JAMAIKA: Jurnal Abdi Masyarakat
Universitas Pamulang
Volume: 3 Nomor: 2
p-ISSN: 2716-4780 e-ISSN: 2721-6144

Sosialisasi Pentingnya Cyber Security Guna Mengurangi Resiko Tingkat Pencurian Data Yang Berimbas Pada Tindak Penipuan Kepada Para Karang Taruna Benda Baru Pamulang

Leni Susanti*,Akrom, Debby Rahadian Baskhara, Khairudin, Aniq Astofa
Universitas Pamulang
*Email: dosen02617@unpam.ac.id

ABSTRAK

Perlindungan dan keamanan informasi individu terus menjadi berarti, paling utama ketika pandemi pada saat bisnis mulai berpindah ke online dampak terdapatnya pembatasan mobilitas masyarakat. Polisi siber mencatat sebanyak 182 kasus pencurian data dilaporkan oleh masyarakat. Angka ini meningkat 27,3% dibandingkan dengan tahun sebelumnya yang sebanyak 143 laporan. Selama lima tahun terakhir, peningkatan laporan pencurian data meningkat 810% dari 20 laporan pada 2016. Aspek lain yang tidak menyerah yaitu merupakan melindungi keamanan data informasi diri seorang di akun sosial media. Oleh karena itu, wawasan guna tingkatkan pemahaman diri sehingga dapat melindungi keamanan data informasi diri perlu selalu digalakkan, paling utama di kalangan para anggota Karang Taruna khususnya Karang Taruna Benda Baru, Pamulang Tangerang Selatan yang mana hampir keseluruhan anggotanya merupakan pemuda dan menjadi penggiat sosial media bagus buat kebutuhan individu ataupun institusi. Dalam rangka pengurangan tingkat penipuan karena sering terjadinya kasus pencurian data, maka untuk menjawab kebutuhan tersebut perlu diadakannya Kegiatan Pengabdian Kepada Masyarakat (PKM), dimana kegiatan ini merupakan suatu upaya Universitas Pamulang untuk memberikan sumbangsih ilmu pengetahuan dan teknologi kepada masyarakat. Kegiatan dilaksanakan dengan memberikan sosialisasi tentang pentingnya menjaga keamanan data (cyber-security) pribadi yaitu dengan cara tidak memberikan kode one-time password (OTP) kepada orang lain, jangan klik tautan yang belum jelas sumbernya, gunakan password yang sulit untuk ditebak dan selalu membaca terms and conditions sebelum mengisi suatu data ke aplikasi. Hasil dan luaran kegiatan setelah dilaksanakan kegiatan sosialisasi tentang cyber-security adalah setiap masyarakat khususnya anggota Karang Taruna Benda Baru, Pamulang Tangerang Selatan mempunyai pemahaman dan kesadaran mengenai pentingnya memperhatikan aspek – aspek keamanan data dan harus ditanamkan sedini mungkin oleh setiap organisasi terhadap seluruh anggotanya. Setiap individu yang berada di dalam organisasi mempunyai tanggung jawab untuk melindungi keamanan data dan informasi yang dimilikinya. Serta diharapkan agar selalu dapat menjaga akun privasinya agar dapat terhindar dari pencurian data yang dapat mengakibatkan data tersebut disalahgunakan oleh pihak yang tidak bertanggungjawab untuk melakukan aksi penipuan. Setelah diadakan kegiatan PKM ini peserta menjadi paham dan mengerti bahwa tidak boleh sembarangan dalam klik tautan yang belum jelas sumbernya serta mengetahui bahayanya menggunakan koneksi dengan VPN.

