



**EDUKASI POLA KEJAHATAN SIBER UNTUK ANTISIPASI PENIPUAN PADA SISWA
SMA SANTO THOMAS 4 BINJAI**

*Cybercrime Pattern Education to Anticipate Fraud for Students of Santo Thomas 4 Binjai
High School*

**Manutur Pandapotan Siregar*, Abwabul Jinan, Windi Saputri Simamora, Siti Sarah
Harahap**

Program Studi Teknik Informatika Universitas Satya Terra Bhinneka

Jalan Sunggal Gg. Bakul, Sunggal, Kec. Medan Sunggal, Kota Medan, Sumatera Utara 20128

*Alamat Korespondensi: manutursiregar@satyaterrabhinneka.ac.id

(Tanggal Submission: 3 November 2025, Tanggal Accepted : 20 Maret 2026)



Kata Kunci :

*Handphone,
Data, Posting,
Link, CyberCrime*

Abstrak :

Penggunaan *handphone* telah menjadi bagian dari kehidupan sehari-hari masyarakat. Tingginya aktivitas di dunia maya juga membuka peluang terjadinya *cybercrime* seperti penyebaran *spam*, *malware*, virus, serta *link* palsu yang dapat mengarah pada pencurian data maupun penipuan finansial. Kurangnya pemahaman masyarakat mengenai keamanan digital menjadi salah satu faktor meningkatnya kasus *cybercrime*. Tujuan kegiatan PKM ini adalah untuk meningkatkan pengetahuan dan kesadaran siswa mengenai bentuk-bentuk kejahatan siber serta cara mengidentifikasi tautan yang mencurigakan. Selain itu, kegiatan ini diharapkan dapat menjadikan siswa sebagai agen edukasi digital di lingkungan keluarga. Metode yang digunakan dalam kegiatan ini adalah penyuluhan mengenai *cybercrime* kepada siswa. Materi yang disampaikan meliputi pengenalan jenis-jenis *cybercrime*, cara memeriksa validitas *link*, serta pemahaman tentang pengaturan keamanan dan hak akses aplikasi pada *handphone*. Kegiatan dilakukan melalui presentasi, dan diskusi sederhana terkait identifikasi tautan mencurigakan. Hasil kegiatan menunjukkan adanya peningkatan pemahaman siswa mengenai bahaya kejahatan siber dan cara mengantisipasinya. Siswa mampu mengenali ciri-ciri tautan yang mencurigakan serta memahami pentingnya tidak sembarangan memberikan izin akses kepada aplikasi. Selain itu, siswa juga menunjukkan peningkatan kesadaran untuk lebih berhati-hati saat menerima pesan atau tautan dari sumber yang tidak dikenal. Diskusi yang dilakukan selama kegiatan memperlihatkan bahwa sebagian besar siswa sebelumnya belum memahami sepenuhnya potensi ancaman *cybercrime*. Setelah kegiatan berlangsung, siswa mampu menjelaskan kembali langkah-langkah dasar untuk menghindari *cybercrime*. Hal ini menunjukkan bahwa kegiatan edukasi memiliki dampak

	positif terhadap peningkatan literasi keamanan digital. Kesimpulan dari kegiatan ini adalah bahwa edukasi mengenai keamanan digital kepada siswa efektif dalam meningkatkan pemahaman tentang <i>cybercrime</i> . Siswa berpotensi menjadi agen edukasi bagi keluarga dalam mencegah <i>cybercrime</i> .
Key word :	Abstract :
<i>Mobile, Data, Posts, Links, Cybercrime</i>	The use of digital devices such as mobile phones has become an integral part of everyday life in modern society. Increased intensity of online activities also creates opportunities for cybercrime, including the distribution of spam, malware, viruses, and fraudulent links that may lead to data theft and financial scams. Limited public awareness and understanding of digital security are among the factors contributing to the increasing number of cybercrime cases. The purpose of this activity is to improve students' knowledge and awareness regarding various forms of cybercrime and how to identify suspicious links. In addition, this activity aims to encourage students to act as digital literacy agents within their families. The method used in this activity was an educational outreach program on cybercrime for students. The materials presented included an introduction to the types of cybercrime, techniques for verifying the validity of links, and an understanding of mobile phone security settings and application permission management. The activity was conducted through presentations and interactive discussions related to the identification of suspicious links. The results of the activity indicate an improvement in students' understanding of cybercrime threats and strategies to prevent them. Students were able to identify the characteristics of suspicious links and understand the importance of carefully managing application access permissions. In addition, students demonstrated increased awareness and caution when receiving messages or links from unknown sources. The discussions conducted during the activity revealed that most students previously had limited understanding of potential cyber threats. After participating in the activity, students were able to explain basic preventive measures to avoid cybercrime. These findings indicate that educational activities have a positive impact on improving digital security literacy. In conclusion, digital security education for students is effective in increasing awareness and understanding of cybercrime. Students have the potential to serve as agents of digital literacy within their families to help prevent cybercrime incidents.

