

CYBER SAFETY, HEALTH AND WELFARE IN THE USE OF THE INTERNET

¹Diana Fitri, ²Dimas Muhammad Ramdani, ³Hijrotul Aini, ⁴Muhammad Efendi, ⁵Muhammad Qodri

Institut Agama Islam Syekh Maulana Qori Bangko

¹dianaputriiii2002@gmail.com, ²dismas271122@gmail.com, ³ainihijrotul@gmail.com,

⁴ependimuhammad527@gmail.com, ⁵godrimuhammad3@gmail.com

RIWAYAT ARTIKEL

Received : 29 April 2023

Revised : 30 April 2023

Accepted : 30 April 2023

Abstract: This article tries to present various and in-depth opinions related to Cyber Safety and Health and Wellness which are often happening lately. To convey this, the author uses the method of literature from various sources, so that a good description of cyber safety, health, and welfare in using the internet can be described. The conclusion obtained by cyber safety, health and welfare in using the internet, namely cyber safety or digital safety is the safe and responsible use of information and communication technology, which not only discusses maintaining the security and security of information, but also about being responsible for that information. , respect others online. While digital health and fitness is the ability to use technology not too long to the point where it is detrimental, and not excessively which can cause lifestyle changes, so as to regulate the duration of activities, ergonomic sitting postures and positions, as well as prevention of pornography and sexual exploitation.

Abstrak: Tulisan mencoba mengemukakan berbagai pendapat dan mendalam yang berkaitan dengan Cyber Safety dan Health and Wellness yang sering terjadi akhir-akhir ini. Untuk mengemukakan hal tersebut penulis menggunakan metode literatur dalam berbagai sumber, sehingga dapat mendeskripsikan dengan baik cyber safety, health and welfare dalam menggunakan internet. Kesimpulan yang diperoleh cyber safety, health and welfare dalam menggunakan internet, yakni cyber safety atau keselamatan digital merupakan penggunaan teknologi informasi dan komunikasi yang aman dan bertanggung jawab, yang tidak hanya membahas tentang menjaga keamanan dan keamanan informasi, tetapi juga tentang bertanggung jawab atas informasi tersebut, menghormati orang lain secara online. Sementara kesehatan dan kebugaran digital merupakan kemampuan untuk menggunakan teknologi tidak terlalu lama sampai titik di mana itu merugikan, dan tidak berlebihan yang dapat menyebabkan perubahan gaya hidup, sehingga dapat mengatur durasi beraktivitas, postur dan posisi duduk ergonomis, serta pencegahan pornografi dan eksploitasi Seksual.

Keywords:

Cyber Safety, Health and Welfare

Kata Kunci:

Keamanan Cyber, Kesehatan dan Kesejahteraan

PENDAHULUAN

Seiring meningkatnya penggunaan internet dan sosial media, terutama saat pandemi Covid-19 dan perkuliahan dilakukan dari rumah, terjadi peningkatan signifikan dalam akses dan pengguna internet di Indonesia. Cyber safety atau keselamatan digital merupakan penggunaan teknologi informasi dan komunikasi yang aman dan

bertanggung jawab, seperti internet, media sosial, game online, ponsel pintar, tablet, dan perangkat terhubung internet lainnya. Keselamatan siber tidak hanya membahas tentang menjaga keamanan dan keamanan informasi, tetapi juga tentang bertanggung jawab atas informasi tersebut, menghormati orang lain secara online (Hidayat et al., n.d.).

Kesehatan dan kebugaran digital merupakan hal yang penting untuk

menunjukkan kemampuan dalam menggunakan teknologi seperti ponsel, laptop, desktop dan tablet dan tidak menggunakan terlalu lama sampai titik di mana itu merugikan. Penggunaan berlebihan dan tidak tepat dalam teknologi dapat menyebabkan perubahan gaya hidup. Tulisan ini membahas seputar durasi beraktivitas, postur dan posisi duduk ergonomis, serta pencegahan Pornografi dan Eksploitasi Seksual.

METODE

Metode yang digunakan dalam penulisan artikel ini dengan melakukan studi literatur dari berbagai sumber sehingga dapat mendeskripsikan keamanan, kesehatan, dan kesejahteraan cyber dalam penggunaan internet, agar dapat dipahami oleh pembaca yang budiman.

