

ANALISIS TINGKAT KESADARAN MASYARAKAT TERHADAP BAHAYA CYBERCRIME (STUDI KASUS KECAMATAN JATIIYOSO)

Miswanto^{1*}, Nova Tri Romadloni², Imam Santoso³, Nana Mulyana⁴

^{1,3,4}Universitas Teknologi Muhammadiyah Jakarta; Jl. Minangkabau Barat No.60;

³Universitas Muhammadiyah Karanganyar; Jl. Raya Solo-Tawangmangu No.KM. 12;

Received: 7 Maret 2025

Accepted: 27 Maret 2025

Published: 14 April 2025

Keywords:

analysis;
community awareness;
cybercrime;
danger of cybercrime.

Correspondent Email:

miswanto@utmj.ac.id

Abstrak. Dalam era digital, penggunaan internet dan teknologi semakin meluas. Urgensi dari penelitian ini adalah banyaknya pengaduan masyarakat terkait kasus *cybercrime*, sehingga perlindungan data pribadi dan keamanan siber menjadi sangat penting. Kesadaran masyarakat akan potensi risiko ini adalah kunci untuk melindungi informasi pribadi dan keuangan mereka. Kesadaran masyarakat tentang jenis-jenis *cybercrime* dan tindakan yang dapat mereka ambil untuk mencegahnya dapat membantu mengurangi insiden kejahatan siber. Pengetahuan dan kesadaran masyarakat tentang kejahatan siber merupakan langkah pertama dalam mempersiapkan diri untuk menghadapi ancaman digital yang semakin kompleks. Penelitian ini bertujuan untuk memahami sejauh mana masyarakat di wilayah tersebut memiliki kesadaran tentang potensi bahaya yang dihadapi dari kejahatan siber atau *cybercrime*, termasuk pemahaman tentang jenis-jenis *cybercrime* yang mungkin mereka hadapi. Selain itu, dapat mengidentifikasi faktor-faktor yang mungkin memengaruhi tingkat kesadaran masyarakat terhadap bahaya *cybercrime*, seperti usia, pendidikan, akses internet, atau pengalaman

Sebelumnya. Tahap awal dari penelitian dilakukan pada tingkat kecamatan Jatiyoso yang terdiri dari 9 desa. Sehingga dapat diperoleh sebanyak 135 responden yang mengisi Pre-Test dan Post-Test Kuesioner dari kriteria orang dewasa yakni usia 17 - 40 tahun serta mengidentifikasi faktor-faktor yang berkontribusi pada tingkat kesadaran tentang kejahatan siber, termasuk analisis data demografis. Kemudian, dapat membantu masyarakat setempat untuk lebih memahami ancaman *cybercrime*, sehingga senantiasa melindungi data pribadi mereka dan berkontribusi pada keselamatan siber di wilayah kecamatan Jatiyoso. Demikian pula, dapat memberikan rekomendasi kepada pemerintah setempat atau lembaga terkait seperti sekolah, dan organisasi masyarakat untuk meningkatkan kesadaran masyarakat terhadap bahaya *cybercrime* melalui program-program edukasi atau kesadaran.

Abstract. In the digital era, the use of the internet and technology is increasingly widespread. The urgency of this research is the number of public complaints related to cybercrime cases, so the protection of personal data and cybersecurity is very important. protection of personal data and cybersecurity is very important. Public awareness of the potential this risk is key to protecting their personal and financial information. Awareness aware-ness of the types of cybercrime and the actions they can take to prevent them can help reduce incidents of cybercrime. prevent it can help reduce the incidence of cybercrime. Knowledge and awareness aware-ness of cybercrime is the first step in preparing themselves to deal with increasingly complex digital threat. This research aims to understand the extent to which people in the region have

an awareness of the potential dangers faced from cybercrime, including an understanding of the types of cybercrime they may face.

In addition, it can identify factors that may affect the level of public awareness of the dangers of cybercrime, such as age, education, internet access, or previous experience. The research was conducted at the Jatiyoso sub-district level which consists of 9 villages. So as to obtain 135 respondents who filled out the Pre-Test and Post-Test Questionnaire from the criteria of adults aged 17 - 40 years and identify factors that contribute to the level of awareness about cybercrime, including demographic data analysis. Then, it can help local communities to better understand the threat of cybercrime, so that they always protect their personal data and contribute to cyber safety in the Jatiyoso sub-district area. Similarly, it can provide recommendations to the local government or related institutions such as schools, and community organizations to increase community awareness of the dangers of cybercrime. organizations to increase public awareness of the dangers of cybercrime through education or awareness programs. educational or awareness programs.

