Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 59-72
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Keamanan Internet Untuk Anak Dibawah Usia 17 Tahun

Muhammad Azwin Rifai [1,*], Reggya Ahmad Armansyah [1], Muhammad Riza Hashbillah [1]

[1] Informatika; Universitas Bhayangkara Jakarta Raya; Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143, (021) 88955882, 202210715210@mhs.ubharajaya.ac.id, 202210715222@mhs.ubharajaya.ac.id, 202210715194@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715210@mhs.ubharajaya.ac.id

Diterima: 13 Des 24; Review: 26 Des 24; Disetujui: 26 Des 24; Diterbitkan: 27 Des 24

Abstract

Internet security for children under the age of 17 has become an increasingly important issue in line with the rapid development of digital technology. This research aims to identify the risks faced by children when accessing the internet and to explore solutions that can be implemented to protect them from online threats. The method used in this research is the Quantitative Descriptive Research Method with Questionnaire Surveys and Literature Studies, focusing on the analysis of internet dangers, understanding of internet safety, and the roles of parents, educators, and related parties in protecting children in the online world. The research results show that despite various measures being implemented and the level of understanding of internet safety among children and teenagers in this study, there are still many issues in ensuring the safety of children when they use the internet. This research suggests the development of artificial intelligence (AI)-based technology to monitor children's online activities, raising awareness among parents and educators about the importance of supervision, and the need for stricter government policies. With the collaboration of various parties, it is hoped that a safer digital environment for children will be created.

***Keywords**: Internet security, children, parental supervision, internet dangers.*

Abstrak

Keamanan internet bagi anak-anak di bawah usia 17 tahun menjadi isu yang semakin penting seiring dengan pesatnya perkembangan teknologi digital. Penelitian ini bertujuan untuk mengidentifikasi risiko yang dihadapi oleh anak-anak saat mengakses internet dan untuk mengeksplorasi solusi yang dapat diterapkan guna melindungi mereka dari ancaman online. Metode yang digunakan dalam penelitian ini adalah Metode Penelitian Deskriptif Kuantitatif dengan Survei Kuisioner dan Studi Literatur, dengan fokus pada analisis bahaya internet, pemahaman tentang keamanan internet, serta peran orang tua, pendidik dan pihak yang berkaitan dalam menjaga keselamatan anak-anak di dunia maya. Hasil penelitian menunjukkan bahwa meskipun berbagai langkah sudah diterapkan dan dengan tingkat pemahaman anak-anak dan remaja tentang keamanan internet pada penelitian ini, masih ada banyak masalah dalam menjaga keselamatan anak-anak ketika mereka menggunakan internet. Penelitian ini menyarankan pengembangan teknologi berbasis kecerdasan buatan (AI) untuk memantau aktivitas online anak-anak, peningkatan kesadaran orang tua dan pendidik tentang pentingnya pengawasan, serta perlunya kebijakan yang lebih ketat dari pemerintah. Dengan kolaborasi berbagai pihak, diharapkan tercipta lingkungan digital yang lebih aman bagi anak-anak.

Kata kunci: Keamanan internet, anak-anak, pengawasan orang tua, bahaya internet.

1. Pendahuluan

Internet adalah jaringan global yang menghubungkan berbagai perangkat yang dapat bertukar informasi dengan cepat dan mudah. Kehadiran internet telah memberikan banyak manfaat dalam berbagai sektor seperti edukasi atau pendidikan, hiburan, kebutuhan bisnis, dan komunikasi antar satu dengan yang lain. Dengan berkembangnya teknologi dan hadirnya kemudahan akses, internet juga membawa risiko dan tantangan, terutama bagi pengguna yang masih di bawah usia 17 tahun yang rentan terhadap berbagai hal yang ada di internet.

Mengutip dari website Databoks BPS atau yang akrab dikenal dengan Badan Pusat Statistik, pada 2019 terdapat sejumlah 48,2% anak-anak di negara Indonesia yang telah menginjak usia 7-17 tahun pernah menggunakan internet. Data ini menunjukkan bahwa internet cukup mudah diakses bahkan oleh anak di bawah umur. Meskipun demikian, anak-anak cenderung terlena dengan penggunaan internet tanpa pengawasan orang tua, menempatkan mereka dalam bahaya. Walaupun internet mempunyai manfaat seperti mudahnya mengakses informasi dan memudahkan komunikasi, internet juga mempunyai dampak negatif. Beberapa dampak negatif penggunaan internet termasuk kecanduan, terpapar konten negatif, salah pergaulan, dan sebagainya (A. Irawan, 2019).

Maka dari itu, penting bagi orang tua dan wali untuk memperhatikan penggunaan internet anak agar terhindar dari masalah yang ditimbulkan oleh internet serta dapat mengambil langkah yang tepat untuk melindungi anak-anak dari dampak buruk internet. Edukasi dan pengawasan orang tua serta wali memiliki peran krusial dalam hal keamanan online anak mereka. Edukasi yang baik bisa membantu anak-anak memahami dan menghindari informasi yang tidak pantas serta mengetahui batasan apa yang harus diikuti ketika menggunakan internet. Dengan meningkatnya penggunaan internet di kalangan anak-anak, perlunya strategi keamanan yang efektif menjadi semakin mendesak.

