AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.12 Januari (2024)
ISSN 2828-6634 (media online)
Hal 1508-1514

Pentingnya Edukasi *Cyber Security* Untuk Menjaga Keamanan Data Pribadi dari Serangan *Cyber Phishing* Bagi Siswa/Siswi PKBM INTAN Tangerang Selatan

Akrom[1], Fingki Marwati[2], Aniq Astofa[3*]

[1]Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang, Indonesia
[2]Ilmu Komputer, Sistem Informasi, Universitas Pamulang, Tangerang, Indonesia
Email: [1]dosen02613@unpam.ac.id, [2*]dosen02817@unpam.ac.id, [3*]dosen02360@unpam.ac.id
(* : coressponding author)

Abstrak - Maraknya serangan *Cyber* di Internet semakin mengkhawatirkan dan semakin banyak memakan korban, oleh karena masyarakat perlu diberikan edukasi tentang pentingnya *Cyber Security* dan pentingnya menjaga keamanan data pribadi khususnya bagi Siswa/Siswi PKBM INTAN dan bagi masyarakat umum. Tidak bisa dipungkiri lagi, bahwa kemajuan teknologi yang semakin pesat saat ini dapat membuka berbagai peluang baru dalam hal yang baik, tapi juga hal yang buruk, kemudahan untuk mengakses internet bagi semua oarng merupakan salah satu hal yang positif, artinya efek kemajuan teknologi bisa dirasakan oleh hampir semua masyarakat, namun hal ini bisa menjadi suatu masalah serta berkembang sebagai hal yang buruk jika masyarakat tidak memahami adanya ancaman bahaya serangan *cyber* atau serangan kejahatan melalui internet, salah satu serangan *cyber* yang semakin mengkhawatirkan saat ini adalah serangan *cyber* melalui *Phishing*. Salah satu dampak atau efek dari serangan *Phishing* adalah bisa menyebabkan kebocoran data pribadi kita. Melihat permasalahan yang dihadapi di Masyarakat umum dan para Siswa/Siwsi PKBM INTAN khususnya, kami dari tim PKM Dosen Universitas Pamulang ingin memberikan sosialisasi kepada para Siswa/Siswi PKBM INTAN dengan judul : "Pentingnya Edukasi *Cyber Security* Untuk Menjaga Kemanana Data Pribadi dari Serangan *Cyber Phishing* Bagi Siswa/Siswi PKBM INTAN Tangerang Selatan.

Kata Kunci: *Cyber Security*, *Phishing*, Kebocoran Data, Perlindungan Data Pribadi, PKBM INTAN

Abstract *- The rise of Cyber attacks on the Internet is increasingly worrying and causing more and more victims, because the public needs to be educated about the importance of Cyber Security and the importance of maintaining the security of personal data, especially for PKBM INTAN students and the general public. It cannot be denied that today's increasingly rapid technological progress can open up various new opportunities in good things, but also bad things, the ease of accessing the internet for everyone is one of the positive things, meaning that the effects of technological progress can be felt by everyone. almost all people, but this can become a problem and develop as a bad thing if people do not understand the threat of cyber attacks or criminal attacks via the internet, one of the cyber attacks that is increasingly worrying at the moment is cyber attacks via Phishing. One of the impacts or effects of a Phishing attack is that it can cause leakage of our personal data. Seeing the problems faced by the general public and INTAN PKBM Students in particular, we of time Lecturer PKM Universitas would like to provide outreach to INTAN PKBM Students with the title: "The Importance of Cyber Security Education to Protect the Security of Personal Data from Cyber Phishing Attacks "For Students PKBM INTAN South Tangerang Selatan" to Support Making Final Project Proposals to Students PKBM Intan Tangerang Selatan".*

Keywords*: Cyber Security, Phishing, Data Breach, Protection Personal Data, PKBM INTAN*

