

Nanggroe : Jurnal Pengabdian Cendikia
Volume 4, Nomor 9, December 2025, P. 222-227
Licenced by CC BY-SA 4.0
e-ISSN: [2986-7002](#)
DOI: <https://doi.org/10.5281/zenodo.19650085>

Upaya Peningkatan Kesadaran *Cyber Crime* melalui Penyuluhan pada Organisasi Mahasiswa Universitas Nahdlatul Ulama Cirebon

Efforts to Increase Cyber Crime Awareness through Counseling for Student Organizations at Nahdlatul Ulama University of Cirebon

Asep Hermawan¹, Agustiana², Amir Machmud³

^{1,2,3}Universitas Nahdlatul Ulama Cirebon

Email: asephermawanfarmasi2021@gmail.com¹, agustiana@unucirebon.ac.id²,
amirmachmudtea91@gmail.com³

Abstrak

Perkembangan teknologi informasi yang pesat telah membawa berbagai kemudahan dalam kehidupan, namun juga menimbulkan potensi kejahatan siber (*cyber crime*) yang semakin meningkat. Mahasiswa sebagai pengguna aktif teknologi digital menjadi salah satu kelompok yang rentan terhadap berbagai bentuk kejahatan siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman organisasi mahasiswa mengenai *cyber crime* serta upaya pencegahannya. Metode yang digunakan meliputi penyuluhan, diskusi interaktif, dan simulasi kasus. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta terkait jenis-jenis *cyber crime*, dampak yang ditimbulkan, serta langkah-langkah preventif yang dapat dilakukan. Dengan demikian, kegiatan ini diharapkan mampu membentuk perilaku digital yang lebih bijak dan aman di kalangan mahasiswa.

Kata kunci: *cyber crime, penyuluhan, organisasi mahasiswa, literasi digital*

Abstract

The rapid development of information technology has brought various conveniences to daily life; however, it has also led to an increasing potential for cybercrime. Students, as active users of digital technology, are among the groups most vulnerable to various forms of cybercrime. This community service activity aims to enhance the awareness and understanding of student organizations regarding cybercrime and its preventive measures. The methods used include counseling, interactive discussions, and case simulations. The results of the activity show an improvement in participants' understanding of the types of cybercrime, their impacts, and the preventive steps that can be taken. Thus, this activity is expected to foster more responsible and secure digital behavior among students.

Keywords: *cybercrime, counseling, student organizations, digital literacy*

Article Info

Received date: 15 December 2025

Revised date: 20 December 2025

Accepted date: 25 December 2025

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa transformasi yang sangat signifikan dalam berbagai aspek kehidupan manusia. Kemajuan internet, perangkat digital, serta aplikasi berbasis daring telah menciptakan kemudahan dalam mengakses informasi, berkomunikasi, serta melakukan berbagai aktivitas secara efisien. Di lingkungan pendidikan tinggi, mahasiswa menjadi salah satu kelompok yang paling aktif dalam memanfaatkan teknologi digital. Aktivitas akademik seperti pembelajaran daring, pencarian referensi ilmiah, hingga komunikasi antar mahasiswa kini sangat bergantung pada teknologi digital. Namun demikian, di balik berbagai kemudahan tersebut, terdapat tantangan serius yang muncul, salah satunya adalah meningkatnya ancaman kejahatan siber atau *cyber crime* (Holt et al., 2018).

Cyber crime merupakan bentuk kejahatan yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet sebagai sarana utama. Kejahatan ini mencakup berbagai tindakan ilegal seperti pencurian data pribadi, penipuan online, peretasan sistem, penyebaran malware, serta berbagai

bentuk kejahatan berbasis rekayasa sosial seperti phishing (UNODC, 2020). Seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi digital, kejahatan siber juga mengalami perkembangan yang pesat, baik dari segi jumlah kasus maupun kompleksitas metode yang digunakan oleh pelaku (Organization for Economic Co-operation and Development, 2021). Hal ini menjadikan cyber crime sebagai salah satu ancaman global yang memerlukan perhatian serius dari berbagai pihak, termasuk institusi pendidikan.