Artikel ini bertujuan untuk mengeksplorasi berbagai aspek keamanan internet bagi anak di bawah umur, mengidentifikasi risiko yang ada, dan memberikan rekomendasi praktis bagi orang tua dan pendidik untuk meningkatkan perlindungan anak-anak di dunia maya. Melalui pemahaman yang lebih baik tentang tantangan dan solusi yang ada, diharapkan kita dapat menciptakan lingkungan internet yang lebih safe bagi anak-anak, sehingga bisa memanfaatkan hal baik dari teknologi tanpa terpapar pada risiko yang berbahaya.

2. Metode Penelitian

Metode penelitian yang dipakai di artikel ilmiah ini ialah Metode Penelitian Deskriptif Kuantitatif dengan Survei Kuisioner dan Studi Literatur. Penelitian deskriptif kuantitatif adalah jenis penelitian yang bertujuan untuk menggambarkan, menganalisis, dan menjelaskan suatu objek atau fenomena berdasarkan keadaan sebenarnya. Penarikan kesimpulan dilakukan dengan menggunakan data berupa angka-angka dari fenomena yang dapat diamati.

Metode deskriptif digunakan dalam penelitian ini untuk menunjukkan tingkat kesadaran anak-anak dan remaja terhadap keamanan internet. Data dikumpulkan melalui penyebaran

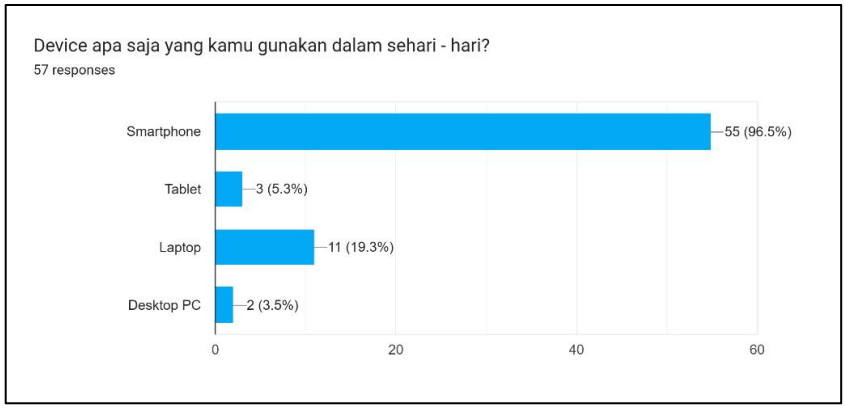
kuesioner kepada para responden. yang terdiri dari anak-anak dan remaja berusia di bawah 17 tahun. Penelitian ini juga menggunakan literatur dari berbagai jurnal ilmiah yang relevan untuk mendukung temuan survei.

3. Hasil dan Pembahasan

3.1. Kebiasaan Penggunaan Internet

Internet telah menjadi komponen yang tak terpisahkan dalam kehidupan masyarakat modern, termasuk di kalangan anak-anak dan remaja. Internet adalah jaringan komputer global yang menghubungkan berbagai perangkat dan jaringan di seluruh dunia dengan memanfaatkan protokol standar untuk berkomunikasi, internet memungkinkan akses ke informasi, komunikasi, hiburan, dan layanan pendidikan dengan cepat dan efisien (Guk Guk et al., 2023).

Namun, karena penggunaan internet yang semakin meningkat, perangkat yang digunakan untuk mengaksesnya pun menjadi bagian penting dari bagaimana anak-anak dan remaja menggunakan teknologi ini. Perangkat seperti smartphone, laptop, dan tablet mempengaruhi aktivitas yang dilakukan, durasi penggunaan, dan dampak terhadap kehidupan sehari-hari.

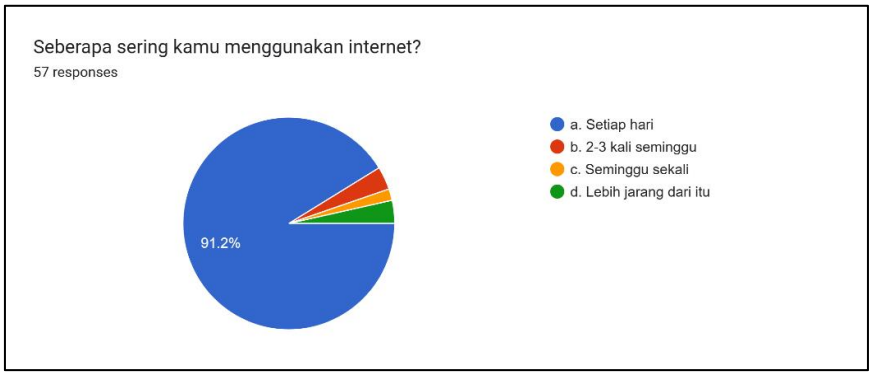


Sumber: Hasil Penelitian (2024)

Gambar 1. Grafik Penggunaan Device

Pada Gambar 1 menunjukkan bahwa Smartphone menjadi device yang paling sering digunakan oleh responden di Indonesia yang mencapai angka sekitar 96,5% lalu tablet di angka 5,3% Laptop di angka 19,3% dan PC di angka 3,5%.

