P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

Analisis Kesadaran Cyber Crime Di Kalangan Masyarakat Menengah Kebawah

[1]Muhamad Haikal Arief,[2]Khairatul Arifa Fitri, [3]Essy Malays Sari [1,2,3]Informatika,
Universitas Persada Indonesia YAI, kota Jakarta Pusat

E-mail: [1]muhamad.haikal.arief@upi-yai.ac.id,
[2]khairatul.arifa.f.2144190024@upi-yai.ac.id,
[3]essy.malays@upi-yai.ac.id,

ABSTRAK

Penelitian ini bertujuan untuk memahami tingkat kesadaran dan perilaku masyarakat menengah ke bawah terkait dengan cybercrime. Metode survei online digunakan untuk mengumpulkan data melalui kuesioner yang mencakup informasi tentang kebiasaan online responden. Hasil kuesioner menunjukkan bahwa kesadaran dan perilaku masyarakat dalam menghadapi cybercrime masih rendah. Rekomendasi untuk meningkatkan kesadaran masyarakat tentang cybercrime termasuk upaya edukasi, sosialisasi, program pelatihan, regulasi yang lebih ketat, dan kerjasama antara pemerintah, swasta, dan masyarakat. Pentingnya literasi digital dan kesadaran keamanan siber juga disorot sebagai langkah pencegahan yang dapat dilakukan oleh masyarakat untuk melindungi diri dari ancaman cybercrime.

Kata kunci : ***Kesadaran Cybercrime, Perilaku Masyarakat,Masyarakat Menengah Kebawah***

ABSTRACT

This study aims to investigate the level of cybercrime awareness and behavior among low- to middle-income individuals. An online survey method was employed to gather data through questionnaires that included information about respondents' online habits. The questionnaire results indicate that public awareness and behavior in dealing with cybercrime are still low. Recommendations to enhance public awareness about cybercrime include education efforts, socialization, training programs, stricter regulations, and collaboration among the government, private sector, and community. The importance of digital literacy and cybersecurity awareness is also highlighted as preventive measures that individuals can take to protect themselves from cybercrime threats.

Keyword : ***Cybercrime Awareness, Public Behavior, Low- to Middle-Income Individuals***

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

1. PENDAHULUAN

1.1. Latar Belakang Masalah

Internet adalah jaringan global yang menghubungkan miliaran perangkat komputer dan memungkinkan pertukaran informasi dan komunikasi tanpa batas. Dalam konteks cyber crime, internet sering kali menjadi medan bagi para pelaku kejahatan untuk melancarkan aksi mereka. Cyber crime, atau kejahatan siber, adalah istilah yang digunakan untuk menggambarkan kejahatan yang dilakukan dengan menggunakan komputer atau jaringan sebagai alat untuk mencapai tujuan ilegal, seperti penipuan, pencurian identitas, pelanggaran privasi, atau penyebaran konten ilegal. (Marcos to New PNP Chief Marbil: Address Terrorism, Cybercrime, n.d.)

Dengan berkembangnya teknologi saat ini yang digunakan untuk menciptakan, menyimpan, mengubah, dan menggunakan informasi dalam segala bentuknya. (Basry & Malays Sari, n.d.). ketergantungan masyarakat pada internet, cyber crime telah menjadi salah satu tantangan terbesar di era digital. Kejahatan ini tidak hanya menyerang individu, tetapi juga perusahaan dan pemerintahan, mengancam keamanan informasi dan menyebabkan kerugian finansial yang signifikan. Jenis-jenis cyber crime termasuk serangan ransomware, phishing, dan penyebaran malware, yang semuanya bertujuan untuk mengeksploitasi kerentanan manusia atau sistem keamanan untuk mencuri kata sandi, data, atau uang secara langsung.(*Cyber Crime - National Crime Agency*, n.d.)

Kejahatan siber telah menjadi ancaman yang semakin nyata, terutama bagi masyarakat yang kurang melek digital. Alur masuknya kejahatan ini sering kali dimulai dengan serangan phishing yang menyasar pengguna yang tidak menyadari bahaya online. Pelaku kejahatan mengirimkan email atau pesan yang tampak meyakinkan, dengan tujuan untuk mengelabui korban agar memberikan informasi sensitif seperti detail login atau data pribadi. Masyarakat kebawah, yang mungkin tidak memiliki pengetahuan yang cukup tentang keamanan siber, menjadi sasaran empuk karena mereka cenderung kurang waspada terhadap taktik penipuan semacam ini

Selanjutnya, kejahatan siber juga menyebar melalui media sosial dan aplikasi perpesanan, di mana pelaku kejahatan memanfaatkan ketidaktahuan pengguna untuk memancing informasi melalui penawaran palsu atau permintaan bantuan finansial yang mendesak. Mereka mungkin juga menggunakan malware yang dapat menginfeksi perangkat dan mencuri data tanpa sepengetahuan korban. Studi menunjukkan bahwa kelompok yang kurang beruntung, seperti mereka dengan pendapatan lebih rendah dan tingkat pendidikan yang lebih rendah, merasa kurang aman dalam pengalaman online mereka dan lebih mungkin menjadi korban serangan siber, sering kali dengan beban emosional yang lebih berat saat merespons serangan tersebut. (*Cybercrime Is Impacting Communities Differently, Study Finds _ Cyber Magazine*, n.d.)