1. PENDAHULUAN

Teknologi yang semakin berkembang saat ini yang seiring dengan kebutuhan manusia akan teknologi tersebut mengakibatkan berbagai inovasi dan penemuan baru yang juga semakin berkembang. Hal ini dapat dilihat dari banyaknya penemuan-penemuan berbasis teknologi (*gadget*) seperti *smartphone*,laptop, televisi, *Air Conditioner*, *Personal Computer* (PC), gelombang radio, dan sebagainya. Namun dibalik semakin maju dan berkembangnya teknologi ini, teknologi tidak hanya memberikan dampak positif bagi masyarakat melainkan juga dampak negatif yang tidak luput dari pemanfaatan teknologi itu sendiri. Salah satu bentuk nyata dari dampak negatif teknologi itu sendiri adalah *Cybercrime*. Tidak hanya menyerang individu secara pribadi, kejahatan dunia maya atau *cybercrime* juga dapat menyerang lembaga pemerintahan seperti pencurian data rahasia milik negara. Hal-hal semacam itu dapat membahayakan keamanan negara. Ancaman keamanan dunia

cybercrime dikarenakan salah satunya terbatasnya para pakar teknologi informasi dan tenaga kerja informasi.

Pengamanan data tidak hanya berlaku untuk data penting di suatu server perusahaan besar, pengamanan data juga perlu diterapkan untuk segala hal yang berkaitan dengan teknologi komputer secara umum. Terlebih lagi Indonesia merupakan negara dengan risiko serangan (Triandi, 2019). *Cyber Security* merupakan praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman yang juga dikenal sebagai keamanan teknologi informasi (Rahmadi & Pratama, 2020). Menurut ISACA dalam (Salim, 2017) terdapat tiga konsep *cyber security* yaitu (1) *confidentially* untuk perlinfungan informasi yang belum diotorisasi atau diungkapan, 2) *integrity* untuk perbaikan data yang rusak harus secepatnya ditangani, 3) *availability* untuk menjamin akses yang tepat untuk penggunaan siste, 2 informasi. *Cyber security* melindungi data akun pengguna dan membatasai hak akses pengguna. Menurut analisis yang lebih baru oleh Australian *Cyber Security* center (ACSC), ada 59.806 laporan kejahatan dunia maya antara juli 2019 dan juni 2020, atau rata-rata 164 kejahatan dunia maya setiap tahun. *Cyber Security* juga menjadi masalah yang serius di Indonesia dengan kebocoran data yang sering terjadi di Indonesia selama 2020-2021. Menurut riset Trend Micro, Indeks Risiko Siber (CRI) Indonesia untuk tahun 2020 adalah 0,26, yang menunjukan tingkat bahaya yang moderat. Sebaliknya, turun menjadi -0,12 pada tahun 2021, menunjukan bahwa bahayanya meningkat walau belum dalam resiko tinggi. (Wahyu Tisno Atmojo, 2021).

Perhatian terhadap pemberian perlindungan kepada data pribadi (*privacy data protection*) yang dicuri semakin mendapat perhatian dari masyarakat ketika salah satu perusahaan (*company*) media sosial terbesar di dunia mengalami pencurian data pribadi oleh beberapa pihak. Sebuah berita pencurian data pribadi tersebut sudah tersebar dengan cepat di berbagai media elektronik yang kemudian dengan mendapat pengakuan dari perusahaan tersebut bahwa telah terjadi pencurian data pribadi atau pengambilan data pribadi milik orang lain tanpa izin yang kemudian dikenal dengan sebutan infromatik "pencurian data atau pembobolan data". Keadaan ini terjadi disebabkan karena adanya kelemahan pada sistem yang digunakan untuk menyimpanan data yang dimiliki oleh perusahaan sehingga data pribadi milik orang lain dapat dicuri oleh pihak yang tidak bertanggung jawab. (Rudi Natamiharja, 2018). Berkaitan dengan pencurian data pribadi seperti yang dilakukan oleh perusahan besar seperti facebook yang pernah ditulis dalam artikel Rudi Natamiharja dalam jurnal Fiat Justisia yang berjudul "*A Case Study on Facebook Data Theft in Indonesia*" mengenai pencurian data yang dialami perusahaan media sosial Facebook (Rudi Natamiharja, 2018). Mekanisme pengumpulan data pribadi dapat dilakukan dengan sederhana. Sebagai contoh, konsumen memberikan data tanpa ada paksaan. Ia memberikan data pribadi kepada Facebook dengan cara mengisi 3 formulir pendaftaran. Hal ini dilakukan dengan penuh kesadaran memberikan persetujuan secara terang-terangan atau tersembunyi. Indonesia sebenarnya saat ini tengah dalam keadaan mendesak *cyber security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cybercrime* di Indonesia sudah mencapai tahap memprihatinkan.

