebagai spam atau email asli dari sumber yang sah. menggunakan algoritma machine learning untuk mendeteksi serangan phishing dengan mengklasifikasikan email phishing dan email yang sah. mereka telah menggunakan enam belas fitur, dataset yang digunakan berisi 4000 instance dengan rasio 0,75 email yang sah dan 0,25 email phishing. Yang membagi dataset menjadi 0,50 pelatihan dan sisanya sebagai tes. akurasi yang di dapatkan adalah 97,99.

Moradpoor peneliti dari iran sebelumnya telah menggunakan dua dataset yang berisi 14.370 email asli dan phishing, prediksi dan klasifikasi model email phishing berdasarkan neural network, akurasi dan ketidak akuratan keseluruhan menjadi 92,2%.

Smadi peneliti sebelumnya. mengusulkan model untuk mendeteksi email phishing dengan mengekstraksi 23 fitur, dengan membandingkan algoritma yang berbeda menggunakan random forest dengan hasil akurasi tertinggi 98,8%.

Dalam jurnal ini menerapkan teknik machine learning, untuk dapat memahami ciri yang melekat pada teks email dan fitur lainnya untuk diklasifikasikan sebagai phishing atau non-phishing sesuai dengan pengelompokan data yang dipilih.

Korban yang ditargetkan

Pada bagian di bawah ini dirangkum dari hasil beberapa karakteristik yang teridentifikasi dari calon korban phishing berdasarkan penelitian sebelumnya:

1. Usia Korban: melakukan role-play demografi dan kerentanan phishing. Peneliti sebelumnya menemukan bahwa usia peserta secara linier memprediksi kerentanan mereka terhadap phishing. Pengguna yang lebih tua cenderung tidak menjadi mangsa phishing, sementara pengguna yang lebih muda khususnya antara usia 18–25 secara konsisten lebih rentan terhadap serangan phishing.
2. Jenis Kelamin Korban: Sebagian besar penelitian menunjukkan bahwa wanita lebih mungkin untuk terkena serangan phishing daripada pria.
3. Pendidikan Umum Korban: sebuah studi yang dilaporkan oleh Kumaraguru et al,

menunjukkan bahwa pengguna dengan latar belakang ilmu komputer berkinerja sedikit lebih baik daripada pengguna dengan latar belakang lain ketika diserang oleh phishing.

4. Kepribadian Korban: dalam tabel dibawah merangkum semua penyebab terkait dengan kerentanan terhadap serangan phishing.

penyebab	Kerentanan tinggi	Kerentanan rendah
Usia	18-24 tahun	25 atau lebih
Jenis kelamin	perempuan	pria
Pengetahuan tentang phising	Tidak mengetahui	mengetahui
Jurusan pendidikan	Lain lain	Teknik komputer
Penyampaian tentang phising	Tidak ada	ada
kepribadian	kesesuaian	kesadaran
penggunaan internet	e-commerce, bank dll	Email dan apk sederhana lainnya

Kaum muda lebih bertanggung jawab atas penggunaan perangkat mereka, tetapi mereka harus tahu cara melindungi keamanan perangkat mereka. Sebuah studi dengan 83 remaja menemukan bahwa remaja kurang dalam membedakan antara pesan yang sah dan phishing dalam tugas eksperimental. peserta menunjukkan perilaku berisiko saat membuat keputusan tentang pesan yang tidak dikenal. Dalam studi Cross-sectional dari 350 anak usia 4 tahun, hasilnya menunjukkan sebagian besar rumah tangga memiliki televisi (0,97), tablet (0,83), dan smartphone (0,77). Pada usia 4 tahun, setengah dari anak-anak memiliki televisi sendiri dan perangkat seluler mereka sendiri. Hampir semua anak (96,6) menggunakan perangkat seluler, dan sebagian besar mulai menggunakan sebelum usia 17. Orang tua memberi anak perangkat saat mengerjakan pekerjaan rumah (0,70), untuk menenangkan mereka (0,65), dan sebelum tidur (0,29). Pada usia 6-7 tahun, sebagian besar anak-anak menggunakan perangkat setiap hari. Sebagian besar perangkat yang digunakan anak berusia 6 dan 7 tahun tanpa pemantauan, dan sepertiganya terlibat dalam multitasking media. Selain itu, anak-anak berusia 8–15 tahun online minimal 8 jam setiap minggu. Contoh aktivitas online yang umum dilakukan anak usia ini antara lain berkomunikasi melalui media sosial, menonton video YouTube, dan bermain game. Salah satu risiko digital utama yang perlu diwaspadai anak-anak adalah phishing, serangan rekayasa sosial umum yang digolongkan sebagai salah satu risiko online paling berbahaya bagi anak-anak.

