IKA BINA EN PABOLO : PENGABDIAN KEPADA MASYARAKAT
Volume : 4 Nomor : 2, Juli 2024, Page : 57 - 65
e-ISSN : 2808-4047
Universitas Labuhanbatu

PELATIHAN BASIC CYBER SECURITY UNTUK KEAMANAN DAN PERLINDUNGAN DATA PRIBADI DI DUNIA DIGITAL

[1]Marnis Nasution, [2]Angga Putra Juledi, [3]Syaiful Zuhri Hrahap, [4]Deci Irmayani, [5]Ibnu Rasyid Munthe

[1235]Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Labuhanbatu
[4]Manajemen Informatika, Fakultas Sains dan Teknologi, Universitas Labuhanbatu

Email: [1]marnisnst@gmail.com, [2]anggapj19@gmail.com, [3]syaifulzuhriharahap@gmail.com, [4]deacyirmayani@gmail.com, [5]ibnurasyidmunthe@gmail.com

Corresponding Author : Marnis Nasution

Abstrak

Pencurian data pribadi melalui layanan yang membutuhkan data pribadi telah menjadi isu yang marak dibicarakan. Sebagai negara hukum, Indonesia wajib melindungi hak asasi manusia sesuai dengan konstitusi dan undang-undang yang berlaku, namun kurangnya pemahaman masyarakat tentang perlindungan data pribadi serta langkah-langkah keamanan yang tepat sering menjadi penyebab utama terjadinya kejahatan siber.Program Pengabdian Masyarakat oleh dosen Fakultas Sains dan Teknologi Universitas Labuhanbatu di SMK 2 Rantau Utara bertujuan untuk memberikan pemahaman mengenai pentingnya melindungi data pribadi dari ancaman dunia siber. Kegiatan ini mencakup edukasi tentang konsep dasar keamanan cyber, penggunaan fitur backup, pengelolaan Personal Identification Number (PIN), penerapan Two-Factor Authentication (2FA), dan mengenali serta memahami penipuan digital. Selain meningkatkan kesadaran dan literasi digital, kegiatan ini juga memberikan solusi teknis untuk melindungi data pribadi agar terhindar dari ancaman keamanan informasi. Dengan pendekatan yang melibatkan berbagai pihak, diharapkan masyarakat dapat lebih bijaksana dalam menjaga dan melindungi data pribadi mereka di era digital.

Kata Kunci: *Cyber, Keamanan, Data Pribadi*

Abstract

Personal data theft through services that require personal data has become a hot topic. As a country of law, Indonesia is obliged to protect human rights in accordance with the

constitution and applicable laws, but the lack of public understanding of personal data protection and appropriate security measures is often the main cause of cybercrime. The Community Service Program by lecturers from the Faculty of Science and Technology, Labuhanbatu University at SMK 2 Rantau Utara aims to provide an understanding of the importance of protecting personal data from cyber threats. This activity includes education on the basic concepts of cyber security, the use of backup features, managing Personal Identification Numbers (PINs), implementing Two-Factor Authentication (2FA), and recognizing and understanding digital fraud. In addition to increasing awareness and digital literacy, this activity also provides technical solutions to protect personal data from information security threats. With an approach that involves various parties, it is hoped that the public can be wiser in maintaining and protecting their personal data in the digital era.

***Keywords**: Cyber, Security, Personal Data*

Pendahuluan

Ramainya kasus pencurian data pribadi lewat layanan yang memerlukan data pribadi sedang hangat diperbincangkan. Sepanjang periode Januari hingga September 2022, setidaknya terdapat tujuh kasus pembobolan data pribadi. Kasus pertama terjadi pada awal tahun dengan kebocoran data Bank Indonesia. Masih di bulan yang sama, terjadi kebocoran data pasien rumah sakit. Kasus ketiga melibatkan data pelamar kerja di PT. Pertamina Training and Consulting (PTC). Pada bulan Agustus, kebocoran data kembali terjadi dengan 21.000 data perusahaan yang bocor. Kasus berikutnya menimpa BUMN, yaitu PLN, dengan 17 juta data pelanggan yang bocor. Selain itu, terdapat kebocoran data 26 juta riwayat pengguna Indihome dan 252 GB data pelanggan Jasa Marga Toll Road Operator (JMTO). Ketujuh kasus tersebut belum termasuk kasus yang sedang hangat dibicarakan, yaitu Bjorka, yang diduga meretas 1,3 miliar data dari proses sim card dan 105 juta data penduduk dari KPU(Farhan. 2022).

