

PENGARUH CYBER SECURITY TERHADAP KESEHATAN MENTAL MAHASISWA PSIKOLOGI

Ardian Firdaus Saputra *¹

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia
202210515179@mhs.ubharajaya.ac.id

Edy Soesanto

Fakultas Teknik, Universitas Bhayangkara Jakarta Raya, Indonesia
edy.soesanto@dsn.ubharajaya.ac.id

Muhammad Farid Alifianto

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia
202210515175@mhs.ubharajaya.ac.id

Difani Cahya Prastiwi

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia
202210515069@mhs.ubharajaya.ac.id

Abstract

The rapid development of Internet technology has led to the emergence of new crimes in this field, such as data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft or hardware theft and many other crimes. Even the level of internet crime (cybercrime) is not monitored by the government so it is difficult to control. The emergence of a number of cyber crime cases in Indonesia has become a threat to the stability of security and public order with a fairly high level of escalation. The aim of this research is to better understand technology so that it is not easily affected by cyber crime and that everyone's cyber security is better maintained. The method we used in preparing this research was literature study. The results of data information found from various journals show that cyber crime cases greatly affect the level of cyber security and mental health of each person.

Keywords: Cyber Crime, Cyber Security, Mental Health

Abstrak

Pesatnya perkembangan teknologi Internet menyebabkan munculnya kejahatan-kejahatan baru di bidang ini, seperti manipulasi data, spionase, sabotase, provokasi, pencucian uang, hacking, pencurian perangkat lunak atau pencurian perangkat keras dan banyak kejahatan lainnya. Bahkan tingkat kejahatan internet (cybercrime) tidak diawasi oleh pemerintah sehingga sulit dikendalikan. Munculnya sejumlah kasus cyber crime di Indonesia telah menjadi ancaman

¹ Korespondensi Penulis

terhadap stabilitas keamanan dan ketertiban masyarakat dengan tingkat eskalasi yang cukup tinggi. Tujuan dalam penelitian ini adalah bertujuan untuk lebih memahami teknologi agar tidak mudah terpengaruh oleh *cyber crime* dan *cyber security* tiap orang lebih terjaga. Metode yang kami gunakan dalam penyusunan penelitian kali ini adalah dengan menggunakan studi literatur. Hasil informasi data yang ditemukan dari berbagai jurnal bahwa kasus *cyber crime* sangat mempengaruhi tingkat keamanan *cyber security* dan kesehatan mental tiap orang.

Kata Kunci : Kejahatan Siber, Keamanan Siber, Kesehatan mental

PENDAHULUAN

Pesatnya perkembangan teknologi internet menyebabkan timbulnya kejahatan-kejahatan baru di bidang ini, seperti manipulasi data, spionase, sabotase, provokasi, pencucian uang, hacking, pencurian perangkat lunak atau pencurian perangkat keras dan banyak kejahatan lainnya. Bahkan tingkat kejahatan internet (*cyber crime*) tidak diawasi oleh pemerintah sehingga tidak mudah untuk dikendalikan. Munculnya beberapa kasus kejahatan internet di Indonesia sudah menjadi ancaman terhadap keseimbangan keamanan dan ketertiban masyarakat dengan tingkat eskalasi yang cukup tinggi. Pemerintah dengan perangkat hukumnya belum mampu mengimbangi teknik kriminal yang menggunakan teknologi komputer, khususnya di Internet dan jaringan Internet. Kejahatan dunia maya yang umum mencakup pencurian identitas, penindasan, penipuan online, pencurian, dan banyak lagi.