Dari data ini bisa disimpulkan smartphone menjadi device yang paling sering digunakan. Popularitas smartphone dapat dikaitkan dengan portabilitasnya yang tinggi, kemudahan penggunaan, serta kemampuan untuk menjalankan berbagai aplikasi yang mendukung hiburan, komunikasi, dan pembelajaran serta relatif mudah untuk digunakan oleh berbagai kalangan.



Sumber: Hasil Penelitian (2024)

Gambar 2. Diagram Penggunaan Internet

Pada Gambar 2 menunjukkan tentang seberapa sering orang Indonesia menggunakan internet, 91,2% dari responden menggunakan internet setiap hari dan hanya sebagian kecil responden yang melaporkan penggunaan internet 2-3 kali seminggu atau lebih jarang. Tingginya frekuensi penggunaan internet mencerminkan ketergantungan anak dan remaja terhadap teknologi digital, baik untuk kebutuhan hiburan, komunikasi, maupun pembelajaran.. Angka yang sangat tinggi ini menjadi kekhawatiran tersendiri bagi orang tua atau wali tentang dampak dari seringnya penggunaan internet ini.

Frekuensi penggunaan internet yang tinggi, didukung dengan dominasi perangkat seperti smartphone, membawa dampak positif maupun negatif dalam kehidupan sehari-hari anak-anak dan remaja. Adapun dampak positif nya seperti yang dipaparkan oleh (Febriyana et al., 2023) adalah sebagai berikut :

1. Meningkatkan pengetahuan, karena dengan teknologi modern, anak-anak dapat dengan mudah dan cepat mengakses informasi yang berkaitan dengan tugas mereka.
2. Memungkinkan perluasan jaringan pertemanan, karena pengguna dapat dengan cepat dan mudah bergabung ke media sosial untuk berinteraksi dengan teman-teman.
3. Memudahkan komunikasi dengan orang lain dari seluruh penjuru dunia.
4. Internet dapat melatih kreativitas anak, karena kemajuan teknologi telah menghadirkan berbagai permainan yang kreatif dan menantang. Permainan ini juga memberikan manfaat bagi anak-anak dengan ADHD, karena dirancang dengan tingkat kreativitas dan tantangan yang tinggi.

Dalam penelitian yang dilakukan oleh Syahputra et al. (2023) dalam jurnal (Ervina Anatasya et al., 2024) ditemukan beberapa dampak negatif dari teknologi informasi dan komunikasi (TIK) pada anak-anak serta remaja, dampak-dampak ini termasuk:

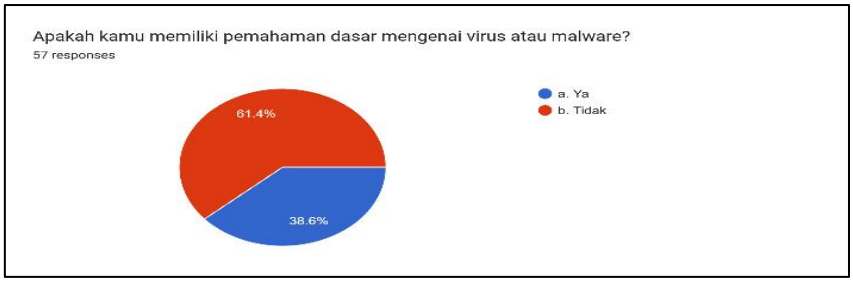
1. Kecenderungan untuk menolak bersosialisasi secara langsung dan lebih memilih berinteraksi melalui internet.
2. Peningkatan kasus penipuan dan kejahatan cyber.
3. Kejadian Cyber Bullying.
4. Peningkatan jumlah konten negatif yang cepat.
5. Kasus fitnah dan pencemaran nama baik yang meluas.
6. Perilaku menjauhkan diri dari hubungan yang dekat.
7. Kurang perhatian terhadap tugas dan pekerjaan.
8. Pemborosan waktu untuk aktivitas yang kurang produktif.
9. Penurunan kemampuan akademik dan kemampuan bekerja

Dengan smartphone sebagai perangkat utama dan tingginya frekuensi pemakaian internet, internet sudah menjadi komponen yang krusial dalam kehidupan anak-anak dan remaja. Hal ini menciptakan peluang besar untuk memanfaatkan teknologi sebagai alat untuk pendidikan dan pengembangan diri. Namun, penggunaan yang tidak terkontrol dapat menyebabkan efek buruk seperti ketergantungan, gangguan tidur, dan kurangnya aktivitas fisik jika tidak diawasi dengan baik.