Isu terkini menunjukkan bahwa perlunya cybersecurity menjadi semakin mendesak, terutama bagi masyarakat yang kurang paham akan

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

teknologi. Di tengah maraknya serangan siber yang semakin canggih, kelompok ini sangat rentan karena mereka sering kali tidak menyadari risiko yang ada atau cara melindungi diri mereka sendiri di dunia maya. Pendidikan cybersecurity yang efektif dan mudah diakses menjadi kunci untuk membantu masyarakat ini mengenali dan menghindari potensi bahaya. Program-program yang dirancang untuk meningkatkan kesadaran dan keterampilan digital dapat memainkan peran penting dalam mempersiapkan mereka menghadapi ancaman siber. (Buchan et al., 2024)

Selain itu, dengan berkembangnya teknologi dan kecerdasan buatan (AI), isu literasi AI juga menjadi perhatian. Masyarakat yang tidak memahami cara kerja AI berisiko tertinggal dan tidak dapat memanfaatkan manfaat yang ditawarkan oleh kemajuan ini. Oleh karena itu, langkah-langkah yang diambil untuk mengatasi ketidakmampuan teknologi tidak hanya penting untuk saat ini, tetapi juga untuk memastikan bahwa semua lapisan masyarakat dapat berpartisipasi secara penuh dalam ekonomi digital yang akan datang. Inisiatif seperti "Internet untuk Semua" yang bertujuan untuk meningkatkan akses dan pemahaman teknologi di kalangan masyarakat yang kurang beruntung, adalah langkah penting dalam mengatasi kesenjangan digital dan memperkuat keamanan siber di tingkat akar rumput. (Hironde, n.d.)

1.2. Batasan Masalah

Dalam konteks penelitian ini, fokus analisis akan dibatasi pada beberapa aspek utama untuk memastikan kejelasan dan kedalaman analisis. Pertama, penelitian akan mengkaji tingkat kesadaran cyber crime di kalangan masyarakat menengah kebawah di area urban dan semi-urban di Indonesia. Kedua, penelitian ini akan terbatas pada penggunaan media sosial sebagai medium utama interaksi digital, mengingat prevalensinya yang tinggi di kalangan masyarakat target. Ketiga, penelitian akan mengeksplorasi persepsi dan pemahaman tentang cyber crime, termasuk jenis-jenis kejahatan yang paling sering ditemui dan dampaknya terhadap individu dan komunitas. Keempat, penelitian ini akan menilai efektivitas sumber daya edukasi yang ada dan inisiatif pencegahan cyber crime yang telah dilakukan oleh pemerintah dan organisasi non-pemerintah. Kelima, penelitian akan dibatasi pada data yang dikumpulkan melalui survei online dan wawancara dengan responden yang dipilih secara acak dari populasi target**.** (Ramadhani & Raf'ie Pratama, n.d.)

1.3 Rumusan Masalah

1. Bagaimana cara meningkatkan literasi digital dan kesadaran keamanan siber bagi masyarakat yang kurang melek digital, terutama di tengah maraknya serangan siber yang semakin canggih dan berkembangnya teknologi kecerdasan buatan (AI)?
2. Bagaimana meningkatkan kesadaran masyarakat tentang risiko dan bahaya kejahatan siber di era digital?

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

3. Bagaimana menjembatani kesenjangan literasi digital antara kelompok masyarakat yang berbeda, terutama bagi mereka yang kurang akses terhadap teknologi dan informasi?

