El-Mujtama: Jurnal Pengabdian Masyarakat
Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

Menguasai Literasi Teknologi untuk Mengatasi Risiko Keamanan Cyber

Predi Ari Repi[1], Muhammad Irwan Padli Nasution[2]
[1,2]Universitas Islam Negeri Sumatra Utara
predi0331234011@uinsu.ac.id[1], irwannst@uinsu.ac.id[2]

ABSTRACT

The growing reliance on digital technology has produced new concerns for cyber security. Technological literacy has been identified as a significant factor in reducing the hazards linked with the usage of technology. This article examines the need of technological literacy in tackling cyber security issues, as well as integrative approaches that incorporate education and digital awareness. This article identifies methodologies and best practices for generating technical literature for cyber-security reasons using a literature review and critical analysis. Practical advice are also provided to improve educational efforts and digital awareness in mitigating cybersecurity risks in a variety of settings.
Keywords: *technology literacy, cyber security, digital education, digital awareness, risk*

ABSTRAK

Peningkatan ketergantungan pada teknologi digital telah menghasilkan kekhawatiran baru untuk keamanan siber. Literasi teknologi telah diidentifikasi sebagai faktor yang signifikan dalam mengurangi bahaya yang terkait dengan penggunaan teknologi. Artikel ini mengeksplorasi kebutuhan untuk keterampilan teknologi dalam menangani masalah keamanan siber, serta pendekatan integratif yang menggabungkan pendidikan dan kesadaran digital. Artikel ini mengidentifikasi metodologi dan praktik terbaik untuk menghasilkan literatur teknis untuk alasan keamanan siber menggunakan ulasan literatur dan analisis kritis. Nasihat praktis juga disediakan untuk meningkatkan upaya pendidikan dan kesadaran digital dalam mengurangi risiko keamanan siber dalam berbagai pengaturan.
Kata Kunci: literasi teknologi, keamanan cyber, pendidikan digital, kesadaran digital, risiko

PENDAHULUAN

Dalam era digital 4.0 ini, hampir semua sektor telah mulai melakukan berbagai kegiatan menggunakan sistem berbasis teknologi digital, juga dikenal sebagai sistem online. Karena semua operasi manusia telah bergeser dari manual ke digital. Bahkan dalam sistem pendidikan, 2018 dimulai dengan revisi sistem ujian nasional, yang sebelumnya menggunakan media tertulis tetapi sekarang telah beralih ke pendekatan online. Sejak saat itu, beberapa sistem pendidikan lainnya telah muncul. (Putriani, 2021)

Begitu juga Di era di mana teknologi digital adalah bagian fundamental dari kehidupan sehari-hari, kesadaran yang menyeluruh tentang penggunaan teknologi dan ancaman keamanan siber menjadi semakin penting. Kemajuan cepat dalam teknologi informasi dan komunikasi telah memberikan beberapa manfaat, tetapi mereka juga telah memperkenalkan ancaman baru untuk keamanan dan privasi data individu dan organisasi. Serangan malware, ransomware, phishing, dan pencurian identitas telah berkembang menjadi masalah keamanan siber yang canggih dan

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

mengkhawatirkan. Sebenarnya, tidak hanya perusahaan besar yang ditargetkan, tetapi juga orang-orang biasa di seluruh dunia. Upaya untuk mengatasi bahaya ini bergantung tidak hanya pada solusi teknis, tetapi juga pada kesadaran dan kemampuan individu untuk mengenali, mencegah, dan menanggapi mereka.

Literasi teknologi adalah strategi yang terkenal untuk mengelola masalah keamanan siber. Literasi ini mencakup tidak hanya kemampuan teknis untuk menggunakan perangkat lunak dan perangkat keras, tetapi juga pemahaman tentang implikasi etika, keamanan, dan privasi dari teknologi informasi dan komunikasi. Individu dapat mendapatkan pemahaman yang lebih baik tentang isu-isu keamanan siber dan bagaimana melindungi diri mereka sendiri dan data mereka dengan menjadi lebih cerdas secara teknologi. Namun, terlepas dari pengakuan kebutuhan untuk keterampilan teknis, implementasi yang sukses tetap menjadi kesulitan. Banyak orang mungkin tidak memiliki akses ke sumber daya pendidikan yang diperlukan, serta dorongan untuk mempelajari pengetahuan dan keterampilan yang diperlukan untuk keterampilan teknologi.