1. PENDAHULUAN

Penggunaan teknologi informasi pada era society 5.0 membawa banyak perubahan dalam kegiatan manusia [1]. Terlebih penggunaan internet yang digunakan oleh siapapun baik dari kalangan individu maupun kelompok masyarakat luas dari berbagai belahan dunia. Penggunaan internet sebagai media informasi sangat dirasakan manfaatnya oleh masyarakat karena dengan internet penyampaian informasi kepada publik lebih cepat dan dapat diakses oleh penerima dengan mudah, tidak hanya dengan penyampaian informasi saja, melainkan berbagai macam aktivitas masyarakat dalam mewujudkan kreatifitasnya dalam memenuhi kebutuhan sehari-hari dan menjadikan pribadi yang terus berkembang dengan kemajuan teknologi ini. Namun dengan adanya perkembangan tersebut internet juga memberikan dampak atau kesalahan-kesalahan baru yang salah satu nya adalah kejahatan yang lebih canggih seperti bentuk kejahatan cybercrime.

Korban cybercrime mengalami kerugian berupa kerugian materi, psikologis, fisik, dan sosial, sebagai contoh kasus kejahatan pencurian uang nasabah dengan cara pembajakan akun internet banking lewat sosial media [2]. Tidak hanya kerugian secara materil, melainkan kerugian atas pencemaran nama baik jurang sering terjadi [3]. Dalam era digital yang semakin berkembang, penggunaan internet dan teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari. Meskipun

teknologi ini memberikan manfaat besar, penggunaan yang semakin meluas juga membawa potensi risiko, khususnya dalam hal kejahatan siber atau cybercrime. Cybercrime mencakup berbagai jenis aktivitas ilegal yang dilakukan melalui internet, seperti pencurian identitas, penipuan online, serangan siber, dan penyebaran malware. Sering banyak yang terjadi peretasan sistem komputer secara illegal [4].

Kejahatan siber ini dapat merugikan individu, organisasi, bahkan negara. Kesadaran masyarakat tentang bahaya cybercrime juga penting untuk mendorong tindakan pencegahan, seperti penggunaan sandi yang kuat, perangkat lunak keamanan yang mutakhir, dan perilaku online yang bijak [5]. Dalam konteks ini, kesadaran masyarakat tentang bahaya cybercrime menjadi sangat penting. Kesadaran ini mencakup pemahaman tentang jenis-jenis kejahatan siber yang mungkin terjadi, cara melindungi diri dari ancaman digital, dan langkah-langkah yang dapat diambil untuk melaporkan atau menghindari kejahatan tersebut. Kesadaran masyarakat merupakan pertahanan pertama dalam melindungi diri dari potensi bahaya cybercrime. Namun, tingkat kesadaran masyarakat tentang kejahatan siber bisa bervariasi tergantung pada faktor-faktor seperti pendidikan, akses internet, usia, pengalaman sebelumnya, dan tingkat pemahaman teknologi.

Oleh karena itu, penting untuk melakukan penelitian yang mendalam untuk menganalisis

tingkat kesadaran masyarakat terhadap bahaya cybercrime di wilayah tertentu. Salah satu diantaranya adalah wilayah kecamatan Jatiyoso, ketika tingkat keterlibatan masyarakat dalam ekosistem digital semakin meningkat, penting untuk memahami tingkat kesadaran mereka tentang bahaya cybercrime [6]. Kesadaran masyarakat merupakan langkah awal yang penting dalam melindungi diri dari ancaman siber. Kemudian Langkah tegas dari pemangku kepentingan dalam hal ini pihak Kepolisian dan Kementerian terkait dapat melakukan sosialisasi terkait bahaya cybercrime ini [7]. Contoh penerapan penegakan hukum yang dilakukan oleh Kepolisian Daerah Sumatera Utara yaitu terkait pencemaran nama baik, judi online dan konten asusila [8].

2. TINJAUAN PUSTAKA

2.1. Konsep Cybercrime di era digital.

Kejahatan dunia maya atau kejahatan dunia maya telah berkembang menjadi masalah yang sejajar dengan kemajuan teknologi dalam revolusi industri keempat. Space & Windiasih (2022) mengatakan kejahatan dunia maya menyakiti para korban dengan menyebabkan kehilangan uang dan stres juga. Masalah ini terdiri dari berbagai jenis seperti informasi komputer curian, akses ilegal ke akun online, dan menyebarkan hal-hal yang tidak benar menggunakan Internet (Aditama, 2021; Arifin & Muthia, 2019).