1.4 Manfaat Penelitian

1. **Peningkatan Kesadaran dan Pendidikan**: Penelitian ini akan memberikan wawasan tentang tingkat kesadaran cyber crime di kalangan masyarakat menengah kebawah, yang dapat digunakan untuk merancang program pendidikan dan kampanye kesadaran yang lebih efektif.
2. **Pengembangan Kebijakan**: Hasil penelitian dapat membantu pembuat kebijakan dalam mengembangkan strategi dan regulasi yang lebih baik untuk melindungi masyarakat dari kejahatan cyber, khususnya di area urban dan semi-urban.
3. **Bantuan untuk Organisasi Non-Pemerintah**: Organisasi non-pemerintah yang bekerja di bidang pencegahan cyber crime dapat menggunakan temuan penelitian ini untuk meningkatkan inisiatif mereka dan menargetkan sumber daya mereka dengan lebih baik.
4. **Kontribusi Akademis**: Penelitian ini akan menambahkan literatur akademis mengenai cyber crime di Indonesia, khususnya mengenai persepsi dan pengalaman masyarakat menengah kebawah.
5. **Pemahaman yang Lebih Baik tentang Peran Media Sosial**: Dengan fokus pada media sosial, penelitian ini akan memberikan pemahaman yang lebih mendalam tentang bagaimana platform ini dapat digunakan untuk meningkatkan kesadaran tentang cyber crime.
6. **Evaluasi Sumber Daya Edukasi**: Penelitian ini akan mengevaluasi efektivitas sumber daya edukasi yang ada, memberikan umpan balik yang berharga untuk perbaikan materi edukasi di masa depan.
7. **Pemberdayaan Masyarakat**: Dengan memahami tingkat kesadaran dan persepsi mereka terhadap cyber crime, masyarakat dapat diberdayakan untuk melindungi diri mereka sendiri dan orang lain di lingkungan digital.
8. **Dasar untuk Penelitian Lanjutan**: Temuan dari penelitian ini dapat menjadi dasar untuk studi lanjutan yang lebih spesifik atau terfokus pada aspek tertentu dari cyber crime.

Penelitian ini diharapkan tidak hanya memberikan manfaat teoretis tetapi juga praktis, dengan implikasi langsung pada kehidupan sehari-hari masyarakat dan upaya pencegahan cyber crime di Indonesia.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

2. LANDASAN TEORI

2.1 Memahami Dunia Kejahatan Siber dan Perlindungan Diri di Era Digital

Di era digital ini, internet menjelma menjadi ruang tanpa batas, tak hanya menawarkan kemudahan akses informasi dan komunikasi, tetapi juga membuka celah bagi berbagai tindakan kriminal yang dikenal sebagai **cybercrime**. Bab ini akan mengupas tuntas tentang cybercrime, mulai dari definisi, jenis-jenisnya, hingga langkah-langkah pencegahan yang dapat dilakukan untuk melindungi diri.

2.2 Memahami Definisi dan Ragam Ancaman

Cybercrime, atau kejahatan siber, mengacu pada berbagai tindakan kriminal yang memanfaatkan teknologi komputer dan jaringan internet. Kejahatan ini dapat menargetkan individu, organisasi, bahkan negara.

Cybercrime bukan hanya sebatas kejahatan yang dilakukan terhadap komputer. Kejahatan ini dapat melibatkan berbagai aktivitas ilegal, seperti:

- **Pencurian Data:** Mengambil informasi pribadi atau sensitif secara ilegal, seperti data kartu kredit, nomor jaminan sosial, atau informasi kesehatan.(*Www.Bssn.Go.Id _ Situs Web Resmi Badan Siber Dan Sandi Negara*, n.d.)
- **Penipuan Online:** Menipu orang untuk memberikan informasi pribadi atau uang melalui situs web palsu, email phishing, atau pesan teks.
- **Malware:** Menyebarkan program jahat seperti virus, worm, atau trojan horse untuk merusak komputer atau mencuri data.(News Revised Toolkit Empowers Law Enforcement with Responsible AI Practices News INTERPOL Welcomes New DNA Legislation in Belgium, n.d.)
- **Cyberbullying:** Mengganggu, melecehkan, atau mengancam orang lain secara online.
- **Kejahatan Pedofilia:** Memanfaatkan internet untuk mengeksploitasi atau melecehkan anak-anak.
- **Kejahatan Finansial:** Melakukan pencurian uang atau penipuan melalui internet, seperti pembobolan bank online atau penipuan kartu kredit.
- **Spionase Siber:** Mencuri informasi rahasia dari individu, organisasi, atau pemerintah.

3. METODOLOGI PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan **kualitatif** dengan metode **survei online**. Pendekatan kualitatif dipilih karena bertujuan untuk memahami dan mendeskripsikan pengalaman dan pemahaman masyarakat menengah ke bawah tentang cyber crime secara mendalam. Metode survei online dipilih karena memungkinkan peneliti untuk mengumpulkan data dari sampel yang besar dan beragam secara geografis

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

dengan cara yang efisien dan hemat biaya.

3.2 Lokasi Penelitian

Penelitian dilakukan secara online melalui media sosial. Media sosial dipilih sebagai platform penelitian karena memiliki jangkauan yang luas dan mudah diakses oleh masyarakat menengah ke bawah.

3.3 Waktu Penelitian

Penelitian ini dilaksanakan dalam kurun waktu 3 Bulan dimulai dari bulan Maret hingga bulan Mei tahun 2024.

3.4 Sumber data

Sumber data dalam penelitian ini adalah **responden** yang merupakan masyarakat menengah ke bawah yang aktif menggunakan media sosial. Responden akan direkrut melalui berbagai platform media sosial, seperti WhatsApp, Facebook, Twitter, dan Instagram.

