JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 591-598
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Ancaman *Cyber Attack* Terhadap Keamanan Data Pengguna Internet

Ivan Kurniawan[1], Putri Aiva Wulandari[2], Dimas Nur Rizky[3], Ibnu Azhar Harahap[4], Riko Taruna[5]

[1,2,3,4,5]Universitas Labuhanabatu, Indonesia

Email: ivannkurnia12@gmail.com[1], aivaputri7@gmail.com[2], dimasjk130406@gmail.com[3], ibnuazharhrp14@gmail.com[4], ricotarigan445@gmail.com[5]

ABSTRAK

Perkembangan teknologi informasi dan penggunaan internet yang semakin pesat memberikan banyak manfaat bagi masyarakat, namun juga meningkatkan risiko terjadinya serangan siber terhadap keamanan data pribadi pengguna. Serangan siber seperti *phishing*, malware, ransomware, peretasan, dan pencurian identitas menjadi ancaman utama di era digital saat ini. Penelitian ini bertujuan untuk menganalisis ancaman *Cyber Attack* terhadap keamanan data pengguna internet serta mengidentifikasi faktor-faktor penyebab terjadinya kebocoran data dan kejahatan siber. Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Teknik pengumpulan data dilakukan melalui observasi, wawancara, kuesioner, dan studi literatur. Penelitian dilaksanakan di Kampung Sidorukun, Kota Aek Nabara, dengan melibatkan 40 pengguna internet sebagai responden. Data yang diperoleh dianalisis secara deskriptif untuk mengetahui tingkat kesadaran keamanan siber serta jenis serangan siber yang sering dialami oleh pengguna internet.

Hasil penelitian menunjukkan bahwa *phishing* merupakan jenis serangan siber yang paling sering dialami oleh responden. Selain itu, masih banyak pengguna internet yang memiliki tingkat kesadaran keamanan siber yang rendah, seperti penggunaan kata sandi yang lemah, mengakses tautan mencurigakan, serta jarang melakukan pembaruan sistem keamanan perangkat. Penelitian ini juga menemukan bahwa kurangnya edukasi keamanan siber dan lemahnya sistem perlindungan digital menjadi faktor utama penyebab terjadinya serangan siber.

Oleh karena itu, peningkatan kesadaran keamanan siber melalui edukasi, penggunaan kata sandi yang kuat, autentikasi dua faktor, antivirus, serta pembaruan sistem secara berkala sangat diperlukan untuk melindungi data pribadi pengguna dari ancaman siber. Penelitian ini diharapkan dapat meningkatkan pemahaman masyarakat mengenai pentingnya keamanan siber di era digital.

Kata Kunci: *Cyber Attack*, Keamanan Siber, Keamanan Data, Pengguna Internet, *Phishing*, Perlindungan Digital.

ABSTRACT

The rapid development of information technology and internet usage has provided many benefits to society, but it has also increased the risk of Cyber Attacks on users' personal data security. Cyber Attacks such as phishing, malware, ransomware, hacking, and identity theft have become major threats in the digital era. This study aims to analyze the threats of Cyber Attacks against internet users' data security and identify the factors causing data breaches and cybercrime incidents. This research used a descriptive qualitative method with data collection techniques including observation, interviews, questionnaires, and literature studies. The study was conducted in Kampung Sidorukun, Kota Aek Nabara, involving 40 internet users as respondents. The collected data were

analyzed descriptively to determine the level of cybersecurity awareness and the types of Cyber Attacks frequently experienced by users.
The results showed that phishing was the most common Cyber Attack experienced by respondents. In addition, many users still had low awareness regarding cybersecurity, such as using weak passwords, accessing suspicious links, and rarely updating system security. The study also found that a lack of cybersecurity education and weak digital protection systems were the main factors contributing to Cyber Attacks. Therefore, improving cybersecurity awareness through education, the use of strong passwords, multi-factor authentication, antivirus software, and regular system updates is highly necessary to protect users' personal data from cyber threats. This research is expected to increase public understanding of the importance of cybersecurity in the digital era.
Keywords: Cyber Attack, Cybersecurity, Data Security, Internet Users, Phishing, Digital Protection