Namun berbeda dengan penangganan kejahatan lainnya, *cyber security* membutuhkan pemikiran yang komprehensif untuk menangganinya. Kejahatan di dunia siber terjadi karena kurangnya pengetahuan dari perlindungan data pribadi oleh masyarakat mengakibatkan masyarakat hanya mengabaikan peristiwa yang terjadi dan menganggap hal tersebut sepele sehingga banyak masyarakat mengabaikan kasus ini, Terlepas dari hal-hal ini, faktor penyebab yang lainnya adalah masyarakat masih kesulitan membedakan mana data yang bisa disebarkan ke publik dan mana yang tidak. Perlu diperingatkan bahwa dalam menginstal sebuah aplikasi apapun terutama media sosial jangan pernah menggunakan data pribadi asli jika memang tidak dibutuhkan untuk di publish, gunakan password yang unik sehingga sulit untuk ditebak oleh orang lain, jangan menginstal aplikasi yang tidak diperlukan dan tetap berhati-hati dengan harus mengetahui seluk beluk aplikasi tersebut apakah aman untuk memasukkan data pribadi kita di dalamnya (Garo Pane, 2021). Untuk mencapai sasaran tersebut perlu dilakukan hal-hal seperti; 1) penyebaran informasi serta sosialisasi terkait isu-isu keamanan informasi serta pencerdasan terkait risiko-risiko dalam penggunaan teknologi informasi guna meningkatkan *security* awareness pada masyarakat luas. 2) transfer pengetahuan yang berhubungan dengan keamanan siber dapat dimasukkan ke dalam pendidikan

formal dalam rangka mempersiapkan generasi penerus dalam menghadapi perkembangan teknologi serta risiko-risiko yang melekat dengannya. (Banyumurti, Indroyatno, 2018).

Peneliti Badan Litbang SDM Kemkominfo menyatakan bahwa diperlukan upaya-upaya untuk meningkatkan kesadaran, pengetahuan dan keterampilan anak dan remaja Indonesia dalam kaitannya dengan keamanan berinternet. Mengingat Internet telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan sehari 4hari anak dan remaja di Indonesia. "Hal ini dapat dicapai melalui sosialisasi, pendidikan Iiterasi maupun pelatihan. Pemahaman penggunaan dan keamanan media digital sangat penting utamanya dari perspektif anak-anak dan remaja, sebelum merancang program-program informasi tentang keamanan digital. Termasuk memahami tentang cara mereka mengartikan dan menggunakan teknologi digital, komunikasi secara online dan perilaku berisiko atau tidak aman (Banyumurti, Indroyatno, 2018). Seringkali para pengguna internet tidak menyadari bahwa pencurian data sangatlah membahayakan diri sendiri maupun orang lain. Pencurian data ini dapat disalahgunakan sebagai bentuk kejahatan, semakin banyak data yang bocor maka akan semakin tinggi pula bahaya yang mengintai. Penyalahgunaannya bisa berbentuk *Phising*, penipuan berkedok pinjaman online (pinjol), atau juga peretasan akun media sosial untuk menipu keluarga dan kerabat dekat yang dimiliki oleh pengguna terkait. Hal ini tentu saja sangat mengkhawatirkan bahkan dapat membuat kita yang kehilangan data mengalami kerugian baik secara materil maupun non-materiil. Menurut Yuwinanto, (2015) penggunaan perangkat sistem informasi yang terhubung ke jaringan atau online memunculkan isu privasi dan menurutnya ada beberapa langkah yang bisa digunakan untuk menjaga privasi itu yaitu memberikan pengguna mekanisme pengontrolan khususnya pada data atau informasi yang dimiliki.

