Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat
e-ISSN : 2722-3957
Vol. 1 No. 1 (Juli 2020)

Fakultas Teknik
Universitas Bhayangkara Jakarta Raya
Available online at
http://ejurnal.ubharajaya.ac.id/index.php/JSTPM

Editorial Team

Articles

Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat
e-ISSN : 2722-3957
Vol. 1 No. 1 (Juli 2020), Hal : 1-10

Sosialisasi Keamanan Siber untuk Anak-anak di Panti Asuhan Aisiyah Bekasi

Kusdarnowo Hantoro[1*], Asep Ramdhani[2], Khaerudin[3], Rasim[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan, Marga Mulya, Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Telp : (021) 88955882, 889955883, kusdarnowo@dsn.ubharajaya.ac.id, asep.ramdhani@dsn.ubharajaya.ac.id, khaerudin@dsn.ubharajaya.ac.id, rasim@dsn.ubharajaya.ac.id

***Korespondensi : kusdarnowo@dsn.ubharajaya.ac.id**

Diterima: 29 April 2020 ; Review: 15 Mei 2020 ; Disetujui: 1 Juli 2020 ; Diterbitkan: 27 Juli 2020

Abstract

Now, children and teenagers often posted on social media such as Facebook, Twitter, Instagram often become victims of cybercrimes like phishing, bullying, social engineering by predators by utilizing social media, email and other cyber facilities. With a variety of cases and modes of cybercrime, it is necessary to set up cybersecurity awareness for young people. This activity provides tips and tricks as well as information on how to surf in a cyber world that is safe in dealing with cybercrime.

***Keywords** : Social media, email, predator, cybercrime*

Abstrak

Anak-anak dan remaja sekarang banyak yang memposting di sosmed seperti Facebook, Twitter, Instagram seringkali menjadi korban kejahatan siber seperti phishing, bullying, social engineering oleh para predator dengan memanfaatkan sosial media, email dan fasilitas siber lainnya. Dengan berbagai macam kasus dan modus kejahatan siber seperti tersebut, maka perlu dibangun kesadaran di kalangan muda untuk memiliki bekal pengetahuan keamanan siber. Kegiatan ini memberikan tip dan tricks serta informasi bagaimana cara berselancar di dunia siber yang aman dalam menghadapi kejahatan siber.

Kata kunci : Media sosial, email, predator, kejahatan siber

1. PENDAHULUAN

April 2018, APJII (Asosiasi Penyedia Layanan Internet Indonesia) menginformasikan jumlah pengguna internet di Indonesia adalah 171,17 juta pengguna dari 264,16 juta populasi, dengan pengguna aktif social media sebanyak 130 juta. Terdapat 4.02 milyar pengguna internet dari total 7,6 milyar penduduk seluruh dunia. Jumlah akses terhadap konten web hanya 4% atau sekitar 8 miliar halaman melalui browser seperti Google, Internet Explorer atau Firefox, sebagian digunakan untuk belanja online seperti Amazon

Diterima: **29/04/2020**; Review: **15/05/2020**; Disetujui: **01/07/2020**; Diterbitkan: **27/07/2020**

(Wang & Yu, 2017). Semakin banyaknya konten-konten negatif *Dark Web* (dunia hitam) dan *Deep Web* (dunia rahasia) lebih dari 96% atau 7.9 zetabytes yang diakses melalui TOR (*The Onion Router*) *hidden service*, seperti pasar gelap, untuk jual beli barang ilegal diantaranya senjata, virus, *malware, ransomware, hitman*, pornografi dan narkoba. Hanya 4% yang kasat mata dapat diakses dengan mesin pencari Google, Yahoo, Bing, dll. (Can & Kaya, 2016). Sedangkan sisanya merupakan daerah gelap para *cracker* (peretas), mafia, pengedar narkoba, pornografi, dunia spionase, jual beli senjata dan terorisme, hal ini diperlihatkan pada Gambar 1.

Peraturan Perlindungan Data Pribadi (PDP) RI hingga saat ini masih dalam pembahasan, seperti PP 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Institusi atau Perusahaan yang mengelola basis data pribadi konsumen atau pengguna yang biasa disebut *Data Controller* disingkat menjadi DCO. DCO bertanggungjawab terhadap perlondungan Data Pribadi Konsumen sebagai pemilik data. Setiap perlakuan terhadap data dari seorang pengguna harus diberikan secara bebas atau berdasarkan keinginan atau tanpa tekanan, dengan kata lain harus dengan persetujuan dari pegguna.