Dengan prevalensi dan potensi konsekuensi phishing, upaya terus menerus dilakukan untuk meningkatkan pengetahuan keamanan siber pada masyarakat dan untuk mengembangkan perlindungan terhadap serangan phishing. Para peneliti telah mengeksplorasi solusi teknis, kesadaran melalui permainan edukasi keamanan siber dan materi pelatihan, penambahan isyarat di antarmuka pengguna untuk membantu deteksi phishing. Sebagai pengguna situs media sosial yang energik, remaja dapat secara teratur berbagi sejumlah data saat berinteraksi dan berkomunikasi satu sama lain. Berbagi informasi pribadi mungkin berisiko meningkatkan Jumlah serangan phishing selama bertahun-tahun. Sebuah survei baru-baru ini pada hampir 15.000 pengguna akhir dari tujuh negara menunjukkan bahwa 0,83 responden memiliki mengalami serangan phishing pada tahun 2021 dibandingkan dengan 0,76 pada tahun 2020. Phishing sangat berdampak pada bisnis; perusahaan menengah membayar rata-rata 1,6 juta dolar untuk pulih dari serangan phishing yang sukses di mana konsekuensinya termasuk infeksi malware, akun yang disusupi, dan kehilangan data

Cain et al. peneliti sebelumnya membuat pada orang berusia 18 hingga 55 tahun dan mengamati bahwa orang yang lebih muda memiliki keamanan siber yang buruk kebiasaan yang terkait dengan pengelolaan kata sandi dan phishing.

3. ANALISIS DAN PERANCANGAN

Metodologi penelitian berdasarkan Pengumpulan Kumpulan Data, Prapemrosesan Kumpulan Data, Menggunakan teknik klasifikasi machine learning. Model direkomendasikan untuk mengklasifikasikan email karena setiap model telah dibangun dengan fungsi yang berbeda berdasarkan tiga dataset dengan perbedaan fitur yang berbeda. Dengan probabilitas tinggi dan menyaring email sah sesedikit mungkin. Hasil yang dihasilkan lebih unggul daripada metode deteksi yang ada dan memverifikasi efektivitas model dalam mendeteksi email phishing.

Sebagai Langkah terpenting pertama adalah memiliki kumpulan data yang diperlukan, dalam jurnal ini telah menggunakan tiga kumpulan data yang telah diambil dari sumber daya yang opensource. Alasan menggunakan tiga set data dengan fitur yang berbeda adalah tingginya tingkat perubahan

teknik serangan phishing yang meningkatkan kesulitan dalam mendeteksi dan memfilter serangan email phishing. Agar dapat mengklasifikasikan email phishing dan mengidentifikasi bagaimana jumlah fitur akan mempengaruhi secara efisien. Seperti dalam gambar 1 dibawah yang mengilustrasikan struktur model deteksi yang direkomendasikan oleh para peneliti sebelumnya.

4. KESIMPULAN

Email phishing telah menjadi masalah umum dalam beberapa tahun terakhir. Serangan email phishing adalah serangan email rekayasa sosial yang dibuat dengan cerdas di mana korban ditipu melalui email untuk memberikan informasi penting dan kemudian langsung mengirimkannya ke penipu.

Pengguna muda lebih cenderung terkena serangan phishing terutama wanita lebih cenderung memberikan detail pribadi dan keuangan mereka ke email dan situs web phishing.

Ada banyak teknik untuk mendeteksi email phishing. Namun, ada beberapa keterbatasan seperti akurasi yang rendah. Media yang digunakan mungkin sama dengan email yang sah sehingga tidak dapat dideteksi, tingkat deteksinya tidak tinggi.

DAFTAR PUSTAKA

[1] Aldabbas, H., Amin, R.: Mekanisme baru untuk menangani serangan spoofing alamat di iot berbasis sdn. kelompok. Hitung. 24(4), 3011–3026 (2021)

[2] Kim, D., Kim, Y.-H., Shin, D., Shin, D.: Sistem deteksi serangan cepat menggunakan analisis log dan pembuatan pohon serangan. Kelompok. 22(1), 1827-1835(2019)

[3] Aldabbas, H., Amin, R.: Mekanisme baru untuk menangani serangan spoofing alamat di iot berbasis sdn. kelompok. Hitung. 24(4), 3011–3026 (2021)

[4] Abuusukhon, A., AlZu'bi, S.: New direction of cryptography: review tentang algoritma enkripsi text-to-image berdasarkan nilai warna rgb. Dalam: Prosiding Konferensi Internasional Ketujuh 2020 tentang Sistem yang Ditetapkan Perangkat Lunak (SDS), hlm. 235–239. IEEE (2020)

[5] Obeidat, I., Mughaid, A., Alzoubi, S.: Sebuah protokol terenkripsi yang aman untuk handshaking klien di jaringan yang sama. Int. J. Inter bertindak. Massa. teknologi. 13, 47–57 (2019)

[6] Salahdine, F., Kaabouch, N.: Serangan rekayasa sosial: survei. 11(4), 89(2019)