Sebagaimana yang kita ketahui bahwa siswa/i menengah adalah usia remaja dan merupakan komunitas terbesar dalam masyarakat Indonesia yang menggunakan media sosial secara regular. Alasan awal mereka sangat aktif menggunakan media sosial adalah untuk mencari perhatian, meminta pendapat dan menumbuhkan citra, namun lama kelamaan akhirnya menjadi ketergantungan. Walaupun media sosial memberikan dampak positif pada remaja, namun pada saat mereka sulit melepaskan diri dari kegiatan yang berkaitan dengan media sosial maka akan memberikan dampak yang kurang positif. Sejumlah studi menunjukkan bahwa akibat penggunaan media sosial yang berlebihan, remaja ditemukan mengalami ingkongruensi pada konsep dirinya. 5 Melihat penjabaran tentang bahaya dari dampak pencurian data di atas maka dirasa perlu dilakukan edukasi tentang pentingnya *cyber security* kepada para siswa/siswi PKBM Intan. Diharapkan dari kegiatan ini dapat selalu menjaga keamanan datanya sebagai antisipasi pengurangan dampak kebocoran data, sehingga mampu mengurangi jumlah resiko penipuan serta diharapkan mampu memberikan pengarahan kepada orang-orang disekitarnya agar selalu waspada dalam penggunaan internet.

2. METODE PELAKSANAAN

Dalam menyelesaikan permasalahan yang dihadapi, tim PKM menawarkan sosialisasi tentang pentingnya *cyber security* kepada para siswa/siswi PKBM Intan. Tim PKM melalui dana PKM memberikan bantuan untuk pelaksanaan pemenuhan sarana dan prasarana yang dapat mendukung pelaksanaan sosialisasi kepada siswa/siswi. Sehingga luaran program yang diharapkan dapat terlaksanakan dengan baik dan lancar.

Pelaksanaan penyuluhan program PKM ini sendiri dapat dihadiri minimal 30 peserta. Dan nanti setelah acara, tim PKM akan melakukan pengawasan untuk memastikan sosialisasi ini berjalan dengan baik. Namun apabila luarannya tidak sesuai dengan harapan, tim PKM akan melakukan evaluasi dan perbaikan di setiap pertemuannya serta mencoba semaksimal mungkin membantu agar semuanya dapat berjalan dengan baik.

2.1 Tahapan Kegiatan

Evaluasi kegiatan dilakukan setelah kegiatan sosialisasi kepada para siswa siswi PKBM Intan dengan cara mengisi form evaluasi yang disiapkan oleh TIM PKM terkait bagaimanakah tanggapan para peserta terhadap kegiatan PKM yang dilakukan oleh Tim Dosen Teknik Informatika Universitas Pamulang

AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.12 Januari (2024)
ISSN 2828-6634 (media online)
Hal 1508-1514

Agar pelaksanaan kegiatan dapat tercapai sesuai dengan yang diharapkan, maka pengabdi berusaha melakukan proses evaluasi dari kegiatan tersebut, dengan menentukan kriteria dan menetapkan indikator keberhasilan sebagai berikut :

Tabel 1. Tahapan Kegiatan

Kegiatan	Kriteria	Indikator
Persiapan	Menyiapkan materi sosialisasi, alatalat dan bahan-bahan yang diperlukan untuk kegiatan sosialisasi	Tempat dan alat pelaksanaan siap
Sosialisasi	Memberikan edukasi tentang pentingnya *cyber security* guna menjaga keamanan data diri di era digital pada siswa/siswi PKBM INTAN	Pelaksanaan lancar, peserta yang terdiri dari siswa/siswi memahami akan pentingnya menjaga data diri.
Evaluasi dan Pelaporan	Evaluasi hasil kerja untuk mengetahui kendala selama pelatihan dan menyusun laporan kegiatan.	Tersusunnya laporan kegiatan PKM