2.2. Bentuk dan mode kejahatan dunia maya.

Beberapa bentuk kejahatan dunia maya yang sering terjadi di Indonesia termasuk.

- **Pencurian Data.** Artikel keamanan siber oleh Aditama (2021) menjelaskan bagaimana pencuri menggunakan media sosial untuk mencuri informasi perbankan online menggunakan trik dan manipulasi.
- **Peretasan.** Studi 2023 oleh Wijoseno et al. Berbicara tentang masalah hukum untuk peretas yang masuk ke komputer secara ilegal di bawah hukum Indonesia.
- **Pencemaran Nama Baik.** Studi oleh Arifin & Muthia (2019) melihat kasus pencemaran nama baik online dan kesulitan membuktikannya di pengadilan.

2.3. Tantangan Penegakan Hukum Cybercrime.

Penegakan hukum Cybercrime di Indonesia masih menghadapi berbagai hambatan, seperti.

Indonesia harus meningkatkan untuk menangani kejahatan online yang rumit. Sesuai Sofyantoro et al. (2021), Pengetahuan masyarakat yang buruk tentang kejahatan online menyebabkan lebih banyak korban. Temuan ini lebih lanjut didukung oleh Laporan Coil (2024) yang menunjukkan keakraban publik dengan kejadian sosial sosial harus ditingkatkan.

2.4. Urgensi Hukum Cyber di Indonesia.

Legislasi cyber diperlukan untuk jaring keamanan hukum yang pasti dalam mengatasi penyimpangan cyber. Ferry & Febriansyah (2023) mengusulkan kerangka hukum nasional yang luas untuk menangkai pelanggaran dunia maya. Sementara itu, Halaman Kepolisian Nasional Kepulauan Riau (2024) mendefinisikan kejahatan dunia maya sebagai pelanggaran cyber yang memanfaatkan teknologi, memerlukan peraturan tertentu untuk diatur agar dapat menjadi landasan hukum.

3. METODE PENELITIAN

Dalam penelitian melibatkan serangkaian langkah-langkah untuk mencapai tujuan yaitu, sebagai berikut:

1. Survei dan Analisis Data yaitu melakukan survei di wilayah Jatiyoso untuk mengukur tingkat kesadaran masyarakat terhadap bahaya cybercrime. Serta mengumpulkan data mengenai tingkat pengetahuan dan pemahaman masyarakat tentang jenis-jenis cybercrime [10]. Kemudian, Mengidentifikasi dimensi yang mempengaruhi tingkat kontribusi terbesar dalam mencapai kesadaran masyarakat.



Gambar 1. Proses survey pada saat ada pelapor

2. Evaluasi Pemantauan. Melakukan pemantauan secara berkala untuk mengukur perkembangan tingkat kesadaran masyarakat. Kemudian, Menganalisis efektivitas program yang mungkin sudah ada seperti penyuluhan di pertemuan wilayah untuk memastikan bahwa pesan pesan tersebut sampai kepada masyarakat dengan baik.



Gambar 2. Proses monitoring laporan

3. Adapun metode yang digunakan pada penelitian ini adalah dengan pengisian kuesioner setiap kali pelapor datang ke Sentra Pelayanan Kepolisian Terpadu (SPKT) dan telah selesai melaporkan apa yang menjadi masalah kepada pihak Polsek [11]. Kemudian data diolah menggunakan Uji Deskriptif, Uji Normalitas, dan Uji Wilcoxon Signed-Rank Test hingga didapatkan hasil yang disajikan pada penelitian ini.



Gambar 3. Proses pemaparan hasil analisis

4. HASIL DAN PEMBAHASAN

Menurut seorang tokoh pendidikan dari Brazil sekaligus teoritikus pendidikan yang berpengaruh di dunia, yaitu Paulo Freire. Dalam gagasannya mengenai teori kesadaran manusia terbagi menjadi 3 jenis tingkat

kesadaran, yaitu kesadaran magis, naif dan kritis. Paulo Freire menjelaskan, fase kesadaran ini berangkat dari masyarakat yang awalnya berpikir magis, lalu naik level ke naif, dan akhirnya menjadi kritis yaitu tingkatan tertinggi dari proses kesadaran masyarakat. Ketiga kesadaran itu dipengaruhi oleh pendidikan yang diterima oleh Masyarakat [9].