PEMBAHASAN

1. Mengenal Cyber Safety (keselamatan digital)

Seiring meningkatnya penggunaan internet dan sosial media, terutama saat pandemi Covid-19 dan perkuliahan dilakukan dari rumah, terjadi peningkatan signifikan dalam akses dan pengguna internet di Indonesia. Kuota data sudah menjadi kebutuhan sehari-hari dan gawai atau perangkat digital kini diakses oleh pelajar, anak muda, juga mahasiswa dengan intensitas yang luar biasa. Jejaring web di seluruh dunia memungkinkan pelajar dan mahasiswa kita untuk memperbesar akses, tidak sekedar pertemuan kelas virtual, bahkan juga mengakses internet setiap hari untuk bekerja dan bersenang-senang untuk menyelesaikan penelitian untuk esai dan tugas, tetap berhubungan melalui media sosial, melakukan pembelian online, dan mencari hiburan terbaru.

Cyber safety atau keselamatan siber merupakan penggunaan teknologi informasi dan komunikasi yang aman dan bertanggung jawab, seperti internet, media sosial, game online, ponsel pintar, tablet, dan perangkat

terhubung internet lainnya. Hal ini tidak hanya membahas tentang menjaga keamanan dan keamanan informasi, tetapi juga tentang bertanggung jawab atas informasi tersebut, menghormati orang lain secara online, dan menggunakan 'netiket' (etiket internet) yang baik. Keamanan siber juga mencakup menjaga komputer dan browser Anda tetap mutakhir, menggunakan perangkat lunak antivirus dan firewall terbaru, dan mempelajari seperti apa perilaku online yang mencurigakan atau antisosial (Hidayat et al., n.d.).

Maria mengatakan, Cyber Safety adalah sebuah bentuk keamanan saat mengakses internet. Seperti yang kita ketahui bahwa segala jenis kejahatan sekarang bisa terjadi dengan melalui jaringan internet, untuk itulah keamanan internet menjadi salah satu hal yang penting. sangat penting terutama untuk anak-anak yang rasa ingin tahunya tinggi (Budiono, n.d.)

a. Urgensi Cyber Safety

Revolusi teknologi telah sepenuhnya membuka dunia kita dan mengubah cara kita belajar, menyaring, dan menyerap informasi. Tetapi kemajuan tidak datang tanpa kelemahan atau kerugian. Untuk setiap perkembangan baru, ada konsekuensi yang harus dihadapi.

Komputer dan Internet telah membuka wawasan pengetahuan baru dan membawa seluruh sistem pendidikan lebih dekat kepada siswa. Penelitian menjadi mudah dengan akses mudah ke World Wide Web, dan bahkan peneliti yang mengandalkan data sekunder pun dapat menggunakan media tersebut untuk mendapatkan semua data relevan yang diperlukan untuk proyek serta tugas kuliah.

Internet telah menjadi pendukung talenta masyarakat luas, karena sekarang bahkan siswa umum saja dapat membuat proyek yang luar biasa dengan kemudahan bantuan penelitian online yang aksesibel. Meski, dibalik media animasi, audio-visual yang melimpah itu terdapat potensi distraktor

atau pemecah konsentrasi serta potensi kecanduan pada gawai. Namun masalah ini termasuk hal kecil dan dapat dengan mudah ditangani dengan akses dan pengawasan yang terkontrol.

Bahaya yang lebih besar terletak pada pemangsa yang menunggu untuk menerkam korban yang lengah. Pemangsa bisa berniat untuk menyakiti mereka secara fisik, sosial dan finansial. Pelajar sangat rentan karena mereka terbiasa di dalam lingkungan terlindung dan lingkungan positif di sekolah atau kampus, yang dimaksudkan untuk menumbuhkan kepercayaan diri dan kreativitas mereka, sehingga tidak sadar bahwa tidak semua pengguna internet adalah orang baik dan beraktivitas positif di luar sana.

Umpan Seperti janji palsu, informasi yang salah, dan penawaran yang menguntungkan agar target mereka terperdaya dan tertipu. Oleh karenanya, membangun paradigma bahwa ada di luar sana orang yang berniat jahat dan melakukan kriminalitas melalui dunia maya. Lebih baik mencegah daripada mengobati, lebih baik waspada daripada menyesal. Oleh karenanya, mendidik pengguna muda Internet tentang kejahatan di Internet mungkin bukan hal yang buruk.