Tabel 2. Jenis-Jenis Serangan *Cybersecurity*

Jenis Serangan *Cyber*	Keterangan
Phishing	*Phising* adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan
Virus	Virus komputer adalah program atau kode yang dirancang untuk menyebabkan kerusakan atau merusak sistem komputer atau data
Trojan	Virus Trojan adalah jenis malware yang menyerang komputer dengan menyamar sebagai program atau sistem operasional resmi.
Denial of Service	Serangan *Denial of Service* (*DoS*) merupakan jenis serangan terhadap sistem dalam jaringan internet dengan cara menghabiskan resource
Hacking	*Hacking* adalah kegiatan yang dilakukan penjahat siber untuk mendapatkan akses tidak sah dan mencuri data serta melakukan serangan siber
Malware	*Malware* (*Malicious Software*) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer
Ransomeware	*R*ansomware adalah salah satu jenis *malware* yang menyerang perangkat Anda dengan mengenkripsi file atau data Anda sehingga tidak dapat

Tabel 3. Kegiatan

Waktu	Kegiatan
10.00 – 10.15	Pembukaan kegiatan
10.15 – 10.30	Sambutan-sambutan

10.30 – 11.00	Pemaparan materi
11.00 – 11.45	Tanya jawab dan pendampingan
11.45 – 12.00	Pembagian souvenir

Gambar 1. Gambar Jenis-Jenis Anti Virus

Gambar 2. Pembukaan Acara Oleh Tim Dosen

Gambar 3. Pemaparan Materi Oleh Pak Akrom, S.Kom., M.Kom.

AMMA : Jurnal Pengabdian Masyarakat
Volume 2, No.12 Januari (2024)
ISSN 2828-6634 (media online)
Hal 1508-1514

Gambar 4. Penjelasan Tentang Kejahatan *Cyber* Oleh Pak Akrom, S.Kom., M.Kom

Gambar 5. Foto bersama Wakil Ketua Yayasan PKBM Intan

3. HASIL DAN PEMBAHASAN

Kegiatan PKM ini diarahkan kepada para siswa/siswi kelas XII PKBM Intan dengan total peserta sebanyak 30 orang, yang juga dihadiri oleh Kepala Sekolah yaitu bapak Nurman, M.Pd. Kami dengan pihak sekolah sudah berkoordinasi untuk penggunaan ruangan lab dalam pelaksanaan kegiatan ini agar memudahkan peserta didik dalam mengikuti sosialisasi yang diberikan. Kami berharap kegiatan PKM ini dapat dijadikan sebagai media pembelajaran dan pemahaman baru agar menambah wawasan pengetahuan serta memahami pentingnya *Cyber Security* bagi siswa untuk membangun keamanan informasi dalam era digital. Hasil kegiatan pengabdian pada masyarakat secara garis besar mencakup beberapa komponen sebagai berikut :

1) Keberhasilan target jumlah peserta sosialisasi
2) Ketercapaian target materi yang telah direncanakan.

Target peserta pelatihan seperti direncanakan sebelumnya adalah 30 orang siswa/siswi PKBM Intan. Dalam pelaksanaannya, kegiatan ini diikuti oleh 30 orang peserta. Dengan demikian dapat dikatakan bahwa target peserta mencapai 100%. Angka tersebut menunjukkan bahwa kegiatan pengabdian pada masyarakat ini dilihat dari jumlah peserta yang mengikuti dapat dikatakan berhasil/ sukses. Ketercapaian target materi pada kegiatan pengabdian pada masyarakat ini cukup baik, karena materi sosialisasi telah dapat disampaikan secara keseluruhan. Pemahaman materi dapat dilihat dari respon para siswa/siswi. Mereka sangat antusias saat diskusi dan sesi tanya jawab sehingga para siswa/siswi dapat mengerti dan dapat menerapkannya dalam kehidupan sehari-hari

a. Persiapan Pelaksanaan PKM

Persiapan dilakukan dengan melakukan breafing kepada semua panitia pelaksanaan kegiatan PKM termasuk kepada rekan-rekan mahasiswa yang ikut hadir dalam kegiatan tersebut.