Kesehatan mental merupakan keharmonisan dalam kehidupan yang terwujud antara fungsifungsi jiwa, kemampuan menghadapi problematika yang dihadapi, serta mampu merasakan kebahagiaan dan kemampuan dirinya secara positif (Daradjat 1988). Selanjutnya ia menekankan bahwa kesehatan mental adalah kondisi dimana individu terhindar dari gejala-gejala gangguan jiwa (*neurose*) dan dari gejala penyakit jiwa (*psychose*). permasalahan kesehatan mental menyangkut pengetahuan serta prinsip-prinsip yang terdapat lapangan psikologi, kedokteran, psikiatri, biologi, sosiologi, dan agama. Kesehatan mental adalah ilmu yang meliputi sistem tentang prinsip-prinsip, peraturan-peraturan serta prosedur-prosedur untuk mempertinggi kesehatan ruhani. Orang yang sehat mentalnya ialah orang yang dalam ruhani atau dalam hatinya selalu merasa tenang, aman, tenteram. (Susilawati, 2017)

METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan metode studi literatur dengan memperoleh data yang dapat membaca, mencatat dan mengelola laporan bahan penelitian terdahulu. Penelitian dengan studi literatur sebuah penelitian yang persiapannya sama dengan penelitian lainnya akan tetapi sumber dan metode pengumpulan data dengan mengambil data di pustaka, membaca, mencatat, dan mengolah bahan penelitian. Penelitian dengan studi literatur juga sebuah penelitian yang dikategorikan sebagai

sebuah karya ilmiah karena pengumpulan data dilakukan dengan sebuah strategi dalam bentuk metodologi 3 penelitian. Variabel pada penelitian studi literatur bersifat tidak baku. Data yang diperoleh dianalisis secara mendalam oleh penulis. Sumber data untuk penelitian studi literatur dapat berupa sumber yang resmi akan tetapi dapat berupa laporan/kesimpulan seminar, catatan/rekaman diskusi ilmiah, tulisan-tulisan resmi terbitan pemerintah dan lembaga-lembaga lain, baik dalam bentuk buku/manual maupun digital seperti bentuk piringan optik, komputer atau data komputer. (Melfianora & Si, n.d.)

Analisa Data

Jika seluruh data telah dikumpulkan dengan valid menurut jurnal/artikel/buku yang, lalu seseorang peneliti melanjutkannya lagi data-data tersebut dengan menganalisa data-data dan permasalahan yang telah dikutip melalui sumber tersebut. Menganalisa disini maksud nya yaitu memahami pokok-pokok masalah yang terjadi dalam jurnal/artikel/buku yang dikutip dan dicarikan solusi-solusi yang tepat untuk menyelesaikan masalah-masalah yang diangkat dalam penelitian tersebut. Analisis data ini bertujuan untuk menganalisa hal-hal yang terjadi dalam masalah dalam penelitian tersebut dan mencari solusi terbaik pada pokok permasalahan tersebut. Analisis data ini memudahkan seorang pembaca dalam memahami pokok-pokok masalah yang terjadi dalam penelitian tersebut.

HASIL DAN PEMBAHASAN

Cyber security adalah praktik atau kumpulan teknologi, proses, dan praktik perlindungan yang bertujuan untuk melindungi sistem komputer, jaringan, perangkat lunak, dan data dari ancaman, serangan, atau akses yang tidak sah. Cyber crime adalah sebuah tindakan yang bersifat ofensif yang dilakukan oleh negara, individu, kelompok, atau organisasi yang menargetkan sebuah sistem informasi, infrastruktur, jaringan komputer, dan/atau perangkat komputer pribadi untuk melakukan tindakan berbahaya seperti mencuri data pribadi tanpa sepengetahuan, melakukan pemalsuan data, atau membocorkan data yang bersifat rahasia atau melakukan kerusakan pada sebuah sistem sehingga tidak berjalan sebagai mana mestinya. Kesehatan mental merupakan sebuah kondisi dimana individu terbebas dari segala bentuk gejala-gejala gangguan mental. Individu yang sehat secara mental dapat berfungsi secara normal dalam menjalankan hidupnya khususnya saat menyesuaikan diri untuk menghadapi masalah-masalah yang akan ditemui sepanjang hidup seseorang dengan menggunakan kemampuan pengolahan stres.