Tingkatan Kesadaran Masyarakat yang pertama adalah Kesadaran magis adalah kesadaran yang mana dalam kehidupan sehari-hari, masyarakat lebih percaya pada kekuatan takdir dan intervensi Tuhan terhadap apa yang dialaminya. Kesadaran magis menggambarkan keadaan masyarakat yang tidak mampu melihat adanya kaitan antar satu faktor dengan faktor lainnya. Masyarakat dengan kesadaran magis beranggapan bahwa perubahan yang terjadi di desa merupakan rencana dan kehendak Tuhan, jadi mereka tidak perlu mengintervensi hal tersebut.

Pentingnya proses untuk memberikan pemahaman, memberikan penjelasan kepada Masyarakat merupakan salah satu bentuk faktor pendukung yang dapat mempengaruhi Tindakan Masyarakat ke depannya. Dengan semakin banyak informasi yang didapatkan dan informasi tersebut valid, maka Masyarakat dapat berpikir secara rasional dan mampu mengambil sebuah Keputusan yang lebih baik. Serta dapat mengurangi resiko untuk Masyarakat terkena hal-hal yang tidak diinginkan secara berulang kali dikarenakan mereka sudah paham dan tidak akan terjebak pada masalah yang sama [13].

Cybercrime atau kejahatan dunia maya adalah suatu tindakan ilegal yang dilakukan melalui jaringan komputer dengan media internet untuk mendapatkan keuntungan dengan cara merugikan pihak lain. Kejahatan dunia maya ini bisa dilakukan dengan berbagai macam cara dan tujuan yang beragam. Pada umumnya, kejahatan tersebut dilakukan oleh orang-orang yang mengerti dan menguasai bidang teknologi informasi.

Salah satu contoh dari cybercrime yang sangat berbahaya adalah Doxxing, yang berujung pada cyberbullying hingga pengambilan data pribadi dan menyebarkannya di internet. Tujuan dari tindakan ini sangat bermacam-macam. Mulai dari ancaman, pemerasan, mempermalukan seseorang dan mengambil keuntungan yang lainnya. Seiring

dengan pesatnya kemajuan teknologi dan internet, ancaman kejahatan siber atau cybercrime semakin banyak bermunculan. Untuk melindungi diri dari berbagai aksi serangan siber tentunya kita harus mengetahui bagaimana cara meminimalisirnya [12].

Hasil yang didapatkan pada Penelitian ini yaitu berjumlah 135 responden aktif, yang telah dilakukan proses Pre-Test dan Post-Test terkait penjelasan dan pemahaman dari Cybercrime. Berikut adalah beberapa hasil yang dapat dijelaskan:

1. Peningkatan jumlah responden: Pada laporan kemajuan sebelumnya, didapatkan data 52 responden yang bersedia mengisi Pre-Test dan Post-Test. Seiring berjalannya waktu dan proses, jumlah responden mengalami peningkatan menjadi 135 responden. Terdapat kenaikan sejumlah 83 responden sampai akhir dari masa pembuatan laporan akhir.
2. Peningkatan Cybercrime: Peningkatan tindak pidana cybercrime terlihat dari hasil uji deskriptif yang dilakukan oleh Peneliti. Hal ini dapat dilakukan mitigasi resiko dengan memberikan informasi dan penjelasan kepada masyarakat Kecamatan Jatiyoso pada khususnya dan masyarakat lainnya pada umumnya agar tidak terkena modus yang sama.
3. Hasil Analisis Data: Berikut ini merupakan hasil analisis data yang didapatkan berdasarkan beberapa metode yang dilakukan:

A. Uji Deskriptif

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Cyber_Pre	135	.000	1.000	.57037	.203518
Pengamanan_Pre	135	.0	1.0	.680	.2530
Hukum_Pre	135	.0	1.0	.680	.2530
Cyber_Post	135	.000	1.000	.58611	.197623
Pengamanan_Post	135	.0	1.0	.676	.2490
Hukum_Post	135	.000000000000	1.000000000000	.568253968253	.224501794970
		000	0000	.968	.031
Valid N (listwise)	135				

Gambar 4. Statistik Deskriptif

Berdasarkan hasil analisis deskriptif yang ditampilkan dalam tabel, berikut adalah interpretasi dari masing-masing variable:

- Cyber_Pre (Mean = 0.57037) menunjukkan Rata-rata masyarakat menunjukkan aktivitas terkait cybercrime sekitar 57.0% sebelum intervensi/pretest. Sedangkan Cyber_Post (Mean =

0.58611) Setelah intervensi/posttest, rata-rata aktivitas meningkat menjadi 58.6%. hal tersebut menunjukkan Perubahan: Ada peningkatan kecil (1.6%), yang menunjukkan adanya sedikit perkembangan dalam aktivitas yang terkait cybercrime. Standar deviasi menunjukkan variabilitas yang stabil (0.203 untuk Pre dan 0.197 untuk Post). Sehingga dari Aktivitas cybercrime sedikit meningkat setelah intervensi, meskipun peningkatan ini perlu diuji secara statistik untuk melihat signifikansinya.