3.5 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian ini adalah **kuesioner online**. Kuesioner online akan dikembangkan menggunakan platform survei online yang terpercaya dan mudah digunakan oleh responden. Kuesioner akan berisi pertanyaan-pertanyaan yang dirancang untuk mengukur pengetahuan, sikap, dan perilaku responden terkait cyber crime.

3.6 Teknik Analisa Data

Analisis data dalam penelitian ini menggunakan metode **analisis statistik deskriptif**. Analisis statistik deskriptif akan digunakan untuk mendeskripsikan karakteristik responden, menganalisis distribusi frekuensi dan persentase jawaban responden, serta mengidentifikasi pola dan tren dalam data.

3.7 Etika Penelitian

Penelitian ini akan dilakukan dengan menjunjung tinggi etika penelitian. Etika penelitian yang akan dipatuhi dalam penelitian ini adalah:

- **Informed consent**: Responden akan diberikan penjelasan tentang tujuan penelitian, prosedur penelitian, dan potensi risiko dan manfaat penelitian sebelum mereka memberikan persetujuan untuk berpartisipasi.
- **Kerahasiaan**: Identitas responden akan dirahasiakan dan data penelitian hanya akan digunakan untuk keperluan penelitian.
- **Kejujuran**: Peneliti akan berusaha untuk jujur dan

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

objektif dalam mengumpulkan dan menganalisis data.

3.8 Keabsahan Data

Keabsahan data dalam penelitian ini akan dijaga dengan menggunakan beberapa teknik, antara lain:

- **Validitas kuesioner**: Kuesioner online akan diuji validitasnya sebelum disebarluaskan kepada responden.
- **Reliabilitas kuesioner**: Kuesioner online akan diuji reliabilitasnya untuk memastikan konsistensi hasil.
- **Triangulasi**: Data penelitian akan triangulasi dengan menggunakan sumber data lain, seperti studi literatur dan wawancara mendalam.

3.9 Jadwal Penelitian

Table 1. Tahapan kegiatan
Sumber: Pribadi

Tahap	Kegiatan	Waktu
1	Pengembangan kuesioner online	4 Minggu
2	Uji validitas dan reliabilitas kuesioner online	3 Minggu
3	Penyebaran kuesioner online	1 Mimggu
4	Pengumpulan data	1 Minggu
5	Analisis data	2 Minggu
6	Penyusunan laporan penelitian	1 Minggu

3.10 Hasil Yang di Harapkan

Hasil yang diharapkan dari penelitian ini adalah:

- Deskripsi yang mendalam tentang pengetahuan, sikap, dan perilaku masyarakat menengah ke bawah tentang cyber crime.
- Faktor-faktor yang memengaruhi tingkat kesadaran dan pemahaman masyarakat menengah ke bawah tentang cyber crime.
- Rekomendasi untuk meningkatkan kesadaran dan pemahaman masyarakat menengah ke bawah tentang cyber crime.

4. HASIL DAN PEMBAHASAN

4.1 Profil Responden

Dalam Penelitian ini penulis mengambil sample dari masyarakat sebanyak 100 orang. Dengan profil responden sebagai berikut

Table 2. Profil Responden
Sumber: Pribadi

Kriteria	Sub Kriteria	Jumlah
Jenis Kelamin	Laki-Laki	50
	Perempuan	50

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

4.2 Analisis Hasil Penelitian

Untuk mengetahui gambaran terhadap masyarakat tentang bahaya nya kejahatan Cyber Crime, digunakan analisis deskriptif berdasarkan tanggapan dan atas pertanyaan-pertanyaan dalam kuesioner. Item-item pertanyaan dalam edukasi kepada masyarakat digambarkan dalam bentuk table deskrispsi frekuensi.

Table 3.Tanggapan Responden Terhadap Kejahatan Cyber Crime
Sumber: Pribadi

No	Pertanyaan	Pernah	Tidak
1	Pernah kah Anda membagikan informasi pribadi Anda secara online?	40	60
2	Pernah kah Anda mengklik tautan yang mencurigakan dalam email atau pesan teks?	90	10
3	Pernah kah Anda membuka lampiran dari orang yang tidak dikenal? (Seperti Undangan Online)	95	5
4	Pernah kah Anda menggunakan password yang sama untuk beberapa akun online?	98	2
5	Pernah kah Anda melakukan transaksi online tanpa memastikan keamanan situs web?	80	20

Penjelasan tabel di atas:

Analisis Tanggapan

Berdasarkan tabel, dapat disimpulkan bahwa:

Frekuensi

- **F_x** = Jumlah responden yang memilih kategori "x"
- **F_total** = Jumlah total responden

Persentase

- **P_x** = (F_x / F_total) x 100%

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

Analisis

Pertanyaan 1: Pernahkah Anda membagikan informasi pribadi Anda secara online?