Korban cybercrime seringkali mengalami dampak yang signifikan dari segi psikologis akibat kejadian yang mereka alami. Beberapa dampak negatif yang dialami korban dari sudut pandang psikologis meliputi:

| No | Dampak | Penjelasan |
|----|--|--|
| 1 | Ketakutan dan Kecemasan Berlebihan | Korban serangan cyber sering merasakan ketakutan yang signifikan terkait dengan keamanan data pribadi dan informasi sensitif mereka. Hal ini bisa memunculkan kecemasan yang berkelanjutan terkait potensi ancaman yang mungkin terjadi. |
| 2 | Stres Emosional | Serangan siber atau kejahatan online dapat menyebabkan stres emosional yang berat. Kerugian keuangan, kehilangan data penting, atau pelanggaran privasi dapat memberikan tekanan emosional yang besar bagi korban |
| 3 | Rasa Tidak Aman dan Kerentanan | Merasa tidak aman dan rentan adalah dampak psikologis yang sering dirasakan oleh korban cybercrime. Mereka mungkin merasa tidak aman secara emosional dan psikologis setelah serangan tersebut. |
| 4 | Kehilangan Kepercayaan dan Distrust | Korban mungkin kehilangan kepercayaan terhadap teknologi, lembaga, atau bahkan orang-orang di sekitarnya akibat pengalaman buruk yang mereka alami. Hal ini bisa mengakibatkan tingkat kecurigaan yang lebih tinggi terhadap lingkungan digital. |
| 5 | Depresi dan Stigma | Dampak psikologis dari serangan siber dapat menyebabkan gejala depresi, terutama karena beban emosional yang berat dan kehilangan rasa keamanan. Selain itu, beberapa korban juga mungkin mengalami stigma sosial atau kurangnya dukungan karena kurangnya pemahaman sebagian orang terhadap dampak psikologis dari cybercrime |
| 6 | Gangguan Kesehatan Mental yang Bersifat Jangka Panjang | Dalam beberapa kasus, korban cybercrime dapat mengalami gangguan kesehatan mental yang bersifat jangka panjang, seperti kecemasan kronis, gangguan stres pasca trauma (PTSD), atau masalah kesehatan mental lainnya yang memerlukan perawatan profesional |
| 7 | Isolasi Sosial dan Dukungan yang Kurang | Beberapa korban mungkin merasa terisolasi atau kesulitan mendapatkan dukungan sosial. Pengalaman cybercrime dapat memicu isolasi sosial karena korban merasa sulit untuk berbagi pengalaman mereka atau karena kurangnya pemahaman dari lingkungan sekitar |

Terdapat berbagai faktor yang dapat mempengaruhi terjadinya cybercrime. Beberapa di antaranya termasuk:

| No | Faktor-Faktor | Penjelasan |
|----|---|--|
| 1 | Kelemahan Keamanan Teknologi dan Sistem | Jika sistem, aplikasi, atau perangkat lunak memiliki kerentanan keamanan, peretas bisa memanfaatkannya untuk melakukan serangan. |
| 2 | Motivasi Pelaku | Diantara motivasi pelaku melakukan cyber crime tersebut yaitu adalah Keuntungan Finansial yang sangat menggiurkan bagi para pelaku tersebut, Pencitraan Diri (Ego) faktor ini bagian dari rasa unjuk keahlian yang terdapat pada dirinya yang menyatakan bahwa dirinya tersebut itu bisa untuk meretas suatu akses, Keinginan Merusak, Ada yang melakukan serangan dengan tujuan merusak atau mengganggu sistem atau infrastruktur |
| 3 | Anonimitas dan Kesulitan Pelacakan | Karakteristik internet yang memungkinkan pelaku kejahatan untuk menyembunyikan identitas mereka atau sulit dilacak, mempermudah terjadinya serangan cybercrime |
| 4 | Kurangnya Kesadaran Keamanan | Ketidaktahuan atau kurangnya pemahaman tentang ancaman keamanan online oleh individu, perusahaan, atau organisasi juga dapat menyebabkan rentannya terhadap serangan cybercrime |
| 5 | Teknologi yang Terus Berkembang | Perkembangan teknologi yang cepat juga menciptakan celah baru dan tantangan baru dalam hal keamanan. Penjahat siber terus beradaptasi dengan teknologi baru untuk melakukan serangan |
| 6 | Kurangnya Hukuman atau Penegakan Hukum yang Efektif | Kondisi hukum yang tidak jelas, hukuman yang lemah, atau penegakan hukum yang tidak efektif dapat menjadi insentif bagi pelaku kejahatan siber |
| 7 | Globalisasi dan Keterhubungan Digital | Semakin terhubungnya dunia digital secara global juga berarti bahwa serangan dapat terjadi dari berbagai negara dengan berbagai motivasi dan tujuan. |