Kata Kunci : Cyber-Security, Cyber-Crime, Pencurian Data, Karang Taruna Benda Baru Pamulang

ABSTRACT

The protection and security of personal data is increasingly important, especially during the pandemic when transactions begin to switch to online due to restrictions on people's mobility. The cyber police recorded 182 cases of data theft reported by the public. This figure increased by 27.3% compared to the previous year which was 143 reports. During the last five years, the increase in reports of data theft increased by 810% from 20 reports in 2016. Another aspect that is no less important is maintaining the security of one's personal data information on social media accounts. Therefore, knowledge to increase self-awareness of the importance of maintaining the security of personal data information needs to be continuously promoted, especially among members of Karang Taruna, especially Karang Taruna Benda Baru, Pamulang, South Tangerang where almost all of the members are youth

and become social media activists both for personal and institutional interests. In order to reduce the level of fraud due to frequent cases of data theft, it is necessary to hold Community Service Activities, where this activity is an effort of Pamulang University to contribute science and technology to the community. The activity was carried out by providing socialization about the importance of maintaining personal data security (cyber-security), namely by not giving one-time password (OTP) codes to others, do not click on links that have no clear source, use passwords that are difficult to guess and always read terms and conditions before entering data into the application. The results and outputs of the activities after the cyber-security socialization activities were carried out were that every community, especially members of the Karang Taruna Benda Baru, Pamulang, South Tangerang, had an understanding and awareness of the importance of paying attention to data security aspects and must be instilled as early as possible by each organization to all its members. Every individual within the organization has a responsibility to protect the security of the data and information they have. And it is hoped that they can always maintain their privacy accounts in order to avoid data theft which can result in the data being misused by irresponsible parties to commit fraudulent actions. After this activity was held, participants became aware and understood that it should not be careless to click on links that have no clear source and know the dangers of using a connection with a VPN.

Keywords : Cyber-Security, Cyber-Crime, Data Theft, Karang Taruna Benda Baru Pamulang

PENDAHULUAN

Saat ini hampir setiap manusia telah menggunakan berbagai macam alat elektronik dan bahkan sebagian manusia tidak lepas dari alat elektronik tersebut. Perkembangan teknologi dan komunikasi semakin memudahkan manusia dalam berhubungan meskipun terpisah jauh, bahkan berbeda negara. Dihadapkan dengan adanya perkembangan teknologi dan informasi yang sangat pesat saat ini, masyarakat diharapkan agar dapat memanfaatkan teknologi ke dalam hal-hal yang positif karena banyak manfaat dan kemudahan yang didapatkan dari internet. Pemanfaatan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga melahirkan sejumlah permasalahan termasuk masalah hukum. Salah satu masalah hukum yang muncul adalah masalah yang berkaitan dengan perlindungan data pribadi (the protection of privacy rights) (Latumahina, 2014).

Tidak hanya menyerang individu secara pribadi, kejahatan dunia maya atau cybercrime juga dapat menyerang lembaga pemerintahan seperti pencurian data rahasia milik negara. Halhal semacam itu dapat membahayakan keamanan negara. Ancaman keamanan dunia cybercrime dikarenakan salah satunya terbatasnya para pakar teknologi informasi dan tenaga kerja informasi. Penjagaan informasi tidak cuma berlaku buat informasi berarti di sesuatu server industri besar, pengamanan informasi pula butuh diaplikasikan buat seluruh perihal yang berhubungan dengan teknologi pc dengan cara biasa. Terlebih lagi Indonesia ialah negeri dengan ancaman serangan (Triandi, 2019).

Bagi ISO(International Organization for Standardization), persisnya ISO atau IEC 27032; mengambil dari beberapa pangkal, cyber security ataupun cyberspace security merupakan konservasi dari kerahasiaan, integritas, serta ketersediaan data di cyberspace. Ada pula cyberspace merujuk pada

area yang lingkungan yang ialah hasil dari interaksi antara orang, peranti lunak, serta layanan- layanan internet lewat pemakaian berbagai macam fitur teknologi serta bermacam koneksi jaringan; area yang tidak mempunyai bentuk. Menurut Micro Focus, keamanan data adalah proses melindungi data bersifat privat, dari kerusakan yang dilakukan pihak tidak berwenang. Keamanan data ini mencakupi enkripsi data, hashing, tokenisasi dan manajemen kunci. Keamanan data sangat penting untuk mencegah terjadinya kerugian material seperti melakukan pemerasan sejumlah uang. Selain itu, keamanan data personal harus dijaga untuk mengurangi penyalahgunaan informasi, serta memperkecil peluang terjadinya tindakan kriminal.