Panduan sitasi / citation guidance (APPA 7th edition) :

Siregar, M. P., Jinan, A., Simamora, W. S., & Harahap, S. S. (2026). Edukasi Pola Kejahatan Siber Untuk Antisipasi Penipuan Pada Siswa SMA Santo Thomas 4 Binjai. *Jurnal Abdi Insani*, 13(3), 2017-2032. <https://doi.org/10.29303/abdiinsani.v13i3.3487>

PENDAHULUAN

Analisis Situasi

Perkembangan teknologi informasi dan komunikasi telah memberikan berbagai kemudahan dalam aktivitas manusia, terutama dalam bidang komunikasi, ekonomi digital, pendidikan, dan layanan publik. Namun demikian, kemajuan teknologi tersebut juga memunculkan berbagai bentuk kejahatan baru yang memanfaatkan jaringan internet dan sistem komputer, yang dikenal sebagai kejahatan siber atau *cybercrime*. Cybercrime merupakan tindakan kriminal yang dilakukan dengan memanfaatkan teknologi informasi sebagai sarana maupun target kejahatan (Sitompul *et al.*, 2023).



Fenomena cybercrime di Indonesia mengalami peningkatan seiring dengan meningkatnya jumlah pengguna internet dan pesatnya transformasi digital dalam berbagai sektor. Kondisi ini menyebabkan ruang siber menjadi salah satu media yang rentan dimanfaatkan oleh pelaku kejahatan untuk melakukan berbagai aktivitas ilegal seperti penipuan online, pencurian data, peretasan sistem, dan penyebaran informasi palsu (Hartati & Muhammad, 2022). Selain itu, perkembangan teknologi digital juga menyebabkan munculnya bentuk-bentuk kejahatan siber yang semakin kompleks dan sulit dilacak, terutama karena pelaku dapat menyembunyikan identitasnya melalui sistem jaringan global (Siregar, 2024).

Dalam konteks hukum di Indonesia, pemerintah telah berupaya mengatur dan menanggulangi cybercrime melalui berbagai regulasi, salah satunya melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Regulasi ini menjadi dasar hukum bagi penegakan hukum terhadap berbagai bentuk kejahatan yang terjadi di ruang digital (Waliadin, 2024). Meskipun demikian, implementasi penegakan hukum terhadap cybercrime masih menghadapi berbagai kendala, terutama dalam proses penyidikan yang memerlukan kemampuan teknis dan metode investigasi digital yang memadai (Indradjaja *et al.*, 2024).

Selain aspek penegakan hukum, cybercrime juga memberikan dampak yang signifikan terhadap keamanan data pribadi serta stabilitas sistem informasi. Kasus kebocoran data (*data breach*) yang terjadi di berbagai institusi menunjukkan bahwa perlindungan data digital masih menjadi tantangan besar dalam era transformasi digital saat ini (Silalahi *et al.*, 2025). Kondisi ini juga dapat menurunkan tingkat kepercayaan masyarakat terhadap keamanan sistem digital yang digunakan dalam berbagai layanan publik dan ekonomi digital.