Pencegahan cybercrime melibatkan serangkaian langkah dan praktik keamanan yang dapat membantu mengurangi risiko serangan siber. Berikut adalah beberapa langkah pencegahan yang dapat diambil :

| No | Pencegahan | Penjelasan |
|----|---|--|
| 1 | Menggunakan Perangkat Lunak Keamanan | Perangkat Lunak Antivirus dan Antimalware: Instal dan perbarui perangkat lunak antivirus dan antimalware secara teratur untuk melindungi perangkat dari serangan malware dan virus. |
| 2 | Pembaruan Sistem dan Aplikasi | Pastikan sistem operasi, perangkat lunak, dan aplikasi selalu diperbarui dengan pembaruan terbaru. Pembaruan ini seringkali memperbaiki kerentanan keamanan yang dapat dimanfaatkan oleh penjahat siber. |
| 3 | Penggunaan Sandi Kuat dan Pengelolaan Sandi | Gunakan sandi yang kuat dan unik untuk setiap akun online. Manajemen sandi yang baik, seperti menggunakan manajer sandi, dapat membantu mengelola sandi dengan aman. |
| 4 | Proteksi Data dan Informasi Pribadi | Enkripsi data penting dan informasi pribadi. Backup data secara teratur dan simpan salinan cadangan di tempat yang aman. |
| 5 | Kesadaran Keamanan | Tingkatkan kesadaran keamanan di antara pengguna. Berikan pelatihan keamanan cyber kepada karyawan untuk mengenali dan menghindari ancaman seperti phishing, spear phishing, dan social engineering. |
| 6 | Pengaturan Privasi Sosial Media | Atur pengaturan privasi sosial media agar tidak memberikan akses terlalu banyak informasi pribadi kepada publik atau pihak yang tidak terpercaya. |
| 7 | Jaringan Virtual Pribadi (VPN) dan Koneksi Aman | Gunakan VPN untuk koneksi internet yang aman, terutama saat menggunakan jaringan Wi-Fi publik. |
| 8 | Membangun Kebijakan Keamanan Perusahaan | Perusahaan harus memiliki kebijakan keamanan yang ketat, serta melakukan pelatihan dan pengawasan terhadap karyawan dalam menggunakan sistem informasi perusahaan. |
| 9 | Monitoring Aktivitas Sistem | Rutin memonitor aktivitas sistem untuk mendeteksi potensi serangan siber sejak dini. |
| 10 | Melaporkan dan Menindaklanjuti Serangan | Jika terjadi serangan, segera laporkan ke pihak yang berwenang dan lakukan tindakan tanggap darurat sesuai prosedur yang telah ditetapkan. |

KESIMPULAN

Perlindungan siber dalam konteks kesehatan mental mahasiswa psikologi menjadi semakin penting ancaman keamanan siber, seperti serangan phising atau kebocoran data, dapat menimbulkan stress dan kekhawatiran yang dapat

mempengaruhi kesehatan mental mahasiswa. Serangan phishing atau kebocoran data dapat menimbulkan tingkat stress dan kekhawatiran pada mahasiswa dikarenakan adanya data pribadi yang diletakkan di dalam suatu web/aplikasi menjadikan data tersebut untuk bisa di retas oleh kelompok atau pribadi seseorang, sehingga dengan itu seseorang timbul rasa khawatir. Maka dari itu sangat penting sekali edukasi terhadap praktik keamanan dengan tujuan untuk mengamankan data-data atau sistem-sistem yang kita letakkan di web menjadi aman tanpa adanya kecemasan. Selain itu edukasi terhadap kesehatan mental juga penting dikarenakan menjadi sebuah aspek/pondasi dasar karena seseorang untuk mengantisipasi hal-hal pemikiran negatif yang menghantui dirinya.