Mengingat berapa banyak pihak yang masih awam atau bahkan tidak menyadari teknologi, harus mungkin untuk mengatur pelatihan atau sesuatu yang serupa untuk memberikan guru dengan pengetahuan dan pemahaman tentang teknologi sehingga sistem belajar yang diaimplementasikan tidak terlambat. (Liady et al., 2022) Akibatnya, perlu untuk merancang rencana yang komprehensif dan terintegrasi untuk meningkatkan keterampilan teknologi untuk tujuan keamanan siber. Dalam lingkungan ini, memahami bagaimana literatur teknologi dapat digunakan untuk memecahkan ancaman keamanan siber menjadi semakin penting. Pemeriksaan mendalam tentang cara, masalah, dan taktik terbaik untuk menerapkan keterampilan teknis yang baik dapat memberikan wawasan yang berguna bagi individu, bisnis, dan komunitas secara keseluruhan dalam mengatasi risiko keamanan siber yang kompleks di era digital.

METODE PENELITIAN

Jenis penelitian yang akan digunakan dalam penelitian ini yaitu penelitian studi kepustakaan, yaitu penelitian yang dilakukan dengan cara meneliti bahan melakukan pengumpulan data dan menelaah terhadap berbagai buku, literatur, jurnal, makalah, danberbagai laporan yang berhubungan denga masalah yang akan di pecahkan. Penelitiansecara studi kepustakaan mencakupuraian sistematis tentang kajianliteratur serta hasil peneltian sebelumnya para peneliti yang mempunyai kesesuian antara hasil penelitian dari para peneliti terhadap masalah yang akan diteliti. Penelitian Menguasai Literasi Teknologi untuk Mengatasi Resiko Keamanan Cyber.

Teknik pengumpulan data dapat dilakukan dengan studi kepustakaan. Metode analisis data yang digunakan dalam penelitian ini adalah yaitu dengan menggunakan teknik analisis diskriptif yaitu merupakan Teknik yang paling mendasar dan bersifat mutlak. Hal ini mengandung pengertian, Teknik ini harus dilaksanakan dalam pembahasan agar pembahasan dapat dipahami oleh orang lain.

El-Mujtama: Jurnal Pengabdian Masyarakat
Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

HASIL DAN PEMBAHASAN

1. Definisi literasi Teknologi

Maryland Technology Education State Curriculum mendefinisikan keterampilan teknis sebagai kemampuan untuk memanfaatkan, memahami, mengatur, dan mengevaluasi inovasi yang menggunakan prosedur dan ilmu pengetahuan untuk memecahkan masalah dan memperluas kapasitas seseorang. (Maryland State Department of Education., 2005)

Menurut National Academy of Engineering dan National Research Council of the National Academic, teknologi literasi adalah tingkat pemahaman teknologi yang memungkinkan penggunaan teknologi modern secara efektif di masyarakat. Ini terdiri dari tiga komponen utama: pengetahuan, kemampuan dan pemikiran kritis, dan pengambilan keputusan. (*Tech Tally*, 2006)

Rose (2007:43) mendefinisikan "literasi teknologi" sebagai berikut:

a. Memahami hasil kerja manusia.
b. Hubungan antara ilmu pengetahuan, lingkungan dan teknologi
c. Kemampuan untuk menggunakan teknologi, terutama dalam belajar dan mengajar ilmu pengetahuan, dan kemampuan untuk menginterogasi kemampuan untuk menilai dan membuat keputusan.

Berdasarkan tiga kategori di atas, keterampilan teknis dapat didefinisikan sebagai kompetensi yang mencakup komponen ilmu pengetahuan, kemampuan berpikir kritis, dan pengambilan keputusan untuk berhasil menggunakan hasil teknologi/inovasi dari aktivitas manusia, khususnya di bidang pendidikan. (Mary Annette Rose, 2007)

Teknologi literasi adalah istilah yang mengacu pada kemampuan seseorang untuk memahami, menggunakan, dan mengkritisi berbagai teknologi yang ada dalam kehidupan sehari-hari. Ini mencakup pemahaman tentang bagaimana teknologi bekerja, kemampuan untuk menggunakan berbagai alat dan platform secara efektif, serta kemampuan untuk mengevaluasi informasi yang diperoleh melalui teknologi tersebut. Aspek-aspek teknologi literasi termasuk pemahaman tentang bagaimana menggunakan perangkat keras dan perangkat lunak, keterampilan dalam navigasi internet dan media sosial, kemampuan untuk mengevaluasi kebenaran dan kredibilitas informasi online, serta kesadaran tentang isu-isu privasi dan keamanan digital.