Pembahasan tentang pencurian data pribadi semakin menjadi trending topic di kalangan masyarakat. Banyak yang mengaitkan kejadian ini dengan perundang-undangan di Indonesia dan status Indonesia sebagai negara hukum sesuai dengan UUD 1945 yang menyatakan bahwa Indonesia adalah negara hukum. Terus terjadinya pencurian data pribadi membuat masyarakat tidak tenang dan kurang percaya terhadap layanan yang ada. Sebagai negara hukum, Indonesia memiliki kewajiban melindungi hak asasi manusia dalam konstitusi, sebagaimana diatur dalam Pasal 28D ayat (1) UUD 1945. Berdasarkan Pasal 79 Ayat (1) UU No. 24/2013 tentang Perubahan Atas UU No. 23 Tahun 2006 tentang Administrasi Kependudukan, serta Pasal 58 PP No. 37/2007 tentang Pelaksanaan UU No. 23 Tahun 2006 tentang Administrasi Kependudukan, pemerintah berkewajiban melindungi kepentingan umum dari gangguan transaksi elektronik yang melanggar hukum dan berwenang melakukan pemutusan akses yang melanggar hukum(Farhan. 2022).

Kejahatan siber sering terjadi karena masyarakat kurang memahami perlindungan data pribadi, sehingga banyak yang mengabaikan dan menganggapnya sepele. Selain itu, masyarakat sering kesulitan membedakan data yang boleh dipublikasikan dan data yang tidak. Penting diingat, saat menginstal aplikasi, terutama media sosial, jangan gunakan data pribadi asli jika tidak perlu. Gunakan password yang unik dan sulit ditebak, hindari menginstal aplikasi yang tidak diperlukan, dan pastikan untuk mengetahui keamanan aplikasi sebelum memasukkan data pribadi (Yuda. 2023).

Menjaga aset informasi sangat penting agar data pribadi maupun institusi terhindar dari risiko keamanan informasi yang dapat menyebabkan kerugian terstruktur. Misalnya, malware yang berjalan di latar belakang aplikasi atau kelalaian pengguna dalam memasang aplikasi tertentu sulit terdeteksi. Oleh karena itu, langkah yang tepat diperlukan untuk menghindari atau menyelesaikan masalah ini dengan baik. Di era society 5.0, pemahaman dan solusi terhadap keamanan informasi, khususnya keamanan siber, sangat penting. Jika tidak dilakukan, ancaman akan semakin meningkat. Upaya teknis terus dilakukan meskipun tidak selalu sempurna, seperti pemeliharaan perangkat keras, penerapan aturan hukum, serta prosedur dan panduan pelaksanaan(Nur Isnaini et al. n.d. 2024).

Fungsi utama keamanan siber adalah melindungi sistem komputer dan data dari ancaman atau serangan digital. Ini mencakup berbagai jenis keamanan, seperti keamanan jaringan, aplikasi, endpoint, cloud, dan data, dengan tujuan menjaga kerahasiaan, integritas, dan ketersediaan data serta sistem komputer. Selain itu, keamanan siber juga melibatkan edukasi dan kesadaran pengguna tentang praktik keamanan siber yang baik, termasuk pelatihan tentang ancaman siber, penggunaan kata sandi yang aman, identifikasi serangan phishing, dan tindakan keamanan lainnya untuk mengurangi risiko. Teknologi akan efektif jia penggunaannya disesuaikan dengan nilai-nilai masyarakat dan peraturan nasional yang melindungi masyarakat dari dampak negatif(Indra Wijaya et al. 2023).