PENDAHULUAN

Perkembangan teknologi informasi dan internet pada era digital saat ini memberikan dampak yang sangat besar terhadap kehidupan masyarakat. Internet tidak hanya digunakan sebagai sarana komunikasi, tetapi juga dimanfaatkan dalam berbagai aktivitas seperti pendidikan, bisnis, perbankan, hiburan, hingga penyimpanan data pribadi. Kemudahan akses internet membuat pertukaran informasi menjadi lebih cepat dan efisien. Namun, di balik perkembangan tersebut muncul berbagai ancaman keamanan siber (*cyber security*) yang dapat membahayakan data dan privasi pengguna internet (Singer & Friedman, 2014; Stallings, 2017; NIST, 2020). Ancaman *Cyber Attack* atau serangan siber merupakan tindakan yang dilakukan oleh pihak tertentu untuk merusak, mencuri, atau mengakses sistem dan data tanpa izin. Bentuk serangan siber yang sering terjadi antara lain *phishing*, malware, ransomware, *hacking*, dan pencurian identitas digital. Serangan tersebut dapat menyebabkan kerugian besar, baik bagi individu maupun organisasi, seperti kebocoran data pribadi, kehilangan informasi penting, hingga kerugian finansial (Stallings & Brown, 2018; Kaspersky, 2021; Cisco, 2022).

Selain itu, meningkatnya penggunaan internet juga menyebabkan meningkatnya risiko kejahatan siber terhadap pengguna digital. Kurangnya kesadaran masyarakat mengenai pentingnya keamanan data menjadi salah satu faktor utama yang mempermudah terjadinya serangan siber. Banyak pengguna internet masih menggunakan kata sandi yang lemah, mengakses tautan mencurigakan, dan kurang memahami cara melindungi data pribadi mereka di dunia digital (Taylor, 2013; Microsoft, 2021; IBM, 2022). Oleh karena itu, diperlukan penerapan sistem keamanan yang baik seperti penggunaan enkripsi data, autentikasi dua faktor (*multi-factor authentication*), firewall, dan pembaruan sistem keamanan secara berkala untuk mengurangi risiko serangan siber. Edukasi mengenai keamanan siber juga sangat penting untuk meningkatkan kesadaran pengguna internet dalam menjaga keamanan data pribadi mereka (NIST, 2020; ITU, 2020; Stallings, 2017).

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian deskriptif dengan pendekatan kualitatif. Metode deskriptif digunakan untuk menganalisis berbagai jenis ancaman

Cyber Attack yang dapat memengaruhi keamanan data pengguna internet. Pendekatan kualitatif bertujuan untuk memahami bentuk serangan siber, faktor penyebab, dampak yang ditimbulkan, serta upaya pencegahan yang dapat dilakukan untuk meningkatkan keamanan data digital.

1. Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan di **Kampung Sidorukun, Kota Aek Nabara, Sumatera Utara**. Lokasi penelitian dipilih karena masyarakat di daerah tersebut telah aktif menggunakan internet dan media digital dalam kehidupan sehari-hari, seperti penggunaan media sosial, aplikasi komunikasi, dan transaksi online. Hal ini menjadikan wilayah tersebut relevan untuk dijadikan objek penelitian terkait ancaman *Cyber Attack* terhadap keamanan data pengguna internet.

Waktu penelitian dilaksanakan selama kurang lebih 3 (tiga) bulan, dimulai dari bulan Juni 2026 hingga Agustus 2026. Kegiatan penelitian meliputi proses pengumpulan data, penyebaran kuesioner, wawancara, observasi, hingga analisis data penelitian.

2. Sumber Data

Sumber data yang digunakan dalam penelitian ini terdiri dari:

a. Data Primer

Data primer diperoleh melalui penyebaran kuesioner dan wawancara kepada pengguna internet mengenai pengalaman mereka terhadap ancaman keamanan siber, seperti phishing, malware, dan pencurian data.

b. Data Sekunder

Data sekunder diperoleh dari jurnal ilmiah, buku, artikel, laporan keamanan siber, dan sumber terpercaya lainnya yang berkaitan dengan cyber security dan *Cyber Attack*.

3. Teknik Pengumpulan Data

Adapun teknik pengumpulan data dalam penelitian ini adalah sebagai berikut:

a. Observasi

Peneliti melakukan pengamatan terhadap aktivitas penggunaan internet dan potensi ancaman keamanan data yang sering terjadi pada pengguna internet.

b. Wawancara

Wawancara dilakukan kepada beberapa pengguna internet untuk memperoleh informasi mengenai pengalaman mereka terkait serangan siber dan cara menjaga keamanan data pribadi.

c. Kuesioner

Kuesioner disebarkan kepada responden untuk mengetahui tingkat pemahaman dan kesadaran pengguna terhadap pentingnya keamanan siber.

d. Studi Pustaka

Peneliti mengumpulkan referensi dari jurnal, buku, dan artikel ilmiah yang membahas *Cyber Attack* dan keamanan data untuk mendukung penelitian.