[7] Khonji, M., Irak, Y., Jones, A.: Deteksi phishing: survei literatur. Komunitas IEEE. bertahan Guru. 15(4), 2091–2121 (2013)

[8] Whittaker, C., Ryner, B., Nazif, M.: Klasifikasi otomatis skala besar halaman phishing. Dalam: Prosiding Simposium Keamanan Jaringan dan Sistem Terdistribusi (2010)

[9] Hong, J.: Keadaan serangan phishing. komuni. ACM 55(1), 74–81 (2012)

[10] Maqableh, M., Alia, M.: Evaluasi pembelajaran online mahasiswa S1 yang dikarantina di tengah pandemi covid-19: pengalaman belajar online dan kepuasan mahasiswa. Layanan Pemuda Anak. Wahyu 128, 106160 (2021)

[11] Zhao, W., Zhu, Y.: Skema klasifikasi email berdasarkan teori kumpulan kasar teori keputusan dan analisis keamanan email. 1-6. IEEE (2005)

[12] Vinayakumar, R., Soman, K., Poornachandran, P., Akarsh, S., Elhoseny, M.: Kerangka pembelajaran mendalam untuk kesadaran situasional ancaman dunia maya berdasarkan analisis data email dan url. Dalam: Has sanien, AE, Elhoseny, M. (eds.) Keamanan Siber dan Sistem Informasi Aman, hlm. 87– 124. Springer, New York (2019)

[13] AlZu'bi, S., Al-Qatawneh, S., Alsmirat, M.: Transferable hmm matriks terlatih untuk mempercepat waktu segmentasi statistik. Dalam: Prosiding Konferensi Internasional Kelima 2018 tentang Analisis, Manajemen, dan Keamanan Jaringan Sosial (SNAMS), hlm. 172–176. IEEE (2018)

[14] Al-Zubi, S., Hawashin, B., Mughaid, A., Baker, T.: Algoritma segmentasi citra medis 3d yang efisien melalui jaringan multime dia yang aman. Multimed. Alat Aplikasi 80(11), 16887–16905 (2021)

[15] AlKhatib, AA, Sawalha, T., AlZu'bi, S.: Teknik penyeimbangan beban dalam komputasi awan yang ditentukan perangkat lunak: gambaran umum. Dalam: Prosiding Konferensi Internasional Ketujuh 2020

tentang Sistem yang Ditetapkan Perangkat Lunak (SDS), hlm. 240–244. IEEE (2020)

[16] Fette, I., Sadeh, N., Tomasic, A.: Belajar mendeteksi email phishing. Dalam: Prosiding konferensi internasional ke-16 di World Wide Web, hlm. 649–656 (2007)

[17] Elbes, M., Alrawashdeh, T., Almaita, E., AlZu'bi, S., Jararweh, Y.: Platform untuk manajemen daya berdasarkan lokalisasi dalam ruangan di gedung pintar menggunakan jaringan saraf jangka pendek jangka pendek ". Trans. muncul. Telekomunikasi. teknologi. 33, e3867 (2020)

[18] AlZu'bi, S., Shehab, MA, Al-Ayyoub, M., Benkhelifa, E., Jararweh, Y.: Implementasi paralel dari segmentasi volume gambar 3d berbasis fcm. Dalam: Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Appli cations (AICCSA), 2016, hlm. 1–6. IEEE (2016)

[19] Teli, SP, Biradar, SK: Klasifikasi email efektif untuk spam dan non-spam. Int. J. Adv. Res. Hitung. lunak Ind. 4, 2014 (2014)

[20] Basnet, R., Mukkamala, S., Sung, AH: Deteksi serangan phishing: pendekatan pembelajaran mesin. Dalam: Proceedings of the Soft Computing Applications in Industry, hlm. 373–383. musim semi (2008)

[21] Moradpoor, N., Clavie, B., Buchanan, B.: Mempekerjakan teknik pembelajaran mesin untuk deteksi dan klasifikasi email phishing. Hitung. Kon. 2017, 149-156 (2017)

[22] Jagatic, TN, Johnson, NA, Jakobsson, M., Menczer, F.: Phishing sosial. komuni. ACM 50(10), 94–100 (2007)

[23] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, LF, Hong, J.: Mengajarkan johnny untuk tidak jatuh cinta pada phish. ACM Trans. Teknologi Internet. 10(2), 1-31 (2010)

[24] Parrish, JL, Jr., Bailey, JL, Courtney, JF: Model Berbasis Kepribadian untuk Menentukan Kerentanan terhadap Serangan Phishing, hlm. Universitas Arkansas, Little Rock (2009)

[25] Kabali, HK, Irigoyen, MM, Nunez-Davis, R., Budacki, JG, Mohanty, SH, Leister, KP, Bonner, RL: Paparan dan penggunaan perangkat media seluler oleh anak kecil. Pediatri 136(6), 1044–1050 (2015)