Para pelajar dan mahasiswa perlu disadarkan akan bahaya ini agar mereka dapat menggunakan sumber daya yang berharga untuk kebutuhan pendidikan mereka tanpa menjadi korban kejahatan dunia maya apa pun. Semakin banyak edukasi yang mengajarkan pentingnya keamanan Internet bagi siswa, sumber daya yang dapat dibagikan oleh guru, siswa, dan orang tua, semakin komprehensif ada perlindungan yang dibentuk untuk semua pengguna.

b. Jenis-jenis Umum Serangan Siber di Dunia Digital (Internet)

Serangan siber akan terus ada selama masih ada perangkat komputasi yang terhubung ke Internet. Terlebih selama

pandemi Covid-19, serangan siber tersebut angka kian naik saja mengingat makin banyak pula pengguna yang bekerja dan belajar dari rumah dengan memanfaatkan jaringan Internet.

Keamanan siber (Cyber security) adalah praktik untuk melindungi sistem, jaringan, data, dan program dari ancaman atau serangan digital. Serangan-serangan ini biasanya bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif; melakukan pemerasan uang pada korban, atau mengacaukan sistem. Berikut adalah bentuk-bentuk serangan siber yang telah berhasil dideteksi dan dipelajari, untuk diwaspadai (Hidayat et al., n.d.):

1) Malware

Malware adalah perangkat lunak (software) yang dirancang secara khusus untuk mendapatkan akses tidak sah (unauthorized access) atau menyebabkan kerusakan pada komputer. Malware memiliki kadar bahaya tingkat tinggi karena di dalamnya terdapat virus. Saat perangkat lunak itu sudah berhasil menyusup ke perangkat yang digunakan, Malware bisa dengan cepat merusak apa saja yang ada di dalamnya (Hidayat et al., n.d.).

Kerusakan yang disebabkan oleh program jahat ini dapat merusak sistem, mencuri dan menghapus data penting, hingga membajak komputer untuk memantau aktivitas komputer pengguna. Umumnya, serangan berbahaya ini bisa masuk ke perangkat saat pengguna men-download suatu file hingga di-install. Jangan dianggap program yang didownload oleh pengguna ini tampak seram dan mencurigakan, malware kadang diinstal dengan sukarela karena wujudnya yang menarik hati pengguna, seperti software gratis atau game mini yang menarik. Berikut cara menghindari serta melindungi diri dari malware:

a) Instal dan gunakan perangkat lunak anti-malware,

- b) Waspada terhadap unduhan,
- c) Temukan tanda-tanda malware pada perangkat.

2) Phising

Phishing adalah jenis serangan rekayasa sosial yang sering digunakan untuk mencuri data pengguna, termasuk kredensial login (akun), dan nomor kartu kredit. Serangan siber itu terjadi ketika penyerang menyamar sebagai entitas terpercaya (baik berupa website atau email palsu), menipu korban untuk membuka email, pesan instan, atau pesan teks. Praktiknya kadang pula phisher (pelaku phishing) mengirim email palsu yang menyerupai email dari sumber terpercaya.

Phishing menjadi pilihan yang populer di kalangan para peretas karena dinilai murah dan kemudahan, serta efektivitasnya cukup tinggi. Meskipun banyak organisasi yang telah menerapkan sistem keamanan untuk memblokir serangan phishing, namun penyerang juga semakin memiliki peralatan phishing yang lebih canggih. Phishing memiliki ciri-ciri sebagai berikut:

- a) Bahasa yang mengancam Anda atau memaksa Anda untuk
- b) bertindak sekarang Permintaan informasi pribadi atau bagi Anda untuk memverifikasi kata sandi Anda.
- c) Iming-iming hadiah tak terduga seperti memenangkan kontes atau mendapatkan janji vaksin yang tidak Anda daftarkan
- d) Kesalahan ejaan atau tata bahasa, cacat desain, dan tautan atau alamat email yang sepertinya tidak benar

3) Ransomeware

Ransomware adalah bentuk malware yang menginfeksi komputer atau perangkat Anda. Ketika ransomware mengambil alih komputer atau perangkat Anda, itu mengunci Anda dari komputer atau perangkat itu seluruhnya atau file tertentu. Untuk mendapatkan ransomware di komputer atau perangkat Anda, penjahat cyber menipu Anda agar mengunduh program yang terlihat sah.