- Pengamanan_Pre (Mean = 0.680): menunjukkan Rata-rata tindakan pengamanan yang dilakukan masyarakat sebelum intervensi berada di 68.0%. Sedangkan Pengamanan_Post (Mean = 0.676): Setelah intervensi/posttest, rata-rata tindakan pengamanan sedikit menurun menjadi 67.6%. Hal ini menunjukkan Perubahan: Penurunan yang sangat kecil (0.4%), menunjukkan stabilitas tingkat pengamanan yang dilakukan masyarakat. Standar deviasi juga tidak berubah signifikan (0.253 menjadi 0.249). Sehingga dari aspek pengamanan Tidak ada perubahan besar dalam langkah pengamanan masyarakat setelah intervensi, yang menunjukkan perlunya pendekatan lebih dalam edukasi tentang pencegahan cybercrime.
- Hukum_Pre (Mean = 0.680) menunjukkan pengetahuan masyarakat tentang hukum cybercrime sebelum intervensi adalah 68.0%. Sedangkan Hukum_Post (Mean = 0.568): Setelah intervensi/posttest, rata-rata pengetahuan masyarakat menurun menjadi 56.8%. Hal tersebut terjadi Perubahan: Penurunan sebesar 11.2%, yang menunjukkan adanya penurunan signifikan dalam pemahaman masyarakat tentang hukum cybercrime. Standar deviasi sedikit menurun dari 0.253 menjadi 0.224. Sehingga Penurunan ini perlu perhatian lebih lanjut, karena intervensi tampaknya tidak efektif dalam meningkatkan pemahaman hukum masyarakat, atau mungkin ada faktor lain yang memengaruhi.
- Kesimpulan Umum Berdasarkan Deskriptif:

1. Cybercrime: Aktivitas yang terkait cybercrime sedikit meningkat, yang menunjukkan adanya paparan atau pengalaman lebih banyak di masyarakat.
2. Langkah Pengamanan: Stabil tanpa perubahan berarti, sehingga pendekatan lebih mendalam untuk meningkatkan kesadaran diperlukan.
3. Pengetahuan Hukum: Menurun setelah intervensi, yang mungkin mengindikasikan bahwa metode edukasi atau intervensi hukum kurang efektif, atau ada kendala lain seperti kompleksitas materi hukum.

B. Uji Normalitas

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Cyber_Pre	.179	135	.000	.938	135	.000
Pengamanan_Pre	.186	135	.000	.900	135	.000
Hukum_Pre	.186	135	.000	.900	135	.000
Cyber_Post	.178	135	.000	.947	135	.000
Pengamanan_Post	.195	135	.000	.903	135	.000
Hukum_Post	.150	135	.000	.956	135	.000

a. Lilliefors Significance Correction

Gambar 5. Uji Normalitas

Berdasarkan kedua uji normalitas (Kolmogorov-Smirnov dan Shapiro-Wilk), semua variabel menunjukkan nilai p-value < 0.05, yang berarti data tidak terdistribusi normal. Karena distribusi data tidak normal, maka metode analisis statistik non-parametrik harus digunakan untuk menguji perbedaan antara pretest dan posttest. Dilakukan uji Wilcoxon Signed-Rank Test dibawah ini.

C. Uji Wilcoxon Signed-Rank Test

Test Statistics ^a			
	Cyber_Post - Cyber_Pre	Pengamanan_Post - Pengamanan_Pre	Hukum_Post - Hukum_Pre
Z	-3.213 ^b	-.632 ^c	-4.679 ^c
Asymp. Sig. (2-tailed)	.001	.527	<.001

a. Wilcoxon Signed Ranks Test

b. Based on negative ranks.

c. Based on positive ranks.

Gambar 6. Uji Wilcoxon Signed-Rank

Berdasarkan hasil uji Wilcoxon Signed-Rank Test pada Gambar 6, berikut adalah interpretasi untuk masing-masing variabel:

- Cyber_Post - Cyber_Pre
Z = -3.213 Asymp. Sig. (2-tailed) = 0.001
Interpretasi: Nilai p = 0.001 menunjukkan bahwa terdapat perbedaan

signifikan antara Cyber_Pre dan Cyber_Post. Dengan kata lain, terjadi perubahan yang signifikan pada tingkat aktivitas cybercrime setelah intervensi/posttest. Nilai negatif pada Z menunjukkan bahwa banyak individu memiliki skor lebih rendah di Post dibandingkan dengan Pre.