- **F_Pernah** = 40
- **F_Tidak** = 60
- **F_total** = F_Pernah + F_Tidak = 40 + 60 = 100
- **P_Pernah** = (F_Pernah / F_total) x 100% = (40 / 100) x 100% = 40%
- **P_Tidak** = (F_Tidak / F_total) x 100% = (60 / 100) x 100% = 60%

Interpretasi:

- 40% responden pernah membagikan informasi pribadi secara online.
- 60% responden tidak pernah membagikan informasi pribadi secara online.

Hal ini menunjukkan bahwa sebagian besar responden masih berhati-hati dalam membagikan informasi pribadi mereka secara online.

Pertanyaan 2: Pernahkah Anda mengklik tautan yang mencurigakan dalam email atau pesan teks?

- **F_Pernah** = 90
- **F_Tidak** = 10
- **F_total** = F_Pernah + F_Tidak = 90 + 10 = 100
- **P_Pernah** = (F_Pernah / F_total) x 100% = (90 / 100) x 100% = 90%
- **P_Tidak** = (F_Tidak / F_total) x 100% = (10 / 100) x 100% = 10%

Interpretasi:

- 90% responden pernah mengklik tautan yang mencurigakan dalam email atau pesan teks.
- 10% responden tidak pernah mengklik tautan yang mencurigakan dalam email atau pesan teks.

Hal ini menunjukkan bahwa sebagian besar responden berisiko mengklik tautan phishing atau malware.

Pertanyaan 3: Pernahkah Anda membuka lampiran dari orang yang tidak dikenal?

- **F_Pernah** = 95
- **F_Tidak** = 5
- **F_total** = F_Pernah + F_Tidak = 95 + 5 = 100
- **P_Pernah** = (F_Pernah / F_total) x 100% = (95 / 100) x 100% = 95%
- **P_Tidak** = (F_Tidak / F_total) x 100% = (5 / 100) x 100% = 5%

Interpretasi:

- 95% responden pernah membuka lampiran dari orang asing.
- 5% responden tidak pernah membuka lampiran dari orang asing.

Hal ini menunjukkan bahwa mayoritas responden berisiko membuka lampiran berbahaya.

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

Pertanyaan 4: Pernahkah Anda melakukan transaksi online tanpa memastikan keamanan situs web?

- **F_Pernah** = 80
- **F_Tidak** = 20
- **F_total** = F_Pernah + F_Tidak = 80 + 20 = 100
- **P_Pernah** = (F_Pernah / F_total) x 100% = (80 / 100) x 100% = 80%
- **P_Tidak** = (F_Tidak / F_total) x 100% = (20 / 100) x 100% = 20%

Interpretasi:

- 80% responden pernah melakukan transaksi online tanpa memastikan keamanan situs web.
- 20% responden tidak pernah melakukan transaksi online tanpa memastikan keamanan situs web.

Hal ini menunjukkan bahwa sebagian besar responden berisiko menjadi korban penipuan online atau pencurian identitas.

Analisis Tambahan

Jenis Kelamin: Tidak ada perbedaan yang signifikan dalam perilaku online antara responden pria dan wanita.

Pekerjaan: Terdapat beberapa variasi dalam perilaku online di antara berbagai pekerjaan. Sebagai contoh, mekanik cenderung lebih mungkin

4.3 Upaya Pencegahan Cybercrime

Dengan semakin maraknya cybercrime, penting untuk mengambil langkah-langkah untuk melindungi diri sendiri dan organisasi. Berikut beberapa tips pencegahan cybercrime:

- Gunakan kata sandi yang kuat dan unik untuk semua akun online Anda.
- Jaga agar perangkat lunak Anda selalu diperbarui dengan patch keamanan terbaru.
- Berhati-hatilah saat mengklik tautan atau membuka lampiran dalam email.
- Jangan memberikan informasi pribadi kepada orang asing online.
- Laporkan aktivitas cybercrime yang mencurigakan kepada pihak berwenang. (*Cyber Security_ Pengertian, Konsep, Jenis, Dan Ancaman Di Bisnis*, n.d.)

4.4 Konsep dan Jenis Ancaman

Keamanan siber (cybersecurity) adalah aktivitas yang dilakukan untuk melindungi sistem komputer dari serangan ilegal. Keamanan siber dapat berupa perangkat lunak (software), aplikasi, atau apa pun yang berhubungan dengan sistem komputer. Dengan menerapkan keamanan siber yang efektiff, perusahaan dan individu dapat menanggulangi berbagai ancaman di sistem komputer.