SARAN

Saran untuk masyarakat untuk lebih sadar akan bahaya dari serangan siber dengan cara mempelajari melalui memperbanyak ilmu tentang keamanan siber melalui banyak media yang tersedia seperti dari YouTube, berita terbaru, atau buku-buku yang sudah tersedia.

Saran untuk pemerintah lebih ditingkatkan lagi keamanan terhadap hal-hal yang berpengaruh dengan keamanan siber seperti lebih memerhatikan keamanan data milik masyarakat supaya tidak terjadi kebocoran data, lebih memperketat keamanan server yang berpotensi mengalami kebocoran data.

Saran untuk mahasiswa lebih berperan penting dalam menyuarakan akan pentingnya keamanan siber bagi setiap orang agar masyarakat yang kurang memiliki ilmu tentang keamanan siber lebih mengerti tentang bahaya-bahaya yang dapat ditimbulkan dari serangan siber. Mahasiswa bisa melakukan dengan beberapa cara seperti membuat jurnal, menyuarakan melalui berbagai media atau bisa dengan pesan secara langsung kepada masyarakat

DAFTAR PUSTAKA

- Melfianora, I., & Si, M. (n.d.). *PENULISAN KARYA TULIS ILMIAH DENGAN STUDI LITERATUR*. <http://banjirembun.blogspot.co.id/2012/04/penelitian-kepuustakaan.html>
- Susilawati. (2017). *Kesehatan Mental Menurut Zakiah Daradjat*. Universitas Islam Negeri Raden Intan Lampung.
- TINJAUAN MANAJEMEN KEPERCAYAAN, K. D. P. B. K. (n.d.). *TINJAUAN MANAJEMEN KEPERCAYAAN, KEAMANAN DAN PRIVASI BAHASA KEBIJAKAN*.
- Karin Höne and J.H.P. Eloff. (n.d.). *Information security policy – what do international information security standards say?*
- Ardiyanti, H. (n.d.). *CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA*. <http://kominfo.go.id/index.php/content/detail/3980/>
- Azizah, M., Fitri, N. K., Maura, N., & Salsabila, J. (2023). *Parade Riset Mahasiswa 2023 Psychological Security Dalam Dinamika Kehidupan Mahasiswa Fakultas Psikologi*

- Universitas Bhayangkara Jakarta Raya Bullying pada Trend Pick Me Girl/Boy di TikTok (Vol. 1, Issue 1). Cyber.
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3, 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Furnell, S. M., Clarke, N., Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4–19. <https://doi.org/10.1108/09685220910944722>
- Gumara, A., Muthmainah, B., & Sharon Prameswari, A. (2023). Kecemasan Pada Mahasiswa Pengguna Tiktok Yang Melakukan Self Diagnose (Vol. 1, Issue 1).
- Hafid, A., & Sudyana, D. (n.d.). ANALISIS KESADARAN MAHASISWA UMRI TERKAIT PENGGUNAAN TEKNOLOGI & MEDIA SOSIAL TERHADAP BAHAYA CYBERCRIME.
- Keamanan Siber Dalam Mengatasi Konten Negatif, P., Siagian, L., Budiarto, A., & Strategi Pertahanan Udara Universitas Pertahanan, P. (n.d.). THE ROLE OF CYBER SECURITY IN OVERCOME NEGATIVE CONTENTS TO REALIZE NATIONAL INFORMATION RESILIENCE.
- Keamanan siber di tingkat organisa Anteseden untuk meningkatkan tingkat keamanan siber dalam organisasi. (n.d.). <https://doi.org/10.1108/JEIM-06-2020-0>
- Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. *JIOSE: Journal of Indonesian Sharia Economics*, 1(1), 1–20. <https://doi.org/10.35878/jiose.v1i1.360>
- Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 13(1), 43–66. <https://doi.org/10.22212/jp.v13i1.2641>
- Samudra, Y., Hidayat, A., & Wahyu, M. F. (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>
- Soesanto, E., Saputra, F., Puspitasari, D., & Putra Danaya, B. (n.d.). Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher. 2(1). <https://doi.org/10.38035/jim.v2i1>
- Zhao, X., Xue, L., & Whinston, A. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, 30(1), 123–152. <https://doi.org/10.2753/MIS0742-1222300104>