3. Tekhnik Analisis Data

Teknik analisis data dilakukan dengan menggunakan metode analisis deskriptif. Data yang telah diperoleh kemudian dikumpulkan, diklasifikasikan, dan dianalisis berdasarkan jenis ancaman *Cyber Attack*, dampak yang ditimbulkan, serta metode perlindungan data yang digunakan oleh pengguna internet.

Tahapan analisis data meliputi:

1. Pengumpulan data
2. Reduksi data
3. Penyajian data
4. Penarikan kesimpulan.

4. Objek Penelitian

Objek dalam penelitian ini adalah pengguna internet yang aktif menggunakan media digital seperti media sosial, email, aplikasi perbankan online, dan platform digital lainnya yang berpotensi mengalami ancaman *Cyber Attack*.

5. Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menganalisis jenis-jenis ancaman *Cyber Attack* terhadap keamanan data pengguna internet.
2. Mengetahui dampak serangan siber terhadap pengguna internet.
3. Mengidentifikasi faktor penyebab terjadinya kebocoran dan pencurian data.
4. Memberikan solusi dan rekomendasi untuk meningkatkan keamanan data pengguna internet.

HASIL DAN PEMBAHASAN

1. Data Responden Penelitian

Penelitian ini dilakukan terhadap 40 responden yang merupakan pengguna internet di Kampung Sidorukun, Kota Aek Nabara. Responden dipilih berdasarkan aktivitas penggunaan internet sehari-hari seperti penggunaan media sosial, email, aplikasi perbankan digital, dan transaksi online.

Tabel 1. Data Responden Berdasarkan Jenis Kelamin

No	Jenis Kelamin	Jumlah	Persentase
1	Laki-laki	22	55%
2	Perempuan	18	45%
	Total	40	100%

JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 591-598
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Tabel 2 Data Responden Berdasarkan Usia

No	Rentang Usia	Jumlah
1	15–20 Tahun	10
2	21–25 Tahun	15
3	26–30 Tahun	9
4	>30 Tahun	6
	Total	40

2. Hasil Kuesioner Penelitian

Penelitian menggunakan beberapa pertanyaan terkait pemahaman dan pengalaman responden terhadap ancaman *Cyber Attack*.

Tabel 3 Penggunaan Internet per Hari

No	Durasi Penggunaan Internet	Jumlah Responden	Persentase
1	1–3 Jam	8	20%
2	4–6 Jam	14	35%
3	7–9 Jam	10	25%
4	>10 Jam	8	20%
	Total	40	100%

Tabel 4 Jenis Ancaman *Cyber Attack* yang Pernah Dialami

No	Jenis Serangan Siber	Jumlah Responden
1	Phishing	15
2	Malware/Virus	10
3	Pencurian Akun	8
4	Spam Berbahaya	5
5	Ransomware	2
	Total	40

3. Analisis Data Penelitian

Berdasarkan hasil penelitian, jenis serangan siber yang paling sering dialami oleh responden adalah *phishing* dengan jumlah 15 responden. Serangan *phishing* biasanya terjadi melalui tautan palsu yang dikirim melalui email, media sosial, atau pesan singkat yang bertujuan mencuri data pribadi pengguna seperti kata sandi dan informasi akun. Selain itu, sebanyak 10 responden pernah mengalami serangan malware atau virus pada perangkat mereka. Hal ini disebabkan oleh kurangnya perlindungan keamanan seperti antivirus dan kebiasaan mengunduh file dari sumber yang tidak terpercaya. Hasil penelitian juga menunjukkan bahwa sebagian besar responden masih memiliki tingkat kesadaran keamanan siber yang rendah. Beberapa responden masih menggunakan kata sandi yang lemah, menggunakan password yang sama pada beberapa akun, serta jarang melakukan pembaruan sistem keamanan perangkat.

Tabel 5 Tingkat Kesadaran Keamanan Siber Pengguna

No	Tingkat Kesadaran	Jumlah Responden	Persentase
1	Tinggi	8	20%
2	Sedang	17	42,5%
3	Rendah	15	37,5%
	Total	40	100%

Berdasarkan tabel di atas, dapat diketahui bahwa tingkat kesadaran keamanan siber masyarakat masih berada pada kategori sedang dan rendah. Kondisi ini menunjukkan bahwa edukasi mengenai keamanan data digital masih perlu ditingkatkan agar masyarakat lebih memahami risiko *Cyber Attack* dan cara melindungi data pribadi mereka.

4. Pembahasan

Ancaman *Cyber Attack* terhadap keamanan data pengguna internet terus meningkat seiring berkembangnya teknologi digital. Faktor utama yang

menyebabkan terjadinya serangan siber adalah kurangnya pemahaman pengguna mengenai keamanan internet serta lemahnya sistem perlindungan data.