Metode Pelaksanaan

Dalam pelaksamaan program Pengabdian Masyarakat ini, para dosen yang berupa Ketua dan Anggota dari Fakultas Sains dan Teknologi Universitas Labuhanbatu bekerjasama dengan sekolah SMK 2 Rantau Utara. Pelaksanaan Pengabdian ini bertujuan untuk memberikan pemahaman kepada murid-murid SMK 2 Rantau Utara tentang pentingnya melindungi data pribadi dari dunia cyber. Keamanan data pribadi dalam dunia internet sudah seharusnya dilindungi sehingga tidak semua orang dapat melihatnya dapat mendapatkannya, dalam dunia cyber penyalahgunaan data pribadi seseorang dapat berakibat fatal dan menyebabkan kerugian pada berbagai pihak. Program pengabdian masyrakat ini dilakukan pada kelas salah satu 2 SMK 2 Rantau Utara, Dimana jumlah siswa dalam satu kelas tersebut adalah 37 siswa. Sedangkan jumlah keseluruhan siswa pada SMK 2 Rantau Utara adalah 986 siswa yang terbagi dari siswa kelas 1, 2 dan 3 dengan berbagai jurusan

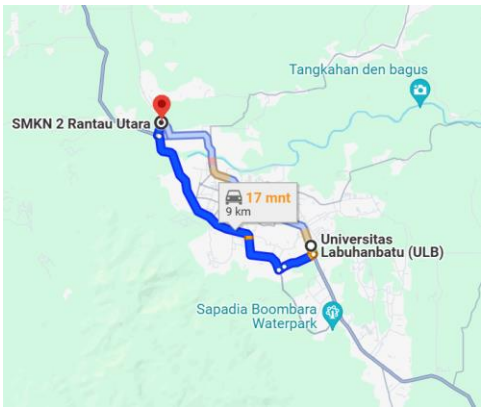
Tabel 1. Tahap pelaksanaan Kegiatan Kepada Masyarakat

No.	Tahap Kegiatan	Deskripsi
1.	Persiapan	-Menjalin kerja sama kepada SMK 2 Rantau Utara sebagai partner kegiatan Pengabdian Kepada Masyarakat -Menyiapkan Materi tentang Pelatihan Basic Cyber Security untuk Keamanan dan Perlindungan Data Pribadi di Dunia Digital
2.	Pelaksanaan	-Memaparkan materi tentang keamanan dan perlindungan data pribadi dari dunia cyber -Pelatihan basic cyber security

Tempat kegiatan

Tempat pelaksanaan kegiatan Pengabdian Kepada Masyarakat ini berada di SMK 2 Rantau Utara, yang berjarak 9 kilo meter dari Universitas Labuhanbatu. Lokasi sekolah terletak pada Jl. Wr. Supratman No. 01 A Rantauprapat, Kecamatan Rantau Utara, Kabupaten Labuhan Batu, Sumatera Utara**.**

Letak Geografis



Gambar 1. Letak Geografis SMK 2 Rantau Utara

Dokumentasi Kegiatan Pengabdian Kepada Masyarakat

Gambar 2. Kegiatan PMK Basic Cyber Security

Gambar 3. Foto Bersama

Hasil dan Pembahasan

Kegiatan Pengabdian Kepada Masyarakat di Sekolah SMK 2 Rantau Utra, merupakan salah satu bentuk tridarma perguruan tinggi yang dilakukan oleh pihak Universitas Labuhanbatu setiap semesternya. Kegiatan ini bersifat memberikan kontribusi secara langsung kepada masyarakat yang berada di sekitar Universitas Labuhanbatu.

Table 2. Susunan acara

No.	Waktu	Kegiatan
1.	09:00-09:10 WIB	Pembukaan
2.	09.10-09:30 WIB	Sambutan -Kepala Sekolah -Ketua PKM
3.	09:30-11:00	Pemaparan Materi dan Pelatihan -Memahami Cyber Security

No.	Waktu	Kegiatan
		-Memahami dan Melindungi Data dengan Fitur Backup -Memahami dan Melindungi Personal Identification Number (PIN) -Memahami dan Melindungi Two-Factor Authentication (2FA) -Mengenali dan Memahami Penipuan Digital
4.	11:00-11:30	Tanya Jawab
5.	11:30-11:45	Penutup

Menyampaikan materi tentang Cybersecurity

Cyber Security adalah upaya untuk melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman, yang juga dikenal sebagai keamanan teknologi informasi. Menurut ISACA, terdapat tiga konsep utama dalam keamanan siber (Samudra, Hidayat, and Wahyu 2023):

1. **Kerahasiaan**: Melindungi informasi dari akses atau pengungkapan yang tidak sah.
2. **Integritas**: Menjamin bahwa data yang rusak segera diperbaiki untuk mempertahankan keakuratannya.
3. **Ketersediaan**: Menjamin bahwa informasi dan sistem selalu tersedia untuk digunakan sesuai kebutuhan.

