

Sosialisasi Pentingnya Cyber Security untuk Menjaga Keamanan Online Studi Fakultas Teknik Informatika Universitas Ibnu Sina

Nofri Yudi Arifin¹, Okta Veza², Albertus Laurensius Setyabudhi³, Atman Lucky
Fernandes⁴

¹⁻⁴Fakultas Teknik, Universitas Ibnu Sina Batam, Indonesia

Alamat: Lubuk Baja Kota, Kec. Lubuk Baja, Kota Batam, Kepulauan Riau 29444, Indonesia

Korespondensi penulis: nofri.yudi@uis.ac.id

Article History:

Received: Juli 08,2024;

Revised: Juli 25,2024;

Accepted: Agustus 22,2024;

Online Available: Agustus 24,2024;

Keyword: Cybersecurity,
Socialization, Digital Education,
Cyber Risks, Information Protection.

Abstract. In the rapidly evolving digital era, cybersecurity has become increasingly crucial as information technology permeates nearly every aspect of life. Students from the Faculty of Informatics Engineering, known for their tendency to adopt new technologies early, face high risks from constantly evolving and complex cyber threats. The importance of cybersecurity cannot be overstated, and educating and socializing safe technology practices are key to protecting oneself from cyberattacks. This community service aims to explore the effectiveness of cybersecurity awareness among students of the Faculty of Informatics Engineering at Ibnu Sina University, focusing on efforts to enhance understanding and protection against online threats. The activities include workshops and involve several stages, from planning to evaluation and reflection. The results indicate a significant improvement in students' understanding and proactive attitudes towards online security practices. Evaluation suggests that these awareness efforts effectively change students' behaviors to enhance digital safety. Recommendations for the future include increasing collaboration between universities and industry to provide additional resources and training. This initiative not only benefits students directly but also serves as a foundation for developing more comprehensive and sustainable cybersecurity education strategies in academic environments.

Abstrak.

Dalam era digital yang terus berkembang pesat, keamanan cyber menjadi semakin penting karena teknologi informasi telah merasuk ke dalam hampir semua aspek kehidupan. Mahasiswa Fakultas Teknik Informatika, dengan kecenderungan untuk menjadi early adopter teknologi baru, memiliki risiko tinggi terkena ancaman keamanan cyber yang terus berubah dan semakin kompleks. Pentingnya cyber security tidak dapat diabaikan, dan edukasi serta sosialisasi mengenai praktik-praktik yang aman dalam penggunaan teknologi menjadi kunci dalam melindungi diri dari serangan cyber. Pengabdian masyarakat ini bertujuan untuk menjelajahi efektivitas sosialisasi tentang cyber security di kalangan mahasiswa Fakultas Teknik Informatika Universitas Ibnu Sina, dengan fokus pada upaya meningkatkan pemahaman dan perlindungan terhadap ancaman online. Kegiatan ini dilakukan dalam bentuk workshop dan melibatkan beberapa tahapan, mulai dari perencanaan hingga evaluasi dan refleksi. Hasil kegiatan menunjukkan peningkatan signifikan dalam pemahaman dan sikap proaktif mahasiswa terhadap praktik keamanan online. Evaluasi mengindikasikan bahwa sosialisasi ini efektif dalam mengubah perilaku mahasiswa menjadi lebih aman secara digital. Rekomendasi untuk masa depan meliputi peningkatan kolaborasi antara universitas dan industri untuk menyediakan sumber daya dan pelatihan tambahan. Kegiatan ini tidak hanya memberikan manfaat langsung kepada mahasiswa tetapi juga menjadi dasar untuk pengembangan strategi pendidikan cyber security yang lebih komprehensif dan berkelanjutan di lingkungan akademis.

Kata kunci: Keamanan Cyber, Sosialisasi, Edukasi Digital, Risiko Cyber, Perlindungan Informasi.