Dari hasil penelitian dapat disimpulkan bahwa:

1. Serangan *phishing* menjadi ancaman paling umum bagi pengguna internet.
2. Kesadaran masyarakat terhadap keamanan siber masih tergolong rendah.
3. Penggunaan password yang lemah dan kurangnya pembaruan sistem menjadi faktor utama penyebab kebocoran data.
4. Edukasi keamanan siber dan penggunaan sistem keamanan tambahan seperti autentikasi dua faktor sangat diperlukan untuk mengurangi risiko serangan siber.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai Analisis Ancaman *Cyber Attack* terhadap Keamanan Data Pengguna Internet di Kampung Sidorukun, Kota Aek Nabara, dapat disimpulkan bahwa perkembangan teknologi internet memberikan banyak manfaat bagi masyarakat, namun juga meningkatkan risiko terjadinya ancaman keamanan siber (*Cyber Attack*). Ancaman tersebut dapat berupa *phishing*, malware, pencurian akun, spam berbahaya, hingga ransomware yang berpotensi merugikan pengguna internet secara finansial maupun privasi data pribadi. Hasil penelitian menunjukkan bahwa jenis serangan siber yang paling sering dialami oleh responden adalah *phishing*. Hal ini disebabkan oleh kurangnya kewaspadaan pengguna terhadap tautan atau pesan mencurigakan yang diterima melalui media sosial, email, maupun aplikasi komunikasi lainnya. Selain itu, masih banyak pengguna yang menggunakan kata sandi lemah, jarang melakukan pembaruan sistem keamanan, dan belum memahami pentingnya perlindungan data digital.

Tingkat kesadaran masyarakat terhadap keamanan siber juga masih tergolong sedang hingga rendah. Kondisi ini menunjukkan bahwa edukasi mengenai keamanan digital sangat diperlukan agar masyarakat mampu memahami risiko penggunaan internet serta mampu melindungi data pribadi dari ancaman kejahatan siber. Penggunaan sistem keamanan tambahan seperti autentikasi dua faktor, antivirus, firewall, dan enkripsi data dapat membantu meningkatkan perlindungan terhadap data pengguna internet. Dengan demikian, penelitian ini menyimpulkan bahwa keamanan siber merupakan aspek yang sangat penting dalam penggunaan teknologi digital. Kerja sama antara pengguna internet, penyedia layanan digital, dan pemerintah sangat diperlukan untuk meningkatkan keamanan data serta mengurangi risiko terjadinya *Cyber Attack* di masyarakat.

Ucapan Terima Kasih

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya jurnal yang berjudul Analisis Ancaman *Cyber Attack* terhadap Keamanan Data Pengguna Internet ini dapat diselesaikan dengan baik.

Penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah memberikan dukungan, bantuan, dan motivasi selama proses penyusunan jurnal ini. Ucapan terima kasih penulis sampaikan kepada:

1. Dosen pembimbing yang telah memberikan arahan, masukan, dan bimbingan dalam penyusunan jurnal ini.
2. Masyarakat Kampung Sidorukun, Kota Aek Nabara, yang telah bersedia menjadi responden dalam penelitian ini.
3. Orang tua dan keluarga yang selalu memberikan doa, dukungan, serta semangat kepada penulis.
4. Teman-teman dan semua pihak yang telah membantu dalam proses penelitian dan penyusunan jurnal ini.

Penulis menyadari bahwa jurnal ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi perbaikan dan penyempurnaan penelitian di masa yang akan datang.

Semoga jurnal ini dapat memberikan manfaat dan menambah wawasan bagi pembaca, khususnya dalam bidang keamanan siber (*cyber security*).

DAFTAR PUSTAKA

Cybersecurity and Cyberwar: What Everyone Needs to Know Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

National Institute of Standards and Technology. (2020). *Framework for Improving Critical Infrastructure Cybersecurity*. NIST.

Computer Security: Principles and Practice Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson Education.

Kaspersky. (2021). *Cyber Threats and Malware Analysis Report*.

Cisco. (2022). *Annual Cybersecurity Report*. Cisco Systems.

Information Security Management Principles Taylor, A. (2013). *Information Security Management Principles*. BCS Learning & Development Ltd.

International Telecommunication Union. (2020). *Global Cybersecurity Index*. ITU Publications.

Network Security Essentials Stallings, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

Microsoft. (2021). *Digital Defense Report*. Microsoft Security.

IBM. (2022). *Cost of a Data Breach Report*. IBM Security.