Namun, di balik dunia digital yang penuh kemudahan, terdapat berbagai jenis ancaman keamanan siber yang mengintai, di antaranya:

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

- **Pemalsuan Identitas:** Pencurian identitas seseorang di media sosial untuk melakukan tindakan kriminal.
- **Phishing:** Penipuan untuk mencuri informasi sensitif melalui pesan atau tautan palsu.
- **Cracking:** Percobaan penyusupan sistem komputer untuk mencuri data.
- **Spoofing:** Peniruan identitas pihak berwenang untuk mencuri data.
- **Serangan DDoS:** Serangan untuk melumpuhkan server website dengan banyak request.
- **Carding:** Pencurian data kartu kredit untuk melakukan transaksi ilegal.
- **Pemalsuan Data:** Pemalsuan informasi penting dalam dokumen digital.
- **SIM Swap:** Pencurian nomor telepon untuk mengakses akun online korban.
- **Botnet:** Jaringan perangkat komputer yang dibajak untuk melakukan penipuan dan serangan siber.
- **Cyberstalking:** Pelecehan dan intimidasi online.
- **Penipuan OTP:** Penipuan dengan meminta kode OTP untuk verifikasi akun.
- **Injeksi SQL:** Menyusupkan kode berbahaya ke database aplikasi.
- **Cyber Espionage:** Pengintaian sistem komputer untuk mencuri data rahasia.
- **Serangan Malware:** Penanaman program jahat untuk merusak komputer atau mencuri data. (Berita & Acara, n.d.)

Memahami cybercrime dan langkah-langkah pencegahannya merupakan langkah awal untuk menciptakan ruang digital yang aman dan terpercaya. Dengan kewaspadaan dan pengetahuan yang memadai, kita dapat melindungi diri dari berbagai ancaman di era digital ini.

4.5 Cara Melindungi Diri dari Ancaman Keamanan Siber

Di era digital ini, di mana berbagai informasi dan transaksi beralih ke dunia online, keamanan siber menjadi hal yang krusial. Berikut beberapa langkah yang dapat dilakukan untuk melindungi diri dari berbagai ancaman keamanan siber:

- **Perbarui perangkat lunak secara berkala:** Pastikan untuk selalu memperbarui software ke versi terbaru. Hal ini untuk mengantisipasi celah keamanan yang dimanfaatkan oleh para penjahat siber. Gunakan notifikasi update software untuk memudahkan Anda dalam memantau dan melakukan update.
- **Gunakan antivirus dan firewall:** Antivirus merupakan solusi utama untuk memerangi malware. Firewall membantu melindungi

P-ISSN: 1411-3635
E-ISSN: 2962-5645

data Anda dari serangan malware. Pilihlah antivirus dan firewall yang terpercaya dan sesuai dengan kebutuhan Anda.

- **Gunakan password yang kuat dan password manager:** Password yang kuat minimal memiliki satu huruf kecil, satu huruf besar, satu angka, dan empat simbol. Gunakan password manager untuk membantu Anda dalam mengelola password yang kompleks dan berbeda untuk setiap akun.
- **Gunakan Two-factor Authentication atau Multi-factor Authentication:** Two-factor authentication (2FA) dan multi-factor authentication (MFA) memberikan lapisan keamanan tambahan saat login. Selain username dan password, Anda akan diminta untuk memasukkan kode identifikasi pribadi seperti sidik jari atau OTP (One Time Password) yang dikirimkan melalui email atau aplikasi autentikasi.
- **Waspada terhadap email dan panggilan telepon mencurigakan:** Email dan panggilan telepon yang mencurigakan dapat menjadi tanda serangan phishing. Berhati-hatilah saat membuka email atau tautan yang tidak dikenal, dan jangan pernah memberikan informasi pribadi melalui panggilan telepon yang tidak terduga.
- **Lindungi informasi identifikasi pribadi:** Informasi identifikasi pribadi (PII) seperti nama, alamat, nomor telepon, data kelahiran, nomor jaminan sosial, alamat IP, dan detail lokasi, dapat disalahgunakan oleh penjahat siber. Jaga kerahasiaan PII Anda dan hindari membagikannya secara online di sembarang platform.
- **Gunakan perangkat seluler dengan aman:** Lindungi perangkat seluler Anda dengan password yang kuat, instal aplikasi hanya dari sumber terpercaya, selalu perbarui perangkat lunak, dan hindari mengirim informasi PII melalui pesan teks atau email.
- **Backup data secara teratur:** Backup data secara berkala membantu Anda dalam mengamankan data pribadi jika terjadi serangan siber atau kerusakan perangkat. Gunakan layanan backup cloud atau penyimpanan eksternal untuk menyimpan data penting Anda.
- **Gunakan WiFi publik dengan bijak:** Hindari melakukan transaksi online saat menggunakan WiFi publik yang tidak aman. Gunakan VPN (Virtual Private Network) untuk mengamankan koneksi internet Anda saat berada di tempat umum.
- **Lindungi dan pantau akun online Anda:** Pantau aktivitas akun online Anda secara berkala dan segera laporkan jika ada aktivitas mencurigakan. Lakukan pembekuan kredit jika Anda merasa data pribadi Anda telah disalahgunakan. (0 Tips Mengamankan Data Pribadi Dari Serangan Siber, n.d.)