Tetapi apa yang sebenarnya Anda unduh adalah perangkat lunak yang dirancang untuk mengendalikan informasi Anda sehingga Anda tidak dapat lagi mengaksesnya. Mereka kemudian menolak akses ke komputer, perangkat, atau file Anda kecuali Anda membayar uang tebusan. Anda biasanya akan tahu ketika Anda terserang ransomware jika Anda menerima pemberitahuan yang menyatakan bahwa komputer atau data Anda telah dikunci dan permintaan agar pembayaran dilakukan agar Anda bisa mendapatkan kembali akses. Terkadang pemberitahuan menyatakan bahwa pihak berwenang telah mendeteksi aktivitas ilegal di komputer Anda, dan pembayarannya adalah denda untuk menghindari penuntutan. Ada dua jenis ransomware yang umum:

- a) Lockscreen ransomware, yakni menampilkan gambar yang mencegah Anda mengakses komputer Anda
- b) Encryption ransomware, mengenkripsi file di hard drive sistem Anda dan terkadang di drive jaringan bersama, drive USB, hard drive eksternal, dan bahkan beberapa drive penyimpanan cloud, mencegah Anda membukanya.
 - a) Berikut adalah langkah-langkah yang dapat Anda ambil untuk melindungi diri dari serangan ransomware:
 - b) Hindari unduhan yang mencurigakan.
 - c) Cadangkan file anda secara teratur.
 - d) Selalu perbarui sistem operasi.

4) Insider Threat

Insider Threat merupakan ancaman berbahaya bagi organisasi yang berasal dari orang-orang di dalam organisasi, seperti karyawan, mantan karyawan, atau rekan bisnis, yang memiliki informasi orang dalam mengenai praktik keamanan, data, dan sistem komputer organisasi. Untuk mencegah ini, perusahaan atau organisasi harus memperkuat keamanan sistemnya untuk mencegah terjadinya insider threat.

5) Credential Reuse

Jenis cyber attack berikutnya adalah Credential Reuse. Jika memiliki username, password dan PIN yang mirip atau sama di beberapa akun, maka itu menjadi makanan empuk dari Credential Reuser ini.

Hal karena konsep dari jenis cyber attack ini yang menggunakan ulang beragam informasi penting yang sudah mereka dapatkan sebelumnya. Ketika hacker sudah mendapatkan informasi penting itu, mereka segera menyerang akun-akun korban lainnya. Ini tentunya sangat berbahaya, tapi untuk mendapatkan itu semua, hacker sudah melancarkan serangan yang lainnya terlebih dahulu untuk mendapatkan berbagai informasi penting. Untuk mencegah serangan jenis ini Anda sebaiknya perlu untuk mengganti password akun secara berkala.

6) Man in the Middle

Jenis cyber attack yang terakhir adalah Man in the Middle. Sesuai dengan namanya, cyber attack jenis ini menempatkan hacker di tengah-tengah komunikasi antara dua orang. Ketika mereka sedang berkomunikasi, maka berbagai informasi penting yang dibagikan di antara keduanya bisa dicuri oleh hacker. Selain mengambil informasi, hacker juga bisa menyisipkan malware ke dalam informasi yang dibagikan sehingga menambah masalah untuk kedua orang tersebut.

c. Hal-hal yang harus dilakukan untuk Menjaga Keamanan Perangkat

Setelah mengetahui jenis-jenis serangan umum pada perangkat kita dan bahayanya, ada baiknya untuk mengikuti langkah-langkah ini untuk membantu memvaksinasi teknologi Anda terhadap kejahatan dunia maya:

- 1) Pembaruan perangkat lunak komputer dan ponsel cerdas membantu memperbaiki kelemahan keamanan dan melindungi data. Saatnya untuk berhenti mengklik "Ingatkan Saya Besok" ketika

perangkat Anda meminta untuk mengunduh dan meng-install pembaruan.

- 2) Hanya unduh perangkat lunak langsung dari produsen dan sumber tepercaya lainnya. Di seluruh web, peretas menggunakan pemalsuan yang meyakinkan (peringatan pembaruan mendesak, halaman unduhan, dll.) untuk menyebarkan malware dan ransomware ke pengguna yang tidak curiga.
- 3) Investasikan dalam perlindungan virus dan spyware yang kuat dan tepercaya, baik Anda memiliki Mac atau PC. Pindai komputer Anda setidaknya seminggu sekali.
- 4) Cadangkan komputer Anda secara berkala ke hard drive eksternal atau sistem penyimpanan berbasis cloud jika Anda perlu memulihkan data dan file setelah serangan siber.
- 5) Saat menjelajahi web, aktifkan pemblokiran pop-up dan pertimbangkan penjelajahan pribadi. Cookie dapat membuka celah keamanan bagi peretas, jadi sebaiknya hapus secara berkala.
- 6) Pantau dengan cermat peringkat kredit, kartu kredit, dan rekening bank Anda. Siapkan pemberitahuan teks yang mengingatkan Anda tentang kemungkinan aktivitas penipuan.
- 7) Gunakan password (kata sandi) yang tidak mudah ditebak atau diretas. Kata sandi menawarkan perlindungan yang relatif lemah untuk informasi dan data pribadi karena sejumlah alasan yaitu bahwa efektivitasnya bergantung pada pengguna manusia. Sebagian besar dari kita bersalah karena menggunakan kembali kata sandi, berbagi kata sandi dengan orang lain, atau menuliskan kata sandi di lokasi yang mudah diakses. Kebiasaan membuat kata sandi yang buruk/lemah dapat membuat orang asing terlalu mudah mengakses perangkat, media sosial, dan akun keuangan Anda.
- 8) Aktifkan autentikasi dua faktor pada akun Anda jika tersedia. Ini dapat melindungi