3.2. Pemahaman Malware, Phising, dan Langkah Keamanan Digital

Selain manfaatnya yang luar biasa, internet juga memiliki banyak ancaman yang dapat membahayakan keamanan data dan perangkat pengguna, salah satunya adalah serangan virus dan malware serta ancaman phising. Memahami secara menyeluruh tentang ancaman ini merupakan langkah pertama yang penting dalam melindungi diri dari bahaya yang muncul saat menggunakan internet.

Malware, juga dikenal sebagai Malicious Software, adalah perangkat lunak yang dirancang khusus untuk melakukan tindakan yang membahayakan perangkat korban, seperti komputer, ponsel pintar, tablet, dll (Rafrastara et al., 2023). Malware adalah serangan siber yang memiliki kemampuan untuk merusak perangkat atau mencuri data pribadi. Kesadaran anak-anak tentang keberadaan virus atau malware umumnya rendah, Banyak anak tidak menyadari cara virus bekerja, seperti mengunduh aplikasi yang tidak aman atau klik tautan mencurigakan.

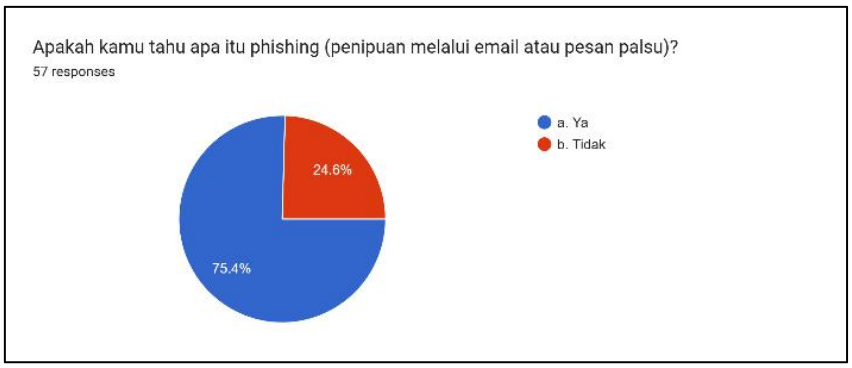


Sumber: Hasil Penelitian (2024)

Gambar 3. Diagram Pemahaman Dasar Mengenai Malware

Pada Gambar 3 menunjukkan mengenai rendahnya tingkat kesadaran anak-anak hingga remaja terhadap keberadaan virus atau malware di Indonesia. Yang dimana sebanyak 61,4% responden tidak memiliki pemahaman tentang malware, hanya sekitar 38,6% responden saja yang mengetahui atau memiliki pemahaman tentang virus atau malware.

Ancaman phising juga menjadi salah satu bentuk serangan siber yang rawan dialami oleh anak-anak dan remaja. Phishing (Password Harvesting Fishing) adalah suatu tindakan penipuan yang memanfaatkan email palsu atau situs web palsu untuk menipu pengguna, dengan tujuan agar pelaku dapat memperoleh data pribadi pengguna tersebut (D. Irawan, 2020).



Sumber: Hasil Penelitian (2024)

Gambar 4. Diagram Distribusi Pemahaman Mengenai Phising

Pada Gambar 4 menunjukkan bahwasannya banyak anak-anak hingga remaja di Indonesia sudah mengetahui apa itu phising. Sekitar 75,4% sudah mengetahui tentang phising, sedangkan 24,6% sisanya tidak mengetahui apa itu phising. Terlepas dari apakah sudah mengetahui apa itu phising anak-anak bahkan hingga remaja sekalipun sering menjadi target mudah karena mereka kurang waspada terhadap tanda-tanda serangan phishing itu sendiri, seperti alamat email yang tidak resmi atau tawaran yang menggiurkan untuk anak-anak seperti mendapat hadiah uang tunai dan sebagainya.

Untuk mengurangi risiko malware dan phishing, langkah-langkah keamanan seperti penggunaan password atau kata sandi yang kuat dan autentikasi dua faktor (2FA) dapat dilakukan. Two Factor Authentication atau autentikasi dua faktor merupakan proses autentikasi dua tahap yang mana proses validasi keabsahan akses oleh akun dilakukan menggunakan proses validasi tambahan selain menggunakan kata sandi yang biasanya menggunakan kode rahasia baik itu dikirimkan melalui layanan pesan singkat maupun menggunakan pembangkit khusus (Syahputri et al., 2023).