Mahasiswa sebagai generasi yang lahir dan tumbuh di era digital sering kali dianggap memiliki kemampuan yang baik dalam menggunakan teknologi. Namun, kemampuan teknis tersebut tidak selalu diiringi dengan pemahaman yang memadai mengenai keamanan digital. Banyak mahasiswa yang masih kurang memahami risiko yang dapat timbul dari penggunaan teknologi, seperti kebocoran data pribadi, penyalahgunaan informasi, serta berbagai bentuk penipuan digital. Kondisi ini menunjukkan bahwa literasi digital, khususnya dalam aspek keamanan siber, masih perlu ditingkatkan (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022).

Rendahnya tingkat kesadaran terhadap keamanan digital menjadi salah satu faktor utama yang menyebabkan meningkatnya kasus cyber crime di kalangan mahasiswa. Banyak pengguna internet yang masih menggunakan kata sandi yang lemah, mengakses tautan yang tidak aman, serta membagikan informasi pribadi secara berlebihan di media sosial. Perilaku tersebut meningkatkan risiko menjadi korban kejahatan siber. Penelitian menunjukkan bahwa aktivitas online yang tidak terkontrol dapat meningkatkan potensi viktimisasi, terutama pada kelompok usia muda (Marcum et al., 2014). Oleh karena itu, diperlukan upaya yang sistematis untuk meningkatkan kesadaran dan pemahaman mahasiswa mengenai pentingnya keamanan digital.

Dalam konteks ini, organisasi mahasiswa memiliki peran yang sangat strategis. Organisasi mahasiswa tidak hanya berfungsi sebagai wadah pengembangan minat dan bakat, tetapi juga sebagai sarana edukasi dan penyebaran informasi. Melalui kegiatan yang terorganisir, organisasi mahasiswa dapat menjadi agen perubahan yang mampu meningkatkan kesadaran anggota dan masyarakat kampus secara luas. Dengan memanfaatkan jaringan sosial yang dimiliki, organisasi mahasiswa dapat menyebarkan informasi mengenai cyber crime secara lebih efektif dan berkelanjutan.

Salah satu pendekatan yang dapat digunakan untuk meningkatkan kesadaran mahasiswa adalah melalui kegiatan penyuluhan. Penyuluhan merupakan metode edukasi yang bertujuan untuk memberikan informasi, meningkatkan pengetahuan, serta membentuk sikap dan perilaku yang lebih baik (Notoatmodjo, 2018). Dalam konteks cyber crime, penyuluhan dapat digunakan untuk memberikan pemahaman mengenai jenis-jenis kejahatan siber, modus operandi pelaku, dampak yang ditimbulkan, serta langkah-langkah pencegahan yang dapat dilakukan. Dengan adanya penyuluhan, diharapkan mahasiswa dapat lebih memahami risiko yang ada serta mampu mengambil langkah-langkah preventif untuk melindungi diri.

Namun demikian, efektivitas penyuluhan tidak hanya ditentukan oleh materi yang disampaikan, tetapi juga oleh metode yang digunakan. Penyuluhan yang bersifat satu arah cenderung kurang efektif dalam meningkatkan pemahaman peserta. Sebaliknya, pendekatan yang interaktif dan partisipatif dinilai lebih mampu meningkatkan keterlibatan peserta serta memperkuat pemahaman mereka terhadap materi yang disampaikan (Bada et al., 2019). Oleh karena itu, dalam pelaksanaan kegiatan penyuluhan, perlu digunakan metode yang memungkinkan peserta untuk aktif berpartisipasi, seperti diskusi kelompok, simulasi kasus, serta sesi tanya jawab.

Universitas Nahdlatul Ulama Cirebon sebagai salah satu institusi pendidikan tinggi memiliki tanggung jawab dalam membekali mahasiswanya dengan pengetahuan dan keterampilan yang relevan dengan perkembangan zaman. Dalam menghadapi tantangan cyber crime, universitas perlu berperan aktif dalam meningkatkan literasi digital mahasiswa, khususnya dalam aspek keamanan siber. Organisasi mahasiswa di lingkungan universitas dapat menjadi mitra strategis dalam pelaksanaan kegiatan edukasi, termasuk penyuluhan mengenai cyber crime.