Sedangkan, bagi Kaspersky, cyber security merupakan sesuatu aplikasi mencegah para pc, server, fitur mobile, sistem elektronik, jaringan, serta informasi dari seranganserangan kejam. Sedemikian itu pula Cisco yang mendeskripsikan cyber security selaku aplikasi mencegah bermacam sistem, jaringan, serta program dari serangan- serangan digital. Cyber security kian populer karena kian banyaknya pemakaian pc semacam desktop, laptop, ponsel pintar, server, serta fitur IoT(internet of things) dan pemakaian jaringan pc semacam internet dalam kehidupan pemeluk orang tiap hari.

Bagi World Bank, bersumber pada informasi ITU(International Telecommunication Union), misalnya jatah konsumen internet di bumi merupakan dekat 49% populasi pada tahun 2017. konsumen itu bertambah cepat dibanding tahun 2000 yang cuma dekat 6, 7%. Seragam perihalnya bagi Internet World Stats dengan berspekulasi bagi konsumen internet di bumi merupakan sebesar 64, 2% populasi pada suku tahun awal tahun 2021. Ada pula jumlah konsumen internet yang diperkirakan itu merupakan sebesar lebih dari 5 miliyar. Jumlah itu bertambah dekat 1. 300% dibanding tahun 2000.

Selain itu, jumlah serangan semakin bertambah. Bagi Deep Instinct misalnya, jumlah cyber attack ataupun serbuan siber memakai malware hadapi kenaikan sebesar 358% pada tahun 2020 dibanding tahun 2019. Sedangkan, spesial ransomware, peningkatannya sebesar 435% pada tahun 2020 dibanding tahun lebih dahulu. Ada pula besarnya kenaikan yang dituturkan Deep Instinct itu bersumber pada dasar informasi Deep Instinct yang menyambut informasi dari bermacam pangkal, tercantum pihak ketiga serta yang diperoleh dari pelanggan Deep Instinct. Informasi yang digabungkan juga diklaim menggambarkan ratusan juta peristiwa pada tahun 2020.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 materiil maupun non-materiil. Menurut Yuwinanto, (2015) pemakaian fitur sistem data yang tersambung ke jaringan ataupun

online menimbulkan rumor privacy serta baginya terdapat sebagian tahap yang dapat dipakai buat melindungi privacy itu ialah memberikan konsumen metode pengontrolan khususnya pada informasi ataupun data yang ada.

METODE

Berdasarkan identifikasi masalah yang sudah dirumuskan dan tujuan yang hendak dicapai maka program pengabdian masyarakat ini dilakukan yaitu :

1. Sosialisasi tentang kegunaan dan manfaat Internet Para anggota Pengabdian yang bertugas sebagai narasumber memberikan sosialisasi tentang peranan, kegunaaan dan manfaat dari Internet
2. Pemaparan tentang pentingnya Cyber-Security Dalam pemaparannya para peserta dari Karang Taruna 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.
3. 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 apa saja 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 12 bertanya secara langsung ketika peserta dirasa pernah mengalami hampir menjadi korban pencurian data. Pada tiap langkah dilakukan penilaian sehingga muncul kepercayaan kalau segala suatu yang sudah diputuskan merupakan betul, serta bisa berjalan ke langkah selanjutnya dengan baik. Bila hasil penilaian membuktikan kekurangan ataupun kelemahan hingga dilakukan perbaikan ataupun adaptasi**.** Pada akhir aktivitas dibuat analisa kepada ketercapaian tujuan serta akibat dari totalitas aktivitas pengabdian kepada masyarakat kepada khalayak target. Penilaian juga dilakukan kepada semua penerapan aktivitas. Berikutnya dibuat kategorisasi Informasi sebagai wujud pertanggung jawaban penerapan kegiatan kepada masyarakat yang telah dilaksanakan.