1. LATAR BELAKANG

Dalam era digital yang terus berkembang pesat, Keamanan siber semakin menjadi isu penting di era digital saat ini. Dalam beberapa tahun terakhir, kita telah melihat peningkatan jumlah dan kompleksitas serangan siber yang mengancam sistem komputer dan data di seluruh dunia [1]. Kemajuan dalam teknologi informatika telah melahirkan internet, fenomena yang telah berkembang menjadi salah satu hal paling penting dalam kehidupan manusia. Internet menjadi media atau wadah terbesar dan paling cepat berkembang untuk kegiatan komersial di seluruh dunia, dengan jaringan yang luas dan bersifat "tanpa batas".

Seiring dengan perkembangan internet, terdapat juga peningkatan yang pesat dalam tindakan-tindakan anti-sosial dan kejahatan melalui jaringan internet yang dikenal sebagai kejahatan Siber. Kebutuhan akan keamanan siber semakin krusial karena ketergantungan kita pada Teknologi Informasi dan Komunikasi (TIK) di berbagai aspek masyarakat kita yang bersifat siber-fisik. Edukasi dan sosialisasi mengenai praktik-praktik yang aman dalam penggunaan teknologi menjadi kunci dalam melindungi diri. Melalui sosialisasi yang efektif, masyarakat dapat meningkatkan kesadaran akan risiko yang ada dan mengadopsi tindakan preventif yang tepat untuk mengurangi kerentanan terhadap serangan cyber.

Keamanan cyber telah menjadi perhatian utama di era digital saat ini, di mana teknologi informasi memainkan peran sentral dalam berbagai aspek kehidupan. Pengamanan data tidak hanya penting untuk melindungi data sensitif di server perusahaan besar, tetapi juga harus diterapkan untuk semua hal yang terkait dengan teknologi komputer secara umum. Terlebih lagi, Indonesia merupakan negara yang menghadapi risiko serangan cyber yang signifikan.

Pengabdian masyarakat ini bertujuan untuk menjelajahi efektivitas sosialisasi tentang cyber security di kalangan mahasiswa fakultas teknik informatika, dengan fokus pada upaya meningkatkan pemahaman dan perlindungan terhadap ancaman online. Studi ini akan mengidentifikasi tantangan utama dalam menerapkan praktik keamanan digital, serta eksplorasi terhadap dampak dari sosialisasi ini terhadap sikap dan perilaku mahasiswa dalam menghadapi risiko cyber.

2. KAJIAN TEORITIS

1. Pentingnya Cyber Security

Cyber security atau keamanan siber adalah praktik melindungi sistem, jaringan, dan program dari serangan digital. Serangan ini biasanya bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu proses

bisnis yang normal. Dalam era digital yang semakin kompleks, pentingnya cyber security tidak dapat diabaikan, mengingat teknologi informasi telah merasuk ke hampir semua aspek kehidupan manusia, termasuk pendidikan, bisnis, kesehatan, dan pemerintahan.

2. Ancaman Cyber

Ancaman cyber bisa datang dalam berbagai bentuk, termasuk malware, phishing, ransomware, dan serangan denial-of-service (DoS). Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mendapatkan akses tidak sah ke sistem komputer. Phishing adalah usaha untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan rincian kartu kredit dengan menyamar sebagai entitas yang tepercaya dalam komunikasi elektronik. Ransomware adalah jenis malware yang mengancam untuk mempublikasikan data korban atau memblokir akses ke data tersebut kecuali tebusan dibayarkan. Serangan DoS bertujuan untuk membuat layanan online tidak tersedia dengan membanjiri situs web atau jaringan dengan lalu lintas yang berlebihan[8].