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

4.6 Faktor-Faktor yang Mempengaruhi Kesadaran Cybercrime di Kalangan Masyarakat Menengah Kebawah

Kesadaran tentang cybercrime di kalangan masyarakat menengah ke bawah masih tergolong rendah. Hal ini disebabkan oleh beberapa faktor, di antaranya:

- **Pendidikan:** Masyarakat dengan tingkat pendidikan yang rendah umumnya memiliki pengetahuan yang terbatas tentang teknologi dan keamanan siber, sehingga mereka lebih mudah menjadi korban cybercrime.
- **Akses internet:** Masyarakat menengah ke bawah umumnya memiliki akses internet yang terbatas, sehingga mereka sulit mendapatkan informasi tentang cybercrime dan cara-cara menghindarinya.
- **Kemampuan finansial:** Masyarakat menengah ke bawah umumnya memiliki kemampuan finansial yang terbatas untuk membeli perangkat lunak keamanan siber dan mengikuti pelatihan tentang cybercrime.
- **Kesadaran hukum:** Masyarakat menengah ke bawah umumnya memiliki kesadaran hukum yang rendah, sehingga mereka lebih mudah menjadi korban cybercrime dan tidak mengetahui hak-hak mereka sebagai korban.
- **Budaya:** Budaya masyarakat menengah ke bawah umumnya kurang menghargai privasi dan keamanan data pribadi, sehingga mereka lebih mudah untuk membagikan informasi pribadi mereka di internet dan menjadi korban cybercrime.(Crimes Awareness Campaigns What You Can Do Cybercrime-#YouMayBeNext Tell Me More ✕, n.d.)

4.7 Dampak Cybercrime di Kalangan Masyarakat Menengah Kebawah

Cybercrime dapat memberikan dampak negatif yang signifikan bagi masyarakat menengah ke bawah, di antaranya:

- **Kerugian finansial:** Cybercrime dapat menyebabkan kerugian finansial bagi korban, seperti kehilangan uang, data pribadi, dan aset lainnya.
- **Kerusakan reputasi:** Cybercrime dapat merusak reputasi korban, baik secara pribadi maupun profesional.
- **Gangguan mental:** Cybercrime dapat menyebabkan gangguan mental bagi korban, seperti stres, kecemasan, dan depresi.

Kehilangan kepercayaan: Cybercrime dapat menyebabkan hilangnya kepercayaan korban terhadap teknologi dan internet.(United Nations Office on Drugs and Crime, n.d.)

4.8 Upaya Meningkatkan Kesadaran Cybercrime di Kalangan Masyarakat Menengah Kebawah

Mengingat dampak negatif cybercrime yang signifikan, maka perlu dilakukan berbagai upaya untuk meningkatkan kesadaran tentang

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

cybercrime di kalangan masyarakat menengah ke bawah. Berikut beberapa inisiatif yang dapat diterapkan:

- **Meningkatkan pendidikan:**
  - Program literasi digital yang membahas keamanan siber dan cybercrime perlu digalakkan.
  - Materi tentang keamanan siber dapat diintegrasikan ke dalam kurikulum pendidikan formal.
  - Pelatihan dan lokakarya tentang cybercrime dapat diadakan di komunitas masyarakat menengah ke bawah.
- **Memperluas akses internet:**
  - Perluasan infrastruktur internet yang terjangkau dan berkualitas dapat membantu masyarakat menengah ke bawah untuk mengakses informasi dan edukasi tentang cybercrime.
  - Program subsidi atau keringanan biaya internet dapat dipertimbangkan untuk meningkatkan akses internet bagi masyarakat berpenghasilan rendah.
- **Meningkatkan kemampuan finansial:**
  - Bantuan pemerintah atau program subsidi dapat membantu masyarakat menengah ke bawah untuk mendapatkan perangkat lunak keamanan siber gratis atau dengan harga terjangkau.
  - Pelatihan tentang cybercrime dapat ditawarkan secara gratis atau dengan biaya minimal untuk meningkatkan kesadaran dan kemampuan masyarakat dalam melindungi diri.
- **Meningkatkan kesadaran hukum:**
  - Sosialisasi tentang hak-hak korban cybercrime dan langkah-langkah yang harus diambil ketika menjadi korban cybercrime perlu dilakukan secara gencar.
  - Bantuan hukum gratis dapat diberikan kepada masyarakat menengah ke bawah yang menjadi korban cybercrime.
- **Membangun budaya privasi:**
  - Kampanye publik yang menekankan pentingnya privasi dan keamanan data pribadi perlu dilakukan untuk mengubah perilaku masyarakat.
  - Edukasi tentang cara melindungi data pribadi di dunia digital perlu disebarluaskan secara luas. (Staying Safe Online Is Easier Than You Think, n.d.e)

5. KESIMPULAN

kesadaran dan perilaku masyarakat menengah ke bawah terkait dengan cybercrime masih rendah. Diperlukan upaya edukasi, sosialisasi, program pelatihan, regulasi yang lebih ketat, dan kerjasama antara pemerintah, swasta, dan masyarakat untuk meningkatkan kesadaran dan perlindungan terhadap cybercrime.