akun Anda dari pelanggaran bahkan jika peretas menebak kata sandi Anda dengan benar.

- 9) Simpan kata sandi Anda dengan hati-hati. Ini berarti tidak ada catatan tempel di meja Anda, tidak ada daftar yang dikirim melalui email ke diri Anda sendiri, dan tidak ada dokumen yang tidak terlindungi di penyimpanan cloud. Sebagai gantinya, pertimbangkan aplikasi manajemen kata sandi, dokumen yang dilindungi kata sandi, atau petunjuk tulisan tangan yang disimpan di lokasi yang aman jauh dari perangkat Anda. (Hidayat, Muhammad Luthfi; Hariyatmi; Astuti, Dwi Setyo, 2021)

2. *Digital health and wellness (menjaga kesehatan fisik dan mental di lingkungan digital*

Kesehatan dan kebugaran digital adalah kemampuan untuk menggunakan teknologi seperti ponsel, laptop, desktop dan tablet dan tidak menggunakan terlalu lama sampai titik di mana itu merugikan. Berlebihan dan tidak tepat penggunaan dalam teknologi dapat menyebabkan perubahan gaya hidup.

Berikut adalah sejumlah tips menjaga posisi aman dan selamat ketika beraktivitas di depan komputer personal atau laptop:

a. Postur dan posisi duduk (Ergonomis)

Sebelum menghabiskan waktu lama di depan layar, baik laptop atau gadget, ada baiknya Anda perhatikan sisi ergonomis saat beraktivitas di lingkungan digital. Memiliki ruang kerja yang dioptimalkan secara ergonomis membantu Anda bekerja secara efisien dan aman. Dengan melindungi tubuh Anda dari cedera atau rasa sakit yang berulang, Anda dapat lebih fokus pada tugas Anda, yang pada gilirannya membuat Anda menjadi pekerja yang lebih efisien dan produktif.

b. Durasi beraktivitas dan Jeda

Apa pun yang digunakan secara berlebihan akan menjadi tidak baik, Karena itu Penting untuk menetapkan batas waktu yang

dihabiskan dengan ponsel, laptop, desktop, dan tablet, supaya memungkinkan untuk melakukan hal-hal penting lainnya dan menjalani kehidupan yang seimbang. Penggunaan ringan teknologi digital bisa bermanfaat, sementara penggunaan berlebihan penggunaan dapat berdampak negatif, penjelasannya sebagai berikut:

1) Masalah Kesehatan Fisik

Seiring waktu yang dihabiskan teknologi digital meningkat, waktu yang dihabiskan untuk aktivitas fisik berkurang, yang mungkin menjadi faktor penyebab anak dan masalah kesehatan fisik remaja seperti stamina yang sedikit dan kondisi tubuh yang kurang bugar. Kurangnya aktivitas fisik dapat mengganggu kesehatan dan kesejahteraan.

2) Gerakan Anggota Badan Terbatas

Ketika seseorang menghabiskan waktu berjam-jam setiap hari dalam menggunakan berbagai jenis perangkat genggam dengan kepala hanya terpaku ke depan, mereka berada di risiko mengalami text neck. Keluhan terkait text neck ini antara lain leher, punggung, lengan, jari, tangan, pergelangan tangan dan siku nyeri, serta sakit kepala dan mati rasa dan kesemutan pada alat gerak atas. Ada peluang untuk berkembang menjadi keluhan pada bahu.

3) Ketegangan Mata

Mata kemerahan atau iritasi karena menatap lampu latar layar yang terang untuk waktu yang lama, mata kering karena mengurangi berkedip, penglihatan kabur dan kelelahan umum dari menatap layar dan berusaha melihat font kecil dan gambar semua gejala ketegangan mata digital.