Sumber: Badan Siber Nasional (2020)

Gambar 1. Serangan Siber 2015 dan 2016

2. METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat dilakukan dengan cara sosialisasi dan simulasi contoh-contoh kejahatan siber beserta contoh pencegahannya seperti :

a. Penerapan *password*
b. Legalitas perangkat lunak
c. Penggunaan perangkat lunak keamanan
d. Pendampingan saat penggunaan internet
e. Penanganan setelah bencana

Beberapa serangan siber yang perlu dipahami diantaranya :

2.1 Virus/*Malware.Worm* Komputer

Virus komputer - program kecil yang mengubah cara komputer beroperasi dan sering melakukan berbagai jenis kerusakan dengan menghapus dan merusak data dan *file* program, atau dengan mengubah komponen sistem operasi, sehingga operasi komputer terganggu atau bahkan dihentikan. (Ren et al., 2015)

2.2 Denial Of Service Attack

Membombardir situs komputer dengan begitu banyak pesan sehingga situs tidak mampu menjawab permintaan yang valid.

2.3 DNS Attack

Serangan DNS adalah eksploitasi kekurangan dengan memanfaatkan kerentanan dalam sistem nama domain (DNS). DNS adalah protokol yang menerjemahkan nama domain yang *user friendly*, seperti *ubharajaya.ac.id*, ke dalam alamat IP yang computer friendly 201.29.49.154.

2.4 *Data Breach*

Data breach adalah kejadian dimana data sensitif, terproteksi, atau rahasia disalin, dipindahkan, dilihat, dicuri, atau digunakan oleh orang yang tidak seharusnya memiliki akses pada data tersebut.

3. HASIL DAN PEMBAHASAN

Kegiatan PKM telah dilaksanakan pada Agustus 2019 selama 1 hari di Panti Asuhan Aisyiah Bekasi, Jawa Barat oleh Tim dosen Jurusan Teknik Informatika, Universitas Bhayangkara Jaya dengan judul ”Sosialisasi Keamanan Siber untuk Anak-anak di Panti Asuhan Aisyiah Bekasi”. Panti Asuhan Aisyiah beralamat di jalan Ki Mangun Sarkoro No 45 Bekasi, berdiri sejak tahun 2015 yang menampung 45 orang berasal dari berbagai tempat di Indonesia. Sejumlah siswa saat ini sudah ada yang lanjut ke perguruan tinggi dan ada juga yang sudah bekerja dan memberikan kontribusi kepada panti.

Diterima: **29/04/2020**; Review: **15/05/2020**; Disetujui: **01/07/2020**; Diterbitkan: **27/07/2020**

Sumber : Hasil Pelaksanaan (2020)

Gambar 2. Bersama putra-putri panti asuhan dan pengurus yayasan

Peninjauan ke lokasi panti asuhan dilaksanakan pada tanggal 7 Agustus 2019. Tim dosen Jurusan Informatika Universitas Bhayangkara disambut dengan baik oleh ketua pengelola panti asuhan yaitu Ibu Risnawati Beliau memberikan penjelasan singkat tentang panti asuhan Aisyiah mulai dari awal didirikan hingga kini serta tujuan dari didirkannya panti asuhan. Gambar 2 merupakan dokumentasi dari pelaksanaan kegiatan PKM ini.

3.1 Memberikan Arahan Pengamanan Data Pribadi di Media Sosial

Seorang pengguna sosial media (sosmed), *website* atau konsumen *ecommerce* (*Data Subject*) memiliki hak privasinya terhadap *Data Controller*:

a. Untuk Data Pribadi (*Personal*) dihapus (*delete*) atau diremajakan (*up to date*);
b. Untuk Data Pribadi (*privacy*) dilindungi kerahasiaannya seperti informasi yang dapat mengidentifikasi (*identifier*): Nama, nomor ID, lokasi data, atau identifikasi dari faktor seperti fisik, genetik, mental, agama, sosial, budaya dan ekonomi seseorang;
c. Untuk perekaman, pengambaran dan analisa atas profile suatu objek harus seijin Data Subjek tersebut termasuk segala bentuk personalisasi, prediksi mengenai kinerja, pekerjaan, ekonomi, keuangan, kesehatan, referensi personal, *interest*, hobi, kelakuan, lokasi dan pergerakannya.

Kewajiban *Data Controller* (DCO) terhadap konsumen (*Data Subject*) :

a. DCO wajib menjaga Keamanan terhadap Pembocoran Data Pribadi (Data Breach). Jika terjadi musibah pembocoran data;
b. Segera melaporkan dalam waktu 72 jam setelah mengetahui (*discovery*);
c. DCO memproses data konsumen dengan cara Sah, tidak melanggar hukum, *fair* (adil) dan transparan terhadap konsumen untuk tujuan spesifik, jelas/eksplisit, valid & sah, sesuai dengan tujuan yang sudah disepakati oleh konsumen;

d. DCO menjamin ketepatan, akurasi data konsumen, tidak kadaluwarsa, *up-to-date* terus diperbarui, sesuai tujuan penyimpanan data yang disetujui oleh konsumen;
e. DCO menjamin lokasi & format penyimpanan atau database disetujui konsumen dan UU yang berlaku;
f. DCO menjaga integritas (tidak rusak dan hilang) data dan kerahasian (*confidentiality*) data subjek dengan enkripsi, *password* dll.