Dengan upaya yang terarah, diharapkan masyarakat dapat menjadi lebih aware dan mampu melindungi diri dari ancaman cybercrime. Penekanan pada literasi digital, kesadaran keamanan siber, dan

Daftar Pustaka

0 Tips Mengamankan Data Pribadi Dari Serangan Siber. (n.d.). https://www.cyberacademy.id/blog/10-tips-mengamankan-data-pribadi-dari-serangan-siber

Basry, A., & Malays Sari, E. (n.d.). *PENGGUNAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) PADA USAHA MIKRO, KECIL DAN MENENGAH (UMKM)*.

Berita & Acara. (n.d.). https://www.cloudeka.id/berita/

Buchan, M. C., Bhawra, J., & Katapally, T. R. (2024). Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments*, *11*(1). https://doi.org/10.1186/s40561-024-00293-x

Crimes Awareness campaigns What you can do Cybercrime-#YouMayBeNext Tell me more ✕. (n.d.). https://www.interpol.int/en/Crimes/Cybercrime

Cybercrime is impacting communities differently, study finds _ Cyber Magazine. (n.d.).

Cyber crime - National Crime Agency. (n.d.).

Cyber Security_ Pengertian, Konsep, Jenis, dan Ancaman di Bisnis. (n.d.).

Hironde, J.-B. (n.d.). *The Digital Divide: Addressing Tech And AI Illiteracy For Our Future*. https://www.forbes.com/sites/forbestechcouncil/2023/11/07/the-digital-divide-addressing-tech-and-ai-illiteracy-for-our-future/?sh=60609d67375e

Marcos to new PNP chief Marbil: Address terrorism, cybercrime. (n.d.). https://www.britannica.com/topic/cybercrime

News Revised toolkit empowers law enforcement with responsible AI practices News INTERPOL welcomes new DNA legislation in Belgium. (n.d.). https://www.interpol.int/en

Ramadhani, M. R., & Raf'ie Pratama, A. (n.d.). *Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia*.

Staying Safe Online is Easier Than You Think. (n.d.). https://www.cisa.gov/secure-our-world

United Nations Office on Drugs and Crime. (n.d.). https://www.unodc.org/unodc/en/cybercrime/home.html

www.bssn.go.id _ Situs Web Resmi Badan Siber dan Sandi Negara. (n.d.).

0 Tips Mengamankan Data Pribadi Dari Serangan Siber. (n.d.). https://www.cyberacademy.id/blog/10-tips-mengamankan-data-pribadi-dari-serangan-siber

Basry, A., & Malays Sari, E. (n.d.). *PENGGUNAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) PADA USAHA MIKRO, KECIL DAN MENENGAH (UMKM)*.

Berita & Acara. (n.d.). https://www.cloudeka.id/berita/

Buchan, M. C., Bhawra, J., & Katapally, T. R. (2024). Navigating the digital world: development of an evidence-based digital literacy program and assessment tool for youth. *Smart Learning Environments*, *11*(1). https://doi.org/10.1186/s40561-024-00293-x

Crimes Awareness campaigns What you can do Cybercrime-#YouMayBeNext Tell me more ✕. (n.d.). https://www.interpol.int/en/Crimes/Cybercrime

Cybercrime is impacting communities differently, study finds _ Cyber Magazine. (n.d.).

Cyber crime - National Crime Agency. (n.d.).

Cyber Security_ Pengertian, Konsep, Jenis, dan Ancaman di Bisnis. (n.d.).

Hironde, J.-B. (n.d.). *The Digital Divide: Addressing Tech And AI Illiteracy For Our Future*.

P-ISSN: 1411-3635
E-ISSN: 2962-5645

https://www.forbes.com/sites/forbestechcouncil/2023/11/07/the-digital-divide-addressing-tech-and-ai-illiteracy-for-our-future/?sh=60609d67375e

Marcos to new PNP chief Marbil: Address terrorism, cybercrime. (n.d.). https://www.britannica.com/topic/cybercrime

News Revised toolkit empowers law enforcement with responsible AI practices News INTERPOL welcomes new DNA legislation in Belgium. (n.d.). https://www.interpol.int/en

Ramadhani, M. R., & Raf'ie Pratama, A. (n.d.). *Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia*.

Staying Safe Online is Easier Than You Think. (n.d.). https://www.cisa.gov/secure-our-world

United Nations Office on Drugs and Crime. (n.d.). https://www.unodc.org/unodc/en/cybercrime/home.html

www.bssn.go.id _ Situs Web Resmi Badan Siber dan Sandi Negara. (n.d.).