HASIL

Secara garis besar hasil dari kegiatan pengabdian kepada masyarakat yang diberikan kepada para anggota karang taruna Benda Baru yaitu dengan memberikan sosialisasi dan pemaparan materi tentang pentingnya menjaga keamanan data (cyber security). Setelah kegiatan pemaparan selesai maka proses berikutnya adalah menerima tanggapan dan pertanyaan dari para peserta. Dari kegiatan kegiatan pengabdian ada 3 pertanyaan yang diajukan para peserta yaitu:

1. Penanya Pertama oleh Bapak Ghozali Sya'bandi, S.E dengan pertanyaan: Bagaimana caranya link yang belum jelas sumbernya itu bisa mengambil data pribadi ?, dan bagaimana caranya mengetahui bahwa link tersebut tidak benar sumbernya ?
2. Penanya Kedua oleh Sdra. Deni Kurnia dengan pertanyaan: Apakah penggunaan VPN pada perangkat HP atau Laptop dapat menjadi akses sebagai pencurian data pribadi? Jelaskan alasannya.
3. Penanya Ketiga oleh Sdri. Chairunnisa dengan pertanyaan: Apa saja yang termasuk dalam kategori data pribadi dan bagaimana cara mengamankannya?

PEMBAHASAN

Dari ketiga pertanyaan diatas jawaban telah disampaikan oleh Bapak Akrom S.Kom, M.Kom sebagai pemateri dalam kegiatan pengabdian masyarakat. Adapun untuk jawaban dari pertanyaan diatas adalah:

1. Biasanya si pengirim link akan mengirimkan link meluali berbagi sumber, misal WA Group, email, atau account sosial media kita, mereka menyamar seolah olah informasi yang diberikan / atau link yang diberikan adalah link yang valid, supaya 13 kita percaya untuk membukanya dan mengikuti instruksi atau arahan dari pemilik link / website, teknik ini biasa disebut phishing. Caranya kita untuk mengetahui bahwa link atau website yang akan kita buka adalah link palsu atau tidak jelas reputasinya yang paling sederhana adalah dengan memperhatikan domain atau alamat websitenya, misal jika link tersebut yang menginformasikan tentang informasi darp pemerintah biasanya domainya akan menggunakan .go.id atau .org.id, atau kita bisa cari informasi dengan sumber yang lain sebelum kita membuka atau mengikuti instruksi dari websiti tersebut, dan biasanya ciri-ciri website yang tidak benar itu akan memnita kita untuk mngisikan data-data pribadi kita, misal tgl lahir,nama Ibu kandung, no ktp, bahkan user atau password kita.
2. Karena prinsip kerja VPN adalah membuat koneksi langsung atau tunneling dari perangkat kita misal handphone atau laptop ke server pemilik VPN, jadi perangkat kita akan satu network atau seolah satu jaringan LAN dengan server mereka, ini sangat berbahaya karena

dengan kita satu jaringan atau satu network dengan mereka, si pemeilik server VPN akan lebih leluasa memantau aktifitas yang kita lakukan di internet, bahkan mereka akan lebih mudah untuk mendapatkan informasi atau data-data yang ada di perangkat kita dengan tools tertentu yang mereka siapkan, jadi data-data pribadi kita misal data perbankan, atau data kependudukan kita bisa mereka ambil untuk keperluan tertentu, misalnya untuk membobol rekening bank kita.

3. Yang termasuk kategori data pribadi adalah tgl lahir, nomor ktp, no handphone, alamat, nama keluarga, nama ibu kandung, user id, dan password. Untuk mengamankan data pribadi kita bisa melakuan dengan cara kita harus berhati-hati kepada setiap orang atau link yang meminta data-data pribadi kita, pastikan kegunaanya dan tidak akan disalahgunakan, dan tentunya dengan cara kita tidak membuka situs-situs yang tidak jelas sumbernya atau situs-situs yang kategori kotor, dan hindari menggunakan VPN yang sifatnya public yang tidak jelas reputasinya

Gambar 1. Proses Pemberian Piagam

Secara umum, mitra cukup responsif dan aktif dalam kegiatan ini dengan kesediaan untuk mengikuti rangkaian kegiatan Pengabdian Kepada Masyarakat dari awal hingga akhir. Ketercapaian sasaran materi pada kegiatan pengabdian masyarakat ini terlaksana dengan baik, sebab materi pendampingan sudah bisa di informasikan dengan cara totalitas. Diharapkan dalam sosialisasi berikutnya dapat dirancang alat ukur yang lebih efektif dan komprehensif serta partisipasi penuh dari seluruh peserta untuk dapat mengikuti proses penilaian akhir.