b. Pemaparan tentang pentingnya *Cyber-Security*

Dalam pemaparannya para peserta dari siswa/siswi diberikan pemahaman tentang pentingnya untuk selalu menjaga keamanan data (*cyber-security*) baik dari perangkat mobile, laptop atau komputer, terutama dalam hal bermedia sosial. Serta memberikan arahan agar selalu waspada dan selalu membaca term and condition dalam setiap mengisi data pribadi sebelum mendownload atau menggunakan suatu aplikasi untuk menghindari adanya pencurian data dan dapat disalahgunakan oleh pelaku sebagai tindak kejahatan.

c. Evaluasi Kegiatan dan Pelaporan

Selama pelaksanaan kegiatan ini berlangsung, ada beberapa evaluasi yang dilakukan pada saat proses kegiatan dilaksanakan, evaluasi yang pertama dilakukan adalah menjelaskan apasaja yang termasuk ke dalam kejahatan dunia maya dan bagaimana cara menyikapinya jika ada seseorang yang berusaha untuk meminta data pribadi kita baik itu password ataupun OTP. Evaluasi kedua adalah memberikan kesempatan kepada peserta untuk bertanya secara langsung ketika peserta dirasa pernah mengalami hampir menjadi korban pencurian data.

Pada setiap tahap dilakukan evaluasi sehingga timbul keyakinan bahwa segala sesuatu yang telah diputuskan adalah benar, dan dapat melangkah ke tahap berikutnya dengan aman. Apabila hasil evaluasi menunjukan kekurangan atau kelemahan maka dilakukan penyempurnaan atau penyesuaian. Pada akhir kegiatan dilakukan analisa terhadap ketercapaian tujuan dan dampak dari keseluruhan kegiatan pengabdian masyarakat terhadap khalayak sasaran. Evaluasi juga dilakukan terhadap seluruh pelaksanaan kegiatan. Selanjutnya dilakukan penyusunan Laporan. Sebagai bentuk pertanggung jawaban pelaksanaan kegiatan pengabdian masyarakat yang telah dilakukan.

4. KESIMPULAN

Dari kegiatan yang telah dilaksanakan dapat disimpulkan bahwa para pesrta merasa senang karena bisa mendapatkan pengetahuan tentang pentingnya menjaga keamanan data pribadi agar terhindar dari kejahatan-kejahatan dunia maya di era digital seperti sekarang ini serta mereka mendapatkan wawasan baru diluar kegiatan belajar mengajar di kelas.

REFERENCES

Banyumurti, Indroyatno, D. (2018). Kebijakan *Cyber Security* Dalam Perspektif Multi Stakeholder

Garo Pane, C. G. (2021). Edukasi Kepada Siswa Sma Negeri 1 Mimika Untuk Mengatasi Ancaman Media Online Pada Data Pribadi. KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi, 1(2), 412–418. https://doi.org/10.24002/konstelasi.v1i2.4166

Rahmadi, G., & Pratama, A. R. (2020). Analisis Kesadaran *Cyber Security* pada Kalangan Pelaku e-Commerce di Indonesia. Automata, 1(2), 7. Retrieved from https://journal.uii.ac.id/AUTOMATA/article/view/15399

Ramadhan, I. (2019). Strategi Keamanan *Cyber Security* di Kawasan Asia Tenggara.Jurnal Asia Pacific Studies,3(2), 181-192

Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia," FIAT JUSTISIA 12, N (2018): 3.

Salim, S. C. (2017). Analisis *Cyber Security* pada Instagram untuk mengukur customer trust. (227), 1–23.

Triandi, B. (2019). Keamanan informasi secara aksiologi dalam menghadapi era revolusi industri 4.0. JURIKOM (Jurnal Riset Komputer), 6(5), 477-483

Wahyu Tisno Atmojo, M. E. (2021). Pengenalan *Cyber Security* Dalam Revousi Industri 4.0 Dan Menyongsong Era Society 5.0. Prosiding PKMCSR, 39-45