3.2 Memberikan Pemahaman Akses Komputer

a. Jangan gunakan *password* dengan suku kata umum. Gunakan campuran huruf, angka, tkita baca dan simbol typografi seperti **"@!AB2-4#%"** agar sulit ditebak dan dirangkai oleh botnet;
b. Selalu ganti (*refresh*) *password* pada perangkat/gawai komputer, *smartphone, wifi router* secara berkala/periodik (30, 60 atau 90 hari);
c. Jangan gunakan *password* yang sama di semua platformdan perangkat;
d. Jangan gunakan *Default Password*. Segera ganti *password* yang diberikan pabrik (*Factory set default password*). Pahami kelemahan *user generated password* otomatis oleh algoritma mesin;
e. Prioritas *password* administrator atau akun *remote user*, karena menjadi target *cracker*;
f. Jangan menyimpan *password* sembarangan ditempat yang diakses umum atau orang lain.
g. Gunakan Pengunci Akun (*Account Lockout*) artinya akan *exit* ketika *cracker* mencoba berulang ulang dengan berbagai kombinasi *password* dikenal dengan upaya *Brute Force Attacks*.

3.3 Tips Menghindari Virus, *Malware, Spam, Ransomeware* dan *Spy Ware*

a. Rutin *Update* Sistem
   Malware/virus selalu mencari kelemahan (*vulnerability)* di setiap sistem agar bisa dibobol. Sistem operasi, *software* anti virus komputer dan *smartphone* harus diperbarui (*update*) sesuai rekomendasi pabrik, sehingga sistem keamanan sudah menggunakan sistem yang terbaru dan sudah diuji coba terhadap *malware* versi sebelumnya.
b. *Back-Up* data
   Backup dokumen, foto atau berkas penting lainnya ke *flashdisk, harddisk* cadangan (*offline*) atau ke layanan *google dropbox (online).* Agar memiliki data cadangan. Jika data kita hilang karena virus atau di sandera oleh *ransomware* yang meminta uang tebusan, maka dapat dipulihkan (*recovery*) dengan data *backup*.
c. Gunakan Anti Virus (AV)
   Anti Spam atau *Anti Spyware/Worm* untuk PC, Gawai dan *Smartphone*, agar selalu mempunyai penangkal virus/spam terbaru. *Scan* secara menyeluruh dan berkala untuk mencegah program *malware, virus, spam, worm* yang ingin masuk ke dalam komputer/*smartphone*.
d. Jangan klik *Link web* & *Download File* yang tidak dikenal
   Karena dapat membangunkan *malaware, virus, ransomware* yang ada di file yang diunduh atau *attachment* yang diklik, konsekuensinya data dalam gawai kita sudah terkontaminasi, termasuk daftar alamat (*address book*) digunakan oleh peretas untuk fase duplikasi *malware* dan penyebaran berikutnya.
e. Berhati-hati Gunakan WiFi Publik

Diterima: **29/04/2020**; Review: **15/05/2020**; Disetujui: **01/07/2020**; Diterbitkan: **27/07/2020**

Terutama jika kita ingin melalukan transaksi keuangan, perbankan, *ecommerce, credit cards* serta aplikasi yang kritis dan strategis. (Pall, 2018)

f. Tidak Gunakan Perangkat Pribadi
   Tidak gunakan perangkat pribadi di tempat bekerja, untuk memproses pekerjaan perusahaan.

3.4 Cara Melindungi Diri dari Predator Online

Predator kerap mengincar anak-anak dengan menyamar di *chatroom* jejaring sosmed, email, *messenger* sebagai seseorang yang ramah, baik, sebaya dan berusaha menjadi teman dengan meraih kepercayaan dari calon korbannya. Predator menyamar sosok yang tampan dan idola dan korban yang termakan bujuk rayu, menjadi budak seks, terlibat aksi teroris, pemalakan atau memuaskan hasrat seksual predator. Mulai dari minta foto pose tak senonoh via *webcam* hingga diajak kopi darat untuk melakukan hubungan intim. Cara menghindari diri dari predator *online* :

a. Hati-hati dengan informasi profil, personal (usia/gender) dan keluarga di akun sosmed, *messenger*.
b. Jangan mengunduh gambar dari sumber yang tidak dikenal dan berpotensi mengandung materi berbau seksual atau kekerasan/teroris dan konten berbahaya.
c. Orang tua bisa menggunakan layanan penyaring/sensor email. Hentikan kontak email dan pesan instan jika sudah menjurus pada pertanyaan personal atau berkonotasi seksual, *bullying* atau teror. Tempel aturan *online* yang disepakati keluarga di dekat komputer sehingga anak bisa melihat dan membacanya setiap saat mereka *online*.