- Pengamanan_Post - Pengamanan_Pre
Z = -0.632 Asymp. Sig. (2-tailed) = 0.527
Interpretasi: Nilai p = 0.527 menunjukkan bahwa tidak terdapat perbedaan signifikan antara Pengamanan_Pre dan Pengamanan_Post. Dengan kata lain, langkah pengamanan masyarakat terhadap cybercrime tidak mengalami perubahan signifikan setelah intervensi/posttest.
- Hukum_Post - Hukum_Pre
Z = -4.679 Asymp. Sig. (2-tailed) < 0.001
Interpretasi: Nilai p < 0.001 menunjukkan bahwa terdapat perbedaan signifikan antara Hukum_Pre dan Hukum_Post. Ini menunjukkan bahwa tingkat pengetahuan hukum masyarakat terkait cybercrime berubah secara signifikan setelah intervensi/posttest. Nilai negatif pada Z menunjukkan bahwa banyak individu memiliki skor lebih rendah di Post dibandingkan dengan Pre, yang berarti ada penurunan pengetahuan hukum.
- Kesimpulan Umum
 1. Cybercrime (Cyber_Post - Cyber_Pre):
 - Terdapat peningkatan aktivitas cybercrime secara signifikan setelah intervensi.
 2. Pengamanan (Pengamanan_Post - Pengamanan_Pre):
 - Tidak ada perubahan signifikan dalam langkah pengamanan masyarakat terhadap cybercrime.
 3. Pengetahuan Hukum (Hukum_Post - Hukum_Pre):
 - Terdapat penurunan signifikan dalam pengetahuan hukum masyarakat terkait cybercrime setelah intervensi

5. KESIMPULAN

- A. Untuk menjawab pertanyaan: "Bagaimana perkembangan cybercrime saat ini yang terjadi di lingkungan masyarakat?",

berdasarkan hasil analisis statistik yang telah dilakukan, berikut kesimpulannya:

Jawaban Berdasarkan Pengolahan Data yang dilakukan:

a. Aktivitas Cybercrime (Cyber_Pre vs Cyber_Post):

- Hasil uji Wilcoxon menunjukkan adanya peningkatan signifikan pada aktivitas yang terkait dengan cybercrime ($p = 0.001$).
- Rata-rata nilai meningkat dari 57.0% (Cyber_Pre) menjadi 58.6% (Cyber_Post). Meskipun peningkatan ini relatif kecil, secara statistik signifikan, yang mengindikasikan bahwa aktivitas cybercrime di masyarakat sedikit meningkat setelah intervensi atau seiring waktu.
- Kesimpulan: Aktivitas cybercrime di lingkungan masyarakat menunjukkan peningkatan, yang mengindikasikan perkembangan (kenaikan) aktivitas cybercrime di masyarakat.

b. Langkah Pengamanan (Pengamanan_Pre vs Pengamanan_Post):

- Tidak ada perubahan signifikan pada langkah pengamanan masyarakat terhadap ancaman cybercrime ($p = 0.527$).
- Rata-rata langkah pengamanan tetap stabil di sekitar 68%, menunjukkan bahwa kesadaran dan perilaku masyarakat dalam mengambil tindakan pengamanan terhadap cybercrime belum meningkat.
- Kesimpulan: Langkah pengamanan masyarakat terhadap cybercrime belum menunjukkan perkembangan yang signifikan.

c. Pengetahuan Hukum (Hukum_Pre vs Hukum_Post):

- Hasil menunjukkan adanya penurunan signifikan dalam pengetahuan hukum masyarakat terkait cybercrime ($p < 0.001$). Rata-rata nilai menurun dari 68.0% (Hukum_Pre) menjadi 56.8% (Hukum_Post).
- Penurunan ini mengindikasikan bahwa masyarakat mungkin semakin kurang memahami hukum terkait cybercrime, baik karena intervensi yang kurang efektif atau karena adanya faktor lain seperti kompleksitas hukum.
- Kesimpulan: Pengetahuan hukum masyarakat tentang cybercrime mengalami penurunan, yang berpotensi memperburuk kemampuan masyarakat untuk melindungi diri dari kejahatan siber.

d. Kesimpulan Umum

Perkembangan cybercrime saat ini di masyarakat menunjukkan tren yang mengkhawatirkan:

- Aktivitas cybercrime meningkat, meskipun secara rata-rata perubahan ini tidak besar.
- Langkah pengamanan tetap stagnan, menunjukkan bahwa masyarakat belum cukup meningkatkan tindakan pencegahan terhadap cybercrime.
- Pengetahuan hukum masyarakat menurun, yang dapat melemahkan kesadaran mereka terhadap ancaman dan konsekuensi hukum dari cybercrime.