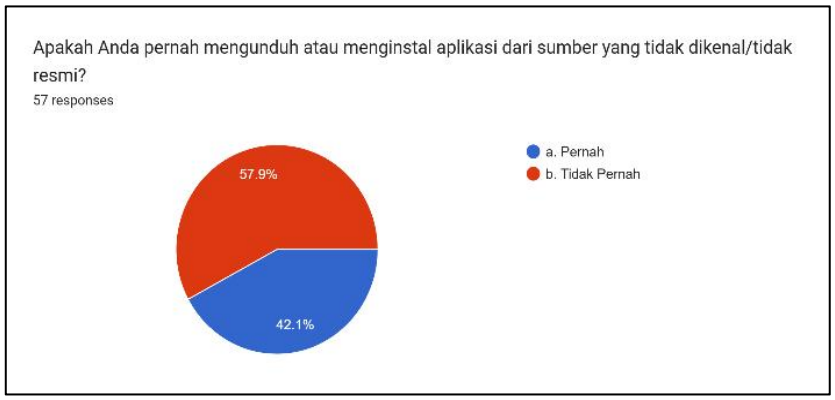
Sumber: Hasil Peneitian (2024)

Gambar 5. Diagram Penggunaan Kata Sandi Kuat

Pada Gambar 5 menunjukkan bahwa mayoritas anak-anak dan remaja di Indonesia telah menggunakan kata sandi yang kuat untuk melindungi akun mereka. Sekitar 86% responden sudah menggunakan kata sandi yang kuat yang menunjukkan bahwa kesadaran akan pentingnya menjaga akun sudah cukup tinggi. Kata sandi yang kuat sebaiknya terdiri dari kombinasi huruf (baik huruf besar maupun kecil), angka, dan simbol, serta memiliki panjang minimal 8 hingga 12 karakter. (Tan et al., 2024). Hal ini sangat penting terutama untuk akun yang menyimpan data yang sensitive.

Maka dari itu dibutuhkan peran dari berbagai pihak seperti sekolah, pemerintah, bahkan dari lingkungan keluarga sekalipun untuk mengedukasi anak-anak dan remaja di Indonesia untuk memberikan pemahaman mengenai pemahaman malware, phising hingga ke Langkah-langkah pencegahan yang dapat dilakukan demi mencegah bahaya dan ancaman negative dari internet yang tidak diinginkan.

3.3. Sumber Aplikasi dan Tautan yang Mencurigakan



Sumber: Hasil Penelitian (2024)

Gambar 7. Diagram Pengunduhan Aplikasi dari Sumber yang Tidak Dikenal

Pada Gambar 7 menunjukkan sebanyak (42,1%) responden yang masih mendownload aplikasi dari sumber yang tidak dikenal, karena tidak memiliki pengetahuan tentang hal tersebut yang menyebabkan banyak yang masih mengunduh di sumber tidak dikenal, dampak bahaya yang sering tidak dipahami oleh pengguna adalah dapat kehilangan data pribadi dan data (57,9%) responden yang tidak pernah mengunduh aplikasi dari sumber yang tidak dikenal, karena responden sudah mempelajari dari orang tua atau dari guru yang mengetahui hal tersebut dan akhirnya responden mengetahui tentang dampak bahayanya dari mengunduh atau menginstal aplikasi dari sumber tidak dikenal.

Hal tersebut menunjukkan bahwa dalam mengunduh atau menginstal aplikasi harus diperhatikan oleh pengguna apakah itu dari sumber resmi atau tidak resmi. Karena seperti yang kita ketahui Aplikasi dari sumber tidak resmi berkemungkinan menyembunyikan sebuah malware atau virus seperti ransomware, spyware, atau trojan yang digunakan untuk mencuri data pribadi pengguna.

Sumber: Hasil Penelitian (2024)

Gambar 8. Diagram Disribusi Penerimaan Pesan atau Link Mencurigakan

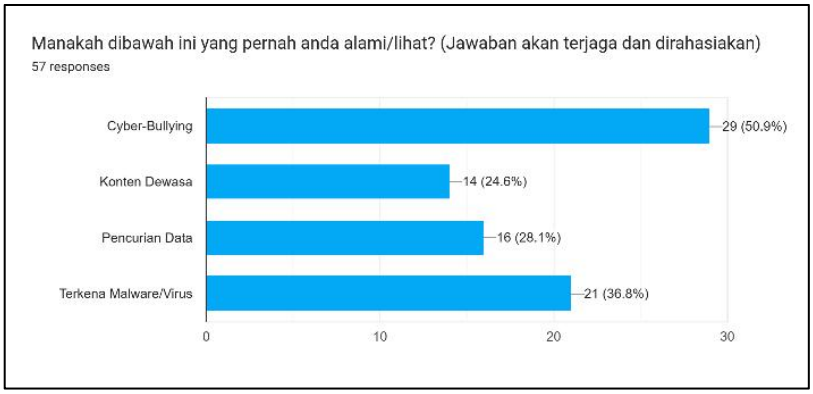
Pada Gambar 8 menunjukkan sebanyak (71,9%) responden yang sering maupun beberapa kali menerima pesan atau tautan dari orang tidak dikenal dan (28,1%) responden tidak pernah menerima pesan ataupun tautan dari orang yang tidak dikenal.