2. Upaya Regulasi Khusus di Bidang Teknologi Informasi dalam Menghadapi Serangan Cyber *(CyberAttack)*

a. Indonesia telah meratifikasi Konvensi Dewan Eropa tentang Kejahatan Siber, Budapest, Hungaria 2001.

   Dewan adalah badan supranasional di Eropa. European Committee on Crime Problems didirikan pada tahun 1985 untuk menangani berbagai masalah hukum yang terkait dengan kejahatan komputer. Konvensi Dewan Eropa tahun 2001 adalah peraturan pertama yang menangani kejahatan siber, dan berfungsi sebagai pedoman untuk penegakan hukum nasional.

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

Akibatnya, Indonesia, yang belum meratifikasi konvensi, harus serius mempertimbangkan untuk melakukannya. Adalah penting untuk memperkuat dasar hukum dan meningkatkan penegakan Undang-Undang Kejahatan Siber Khusus terhadap penjahat di luar negeri. Tentu saja, proses ratifikasi harus mematuhi aturan yang berlaku, baik dalam hukum internasional (Konvensi Wina 1969) dan dalam hukum nasional (Pasal 11 UUD NKRI 1945). (Fuady, 2005)

b. Pembentukan Undang-Undang Khusus tentang Tindak Pidana Siber.

Strategi kriminalisasi kejahatan siber dalam hukum pidana nasional harus diterapkan secara menyeluruh sebagai bagian dari sistem peradilan pidana Indonesia, dengan mempertimbangkan karakteristik dan kategori kejahatannya. Undang-undang ITE saat ini tidak secara langsung menangani kejahatan siber. Penciptaan ITE Act terutama didorong oleh strategi politik pragmatis dan bukan pendekatan kebijakan publik yang melibatkan beberapa pihak. Undang-undang ITE berisi ketentuan yang berkaitan dengan perbuatan jahat atau pidana, seperti kelalaian atau pelanggaran, namun ini tidak unik untuk kejahatan siber. ITE Act juga tidak meresepkan perawatan untuk kejahatan hacking. Kebijakan non-cybercriminalization yang ideal di Indonesia adalah penandatanganan Undang-Undang Kejahatan Cyber yang spesifik. Undang-undang khusus ini akan merumuskan aturan umum yang berlaku untuk semua aspek teknologi informasi dan komunikasi, kejahatan yang berkaitan dengan kerahasiaan, integritas, dan ketersediaan data atau sistem komputer/elektronik, pedoman untuk pembiayaan, hukum peristiwa yang mengatur prosedur investigasi dan penyelidikan di bidang ini, termasuk pencarian dan penangkapan bukti digital, serta kerjasama internasional seperti ekstradisi, bantuan hukum bersama. (Gani, 2020)

3. Literasi Digital sebagai Solusi

Hal ini dapat disimpulkan bahwa literasi digital melibatkan sikap, pemahaman, dan keterampilan dalam mengatur dan menyajikan informasi, serta menerapkan pengetahuan secara efisien di berbagai media dan format. Dengan berbagai perangkat teknologi informasi yang terhubung ke Internet, banyak orang telah beralih dari membaca buku tradisional ke menggunakan komputer untuk mengakses kekayaan informasi. Gadget dan jaringan internet dapat membantu komunitas dan anak-anak memperkuat kemampuan membaca mereka. Pada dasarnya, digitalisasi dapat berfungsi sebagai perantara yang mempromosikan peningkatan kualitas literasi dengan memberikan sumber informasi yang beragam dan berlimpah.

Literasi digital mencakup pengetahuan dan kemampuan dalam memperoleh dan berbagi informasi, serta penggunaan pengetahuan secara efektif di berbagai media dan platform. Banyak orang dengan akses internet telah berhenti membaca buku dengan cara tradisional dan sebaliknya menggunakan PC yang terhubung ke web yang memungkinkan akses instan ke banyak informasi. Akibatnya, gadget digital

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

dan konektivitas ke berbagai jaringan dapat membantu komunitas dan siswa dalam meningkatkan tingkat literasi. Pada dasarnya, digitalisasi dapat membantu meningkatkan kemampuan membaca dengan menyediakan akses mudah ke berbagai macam pengetahuan. (B. K. B. Putra, 2018)