3.5 Mencermati Bahayanya *Social Engineering* dan Cara Menghindari Penipuan *Phising*

Korban yang tidak teliti membaca domain akan tertipu masuk situs *phishing* milik *cracker*. Selanjutnya *cracker* ini akan melakukan data *mining password*, *login* yang diketik oleh si korban, karena si korban sekarang bukan masuk ke situs resmi target tapi masuk ke situs si *cracker*. Akhirnya si Cracker memiliki *login* dan *password* si korban dan dengan cepat menguras saldo si korban dengan cara *phishing*. (Qi, Monod, Fang, & Deng, 2018)

3.6 Tips Melawan *Hoaks* (Can & Kaya, 2016)

a. Sumber berita media atau domain situs tidak jelas atau bodong, meragukan dan tidak familiar.
b. Tanyakan pada penyebar informasi untuk konfirmasi asal informasi yang dikirim.
c. Informasi waktu, tempat,lokasi yang tidak jelas, bahkan mencatut nama tokoh palsu.
d. Berisikan opini seseorang bukan fakta atau sejarah.
e. Sering terdengar mustahil ditunjang oleh penelitian palsu.
f. Cek dan *recheck* dengan media masa *mainstream* (populer).
g. Desain halaman yang aneh. Menggunakan huruf besar dan tkita seru. Menggunakan kata heboh & profokatif karena *hoax* disebarkan untuk timbulkan kehebohan & kekacauan publik.
h. Baca ulang informasi secara utuh dan lihat lebih detail dan teliti isi dan maksudnya.

3.7 Menghindari *Hacking, Cracking* dan Serangan Internal dan Penyadapan

Hacking adalah tindakan peretas dan penetrasi sistem yang lemah (*vulnerable*) oleh *hacker*. Ada golongan *White (hat) Hacker*, yang memiliki etika tidak merusak sistem korban ketika melakukan serangan penetrasi (*Penetration Test/Pentest*), namun memberi tips agar korban memperbaiki kelemahan sistem.

Blackhat hacker atau c*racker* sangat berbahaya menyerang (*attack*), merusak (*replay attack*), menghancurkan, mencuri uang (*system ebanking*), mencuri data (*data breach/theft*), merubah (*deface*) *web portal* korban, menyadap (*MiiT – Man In the middle) attack*, penyadapan (*intercept*) dijalur Internet atau komunikasi. Membuat *backdoor*, menguasai *webcam*, kamera PC, *microphone*, layar PC kita. *Cracker* menggunakan *malware, ransomware* mengacak dan enkripsi data, *harddisk* korban sehingga tidak dapat di baca kecuali membayar *ransom* dengan *bitcoin di Deep Web*. (Halunen & Latvala, 2018)

Penjagaan berlapis serangan *cracker* dari Internet dan dalam sistem yaitu memasang proteksi perimeter di peripheri (pagar) seperti *Firewall, Router* untuk sistem LAN internal perusahaan. *Proxy* di periphery untuk memisahkan *IP Internet Siber* yang beresiko (*compromised*) dengan *IP Private* untuk semua PC dan *gadget* dilingkungan LAN Perusahaan. *Proxy* untuk memisahkan IP dunia *cyber* yang berbahaya (*compromised*) dengan *IP Private* untuk semua PC dan *gadget* dilingkungan LAN Perusahaan (Tayal, Gupta, Gupta, Goyal, & Goyal, 2017). Anti virus, *Anti Spam, Anti Malware*, Sensor konten di *server* dan di setiap PC serta peralatan *Anti Insider Threat* yang merupakan pertahanan berlapis (*defence in depth*) bagi sebuah korporasi dan *enterprise*.

3.8 Cara Lapor Korban Kejahatan Siber

Contoh kasus cara melaporkan kejahatan siber kepada aparat penegak hukum digunakan kasus ujaran kebencian (*hate speech*) menyerang ke lembaga negara, atau SARA (suku, agama, ras, dan antar golongan). Jika pencemaran nama baik menyerang individu, polisi bisa menindak pelaku *hate speech* dengan delik murni yaitu dengan :

a. Siapkan bukti yang cukup seperti tangkapan layar (screenshot), url, foto, atau video dari ujaran kebencian yang akan dilaporkan. Bisa dikumpulkan dalam media penyimpanan seperti *flashdisk, harddisk*, CD/DVD, dan lainnya. Satu bukti yang kuat sudah cukup.
b. Datang ke kantor polisi, dianjurkan setidaknya tingkat Polres untuk tindak pidana siber.
c. Menuju ke ruang SPKT kantor polisi untuk menyampaikan laporan & bukti-buktinya ke petugas.
d. Petugas akan mengajukan beberapa pertanyaan yang berhubungan dengan laporan ujaran kebencian, mengetik dan mencetak bukti pelaporan.
e. Menunggu pemberitahuan selanjutnya dari polisi.

3.9 Melindungi Anak dari *Cyber Bullying*

Kasus *Cyber bullying* (perundungan) dapat berbentuk sebuah komentar pedas, miring,cemooh, ejekan, intimidasi, atau segala hal yang bertujuan untuk mempermalukan atau melecehkan. Namun dampaknya sungguh negatif bagi perkembangan sang buah hati, seperti cemas, takut, merasa dipermalukan, dan lain sebagainya akan sangat

Diterima: **29/04/2020**; Review: **15/05/2020**; Disetujui: **01/07/2020**; Diterbitkan: **27/07/2020**

menghantui anak. Orang tua turut berperan aktif dan proaktif, komunikatif untuk memperhatikan perilaku anak, terutama, jika anak terlihat seperti depresi, aneh dan mengalami perubahan perilaku seperti langsung terbuka, menutupinya, atau hanya diam saja ketika ditanya orang tua. Ajari si anak untuk tidak memberikan informasi pribadi yang dapat menyebabkan pelecehan atau dipermalukan, seperti foto bayi, deskripsi fisik, dll.