Gambar 2. Photo dokumentasi di akhir pelaksanaan

SIMPULAN

Dari kegiatan ini dapat disimpulkan bahwa para peserta menyadari bahwasanya keamanan data (cyber security) pada perangkat pribadi baik handphone maupun laptop sangat penting untuk dipelajari dan dipahami, dimana saat ini semua mengandalkan teknologi dan komunikasi dalam melaksanakan kegiatan sehari-hari. Para peserta juga telah memahami terkait keamanan data pribadi.

UCAPAN TERIMAKASIH

Kegiatan PKM ini dapat terlaksana berkah support dari bermacam pihak. Oleh sebab itu dalam peluang ini perkenankanlah kita mengantarkan dapat kasih pada:

1. Ketua Yayasan Sasmita Jaya Group
2. Rektor Universitas Pamulang
3. Dekan Fakultas Teknik Universitas Pamulang
4. Kepala Program Teknik Informatika Universitas Pamulang
5. Pimpinan Lembaga Penetlitian dan Pengabdian Masyarakat (LPPM) Universitas Pamulang

DAFTAR PUSTAKA

Aji, dkk. 2021. Peningkatan Pemahaman Guru Mengenai Pengamanan Data Ajar Melalui Pelatihan Online di SMPN I Karangwelas. ABSYARA: Jurnal Pengabdian Pada Masyarakat e-ISSN: 2723-6269 Vol. 2, No. 1, Juli 2021. Hal. 62 – 71

Edmon, Makarim. Indonesian Legal Framework for Cyber security. http://www.nisc.go.jp/securitysite/campaign/ajsympo/pdf/lecture2.pdf.

Heryanto, dkk. 2018. Workshop Teknik Keamanan Dalam Menggunakan Internet Pada Siswa SMK Di Indralaya Tahun 2018. Prosiding Annual Research Seminar 2018 Computer Science and ICT ISBN : 978-979-587-813-1 Vol.4 No.1. Hal: 31-33

Jatikusumo, D., & Nurhaida, I. (2020). Data Securing of Patients in Cloud Computing Using A Combination of SHA256 and MD5. ACM International Conference Proceeding Series, September, 16–22

Latumahina, Rosalinda Elsina. 2014. Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. Jurnal Gema Aktualita, Vol. 3 No. 2, Desember 2014. Hal: 14-25.

Pencurian Data Pribadi Makin Marak Kala Pandemi. KATADATA.CO.ID. Last Modified 07 September 2021.https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadimakin-marak-kala-pandemi

Rumlus, Muhamad Hasan & Hanif Hartadi. Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media). Jurnal HAM Volume 11, Nomor 2, Agustus 2020. Hal: 285-299

Sharief, M. (2016). Secure Hash Design & Implementation Based On Md5 & Sha1 Using Merkle – Damgard Construction. International Journal of Advanced Research in Computer Science & Technology (IJARCST, 4(2), 92–94.

Sholikhatin, dkk. 2020. Workshop Strategi Peningkatan Popularitas Konten Serta Menjaga Keamanan Data Pribadi Di Berbagai Platform Media Sosial. Volume 4, Nomor 1, November 2020. p-ISSN : 2614-5251. e-ISSN : 2614-526X Hal: 251-255

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

Ulfah, dkk. 2021. Pelatihan Secure Computer User Untuk Meningkatkan Kesadaran Siswa Terhadap Keamanan Data dan Informasi. J-PEMAS STMIK Amik Riau Vol. 2, No. 1, Februari 2021, pp. 17-24 E-ISSN: 2722 -5143

Yuwinanto, Helmy Prasetyo. 2015. Privasi Online Dan Keamanan Data. Surabaya: Airlangga.