Seperti yang kita ketahui, tautan yang sangat mencurigakan menimbulkan ancaman karena sering digunakan untuk phishing, phishing dengan mengarahkan pengguna kepada suatu situs palsu yang terlihat mirip dengan situs resmi. Risiko yang terlibat dengan suatu seperti ini sangat serius dan memiliki akibat yang berbahaya. Salah satu ancamannya adalah kebocoran data-data pribadi. Selain itu, tautan ini dapat melakukan pengunduhan otomatis file berbahaya yang bisa langsung menginfeksi perangkat tanpa sepengetahuan pengguna. URL palsu dengan nama yang mirip dengan situs asli juga sering digunakan untuk mengelabui pengguna supaya tidak waspada (Vadila & Pratama, 2021).

Berdasarkan 2 hasil data di atas pengguna harus bisa mengubah kebiasaan, ketika mereka ingin mengunduh sebuah aplikasi dan ingin membuka tautan. Langkah yang harus dilakukan pertama kali adalah memastikan bahwa aplikasi diunduh dari sumber aplikasi yang

resmi, dan pengguna juga harus memeriksa izin yang diperlukan oleh suatu aplikasi sebelum diinstal dan menghindari aplikasi yang meminta akses berlebihan. Terkait tautan, sangat penting untuk tidak asal menekan tautan dari pengirim yang tidak dikenal, baik dari email, pesan whatsapp, atau media sosial lainnya. Pengguna harus selalu bisa memverifikasi keaslian situs web yang ingin mereka kunjungi dan pastikan bahwa URL-nya menggunakan https:/ dan nama domainnya yang asli dengan benar untuk menghindari halaman palsu.

3.4. Pengalaman Ancaman dan Bahaya Internet Serta Efektifitas Keamanan yang Diterapkan



Sumber: Hasil Penelitian (2024)

Gambar 9. Grafik Pengalaman/Ancaman yang Pernah Dialami

Pada Gambar 9 menunjukkan bahwa sebagian besar responden (50,9%) menyebutkan bahwa mereka pernah mengalami atau melihat tentang Cyber-Bullying, baik melalui media sosial maupun platform daring lainnya. Sekitar (24,6%) responden melaporkan pernah melihat konten dewasa yang tidak seharusnya diperlihatkan. Dan (28,1%) lainnya menyebutkan bahwa mereka pernah menyaksikan atau mendengar mengenai pencurian data yang terjadi pada lingkungan mereka. Serta (36,8%) pernah mengalami dan melihat kejadian terkena malware/virus.

Cyberbullying merupakan ancaman yang paling umum bagi remaja, yang dapat berdampak pada kesehatan mental dan emosional mereka. Berdasarkan Penelitian (Ningrum & Amna, 2020), mengungkapkan bahwa perundungan daring dapat menyebabkan stres, kecemasan, dan depresi pada anak-anak yang menjadi korban. Oleh karena itu, penting untuk meningkatkan literasi digital dan kesadaran mengenai bahaya ini..

Selain itu dampak paparan konten dewasa juga perlu diperhatikan, meskipun merupakan masalah yang sering kali diabaikan, namun juga menjadi faktor yang berisiko. Hasil penelitian menunjukkan bahwa anak-anak yang terpapar konten dewasa memiliki kemungkinan lebih tinggi untuk mengembangkan perilaku seksual yang tidak sehat atau mengalami gangguan psikologis terkait eksposur tersebut (Anggraini & Maulidya, 2020).

Di sisi lain, masalah pencurian data pribadi juga semakin sering terjadi. Serangan phishing, malware, dan pencurian identitas merupakan ancaman serius yang sering dihadapi oleh pengguna internet muda, dan ini menjadi lebih buruk karena mereka cenderung kurang memiliki pengetahuan tentang keamanan siber yang memadai.

3.5. Respons Terhadap Ancaman Online

Sumber: Hasil Penelitian (2024)

Gambar 10. Diagram Tentang Apa yang Dilakukan Jika Menerima Pesan Mencurigakan

Pada Gambar 10 menunjukaan bahwa anak-anak hingga remaja di Indonesia banyak yang akan mengabaikan ataupun memblokir dan melaporkan jika mereka dikirimi pesan yang tidak pantas dan mengganggu. Berdasarkan data tersebut terdapat (49,1%) yang akan memblokir, (36,8%) yang menghapus pesannya langsung, (8,8%) yang melaporkan kepada platform, (3,6%) yang memblokir dan melaporkan hal tersebut, dan (1,8%) yang mengabaikan saja.

Seperti yang kita tahu, anak-anak merupakan kalangan yang rawan terkena ancaman di internet. Orang tua harus membantu anak-anak dalam merespon ancaman online, seperti pesan mencurigakan, konten yang tidak pantas, dan mekanisme pelaporan serta pemblokiran.