Kegiatan pengabdian kepada masyarakat yang dilakukan dalam penelitian ini merupakan salah satu bentuk kontribusi akademisi dalam meningkatkan kesadaran cyber crime di kalangan mahasiswa. Kegiatan ini dirancang dengan menggunakan pendekatan partisipatif, di mana peserta tidak hanya menjadi objek, tetapi juga subjek yang aktif dalam proses pembelajaran. Melalui pendekatan ini, diharapkan peserta dapat memperoleh pemahaman yang lebih mendalam serta mampu mengaplikasikan pengetahuan yang diperoleh dalam kehidupan sehari-hari.

Selain itu, kegiatan ini juga bertujuan untuk membangun kesadaran kolektif di kalangan mahasiswa mengenai pentingnya keamanan digital. Dengan meningkatnya kesadaran tersebut, diharapkan mahasiswa dapat menjadi agen perubahan yang mampu menyebarkan informasi dan edukasi kepada masyarakat yang lebih luas. Hal ini sejalan dengan peran mahasiswa sebagai agen perubahan yang memiliki tanggung jawab sosial dalam menciptakan lingkungan yang lebih aman dan berkelanjutan.

Dengan demikian, kegiatan penyuluhan cyber crime pada organisasi mahasiswa di Universitas Nahdlatul Ulama Cirebon menjadi sangat penting untuk dilakukan. Kegiatan ini tidak hanya bertujuan untuk meningkatkan pengetahuan, tetapi juga untuk membentuk sikap dan perilaku yang lebih bijak dalam penggunaan teknologi digital. Melalui upaya yang terencana dan berkelanjutan, diharapkan dapat tercipta lingkungan digital yang lebih aman, khususnya di kalangan mahasiswa.

METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan partisipatif dan edukatif dengan tujuan untuk meningkatkan kesadaran serta pemahaman mahasiswa mengenai cyber crime. Pendekatan partisipatif dipilih karena memberikan ruang bagi peserta untuk terlibat secara aktif dalam setiap tahapan kegiatan, sehingga proses pembelajaran menjadi lebih efektif (Sugiyono, 2019). Sementara itu, pendekatan edukatif digunakan untuk memberikan pemahaman konseptual dan praktis terkait cyber crime.

Pelaksanaan kegiatan ini dilakukan melalui beberapa tahapan yang terstruktur, yaitu tahap persiapan, pelaksanaan, dan evaluasi.

1. Tahap Persiapan

Tahap persiapan merupakan langkah awal yang sangat penting dalam pelaksanaan kegiatan pengabdian.

- a. Identifikasi Kebutuhan. Identifikasi kebutuhan dilakukan untuk mengetahui tingkat pemahaman awal mahasiswa mengenai cyber crime serta jenis informasi yang paling dibutuhkan. Proses ini dilakukan melalui observasi awal dan diskusi dengan perwakilan organisasi mahasiswa (Nasution, 2017).
- b. Penyusunan Materi. Materi penyuluhan disusun secara sistematis dan disesuaikan dengan kebutuhan peserta. Materi mencakup pengertian cyber crime, jenis-jenis cyber crime, serta langkah-langkah pencegahan berdasarkan literatur yang relevan (Holt et al., 2018; UNODC, 2020).
- c. Koordinasi dengan Mitra. Koordinasi dilakukan dengan pihak organisasi mahasiswa untuk memastikan kelancaran pelaksanaan kegiatan.

2. Tahap Pelaksanaan

Tahap pelaksanaan merupakan inti dari kegiatan pengabdian.