Dunia cyber dan online tampaknya menawarkan banyak manfaat, tetapi mereka juga mengandung berbagai konten yang tidak diinginkan seperti berita palsu, pidato kebencian, ekstremisme, dan bahkan tindakan penipuan. Kementerian Pendidikan dan Budaya menyatakan bahwa kehancuran ekosistem digital saat ini karena informasi berbahaya dapat dikurangi dengan meningkatkan pengetahuan individu. Spionase pada semua jenis konten yang ditujukan untuk netizen sebagai pelanggan harus didekati dengan hati-hati. Menanggapi terobosan teknologi dan internet saat ini membutuhkan keterampilan literasi digital abad ke-21. (I. Setyawan, 2020)

Sebagai tanggapan terhadap kesulitan abad ke-21 telah dilakukan studi yang luas tentang literasi dan literasi digital. Dalam prakteknya, keterampilan digital sama pentingnya dengan membaca, menulis, dan menghitung atau bidang lain, tetapi membutuhkan kegiatan yang lebih kompleks. Masyarakat saat ini harus mendorong nilai-nilai ini, terutama di antara mereka yang lahir di era internet. Hal ini disebabkan oleh fakta bahwa era digital tumbuh dengan teknologi TI yang mapan, memungkinkan mereka untuk secara bebas mengakses banyak konten dan informasi di media digital, tidak seperti generasi sebelumnya.

Literasi dalam semua aspek kehidupan menghalangi kemajuan peradaban suatu bangsa. Literasi mengacu pada kemampuan untuk membaca dan menulis. Sebaliknya, budaya literasi berfokus pada kebiasaan berpikir yang dimulai dengan tindakan membaca dan menulis sampai sebuah karya diproduksi yang seharusnya mempengaruhi perilaku dan pikiran karyawan. Media literacy, teknologi, dan visual literacy adalah kompetensi yang harus dikembangkan di era teknologi dan internet. Literasi digital dapat membantu menciptakan ketertiban sosial melalui mentalitas dan perspektif kritis dan kreatif. Orang-orang kurang rentan terhadap topik yang menakutkan, materi palsu, atau penipuan berbasis digital karena mereka menyadari legitimasi dan kualitas konten digital yang mereka layak. Akibatnya, kehidupan sosial dan budaya orang akan lebih aman dan lebih menguntungkan. Membangun budaya kecerdasan digital membutuhkan partisipasi aktif masyarakat. Sukses mengembangkan keterampilan digital adalah salah satu metrik pencapaian dalam pendidikan dan budaya. (Isnaini & Widodo, 2022)

4. Penguatan Literasi Digital dalam Pencegahan Pelanggaran Hukum Siber

Di era ketika teknologi informasi dan komunikasi memainkan peran yang semakin dominan dalam kehidupan sehari-hari, meningkatkan keterampilan digital sangat penting untuk mencegah pelanggaran hukum cyber. Kejahatan cyber dapat mencakup berbagai perilaku berisiko seperti penipuan online, serangan cyber, pencurian identitas, penggunaan data pribadi yang tidak sah, dan publikasi informasi yang menyesatkan. Oleh karena itu, meningkatkan kecerdasan digital sangat penting

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

untuk menghindari bahaya ini. Berikut adalah diskusi panjang tentang kebutuhan untuk meningkatkan keterampilan digital dalam pencegahan pelanggaran hukum cyber:

1. Pemahaman Risiko Digital

   Individu yang meningkatkan keterampilan digital mereka dapat lebih memahami risiko yang terkait dengan penggunaan teknologi informasi dan Internet. Individu yang memahami bagaimana informasi dapat disalahgunakan akan lebih menyadari bahaya yang mungkin seperti serangan cyber, penipuan online, dan penyebaran malware. Meningkatkan kecerdasan digital tidak hanya membantu orang memahami ancaman digital, tetapi juga memungkinkan mereka untuk membangun keterampilan penting untuk menilai keandalan informasi online. Individu yang dapat mengidentifikasi antara informasi yang sah dan palsu dapat membantu meminimalkan penyebaran informasi yang salah, yang dapat menyebabkan konflik atau ketidakpercayaan dalam komunitas. Selain itu, keterampilan digital yang baik dapat membantu individu dalam mengenali strategi yang menyesatkan yang digunakan oleh pihak yang tidak bertanggung jawab untuk mengendalikan opini publik atau kesan massal. Individu dapat mengurangi kerentanan mereka terhadap propaganda atau kampanye pemasaran yang menyesatkan dengan mengenali bagaimana informasi dapat digunakan untuk mempengaruhi keyakinan dan perilaku.