Pesan mencurigakan memiliki ciri khas yang dapat dikenali, seperti penggunaan bahasa yang mendesak, nomor atau sumber pengirim yang tidak diketahui, serta isi pesan yang menginginkan informasi pribadi. Jadi anak-anak sangat perlu diajarkan untuk tidak merespon pesan yang tidak dikenal dalam bentuk apapun, karena dengan cara merespon terus dapat memicu lebih banyak interaksi dari pelaku. Anak-anak harus memahami pentingnya memverifikasi tentang isi pesan dari pengirim pesan dengan menanyakan kepada orang tua. Langkah setelah menanyakan kepada orang tua menyimpan pesan mencurigakan sebagai bukti, dan langsung memblokir nomor yang tidak dikenal.

Konten yang tidak pantas sekarang banyak sekali di internet dan memiliki berbagai jenis, seperti kekerasan, pornografi, ujaran kebencian suatu pihak, dan berita-berita hoaks. Jadi sebagai orang tua harus memberitahu tentang konten-konten yang seharusnya tidak di tonton oleh anak-anak agar mereka memahami ciri-ciri konten yang tidak pantas dan dapat mengambil tindakan.

Tindakan yang harus dilakukan jika menemukan konten yang tidak pantas, langkah yang harus dilakukan yaitu dengan membantu anak memahami fitur bawaan platform atau aplikasi, seperti tombol blokir maupun laporkan agar tidak akan muncul lagi konten-konten yang tidak pantas. Anak-anak juga harus memahami bahwa memposting ulang tentang konten tidak pantas dapat memperburuk keadaan.

Sangat penting bagi anak-anak untuk memahami cara menggunakan dan mengakses fitur melaporkan dari sebagian besar platform digital dan aplikasi untuk melindungi diri dari serangan online. Mereka dapat melaporkan konten yang tidak pantas dan akun-akun yang spam atau mengganggu agar mereka tidak dapat menghubungi mereka lagi. Dengan cara ini, anak-anak lebih mudah menanggapi ancaman online.

3.6. Peran Orang Tua Dalam Mengawasi Penggunaan Internet Anak

Sumber: Hasil Penelitian (2024)

Gambar 11. Diagram Distribusi Tentang Apakah Pernah Orang Tua Memberikan Pengarahan Dalam Menggunakan Internet

Pada Gambar 11 menunjukkan data sebagai berikut, diantaranya (33,3%) orang tua atau wali secara teratur sering mengajari anak mereka menggunakan internet, (56,1%) orang tua atau wali sesekali mereka mengajarkan menggunakan internet, dan (10,5%) yang orang tua atau walinya tidak sama sekali mengajarkan kepada anak-anaknya tentang menggunakan internet.

Orang tua bertanggung jawab untuk mengajarkan anak-anak cara menggunakan internet dengan aman dan efektif. Mereka harus memastikan anak-anak memahami cara mengakses internet secara aman, serta mengajarkan mereka untuk menghindari konten yang tidak sesuai atau berbahaya. Selain itu, orang tua perlu memantau aktivitas online anak-anak dan menjaga komunikasi yang terbuka mengenai apa yang mereka lakukan dan pelajari di internet (Guk Guk et al., 2023).

Sumber: Hasil Penelitian (2024)

Gambar 12. Diagram Distribusi Seberapa Sering Orang Tua Mengawasi Penggunaan Internet

Pada Gambar 12 menunjukkan sebesar (22,8%) untuk orang tua yang mengawasi setiap hari, (17,5%) untuk orang tua yang hanya mengawasi beberapa kali dalam seminggu, (42,1%) untuk orang tua yang jarang sekali melakukan pengawasan terhadap anak-anak dan (17,5%) untuk orang tua yang sama sekali tidak pernah mengawasi anak-anaknya menggunakan internet yang menyebabkan tidak terkontrolnya penggunaan internet seorang anak.

Orang tua bertanggung jawab untuk memberikan edukasi, pengawasan, bimbingan, serta pelatihan tentang hal-hal yang berkaitan dengan perkembangan dan pertumbuhan anak supaya bergerak ke arah yang lebih baik (Ervina Anatasya et al., 2024).

Dalam (A. Irawan, 2019) ada sejumlah tindakan yang bisa dilakukan oleh orang tua untuk mengawasi dan menanggulangi efek negatif dari pemakaian internet, terutama pada anak-anak dan remaja diantaranya:

1. Memberikan edukasi perihal dampak buruk internet agar remaja dapat memilih mana yang baik dan mana yang buruk saat menggunakan internet
2. Selalu dampingi atau awasi anak ketika menggunakan internet sehingga orang tua mengetahui kegiatan-kegiatan yang sedang dilakukan oleh anak.
3. Membatasi jumlah waktu yang dihabiskan anak-anak di bawah umur untuk mengakses internet setiap harinya dengan tujuan mencegah mereka mengunjungi situs web yang tidak disarankan untuk anak seumuran mereka.
4. Menanamkan nilai-nilai sosial pada anak-anak tentang dampak buruk internet, sehingga anak-anak dapat menggunakan internet dengan cara yang baik.
5. Melakukan kegiatan yang tidak berhubungan dengan internet, seperti bermain di taman atau jalan-jalan.