B. Untuk menjawab pertanyaan: "Bagaimana mengetahui tingkat kesadaran masyarakat terhadap tindak kejahatan cybercrime?", tingkat kesadaran masyarakat dapat diukur menggunakan tiga indikator utama yang sudah dianalisis dalam penelitian, yaitu:

Hasil Analisis dari Data

a. Deskriptif Statistik:

- Rata-rata skor untuk Cyber_Pre (0.570) dan Cyber_Post (0.586) menunjukkan bahwa lebih dari 50% masyarakat sudah menyadari aktivitas cybercrime, namun tingkat kesadaran ini hanya sedikit meningkat setelah posttest.
- Rata-rata skor untuk Langkah Pengamanan (0.680) menunjukkan bahwa sebagian besar masyarakat sudah mengambil langkah pengamanan, tetapi ini tidak meningkat setelah posttest.
- Rata-rata skor untuk Pengetahuan Hukum (Pre: 0.680, Post: 0.568) menunjukkan bahwa kesadaran hukum masyarakat menurun secara signifikan.

b. Uji Statistik (Wilcoxon Signed-Rank Test):

- Ada perbedaan signifikan pada tingkat aktivitas cybercrime ($p = 0.001$) dan pengetahuan hukum ($p < 0.001$) sebelum dan sesudah intervensi.
- Tidak ada perbedaan signifikan pada langkah pengamanan masyarakat ($p = 0.527$), yang berarti kesadaran masyarakat tentang tindakan preventif tetap stagnan.

c. Kesimpulan Tingkat Kesadaran Masyarakat

- 1) Aktivitas Cybercrime:
 - Tingkat kesadaran masyarakat terhadap bahaya cybercrime cukup baik, namun kesadaran ini tidak terlalu berkembang secara signifikan setelah post-test.
- 2) Langkah Pengamanan:
 - Sebagian besar masyarakat menyadari pentingnya langkah pengamanan, tetapi mereka tidak meningkatkan tindakan pengamanan setelah diberikan informasi atau intervensi.
- 3) Pengetahuan Hukum:

- Tingkat kesadaran hukum masyarakat cenderung menurun, yang menunjukkan bahwa pemahaman mereka terhadap hukum cybercrime kurang efektif setelah intervensi.

Kesimpulan dari kegiatan penelitian yang dilakukan di Kecamatan Jatiyoso terkait Tingkat Kesadaran Masyarakat terhadap bahaya Cybercrime yaitu dari hasil pengujian menggunakan metode uji deskriptif, uji normalitas dan uji Wilcoxon Signed-Rank menyebutkan bahwa tingkat kesadaran masyarakat sudah cukup baik. Dari beberapa hasil yang didapatkan, data menunjukkan masyarakat sudah memiliki perhatian lebih terkait bahaya cybercrime yang mengintai. Hal ini perlu ditingkatkan kembali agar informasi terkait bahaya cybercrime dapat sampai ke semua kalangan masyarakat di pelosok negeri.

Penulis berharap, penelitian ini dapat memberikan gambaran dan informasi yang valid mengenai kondisi di masyarakat khususnya di Kecamatan Jatiyoso dan masyarakat lain pada umumnya yang perlu mendapatkan edukasi dan penjelasan tentang bahaya cybercrime. Tindakan pencegahan dan mitigasi dari resiko yang akan berdampak kepada masyarakat dapat dilakukan sejak dini, dan memastikan bahwa masyarakat bisa lebih hati-hati jika mengalami dan menemui jenis-jenis cybercrime yang banyak terjadi

UCAPAN TERIMA KASIH

Ucapan terimakasih disampaikan pada LPPM Universitas Teknologi Muhammadiyah Jakarta yang telah mendanai pelaksanaan kegiatan Penelitian ini, serta kepada LPPM Universitas Muhammadiyah Karanganyar (Umuka) yang telah menginisiasi kolaborasi terkait penelitian ini. Semoga kolaborasi penelitian maupun pengabdian masyarakat dapat terus berlanjut. Dan yang terakhir, terimakasih kepada pihak-pihak yang telah banyak membantu baik secara langsung maupun tidak langsung sehingga kegiatan penelitian ini dapat berjalan dengan baik.