3.10 Tips agar Anak Aman Bermain Intenet

Internet bagaikan pedang bermata dua, dapat memberikan manfaat, informasi publik dan global yang positif terhadap perkembangan anak dan memberikan banyak informasi publik. Namun Internet juga memiliki *dark web*, dunia hitam berisi konten yang merugikan dan membahayakan, yang membutuhkan bimbingan pengawasan orang tua, dengan :

a. Komunikasi dan edukasi
   Orang tua harus terbuka dan memberikan edukasi sebelum anak-anak mulai akses Intenet. Merekomendasikan situs-situs yang baik dengan muatan edukatif kepada anak-anak. Ingatkan anak-anak untuk tidak memberikan informasi data pribadi, identifikasi personal seperti nama lengkap, alamat rumah, usia, gender, nama ibu, ayah, akun sandi atau akun bank. Jaga informasi profil di akun sosmed dan Siber, karena sifatnya abadi sulit dihapus dan menjadi referensi untuk karir si anak. Pastikan bahwa profil sosmed terlindungi *password* dan gunakan *privacy mode* yang sesuai.
b. Parental Control
   Orang tua menganjurkan anak menggunakan alat pengontrol konten kekerasan, pornografi di internet dan sensor umur di gawai, *game* dan *browser*. Monitor teman dan yang di tonton dan lakukan anaknya di gawainya. Biasakan akses TV, games atau gawai di ruang publik, kamar tamu bersama orang tua.
c. Batasi Waktu dan Tempat
   Berikan batas waktu bermain Internet baik di gawai nya, untuk mencegah kecanduan ketika bermain game online, *chat group* (ie: *Whatsapp group*), internet. Tidak bermain Internet saat makan, tidur, dikamar mandi, dikelas, rapat dan berjalan di tempat umum.
d. Sanksi bagi Anak
   Saat anak melanggar peraturan, orang tua dapat memberikan hukuman seperti tidak boleh memegang gawai selama 24 jam.
e. Berteman di media sosial
   Agar anak-anak berinteraksi dengan teman sebaya/seumur, keluarga, orang tua dan hindari akun serta orang yang tidak dikenal untuk menghindari pemangsa/predator anak dan mencegah intaian orang jahat dan teror. Hormati privasinya. (Vasilakos, Li, Simon, & You, 2015)
f. Jadi Teladan yang baik
   Orang tua jangan bermain gawai ketika mengemudi mobil atau motor, atau sambil makan atau tidur. Biasakan melihat hal positif dari dunia siber. (Craig, 2018)
g. Gunakan *Filter, Proxy* (VPN)
   Biasakan anak melihat hal yang positif dan bukan konten dewasa/ pornografi serta cegah pelacakan oleh situs berbahaya. Jaga alamat IP privat dan aman dibelakang *proxy*. (Xu, Feng, Zhou, & Wu, 2017)

Dengan berbagai macam kasus dan modus serangan sibe seperti contoh diatas, maka kami berinisiatif melaksanakan sosialisasi waspada terhadap kejahatan siber yang

mudah dicerna, berisi tips dan informasi bagaimana berselancar di dunia siber dengan aman dan menghadapi banyaknya serangan siber dan kejahatan siber. Tidak semua modus dan kasus dapat dilaksanakan dengan baik karena kekurangan dalam perangkat yang tersedia dan keterbatasan lainnya. Gambar 3 merupakan dokumentasi kegiatan sosialisasi yang kami lakukan.

Sumber : Hasil Pelaksanaan (2020)

Gambar 3. Pelatihan pencegahan kejahatan siber

4 KESIMPULAN DAN REKOMENDASI

Dari kegiatan PKM ini dapat diambil kesimpulan antara lain: semakin bertambahnya kesadaran untuk menggunakan internet yang aman dan nyaman, kewaspadaan yang semakin baik dalam menanggapi berita-berita hoaks, dapat memilah dan memilih setiap informasi yang diterima untuk mencegah *cyber bullying* atau penipuan lainnya, serta paham terhadap ancaman *virus/malware, spyware atau ransomware*, dan lain-lain.

Ucapan Terima Kasih

Terima kasih kepada rekan-rekan tim PKM yang telah banyak membantu. Juga teman-teman dosen lainnya yang telah mendukung persiapan kegiatan ini. Kepada bapak Jhoni Warta yang telah meluangkan waktunya mempersiapkan materi, Pak Allan Desi yang membantu publikasi online serta rekan-rekan lainnya yang tidak dapat disebutkan satu-persatu.