   Memperkuat literasi digital juga membantu mempromosikan sikap yang lebih bertanggung jawab dan etis tentang teknologi. Individu yang memahami praktik digital yang tepat dapat membantu menciptakan budaya online yang lebih positif dan beradab. Ini melibatkan menghormati privasi orang lain, menggunakan bahasa yang sopan dan tidak berbahaya, dan menggunakan Internet dengan bertanggung jawab, seperti menghindari cyberbullying atau pelecehan online. Memperkuat literasi digital juga dapat berkontribusi pada kesadaran yang lebih baik tentang pentingnya inklusi digital, memastikan bahwa tidak ada yang tertinggal dalam transformasi dan kemajuan digital yang berkelanjutan. Dengan demikian, meningkatkan ketrampilan digital sangat penting dalam mengembangkan masyarakat yang berinformasi secara teknologi, waspada terhadap ancaman digital, dan mampu membuat penilaian yang sehat ketika menggunakan teknologi informasi dan Internet. Kami dapat menciptakan lingkungan digital yang aman, inklusif, dan etis di mana semua orang dapat menyadari potensi baik teknologi dengan bekerja sama untuk meningkatkan sastra digital di semua segmen masyarakat. (Setyaningsih, 2019)

2. Pendidikan Mengenai Identifikasi Ancaman

   Orang dengan keterampilan digital yang kuat dapat melihat risiko digital termasuk phishing, malware berbahaya, dan serangan DDoS. Pengguna internet yang memahami cara mengidentifikasi gejala serangan dapat menghindari perangkap dan menurunkan peluang mereka untuk menjadi

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

korban pelanggaran hukum cyber. Orang yang memahami cara mengenali gejala serangan digital dapat melindungi diri dari berbagai risiko berbahaya. Pengetahuan yang mendalam tentang strategi phishing, misalnya, memungkinkan orang untuk melihat email atau situs web yang menipu yang mencoba mendapatkan informasi pribadi atau keuangan. Individu dapat menghindari mengungkapkan informasi penting kepada orang yang tidak sah, mengurangi risiko penipuan dan pencurian identitas.

Selain itu, keterampilan digital yang sangat baik memungkinkan konsumen untuk mengidentifikasi perangkat lunak berbahaya, seperti virus, cacing, atau Trojan, yang dapat menginfeksi perangkat mereka.

Dengan pemahaman yang kuat tentang prosedur keamanan siber, pengguna internet dapat menghindari mengunduh atau menelusuri konten yang mencurigakan dan menginstal perangkat lunak perlindungan yang dapat diandalkan untuk melindungi perangkat mereka dari serangan malware.

Selain itu, pemahaman yang menyeluruh tentang serangan penolakan layanan terdistribusi (DDoS) memungkinkan perusahaan untuk memprediksi serangan pada infrastruktur jaringan. Mengidentifikasi indikator awal serangan DDoS memungkinkan organisasi untuk mengambil tindakan. Tindakan proaktif termasuk memperluas kapasitas jaringan dan mendistribusikan layanan keamanan yang mengkhususkan diri dalam mendeteksi dan mengurangi serangan DDoS. Melalui inisiatif ini, mereka berharap untuk mengurangi gangguan layanan dan kerugian keuangan yang disebabkan oleh serangan itu. Secara keseluruhan, keterampilan digital yang baik menyediakan masyarakat dengan informasi dan keterampilan yang diperlukan untuk mengidentifikasi, mencegah, dan menanggapi berbagai bahaya digital. Individu dan organisasi dapat melindungi keamanan dan integritas data mereka sambil juga meminimalkan dampak negatif dari pelanggaran hukum cyber dengan menggabungkan keahlian teknis dan kesadaran terhadap tren serangan cyber yang berkembang. (Kurnia Putra, 2016)

3. Pemahaman Mengenai Perlindungan Data Pribadi

Individu dan organisasi dapat belajar tentang pentingnya perlindungan data pribadi dengan mengembangkan keterampilan keterampilan digital yang kuat. Ini melibatkan pengetahuan tentang teknik keamanan digital seperti kata sandi yang kuat, enkripsi data, dan jaminan keamanan jaringan. Ini mengurangi risiko pencurian identitas dan penggunaan data pribadi yang tidak sah.

Individu dan organisasi dengan pemahaman yang baik tentang kebutuhan untuk melindungi data pribadi melalui keterampilan digital lebih dapat menetapkan langkah-langkah keamanan yang tepat untuk informasi sensitif mereka. Membuat kata sandi yang aman dan unik untuk setiap akun online adalah komponen penting dari prosedur keamanan digital. Memahami

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

nilai kata sandi yang rumit memungkinkan orang untuk menghindari menggunakan kata kunci yang dapat diprediksi dan rentan terhadap upaya hacking. Selain itu, mengakui kebutuhan untuk mengubah kata sandi secara berkala Juga penting untuk memastikan perlindungan data pribadi.