- a. Penyuluhan (Ceramah Interaktif). Penyampaian materi dilakukan secara interaktif untuk meningkatkan keterlibatan peserta. Metode ceramah interaktif dinilai efektif dalam proses pembelajaran orang dewasa (Notoatmodjo, 2018).
- b. Diskusi Kelompok. Peserta dibagi ke dalam kelompok kecil untuk mendiskusikan kasus cyber crime. Metode ini bertujuan untuk meningkatkan kemampuan analisis peserta (Sugiyono, 2019).
- c. Simulasi Kasus. Simulasi dilakukan untuk memberikan pengalaman praktis kepada peserta dalam menghadapi ancaman cyber crime.
- d. Tanya Jawab. Sesi ini bertujuan untuk memperdalam pemahaman peserta terhadap materi yang telah disampaikan.

3. Tahap Evaluasi

Evaluasi dilakukan untuk mengukur efektivitas kegiatan.

a. Pre-test dan Post-test. Digunakan untuk mengukur peningkatan pemahaman peserta sebelum dan sesudah kegiatan (Sugiyono, 2019).

b. Observasi. Observasi dilakukan untuk menilai tingkat partisipasi peserta selama kegiatan berlangsung.

c. Umpan Balik Peserta. Umpan balik digunakan untuk mengevaluasi kualitas pelaksanaan kegiatan dan sebagai bahan perbaikan ke depan.

4. Teknik Analisis Data. Data dianalisis secara deskriptif kualitatif untuk menggambarkan hasil kegiatan secara menyeluruh (Sugiyono, 2019).

HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat berupa penyuluhan cyber crime yang dilaksanakan pada organisasi mahasiswa di Universitas Nahdlatul Ulama Cirebon menunjukkan hasil yang cukup signifikan dalam meningkatkan kesadaran dan pemahaman peserta terhadap keamanan digital. Hasil ini diperoleh melalui beberapa instrumen evaluasi, yaitu pre-test dan post-test, observasi selama kegiatan berlangsung, serta umpan balik dari peserta.

1. Peningkatan Pemahaman Peserta

Berdasarkan hasil pre-test, diketahui bahwa sebagian besar peserta hanya memiliki pemahaman dasar mengenai cyber crime. Mayoritas peserta hanya mengenal istilah cyber crime secara umum tanpa mampu mengidentifikasi jenis-jenisnya secara spesifik. Hal ini menunjukkan bahwa literasi digital mahasiswa, khususnya dalam aspek keamanan siber, masih tergolong rendah. Kondisi ini sejalan dengan temuan bahwa tingkat literasi digital masyarakat Indonesia masih perlu ditingkatkan, terutama dalam hal keamanan informasi (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022). Setelah dilakukan penyuluhan, hasil post-test menunjukkan adanya peningkatan yang signifikan dalam pemahaman peserta. Peserta mulai mampu mengidentifikasi berbagai bentuk cyber crime seperti phishing, hacking, malware, dan penipuan online. Selain itu, peserta juga memahami bagaimana modus operandi pelaku dalam menjalankan aksinya, termasuk teknik rekayasa sosial yang sering digunakan untuk memanipulasi korban (Holt et al., 2018).

Peningkatan pemahaman ini menunjukkan bahwa metode penyuluhan yang digunakan cukup efektif dalam menyampaikan materi kepada peserta. Hal ini juga memperkuat pendapat bahwa edukasi yang terstruktur dapat meningkatkan kesadaran individu terhadap risiko kejahatan siber (UNODC, 2020).

2. Perubahan Sikap dan Kesadaran Digital

Selain peningkatan pengetahuan, kegiatan ini juga berdampak pada perubahan sikap peserta terhadap penggunaan teknologi digital. Sebelum kegiatan, banyak peserta yang cenderung mengabaikan aspek keamanan, seperti menggunakan kata sandi yang sederhana, tidak mengaktifkan verifikasi dua langkah, serta sering mengakses tautan yang tidak jelas sumbernya.

Setelah mengikuti penyuluhan, peserta menunjukkan peningkatan kesadaran terhadap pentingnya menjaga keamanan data pribadi. Hal ini terlihat dari komitmen peserta untuk mengganti kata sandi dengan kombinasi yang lebih kuat, menghindari penggunaan jaringan Wi-Fi publik yang tidak aman, serta lebih berhati-hati dalam membagikan informasi pribadi di media sosial. Perubahan perilaku ini menunjukkan bahwa penyuluhan tidak hanya berdampak pada aspek kognitif, tetapi juga pada aspek afektif dan perilaku.