3. METODE PENELITIAN

Metode kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk workshop untuk meningkatkan literasi penilaian mahasiswa di Fakultas Teknik Informatika Universitas Ibnu Sina dengan langkah-langkah kegiatan sebagai berikut:

Dalam perencanaan kegiatan untuk workshop peningkatan literasi penilaian mahasiswa di Fakultas Teknik Informatika Universitas Ibnu Sina, langkah-langkah yang dilakukan termasuk koordinasi dengan tim PKM untuk pembagian tugas, berkomunikasi dengan pihak fakultas untuk sinkronisasi kegiatan, menyusun proposal dan materi kegiatan, serta merancang instrumen monitoring yang mencakup semua tahapan dari perencanaan, pelaksanaan, evaluasi, hingga tindak lanjut program.

Setelah perencanaan disusun, langkah selanjutnya adalah melaksanakan kegiatan. Kegiatan ini direncanakan dilaksanakan dalam satu hari dengan jadwal pelaksanaan yang telah ditetapkan. Pendekatan sosial diterapkan untuk memastikan kelancaran pelaksanaan kegiatan pengabdian masyarakat. Metodologi pelaksanaan pengabdian masyarakat ini mencakup langkah-langkah terstruktur untuk memastikan efektivitasnya.

Kegiatan pengabdian ini fokus pada masalah keamanan teknologi dalam penggunaan perangkat pribadi, serta cara-cara untuk menghadapinya. Solusi yang ditawarkan adalah

peningkatan pemahaman tentang kejahatan di dunia maya dan strategi menghadapinya, yang akan membantu mitra dalam menjaga keamanan perangkat pribadinya.

Refleksi merupakan kegiatan analisis, sintesis, interpretasi, dan penjelasan terhadap semua informasi yang diperoleh dari pelaksanaan tindakan. Tindak lanjut dilakukan jika hasil refleksi menunjukkan bahwa tujuan perbaikan pembelajaran belum tercapai sesuai harapan. Kegiatan refleksi dalam PKM ini didasarkan pada hasil monitoring dan evaluasi keterlaksanaan serta pencapaian tujuan. Bentuk refleksi dalam kegiatan ini meliputi analisis kekurangan selama pelaksanaan, evaluasi keterlaksanaan, dan pencapaian tujuan.

4. HASIL DAN PEMBAHASAN

Hasil

Kegiatan pengabdian masyarakat ini menunjukkan peningkatan signifikan dalam pemahaman mahasiswa Fakultas Teknik Informatika Universitas Ibnu Sina mengenai pentingnya cyber security. Melalui workshop yang diselenggarakan, mahasiswa dapat memahami risiko yang terkait dengan penggunaan teknologi digital serta strategi untuk mengamankan informasi pribadi mereka. Evaluasi terhadap kegiatan ini menunjukkan adanya peningkatan dalam sikap proaktif dalam menerapkan praktik keamanan online, seperti penggunaan kata sandi yang kuat dan pembaruan perangkat lunak secara teratur.

Pembahasan mengenai hasil ini meliputi analisis terhadap dampak sosialisasi cyber security terhadap perilaku mahasiswa, serta tantangan yang dihadapi dalam implementasi praktik keamanan digital di lingkungan kampus. Diskusi juga mengarah pada rekomendasi untuk memperkuat pendidikan tentang cyber security sebagai bagian integral dari kurikulum Teknik Informatika, serta pentingnya kolaborasi antara universitas dan industri untuk menyediakan sumber daya dan pelatihan tambahan bagi mahasiswa dalam menghadapi ancaman cyber yang semakin kompleks.



Gambar 1. Sosialisasi Kegiatan

Pembahasan

Untuk memastikan keberhasilan kegiatan ini, persiapan yang matang dilakukan sebelum pelaksanaan PKM. Ini mencakup melakukan briefing kepada seluruh peserta mahasiswa yang turut serta dalam kegiatan. Solusi yang diimplementasikan dalam kegiatan ini terdiri dari empat tahap penting: perencanaan, pelaksanaan, monitoring dan evaluasi, serta refleksi dan tindak lanjut. Pendekatan ini membantu memastikan bahwa kegiatan berjalan dengan lancar dan mencapai hasil yang diharapkan.