4) Gangguan Pendengaran

Paparan suara volume tinggi dalam waktu lama, terutama dengan penyumbat telinga, headset dan telepon, dapat berkontribusi untuk gangguan pendengaran. Anda dapat menjaga pendengaran Anda tetap utuh dengan mengikuti aturan 60/60. Dengarkan perangkat apa pun dengan maksimal hanya 60 persen darinya volume

penuh untuk total 60 menit sehari. Dengan mengambil ini sebagai saran peringatan dini, kita dapat melindungi pendengaran yang kita miliki sekarang, dan terus menikmati keajaiban suara itu sebagai hidup dan kehidupan.

5) Kecelakaan

Hindari penggunaan aktivitas online seperti selfie, sosial media atau aktivitas online lainnya untuk menghindari kecelakaan saat Anda sedang bergerak. Aturan lalu lintas juga telah membuat ini pelanggaran yang dapat dihukum dan mengundang denda. Meskipun menyenangkan untuk mendapatkan gambar yang bagus untuk mengabadikan momen, jangan biarkan obsesi media sosial untuk selfie sempurna, atau mendapatkan jumlah like yang Anda dapatkan, memengaruhi penilaian atau memengaruhi harga diri Anda atau memaksa diri Anda untuk membandingkan diri Anda dengan orang lain.

6) Penyalahgunaan Dan Ketergantungan

Penggunaan berlebihan mungkin bukan kecanduan. Jika pengguna menggunakan teknologi digital untuk tujuan yang sebenarnya, misalnya, pekerjaan rumah, penelitian, komunikasi penting dan rekreasi sedang, dan tidak menghambat kegiatan rutinitas lainnya, waktu yang dihabiskan dapat dibenarkan.

3. Mencegah Pornografi dan Eksploitasi Seksual

Aktivitas online memberikan kesempatan untuk mengekspresikan pendapat, menguji sikap, dan mengeksplorasi identitas dan sosial hubungan. Tetapi banyak dari kita yang tergoda untuk mengambil risiko, sering kali di bawah persepsi yang. Terkadang menunjukkan kontrol yang lemah atas waktu yang dihabiskan kegiatan online. Di luar ruangan kegiatan sangat penting untuk kesehatan yang baik dan juga dapat membantu untuk mencegah penggunaan berlebihan perangkat digital dan kecanduan

addiction aktivitas online, seperti bermain game (Hidayat et al., n.d.).

KESIMPULAN

Cyber safety atau keselamatan digital adalah penggunaan teknologi informasi dan komunikasi yang aman dan bertanggung jawab, seperti internet, media sosial, game online, ponsel pintar, tablet, dan perangkat terhubung internet lainnya. Keselamatan siber tidak hanya membahas tentang menjaga keamanan dan keamanan informasi, tetapi juga tentang bertanggung jawab atas informasi tersebut, menghormati orang lain secara online. Kesehatan dan kebugaran digital adalah kemampuan untuk menggunakan teknologi seperti ponsel, laptop, desktop dan tablet dan tidak menggunakan terlalu lama sampai titik di mana itu merugikan. Berlebihan dan tidak tepat penggunaan dalam teknologi dapat menyebabkan perubahan gaya hidup. Yang akan membahas seputar durasi beraktivitas, postur dan posisi duduk ergonomis, serta pencegahan Pornografi dan Eksploitasi Seksual

DAFTAR PUSTAKA

- Budiono. (n.d.). *Internet Safety: Tips dan Pentingnya Internet Sehat*. - Sukabumi Update. Internet Safety: Tips dan Pentingnya Internet Sehat. - Sukabumi Update. Retrieved April 30, 2023, from <https://www.sukabumiupdate.com/komputer/70321/internet-safety-tips-dan-pentingnya-internet-sehat>
- Hidayat, M. L., Hariyatmi, & Astuti, D. S. (n.d.). *BUKU BAHAN AJAR KOMPETENSI DIGITAL BAGI CALON PENDIDIK BIOLOGI*. Alinea Media Dipantara.
- Nuzli, M. (2021). *Pemanfaatan Teknologi Pendidikan dalam Pembelajaran*. Makassar: Yayasan Barcode.
- Thoiyibi, M., & Nuzli, M. (2022). *Using Edmodo as a Media of E-Learning*



Journal Educated Nation (JEN)

Learning in Educational Technology
Courses. *Sinkron: Jurnal Dan*

Penelitian Teknik Informatika, 7(2),
478–484.