Temuan ini sejalan dengan teori perilaku yang menyatakan bahwa peningkatan pengetahuan dapat memengaruhi sikap dan pada akhirnya mendorong perubahan perilaku (Notoatmodjo, 2018). Namun demikian, perubahan perilaku yang berkelanjutan tetap memerlukan penguatan melalui edukasi yang dilakukan secara terus-menerus.

3. Efektivitas Metode Penyuluhan

Metode yang digunakan dalam kegiatan ini meliputi ceramah interaktif, diskusi kelompok, simulasi kasus, dan sesi tanya jawab. Kombinasi metode ini terbukti efektif dalam meningkatkan keterlibatan peserta. Selama kegiatan berlangsung, peserta terlihat aktif dalam berdiskusi dan memberikan tanggapan terhadap materi yang disampaikan.

Diskusi kelompok memungkinkan peserta untuk saling berbagi pengalaman terkait cyber crime, sehingga materi menjadi lebih relevan dengan kehidupan sehari-hari. Sementara itu, simulasi kasus memberikan gambaran nyata mengenai bagaimana kejahatan siber terjadi dan bagaimana cara menghadapinya. Pendekatan ini terbukti mampu meningkatkan pemahaman peserta secara lebih mendalam dibandingkan dengan metode ceramah konvensional.

Hasil ini sejalan dengan penelitian yang menyatakan bahwa pendekatan interaktif dalam edukasi keamanan siber lebih efektif dalam meningkatkan pemahaman dan perubahan perilaku dibandingkan pendekatan satu arah (*Bada et al., 2019*). Dengan demikian, penggunaan metode partisipatif menjadi salah satu faktor kunci keberhasilan kegiatan ini.

4. Peran Organisasi Mahasiswa sebagai Agen Edukasi

Salah satu temuan penting dalam kegiatan ini adalah peran strategis organisasi mahasiswa dalam menyebarkan informasi terkait cyber crime. Setelah mengikuti kegiatan penyuluhan, beberapa peserta menyatakan kesediaannya untuk menyampaikan kembali materi yang telah diperoleh kepada anggota organisasi lainnya.

Hal ini menunjukkan bahwa organisasi mahasiswa dapat berfungsi sebagai multiplier effect dalam penyebaran informasi. Dengan memanfaatkan jaringan organisasi, informasi mengenai keamanan digital dapat menjangkau lebih banyak mahasiswa tanpa harus bergantung sepenuhnya pada kegiatan formal.

Peran ini sangat penting dalam menciptakan budaya digital yang aman di lingkungan kampus. Mahasiswa tidak hanya menjadi penerima informasi, tetapi juga menjadi agen perubahan yang aktif dalam meningkatkan kesadaran masyarakat sekitar. Hal ini sejalan dengan konsep mahasiswa sebagai agent of change yang memiliki tanggung jawab sosial dalam memberikan kontribusi positif kepada masyarakat.

5. Tantangan dalam Pelaksanaan Kegiatan

Meskipun kegiatan ini berjalan dengan baik, terdapat beberapa tantangan yang dihadapi selama pelaksanaan. Salah satu tantangan utama adalah perbedaan tingkat pemahaman peserta terhadap teknologi digital. Beberapa peserta memiliki pengetahuan yang cukup baik, sementara yang lain masih sangat terbatas. Hal ini menyebabkan penyampaian materi harus disesuaikan agar dapat dipahami oleh seluruh peserta.

Selain itu, keterbatasan waktu juga menjadi kendala dalam penyampaian materi yang cukup luas. Cyber crime merupakan topik yang kompleks dengan berbagai aspek yang perlu dipahami secara mendalam. Oleh karena itu, diperlukan waktu yang lebih panjang untuk membahas seluruh materi secara komprehensif.