Selain menggunakan kata sandi yang aman, mengetahui enkripsi data adalah komponen penting dari keterampilan digital yang baik. Dengan menggunakan teknik enkripsi yang tepat, data sensitif dapat diterjemahkan ke dalam format yang tidak dapat dimengerti oleh orang yang tidak berwenang, memastikan keamanan dan integritas data bahkan jika disita oleh individu yang tidak sah. Selain itu, mengetahui perlindungan keamanan jaringan memungkinkan perusahaan untuk merancang firewall yang efektif dan sistem deteksi intrusion untuk mempertahankan jaringan mereka dari serangan eksternal. Organisasi dapat mengurangi risiko akses yang tidak sah ke data dan infrastruktur sensitif mereka dengan memahami kebutuhan untuk keamanan jaringan yang komprehensif. Individu dan organisasi dapat menciptakan lanskap digital yang lebih aman dengan meningkatkan keterampilan digital mereka dalam hal perlindungan data pribadi. Bahaya pencurian identitas dan eksploitasi data pribadi dapat dikurangi secara signifikan dengan menerapkan praktik keamanan digital yang efektif seperti menggunakan kata sandi yang kuat, enkripsi data, dan tindakan pencegahan keamanan jaringan yang komprehensif. Orang dapat merasa lebih percaya diri dalam menggunakan teknologi digital tanpa khawatir tentang pelanggaran keamanan dan privasi. (Hussin, 2022)

4. Peningkatan Kesadaran Hukum Digital

Literasi digital yang baik juga membutuhkan pemahaman tentang norma-norma hukum yang mengatur dunia digital. Ini melibatkan memahami aturan yang melindungi privasi online dan kekayaan intelektual, serta batasan pada perilaku kriminal Internet. Individu dengan kesadaran yang mendalam tentang hukum digital lebih mungkin untuk mengikuti aturan dan menghindari pelanggaran hukum cyber. Individu dan organisasi dapat menghindari kesalahan yang dapat melanggar pembatasan hukum yang berlaku di dunia digital jika mereka memahami komponen hukum digital. Memahami aturan yang mengatur privasi online memungkinkan orang untuk menyadari batasan tentang pengumpulan, penggunaan, dan penyiaran informasi pribadi secara online.

Individu dapat menghindari penggunaan informasi yang tidak sah yang dapat melanggar privasi orang lain dengan memahami hak dan tanggung jawab mereka sehubungan dengan privasi internet. Selain itu, pemahaman tentang peraturan kekayaan intelektual memungkinkan individu untuk memahami hak dan kewajiban mereka sehubungan dengan hak cipta, paten, dan merek dagang dalam konteks digital. Individu dengan pemahaman ini dapat menghormati hak kekayaan intelektual orang lain, menghindari

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

pelanggaran hak cipta, dan melindungi karya kreatif mereka sendiri dari penyalahgunaan.

Individu dapat menghindari penggunaan informasi yang tidak sah yang dapat melanggar privasi orang lain dengan memahami hak dan tanggung jawab mereka sehubungan dengan privasi internet. Selain itu, pemahaman tentang peraturan kekayaan intelektual memungkinkan individu untuk memahami hak dan kewajiban mereka sehubungan dengan hak cipta, paten, dan merek dagang dalam konteks digital. Individu dengan pemahaman ini dapat menghormati hak kekayaan intelektual orang lain, menghindari pelanggaran hak cipta, dan melindungi karya kreatif mereka sendiri dari penyalahgunaan. (Suryati, 2024)

5. Pendidikan Mengenai Etika Digital

Individu yang menerima pendidikan etika digital akan memahami dampak sosial dari perilaku *online* yang tidak etis, sehingga membantu meminimalkan penyebaran informasi yang menyesatkan dan konten berbahaya lainnya. Ini termasuk memahami pentingnya membatasi pengumpulan dan penggunaan data pribadi orang lain tanpa izin mereka, serta menghormati preferensi privasi yang dinyatakan oleh orang lain di jejaring sosial atau platform *online*. Individu yang menghormati privasi orang lain dapat menciptakan ekosistem digital yang kaya akan kepercayaan dan keamanan bersama.