Keamanan siber juga bertujuan untuk melindungi data akun pengguna dan membatasi hak akses pengguna.

Untuk mendukung kebebasan berekspresi di internet secara aman dan bijaksana, beberapa pendekatan yang dapat dilakukan adalah:

1. Mengembangkan konten online yang positif, bermanfaat, dan menarik dari, oleh, dan untuk anak-anak, remaja, serta masyarakat lokal.
2. Menerapkan inisiatif penyaringan mandiri di internet pada tingkat keluarga (rumah) dan pendidikan (sekolah).
3. Meningkatkan literasi digital dan perlindungan anak secara online melalui dialog dan kerja sama multistakeholder yang inklusif, setara, transparan, dan akuntabel dalam kerangka Tata Kelola Internet.

Memahami dan Melindungi Data dengan Fitur Backup

1. Data dapat diakses dan disimpan melalui aplikasi seluler, memungkinkan pengguna untuk mengakses dan memulihkan file cadangan dengan mudah. Dengan teknologi cloud computing, pencadangan jaringan menjadi lebih efisien. Pengguna dapat memastikan keamanan data dengan mengenkripsi data yang digunakan, dikirim, dan

disimpan. Penyimpanan data di sistem cloud memastikan data tetap aman dari kerusakan perangkat keras.

2. Layanan penyimpanan cloud yang sering digunakan antara lain Google Drive dan OneDrive dari Microsoft. Dengan akun di layanan tersebut, data dapat disimpan dengan aman dan hanya bisa diakses oleh pemilik akun. Kapasitas penyimpanan juga bisa ditingkatkan sesuai kebutuhan.
3. Untuk data pekerjaan, layanan penyimpanan cloud menjadi solusi populer karena aman dari kerusakan perangkat keras. Layanan seperti Google Drive dan OneDrive memudahkan pencadangan data pekerjaan dengan hanya membuat akun. Pastikan untuk menggunakan kata sandi yang kuat agar data di penyimpanan online tetap aman dari akses tidak sah

Memahami dan Melindungi Personal Identification Number (PIN)

Untuk memudahkan penggunaan berbagai platform digital, kita seringkali menggunakan Personal Identification Number (PIN) yang sama. Namun, penting untuk menghindari memilih kombinasi angka yang mudah ditebak, seperti tanggal dan tahun lahir. Pilihlah kombinasi angka yang kompleks agar sulit diprediksi oleh orang lain.

Beberapa langkah untuk melindungi PIN Anda adalah sebagai berikut:

1. **Buat PIN yang Sulit Ditebak**: Pilih kombinasi angka yang kompleks dan tidak mudah ditebak oleh orang lain.
2. **Jangan Menuliskan PIN di Tempat Terlihat**: Hindari menuliskan PIN di kartu identitas atau pada secarik kertas yang disimpan di dompet. Ini penting agar jika dompet hilang atau tertinggal, PIN tetap aman.
3. **Gunakan PIN yang Berbeda untuk Keperluan Berbeda**: Buat PIN yang berbeda untuk berbagai keperluan agar tingkat keamanannya lebih tinggi.

Memahami dan Melindungi Two-Factor Authentication (2FA)

Aplikasi email saat ini sangat penting dalam berbagai aktivitas pekerjaan. Two-Factor Authentication (2FA) digunakan untuk memastikan bahwa pengguna yang login adalah pengguna yang sah dengan menambahkan lapisan keamanan ekstra, seperti pertanyaan tambahan atau permintaan kode verifikasi.

Proses 2FA melibatkan identifikasi pengguna berdasarkan dua faktor: informasi yang hanya diketahui oleh pengguna dan sistem. Langkah pertama biasanya melibatkan login dengan username atau email. Setelah itu, pengguna diminta untuk memasukkan kode verifikasi yang dikirim melalui SMS atau notifikasi ke perangkat seluler mereka untuk memastikan identitasnya.