DAFTAR PUSTAKA

Can, L., & Kaya, N. (2016). *Social Networking Sites Addiction and the Effect of Attitude towards Social Network Advertising. Procedia - Social and Behavioral Sciences*. https://doi.org/10.1016/j.sbspro.2016.11.059

Craig, J. (2018). *Cybersecurity Research—Essential to a Successful Digital Future.*

Engineering, *4*(1), 9–10. https://doi.org/10.1016/j.eng.2018.02.006

Halunen, K., & Latvala, O.-M. (2018). *Cryptography for Human Senses*.

Pall, M. L. (2018). *Wi-Fi is an important threat to human health. Environmental Research*, *164*(January), 405–416. https://doi.org/10.1016/j.envres.2018.01.035

Qi, J., Monod, E., Fang, B., & Deng, S. (2018). *Theories of Social Media: Philosophical Foundations. Engineering.* https://doi.org/10.1016/j.eng.2018.02.009

Ren, T., Chen, Y., Zhou, B., Lv, H., Wang, Z., Xu, S., … Hong, Z. (2015). *Data Uploading and Exchange Algorithm for Mobile Sensor Networks in the City Traffic Environment. International Journal of Dsitribution Sensor Network*, *2015*.

Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). *A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology*, *10*(5), 763–770. Retrieved from http://www.ripublication.com

Vasilakos, A. V, Li, Z., Simon, G., & You, W. (2015). *Information centric network : Research challenges and opportunities. Journal of Network and Computer Applications*, *52*, 1–10. https://doi.org/10.1016/j.jnca.2015.02.001

Wang, Y., & Yu, C. (2017). *Social interaction-based consumer decision-making model in social commerce: The role of word of mouth and observational learning. International Journal of Information Management*, *37*(3), 179–189. https://doi.org/10.1016/j.ijinfomgt.2015.11.005

Xu, C., Feng, J., Zhou, Z., & Wu, J. (2017). *Cross-Layer Optimization for Cooperative Content Distribution in Multihop Device-to-Device Networks*. *IEEE Internet of Things Journal*, *4662*(c), 1–10. https://doi.org/10.1109/JIOT.2017.2741718

Plagiarism Checker X Originality Report

Similarity Found: 26%

Date: Sunday, October 02, 2022
Statistics: 870 words Plagiarized / 3375 Total words
Remarks: Medium Plagiarism Detected - Your Document needs Selective Improvement.

Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat e-ISSN : 2722-3957 Vol. 1 No. 1 (Juli 2020), Hal : 1-10 Available Online at http://ejurna l.ubharajaya.ac.id/index.php/JSTPM 1 Sosialisasi Keamanan Siber untuk Anak-anak di Panti Asuhan Aisiyah Bekasi Kusdarnowo Hantoro 1 * , Asep Ramdhani2 , Khaerudin3 , Rasim4 1 ,ÿ2ÿ,ÿ3ÿ,ÿ4 Teknik Informatika, Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan, Marga Mulya, Bekasi Utara, Kota Bekasi, Jawa Barat 17121, Telp : (021) 88955882, 889955883, kusdarnowo@dsn.ubharajaya.ac.id , asep.ramdhani@dsn.ubharajaya.ac.id, khaerudin@dsn.ubharajaya.ac.id , rasim@dsn.ubharajaya.ac.id *Korespondensi : kusdarnowo@dsn.ubharajaya.ac.id Diterima: 29 April 2020 ; Review: 15 Mei 2020 ; Disetujui: 1 Juli 2020 ; Diterbitkan: 27 Juli 2020 Abstract Now, children and teenagers often posted on social media such as Facebook, Twitter, Instagram often become victims of cybercrimes like phishing, bullying, social engineering by predators by utilizing social media, email and other cyber facilities. With a variety of cases and modes of cybercrime, it is necessary to set up cybersecurity awareness for young people.

This activity provides tips and tricks as well as information on how to surf in a cyber world that is safe in dealing with cybercrime. Keywords : Social media, email, predator, cybercrim e Abstrak Anak-anak dan remaja sekarang banyak yang memposting di sosmed seperti Facebook, Twitter, Instagram seringkali menjadi korban kejahatan siber seper ti phishing, bullying, social engineering oleh para predator dengan memanfaatkan sosial media, email dan fasilitas siber lainnya.

Dengan berbagai macam kasus dan modus kejahatan si ber seperti tersebut, maka perlu dibangun kesadaran di kalangan muda untuk m emiliki bekal pengetahuan keamanan siber. Kegiatan ini memberikan tip dan tricks serta informasi bagaimana cara berselancar

UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS TEKNIK
Kampus I: Jl. Harsono RM No.67, Ragunan, Pasar Minggu, Jakarta Selatan 12550
Telepon: (021) 27808121 - 27808882
Kampus II: Jl. Raya Perjuangan, Marga Mulya, Bekasi Utara, Jawa Barat
Telepon: (021) 88955882 Fax.: (021) 88955871
Web: *www.ubharajaya.ac.id/ft/*. Email: *ft@ubharajaya.ac.id*

SURAT TUGAS

Nomor : ST/341/VII/2020/FT-UBJ

1. Dasar: Kalender Akademik Ubhara Jaya Tahun Akademik 2019/2020.

2. Dalam rangka mewujudkan Tri Dharma Perguruan Tinggi untuk Dosen di Universitas Bhayangkara Jakarta Raya maka dihimbau untuk melakukan penelitian.