4. Kesimpulan

Sebagaimana diuraikan dalam Pendahuluan, tujuan penelitian ini adalah untuk menemukan cara yang efektif untuk meningkatkan keamanan internet bagi anak-anak di bawah

usia 17 tahun. Fokus utama penelitian ini adalah untuk mendapatkan pemahaman yang lebih baik tentang ancaman yang dihadapi anak-anak saat berada di internet dan untuk memberikan solusi dan langkah praktis yang dapat digunakan oleh orang tua, guru, dan pihak terkait lainnya.

Bagian Hasil dan Pembahasan menunjukkan bahwa meskipun berbagai langkah telah dicoba, masih ada banyak masalah dalam menjaga keselamatan anak-anak ketika mereka menggunakan internet. Oleh karena itu, pendidikan, pengawasan orang tua, dan penguatan hukum untuk perlindungan anak adalah tindakan pencegahan yang harus diprioritaskan.

Penelitian lebih lanjut mungkin menghasilkan teknologi berbasis kecerdasan buatan (AI) yang dapat mendeteksi secara otomatis konten berbahaya atau aktivitas mencurigakan serta meningkatkan kemampuan orang tua untuk mengawasi anak-anak. Selain itu, penelitian ini dapat mengeksplorasi penggunaan alat pendidikan digital yang dapat membantu anak-anak memahami pentingnya menjaga keamanan online.

Berdasarkan hasil penelitian ini, dapat diusulkan penerapan kebijakan yang lebih ketat dalam mengawasi platform digital yang digunakan oleh anak-anak. Selain itu, program pelatihan untuk orang tua dan pendidik tentang pentingnya pengawasan dalam penggunaan internet sangat diperlukan. Dengan langkah-langkah ini, diharapkan dapat terbentuk lingkungan digital yang lebih aman, mendukung perkembangan anak-anak di tengah pesatnya kemajuan teknologi.

Daftar Pustaka

Anggraini, T., & Maulidya, E. N. (2020). Dampak Paparan Pornografi Pada Anak Usia Dini. *Al-Athfaal: Jurnal Ilmiah Pendidikan Anak Usia Dini*, *3*(1), 45–55. https://doi.org/10.24042/ajipaud.v3i1.6546

Ervina Anatasya, Linda Cibya Rahmawati, & Yusuf Tri Herlambang. (2024). Peran Orang Tua Dalam Pengawasan Penggunaan Teknologi Digital Pada Anak. *Jurnal Sadewa : Publikasi Ilmu Pendidikan, Pembelajaran Dan Ilmu Sosial*, *2*(1), 301–314. https://doi.org/10.61132/sadewa.v2i1.531

Febriyana, F., Huzaifi, M., Wulan, C., Rahmadani, S., Praditya, R., Hidayat, S. A., Ashiddiqi, M. F., Oktavia, S. S., Zhafif, M. R., Nabila, M., Komunikasi, P., Islam, F. A., Muhammadiyah, U., Jakarta, M., Dahlan, J. K. H. A., Timur, K. C., Tangerang, K., Arsitektur, P., Teknik, F., … Tengah, P. (2023). Pengawasan Penggunaan Gadget Pada Anak Di RA Aisiyah Sawah Besar Jakarta Pusat. *Dalam Prosiding Seminar Nasional Pengabdian Masyarakat LPPM UMJ*, *1*(1).

Guk Guk, R. R., Cahya, B. D. I., Rahmayanty, D., & Regilsa, M. (2023). Peran Orang Tua Dalam Mengaplikasikan Internet Sebagai Media Pendidikan Bagi Anak. *Jurnal Pendidikan Dan Konseling (JPDK)*, *5*(6), 45–55. https://doi.org/10.31004/jpdk.v5i6.20182

Irawan, A. (2019). Aktivitas Anak - Anak Dan Pemuda Dalam Penggunaan Internet. *Cyber Security Dan Forensik Digital*, *1*(2), 50–56. https://doi.org/10.14421/csecurity.2018.1.2.1372

Irawan, D. (2020). Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising. *JIKI (Jurnal Llmu Komputer & Lnformatika)*, *1*(1), 43–46. https://doi.org/10.24127/jiki.v1i1.671

Ningrum, F. S., & Amna, Z. (2020). Cyberbullying Victimization dan Kesehatan Mental pada Remaja. *INSAN Jurnal Psikologi Dan Kesehatan Mental*, *5*(1), 35. https://doi.org/10.20473/jpkm.v5i12020.35-48

Rafrastara, F. A., Supriyanto, C., Paramita, C., & Astuti, Y. P. (2023). Deteksi Malware menggunakan Metode Stacking berbasis Ensemble. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(1), 11–16. https://doi.org/10.30591/jpit.v8i1.4606

Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(6), 768–773. https://doi.org/10.59837/jpmba.v1i6.256

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & ... (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam. *Jurnal Teknologi Dan …*, *14*(September), 163–173. https://doi.org/10.34010/jati.v14i2

Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, *2*(2), 1–4.