Dengan menerapkan 2FA, keamanan akun ditingkatkan karena memerlukan verifikasi tambahan selain informasi login dasar.

Mengenali dan Memahami Penipuan Digital

Phishing adalah jenis penipuan yang menipu korban dengan membuat mereka percaya bahwa informasi yang mereka berikan diterima oleh pihak yang sah. Phishing biasanya

dilakukan dengan menduplikasi situs web atau aplikasi bank atau penyedia layanan. Ketika kita memasukkan informasi rahasia, pelaku akan mencuri uang kita. Penipuan phishing dilakukan oleh individu yang menghubungi korban potensial melalui email, telepon, atau pesan teks dengan menyamar sebagai lembaga resmi. Mereka sering meminta data sensitif seperti identitas pribadi, detail perbankan, kartu kredit, dan kata sandi. Informasi yang mereka peroleh dapat digunakan untuk mengakses akun penting, yang bisa mengakibatkan pencurian identitas dan kerugian finansial.

Phishing tidak hanya dilakukan melalui email dan situs web, tetapi juga melalui suara (vishing), SMS (smishing), dan berbagai teknik lain yang terus berkembang. Media sosial yang terhubung ke internet juga sering menjadi sarana phishing. Misalnya, kita mungkin menerima pesan dari seseorang yang mengaku sebagai teman lama atau pegawai bank yang memberi tahu bahwa kita telah memenangkan hadiah. Korban kemudian dipandu hingga tanpa sadar membocorkan data pribadi mereka.

Ada beberapa tanda umum phishing, seperti email yang berisi tautan ke situs web phishing atau permintaan kata sandi dan login. Untuk mendeteksi phishing, kita harus waspada terhadap email, SMS, atau situs web yang mencurigakan. Selain itu, menggunakan perangkat lunak seperti PhiGARo atau Honeypot dapat membantu mendeteksi serangan phishing pada perangkat digital kita. Perangkat lunak ini terus dikembangkan oleh ahli siber untuk menghadapi serangan phishing yang semakin canggih.

Kesimpulan

SMK 2 Rantau Utara merupakan salah satu sekolah menengah atas yang berada di lingkup Labuhanbatu. Mengingat saat ini lebih dari setengah waktu mereka dihabiskan di dunia internet maka sangat penting untuk diajarkan kepada para murid sekolah menengah atas tentang pentingnya perlindungan data diri pribadi. Hal ini juga diharapkan untuk menjadikan para murid menjadi lebih awas terhadap kerahasiaan data dan bagaimana keamanan serta melindunginya, bukan hanya untuk data dirinya tapi juga bagaimana mampu menyebarkannya dengan cakupan paling kecil terhadap keluarga mereka. Bagaimana tentang keamanan keamanan dan perlindungan data pribadi dari dunia Cyber.

Daftar Pustaka

Afif Farhan, Cindy. 2022. "*Seminar Nasional Hasil Penelitian Dan Pengabdian Kepada Masyarakat 2022 Penguatan Ekonomi Bangsa Melalui Inovasi Digital Hasil Penelitian Dan PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA"*.

Indra Wijaya, Yusup, Muhammad Saidi Rahman, Herry Adi Chandra, and Muhammad Amin. 2023. "Pelatihan Cyber Security Untuk Menjaga Keamanan Dan Privasi Siswa Smk Negeri 4 Banjarmasin Cyber Security Training To Guarantee Security And Privacy Of Students Of Vocational School 4 Banjarmasin." 1(4): 68–72. doi:10.59024/jnb.v1i4.243.

Nur Isnaini, Khairunnisak, Hernan Febri Rahmatullah, Anisaa K Qothrunnada, Didit Suhartono, MKom Fakultas Ilmu Komputer, Amikom Purwokerto, Jl Letjend Pol Soemarto, et al. 3 *(Januari) 2024, Hal*.

Samudra, Yuda, Amin Hidayat, and Meidy Fajar Wahyu. 2023. "AMMA : Jurnal Pengabdian Masyarakat Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital." *Januari* 1(12). https://journal.mediapublikasi.id/index.php/amma.

Tandirerung, Veronika Asri, dkk. 2023. "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas." 1(2).