3. Sehubungan dengan hal tersebut diatas, maka Dekan Fakultas Teknik Ubhara Jaya menugaskan:

No.	NAMA	JABATAN
1	Kusdarnowo Hantoro, S.Kom., M.Kom.	Dosen Tetap Prodi Teknik Informatika
2	Asep Ramdhani Mahbub, S.Kom., M.Kom.	
3	Ir. Muhammad Khaerudin, M.Kom.	
4	Rasim, S.T., M.Kom.	

Membuat Jurnal dengan judul **"Sosialisasi Keamanan Siber untuk Anak-anak di Panti Asuhan Aisiyah Bekasi"** pada Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat (JSTPM) Vol 1 No 1 Juli 2020.

4. Demikian penugasan ini agar dapat dilaksanakan dengan penuh rasa tanggung jawab.

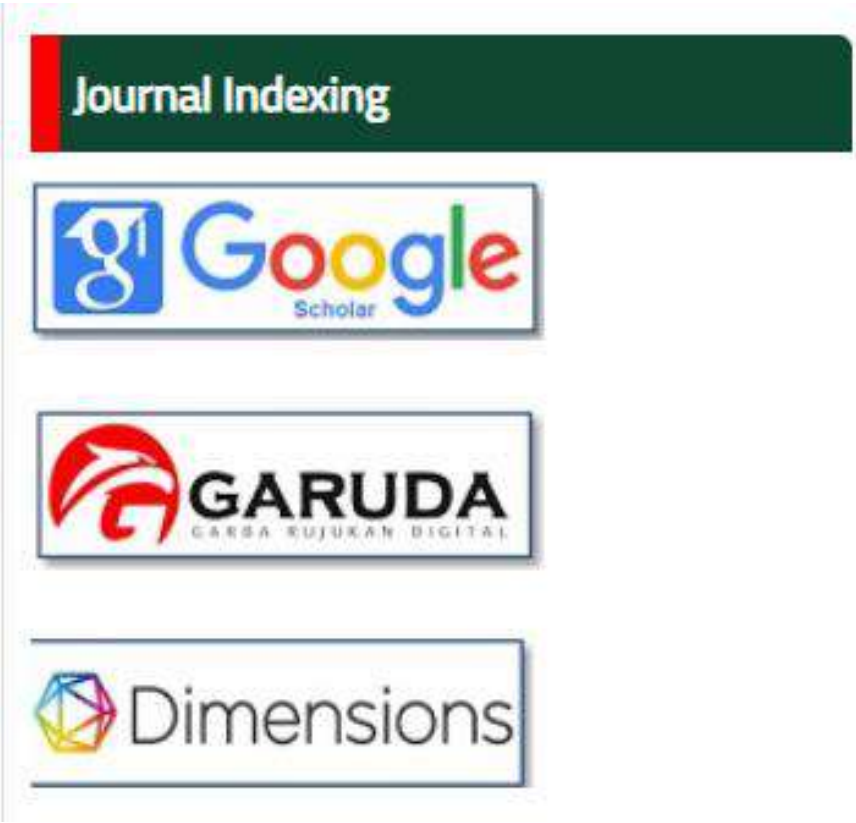
Jakarta, 1 Juli 2020
Pjs. DEKAN FAKULTAS TEKNIK

Ismaniah

Ismaniah, S.Si., MM.
NIP: 9604028

Paraf:
1. Ka. Prodi TIF ..

Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat (JSTPM)



LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL IMIAH

Judul Artikel Ilmiah : Siber Sosialisasi Keamanan Siber Untuk Anak-Anak di Panti Asuhan Aisiyah Bekasi
Jumlah Penulis : 4 Orang
Status Pengusul : Penulis Ke tiga dan Korespondensi
Identitas Jurnal Ilmiah :
a. Nama Jurnal : Jurnal Informatika
b. Nomor ISSN : 2407-1544
c. Vol. No. Bln. Thn : Vol. 1 No. 1 (2020): Juli 2020
d. Penerbit : Sains Teknologi dalam Pemberdayaan Masyarakat (JSTPM)
Jumlah Halaman : 4 Hal

Kategori Publikasi Jurnal Imiah (beri √ pada kategori yang tepat) :
- ☐ Jurnal Ilmiah Internasional Berputasi
- ☐ Jurnal Ilmiah Internasional
- ☐ Jurnal Ilmiah Nasional Terakreditasi
- ☐ Jurnal Ilmiah Nasional Tidak Terakreditasi
- ☐ Jurnal Ilmiah Terindex di DOAJ/lainnya