Selain itu, pendidikan etika digital menekankan pentingnya menyebarkan pengetahuan dengan benar. Individu akan lebih curiga terhadap sumber informasi yang belum terverifikasi jika mereka memahami implikasi siaran informasi yang tidak akurat atau materi yang menyesatkan. Ini akan membantu mengurangi penyebaran berita palsu yang merugikan. Kesadaran yang mendalam tentang pentingnya verifikasi fakta dan kewaspadaan saat menyebarkan informasi akan membantu menciptakan lingkungan online yang dapat dipercaya, mengurangi ambiguitas dan kesalahpahaman di antara pengguna internet. Pendidikan etika digital juga mendorong orang untuk menggunakan internet dengan benar. Ini termasuk memahami konsekuensi sosial dari perilaku online seperti cyberbullying, pelecehan, dan prasangka.

Individu yang memahami bahwa setiap tindakan online memiliki konsekuensi lebih cenderung berperilaku positif dan mendukung lingkungan online yang ramah dan inklusif. Orang dapat membangun budaya online yang didasarkan pada rasa hormat terhadap privasi, kebenaran, dan tanggung jawab sosial dengan meningkatkan keterampilan digital mereka, yang mencakup komponen etika digital. Individu dan komunitas secara keseluruhan akan dapat memupuk lingkungan online yang sehat, produktif, dan etis yang mampu memberikan keuntungan positif bagi masyarakat secara keseluruhan dengan mengikuti standar etika digital. (D. P. and S. A. D. W. Setyawan, 2016)

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

6. Pengembangan Keterampilan Teknis

Individu dan perusahaan dapat melindungi diri dari ancaman cyber dengan menerima pelatihan dalam penggunaan perangkat lunak keamanan, firewall, dan antivirus, serta memahami pengaturan keamanan jaringan yang tepat. Di era di mana bahaya cyber menjadi semakin kompleks, keterampilan digital penuh harus melibatkan akuisisi keterampilan teknis yang diperlukan untuk melindungi sistem dan jaringan dari serangan keamanan siber. Pelatihan dalam penggunaan perangkat lunak keamanan memberikan pemahaman yang menyeluruh tentang cara mengidentifikasi, mencegah, dan memusnahkan ancaman keamanan digital. Individu dan perusahaan dapat memodifikasi strategi keamanan mereka untuk mengatasi ancaman yang terus meningkat dengan mempelajari cara kerja perangkat lunak keamanan.

Individu dengan keterampilan digital yang baik memahami cara menggunakan firewall dan antivirus untuk melindungi komputer mereka dari akses yang tidak sah dan infestasi malware. Individu yang memahami cara mengkonfigurasi dan mempertahankan firewall dan perangkat lunak anti-virus dapat mencegah akses jaringan yang tidak diinginkan dan menemukan dan menghapus risiko keamanan sebelum mereka merusak sistem. Memahami pengaturan keamanan jaringan yang tepat juga merupakan komponen penting dari keterampilan digital yang efektif. Individu dan organisasi dapat meningkatkan keamanan jaringan, mencegah serangan eksternal, dan melindungi data sensitif dari akses yang tidak sah dengan memahami praktik terbaik dalam konfigurasi jaringan. Mereka dapat membangun pertahanan yang kuat terhadap ancaman cyberyang muncul dengan mengetahui pengaturan keamanan jaringan secara menyeluruh. (A. K. Putra, 2015)

Individu dan organisasi dapat meningkatkan keamanan sistem dan jaringan mereka dengan mengembangkan keterampilan teknis yang diperlukan. Mereka dapat mengurangi bahaya serangan cyber dan mengamankan data sensitif mereka dengan menerima pelatihan berkelanjutan dan mendapatkan pemahaman menyeluruh tentang cara menggunakan perangkat lunak keamanan yang tepat, firewall, antivirus, dan pengaturan keamanan jaringan. Individu dan organisasi akan lebih siap untuk menangani masalah kejahatan siber di era digital jika mereka menerima pelatihan keterampilan digital yang memadai. Pemerintah, lembaga pendidikan, sektor komersial, dan masyarakat umum harus bekerja sama untuk meningkatkan pemahaman dan kesadaran tentang peran sastra digital dalam pencegahan kejahatan siber. Hasilnya, semua orang yang menggunakan Internet dapat menikmati lingkungan digital yang lebih aman, lebih etis, dan lebih aman.