DAFTAR PUSTAKA

- [1] A. Angkasa and R. Windiasih, "Cybercrime Di Era Industri 4.0 Dan Masyarakat 5.0

- Dalam Perspektif Viktimologi.” J. Justiciabelen, vol. 2, no. 2, p. 104, 2022, doi: 10.35194/jj.v2i2.2113.
- [2] R. Aditama, “Penegakan Hukum Cyber Crime Terhadap Tindak Pidana Pencurian Uang Nasabah Dengan Cara Pembajakan Akun Internet Banking Lewat Media Sosial,” Wajah Huk., vol. 5, no. 1, p. 118, 2021, doi: 10.33087/wjh.v5i1.360.
- [3] R. Arifin and F. R. Muthia, “Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik di Indonesia,” RESAM J. Huk., vol. 5, no. 1, pp. 21–39, 2019.
- [4] B. Aryo Wijoseno, I. Gusti Agung Ayu Dike Widhiyaastuti, K. Kunci, K. Hukum, T. Pidana, and K. Dunia Maya, “Jerat Pidana Terhadap Pelaku Peretas Sistem Komputer Secara Ilegal (Hacker) Dalam Perpsektif Hukum Pidana Indonesia,” J. Kertha Desa, vol. 11, no. 3, pp. 2031–2041, 2023.
- [5] A. Irawati, H. B. Fadholi, A. N. Alamsyah, D. P. Dwipayana, and M. Muslih, “Proceeding of Conference on Law and Social Studies URGENSI CYBER LAW DALAM KEHIDUPAN MASYARAKAT INDONESIA DI ERA DIGITAL,” Pros. Conf. Law Soc. Stud., pp. 1–15, 2021, [Online]. Available: <http://prosiding.unipma.ac.id/index.php/COLAAS>
- [6] Sofyantoro, S. Triwahyuningsih, Angelina, Jumangin, and E. Sulistya, “Proceeding of Conference on Law and Social Studies Kehidupan Sosial Masyarakat Dan Perspektif Hukum Pidana Mengenai Cyber Crime Di Era,” 2021.
- [7] Ferry, I. Febriansyah, A. Indiantoro, and A. Ikhwan, “Legal Standing Jurnal Ilmu Hukum Model Kejahatan Dunia Maya (Cybercrime) Sebagai Upaya Pembentukan Hukum Nasional,” Issn, vol. 7, no. 2, pp. 2580–3883, 2023.
- [8] R. G. Sembiring, M. Ablisar, M. Mulyadi, and J. Leviza, “Penegakan Hukum Cybercrime di Wilayah Hukum Kepolisian Daerah Sumatera Utara,” Locus J. Acad. Lit. Rev., vol. 2, no. 3, pp. 292–304, 2023, [Online]. Available: <https://doi.org/10.56128/ljoalr.v2i3.145>.
- [9] Halaman website <https://kumparan.com/yogik-chanel/tingkat-kesadaran-masyarakat-dalam-menanggapi-fenomena-sosial-1zWsGPgCSDL/full> diakses pada 4 Oktober 2024.
- [10] Halaman website <https://pid.kepri.polri.go.id/apa-itu-cyber-crime/> diakses pada 4 Oktober 2024
- [11] Halaman website <https://tribrataneews.jateng.polri.go.id/2022/03/07/kunjungan-kerja-di-polsek-jatiyoso-kapolres-karanganyar-berikan-motivasi-kepada-anggota/> diakses pada 4 Oktober 2024.
- [12] Muhammad Ropi. Taofiq Hidayat, Nur Widiyasono, Rohmat Gunawan, “Optimasi Deteksi Malware pada SIEM Wazuh melalui Integrasi Cyber Threat Intelligence dengan MISP dan DFIR-IRIS,” Jurnal Informatika dan Teknik Elektro Terapan (JITET), Vol. 13 No. 1 pISSN:2303-0577 eISSN: 2830-7062, 2025 [Online]. Available: <http://dx.doi.org/10.23960/jitet.v13i1.5686>
- [13] Yuliawati, Nina Sulistyowati, Siska, “Opinion Mining terhadap Penanganan Rohingya di Provinsi Aceh Menggunakan Naïve Bayes pada Media Sosial Twitter,” Jurnal Informatika dan Teknik Elektro Terapan (JITET), Vol. 12 No. 3 pISSN:2303-0577 eISSN: 2830-7062, 2024 [Online]. Available: <http://dx.doi.org/10.23960/jitet.v12i3.4990>