I. Hasil Penilaian Validasi :

No	Aspek	Uraian/Komentar Penilaian
1	Indikasi Plagiasi	Tidak ada indikasi untuk plagiarisme
2	Linieritas	Sesuai dgn bidang ilmu dari penerbit

II. Hasil Penilaian Peer Review:

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah (isi kolom yang sesuai)					Nilai Akhir Yang Diperoleh
	Internasional Bereputasi	Internasional	Nasional Terakreditasi	Nasional Tidak Terakreditasi	Nasional Terindex DOAJ dll.	
Kelengkapan dan kesesuaian unsur isi jurnal (10%)				1		0,8
Ruang lingkup dan kedalaman pembahasan (30%)				3		2,9
Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)				3		2,8
Kelengkapan unsur dan kualitas Penerbit (30%)				3		2,7
Total = (100%)				10		9,2
Kontribusi pengusul: Penulis ke 4 dari 4 penulis						1,2

Komentar/ Ulasan *Peer Review* :

Kelengkapan kesesuaian unsur	Kelengkapan baik

Ruang lingkup dan kedalaman pembahasan	Ruang lingkup dan pambahasan materi baik
Kecukupan dan kemutakhiran data/informasi dan metodologi	Data yg disajikan sesuai dgn instrumen penelitian dan Metodologinya
Kelengkapan unsur dan kualitas Penerbit	lengkap

Penilai I

NIDN : 0413066604
Unit kerja : Fasilkom Ubharajaya
Bidang Ilmu : Sistem Informasi
Jabatan Akademik (KUM) : Lektor Kepala (477,4)
Pendidikan Terakhir : S2

LEMBAR
HASIL PENILAIAN SEJAWAT SEBIDANG ATAU *PEER REVIEW*
KARYA ILMIAH : JURNAL IMIAH

Judul Artikel Ilmiah	:	Sosialisasi Keamanan Siber untuk anak anak di Panti Asuhan Aisyiah Bekasi		
Jumlah Penulis	:	4		
Status Pengusul	:	Penulis keempat		
Identitas Jurnal Ilmiah	:	a. Nama Jurnal	:	Jurnal Sains Teknologi dalam Pemberdayaan Masyarakat (JSTPM)
		b. Nomor ISSN	:	2722-3957
		c. Vol. No. Bln. Thn	:	Vol 1 No 1 (Juli 2022). http://ejurnal.ubharajaya.ac.id/index.php/jucosco/article/view/943. DOI: https://doi.org/10.31599/jstpm.v1i1
		d. Penerbit	:	Fakultas Teknik Universitas Bhayangkara Jakarta Raya.
		e. Jumlah Halaman	:	10 (1-10)

Kategori Publikasi Jurnal Imiah (beri √ pada kategori yang tepat) :

- ☐ Jurnal Ilmiah Internasional Berputasi
- ☐ Jurnal Ilmiah Internasional
- ☐ Jurnal Ilmiah Nasional Terakreditasi
- ☑ Jurnal Ilmiah Nasional Tidak Terakreditasi
- ☐ Jurnal Ilmiah Terindex di DOAJ/lainnya

I. Hasil Penilaian Validasi :

No	Aspek	Uraian/Komentar Penilaian
1	Indikasi Plagiasi	Tidak ada indikasi plagiarism
2	Linieritas	Sesuai dengan bidang ilmu

II. Hasil Penilaian Peer Review:

Komponen Yang Dinilai	Nilai Maksimal Jurnal Ilmiah (isi kolom yang sesuai)					Nilai Akhir Yang Diperoleh
	Internasional Bereputasi	Internasional	Nasional Terakreditasi	Nasional Tidak Terakreditasi	Nasional Terindex DOAJ dll.	
Kelengkapan dan kesesuaian unsur isi jurnal (10%)				1		0,7
Ruang lingkup dan kedalaman pembahasan (30%)				3		2,5
Kecukupan dan kemutakhiran data/informasi dan metodologi (30%)				3		2,6
Kelengkapan unsur dan kualitas Penerbit (30%)				3		2,5
Total = (100%)				**10**		8,3
Kontribusi pengusul: Penulis pertama dari empat penulis = (8,3 X 40%) / 3 =						3,32

Komentar/ Ulasan *Peer Review* :	
Kelengkapan kesesuaian unsur	lengkap dan sistematika penulisan memenuhi kriteria standar penulisan

Ruang lingkup dan kedalaman pembahasan	Pembahasan mendalam, jelas, dan mudah dipahami
Kecukupan dan kemutakhiran data/informasi dan metodologi	Mutakhir saat diterbitkan
Kelengkapan unsur dan kualitas Penerbit	Unsur penerbit lengkap dan termasuk penerbit yang baik.

Penilai II

NIDN	:	0430087003
Unit kerja	:	Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya
Bidang Ilmu	:	Informatika
Jabatan Akademik (KUM)	:	Lektor (200)
Pendidikan Terakhir	:	S2 - Informatika