El-Mujtama: Jurnal Pengabdian Masyarakat
Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

KESIMPULAN

Menguasai literasi teknologi adalah kunci untuk menghadapi dan mengatasi risiko keamanan cyber yang semakin kompleks di era digital ini. Dengan pemahaman yang baik tentang teknologi, individu dan organisasi dapat lebih efektif mengenali dan mencegah berbagai ancaman cyber, seperti malware, phishing, dan serangan ransomware. Literasi teknologi meliputi pemahaman tentang penggunaan perangkat lunak keamanan, praktik terbaik dalam pengelolaan kata sandi, dan pentingnya pembaruan sistem secara rutin. Peningkatan literasi teknologi juga mendorong kesadaran akan perilaku online yang aman, seperti berhati-hati dalam berbagi informasi pribadi dan mengenali tanda-tanda aktivitas mencurigakan. Selain itu, pendidikan dan pelatihan yang terus-menerus dalam bidang keamanan cyber adalah investasi penting untuk melindungi data dan sistem dari ancaman yang terus berkembang. Secara keseluruhan, menguasai literasi teknologi tidak hanya melindungi individu dan organisasi dari risiko keamanan cyber, tetapi juga membangun budaya keamanan yang proaktif dan tangguh di masyarakat digital.

Dengan demikian, peningkatan literasi teknologi harus menjadi prioritas dalam agenda pendidikan dan pelatihan untuk menciptakan ekosistem digital yang lebih aman dan terlindungi.

Vol 4 No 4 (2024) 2038–2049 P-ISSN 2746-9794 E-ISSN 2747-2736
DOI: 10.47467/elmujtama.v4i4.3583

DAFTAR PUSTAKA

Fuady, M. E. (2005). Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. *Mediator: Jurnal Komunikasi*, *6*(2), 255–264.

Gani, A. (2020). Cybercrime (Kejahatan Berbasis Komputer. *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, *5*(1), 16–29.

Hussin, M. H. and M. A. and L. G. (2022). Penguatan Literasi Digital dalam Merespons Peningkatan Ekonomi Digital pada Masa Pandemi COVID-19. *JPPM (Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, *6*(2), 349–356.

Isnaini, K., & Widodo, W. (2022). LITERASI DIGITAL BAGI KOMUNITAS DIGITAL MARKETER PURWOKERTO DALAM UPAYA MENCEGAH ANCAMAN KEAMANAN DATA DI DUNIA SIBER. *SELAPARANG: Jurnal Pengabdian Masyarakat Berkemajuan*, *6*(4), 1795. https://doi.org/10.31764/jpmb.v6i4.10764

Kurnia Putra, A. (2016). ANALISIS HUKUM YURISDIKSI TINDAK KEJAHATAN SIBER (CYBERCRIME) BERDASARKAN CONVENTION ON CYBERCRIME. *FAKULTAS HUKUM UNIVERSITAS JAMBI*, 22.

Liady, F., Jasiah, J., Fitria, E., Anggraeni, N., Oktarina, H., & Nurlita, S. (2022). PENDAMPINGAN LITERASI TEKNOLOGI. *E-Amal: Jurnal Pengabdian Kepada Masyarakat*, *2*(1), 547–554. https://doi.org/10.47492/eamal.v2i1.1186

Mary Annette Rose. (2007). Perceptions of Technological Literacy among Science, Technology, Engineering, and Mathematics Leaders . *Journal of Technology Education*, *19*.

Maryland State Department of Education. (2005). *Maryland Technology Education StateCurriculum .*

Putra, A. K. (2015). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. *Jurnal Ilmu Hukum*, *5*(2), 12.

Putra, B. K. B. (2018). Kebijakan aplikasi tindak pidana siber (cyber crime) di indonesia. *Pamulang Law Review Journal of Law*, *1*(1), 1.

Putriani, J. . , & H. (2021). Penerapan Pendidikan Indonesia di Era Revolusi Industri 4.0. *Jurnal Ilmu Pendidikan*, *3*.

Setyaningsih, R. and A. A. and P. E. and H. H. (2019). Model penguatan literasi digital melalui pemanfaatan e-learning. *Jurnal Aspikom*, *3*(6), 1200–1214.

Setyawan, D. P. and S. A. D. W. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity Melalui ASEAN Regional Forum On Cybersecurity Initiatives. *Jurnal Penelitian Politik*, *13*(1), 1–20.

Setyawan, I. (2020). *Penguatan literasi di era digital*. Prosiding Seminar Nasional PBSI-III Tahun 2020.

Suryati, S. and S. L. and D. R. and P. Y. S. (2024). Penguatan Literasi Digital Dalam Pencegahan Pelanggaran Hukum Siber (Cyber Law). *Wajah Hukum*, *8*(1), 84–94.

Tech Tally. (2006). National Academies Press. https://doi.org/10.17226/11691