Tantangan lainnya adalah mempertahankan perubahan perilaku peserta setelah kegiatan selesai. Tanpa adanya tindak lanjut, ada kemungkinan peserta kembali pada kebiasaan lama yang kurang aman dalam menggunakan teknologi digital. Oleh karena itu, diperlukan strategi lanjutan seperti pelatihan berkala atau kampanye digital untuk memperkuat hasil yang telah dicapai.

6. Implikasi dan Rekomendasi

Hasil kegiatan ini memberikan beberapa implikasi penting. Pertama, penyuluhan cyber crime terbukti efektif dalam meningkatkan kesadaran dan pemahaman mahasiswa. Oleh karena itu, kegiatan serupa perlu dilakukan secara berkelanjutan dengan melibatkan lebih banyak peserta.

Kedua, penggunaan metode interaktif perlu terus dikembangkan untuk meningkatkan efektivitas penyuluhan. Metode seperti simulasi dan studi kasus dapat memberikan pengalaman belajar yang lebih nyata dan relevan.

Ketiga, organisasi mahasiswa perlu diberdayakan sebagai mitra strategis dalam penyebaran informasi. Dengan melibatkan organisasi mahasiswa secara aktif, dampak kegiatan dapat diperluas secara signifikan.

Keempat, diperlukan dukungan dari institusi pendidikan untuk mengintegrasikan literasi keamanan digital ke dalam kurikulum atau kegiatan akademik lainnya. Hal ini penting untuk memastikan bahwa mahasiswa memiliki pemahaman yang memadai mengenai cyber crime sejak dini.

7. Keterkaitan dengan Penelitian Sebelumnya

Hasil kegiatan ini konsisten dengan berbagai penelitian sebelumnya yang menunjukkan bahwa edukasi memiliki peran penting dalam meningkatkan kesadaran keamanan siber. Studi yang dilakukan oleh Holt et al. (2018) menunjukkan bahwa pemahaman yang baik mengenai cyber crime dapat mengurangi risiko menjadi korban. Selain itu, penelitian oleh Bada et al. (2019) juga menegaskan bahwa pendekatan edukatif yang interaktif lebih efektif dalam mengubah perilaku pengguna.

Dengan demikian, kegiatan pengabdian ini tidak hanya memberikan manfaat praktis, tetapi juga memperkuat temuan empiris yang telah ada sebelumnya.

SIMPULAN

Secara keseluruhan, kegiatan penyuluhan cyber crime pada organisasi mahasiswa di Universitas Nahdlatul Ulama Cirebon menunjukkan hasil yang positif. Terdapat peningkatan pemahaman, perubahan sikap, serta munculnya kesadaran akan pentingnya keamanan digital di kalangan peserta. Metode penyuluhan yang interaktif dan partisipatif menjadi faktor utama keberhasilan kegiatan ini.

Namun demikian, untuk mencapai dampak yang berkelanjutan, diperlukan upaya lanjutan yang lebih sistematis dan terintegrasi. Dengan demikian, diharapkan mahasiswa tidak hanya menjadi pengguna teknologi yang cerdas, tetapi juga mampu melindungi diri dari berbagai ancaman cyber crime.

REFERENSI

- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction* (2nd ed.). Routledge.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Laporan literasi digital Indonesia*. Kominfo.
- Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 35(7), 523–541. <https://doi.org/10.1080/01639625.2014.897116>
- Nasution, S. (2017). *Metode research (penelitian ilmiah)*. Bumi Aksara.
- Notoatmodjo, S. (2018). *Promosi kesehatan dan perilaku kesehatan*. Rineka Cipta.
- Organization for Economic Co-operation and Development. (2021). *Enhancing digital security risk management*. OECD Publishing. <https://doi.org/10.1787/0d36d1a4-en>
- Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.
- United Nations Office on Drugs and Crime. (2020). *Comprehensive study on cybercrime*. UNODC. <https://www.unodc.org>
- Arief, B. N. (2018). *Kebijakan hukum pidana dalam penanggulangan cyber crime*. Kencana.