Khalayak sasaran dari kegiatan pengabdian kepada masyarakat ini adalah mahasiswa Fakultas Teknik Informatika Universitas Ibnu Sina Batam. Mereka menjadi fokus utama dalam upaya penyampaian materi dan solusi yang telah disiapkan. Tempat pelaksanaan kegiatan ini adalah di Fakultas Teknik Informatika Universitas Ibnu Sina, dan kegiatan ini berlangsung pada hari Senin, 1 Juli 2024. Dengan demikian, waktu dan lokasi pelaksanaan telah ditentukan dengan jelas untuk memastikan kesuksesan dan efektivitas kegiatan ini dalam memberikan manfaat kepada khalayak sasaran yang dituju.

5. KESIMPULAN DAN SARAN

Kegiatan pengabdian masyarakat ini berhasil meningkatkan pemahaman mahasiswa Fakultas Teknik Informatika Universitas Ibnu Sina mengenai pentingnya cyber security. Workshop yang diselenggarakan berhasil memberikan wawasan mendalam tentang risiko yang terkait dengan penggunaan teknologi digital serta strategi untuk melindungi informasi pribadi. Evaluasi menunjukkan peningkatan signifikan dalam sikap proaktif mahasiswa dalam menerapkan praktik keamanan online, seperti penggunaan kata sandi yang kuat dan pembaruan

perangkat lunak secara teratur. Meskipun terdapat tantangan dalam sinkronisasi dan koordinasi, pendekatan yang terstruktur dan refleksi yang dilakukan memastikan bahwa kegiatan ini berjalan efektif dan mencapai hasil yang diharapkan.

Untuk meningkatkan efektivitas kegiatan di masa mendatang, disarankan agar pendidikan cyber security diintegrasikan ke dalam kurikulum Teknik Informatika, memperbanyak kegiatan sosialisasi berkala, serta menjalin kerjasama dengan industri untuk menyediakan sumber daya tambahan dan pelatihan praktis. Selain itu, penting untuk memanfaatkan teknologi terbaru dalam kegiatan sosialisasi dan melakukan evaluasi serta monitoring secara rutin untuk memastikan tujuan tercapai dan melakukan perbaikan berkelanjutan. Dengan penerapan saran-saran ini, diharapkan kesadaran dan keamanan online di kalangan mahasiswa dapat terus ditingkatkan.

DAFTAR REFERENSI

- Whitman, M. E., & Mattord, H. J. (2018). Principles of information security. Cengage Learning.
- Triandi, B. (2019). Keamanan informasi secara aksiologi dalam menghadapi era revolusi industri 4.0. JURIKOM (Jurnal Riset Komputer), 6(5), 477-483.
- Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen keamanan cyber di era digital. Journal of Business and Entrepreneurship, 11(1), 23-33.
- Supendar, H., & Handrianto, Y. (2017). Simple queue dalam menyelesaikan masalah manajemen bandwidth pada mikrotik bridge. Bina Insani ICT Journal, 4(1), 21-30.
- Stallings, W. (2017). Network security essentials: Applications and standards. Pearson.
- Purnomo, M. F. E., Priyono, W. A., Sari, S. N., Ambarwati, R., & Wulandari, A. (2012). Implementasi algoritma kriptografi RC4 pada DSP TMS320C6713 sebagai pendukung sekuritas jaringan komunikasi voice over internet protocol (VoIP). Jurnal EECCIS (Electrics, Electronics, Communications, Controls, Informatics, Systems), 6(2), 183-188.
- Manurung, J., Sihombing, A. P. E., & Pandiangan, B. (2023). Sosialisasi dan edukasi tentang keamanan data dan privasi di era digital untuk meningkatkan kesadaran dan perlindungan masyarakat. Jurnal Pengabdian Masyarakat Nauli, 2(1), 1-7.
- Aziz, A. (2023). Pentingnya pengetahuan cybersecurity untuk publik dan negara. Prosiding Sains dan Teknologi, 2(1), 75-82.