Cybercrime juga dapat menimbulkan dampak sosial yang cukup serius bagi korban, baik dalam bentuk kerugian finansial maupun gangguan psikologis. Oleh karena itu, perlindungan hukum terhadap korban kejahatan siber menjadi salah satu aspek penting yang perlu diperhatikan dalam sistem hukum di Indonesia (Pratama, 2025). Dalam beberapa kasus, cybercrime bahkan berkembang menjadi bentuk kejahatan yang bersifat lintas negara (*transnational crime*), sehingga membutuhkan kerja sama internasional dalam proses penegakan hukumnya (Rahman, 2024). Selain itu, beberapa bentuk cybercrime seperti *cyberstalking* juga semakin banyak ditemukan dalam interaksi digital masyarakat. Kejahatan ini dapat menimbulkan dampak psikologis yang serius bagi korban karena dilakukan secara terus menerus melalui media digital (Nasution, 2025). Oleh karena itu, upaya pencegahan dan penanganan cybercrime tidak hanya memerlukan pendekatan hukum semata, tetapi juga memerlukan peningkatan literasi digital masyarakat serta penguatan sistem keamanan siber nasional (Saputra, 2021).

Dalam era transformasi digital saat ini, upaya penanggulangan cybercrime perlu dilakukan secara komprehensif melalui kolaborasi antara pemerintah, lembaga penegak hukum, sektor swasta, dan masyarakat. Penguatan kebijakan keamanan siber serta peningkatan kesadaran masyarakat terhadap risiko kejahatan digital menjadi langkah penting dalam menciptakan ruang digital yang aman dan terpercaya (Djibu, 2025).

Masyarakat di sekitar Kota Binjai memiliki latar belakang sosial, ekonomi, dan pendidikan yang beragam. Sebagian besar keluarga di wilayah tersebut menyekolahkan anak-anak mereka di SMA Santo Thomas 4 Binjai, yang merupakan salah satu sekolah menengah atas yang cukup dikenal di kota Binjai. Seiring dengan perkembangan teknologi informasi, para siswa di sekolah ini telah terbiasa menggunakan perangkat digital seperti handphone untuk mendukung aktivitas belajar maupun kegiatan sehari-hari. Penggunaan perangkat tersebut meliputi pencarian informasi di internet, komunikasi melalui aplikasi pesan, serta interaksi di berbagai platform media sosial. Tingginya intensitas penggunaan handphone dan media sosial juga membuka peluang terjadinya berbagai bentuk kejahatan siber, seperti penyebaran tautan palsu, pencurian data pribadi, maupun penipuan digital. Kondisi ini semakin rentan terjadi apabila pengguna memiliki tingkat literasi keamanan digital yang masih terbatas, sehingga diperlukan upaya edukasi untuk meningkatkan kesadaran dan

kemampuan siswa dalam mengenali serta mengantisipasi potensi ancaman *cybercrime* di lingkungan digital.

Dalam kehidupan bermasyarakat terdapat berbagai komunitas yang terbentuk atas dasar kesamaan tertentu, seperti kesamaan agama, kesamaan sekolah anak, maupun kesamaan lingkungan tempat tinggal. Komunitas-komunitas tersebut sering dimanfaatkan sebagai sarana bertukar informasi dan berdiskusi mengenai berbagai persoalan yang dihadapi oleh anggota masyarakat. Beberapa kasus yang pernah dibahas dalam komunitas masyarakat antara lain adanya pengiriman tautan file berformat *apk* dari nomor telepon yang tidak dikenal (Al-Dhaqm *et al.*, 2020; Karim *et al.*, 2019), adanya email pemanggilan kerja yang mengatasnamakan salah satu BUMN namun menimbulkan kecurigaan karena mewajibkan pelamar menggunakan akomodasi dan transportasi travel tertentu menuju Jakarta, kasus anggota masyarakat yang diarahkan hingga ke mesin ATM dan mengikuti instruksi dari pihak yang tidak bertanggung jawab (Kovačević *et al.*, 2020; Sharma & Gillanders, 2022), serta upaya masyarakat dalam mengantisipasi nomor telepon yang tidak dikenal dengan menggunakan aplikasi seperti Get Contact. Berbagai kasus tersebut menunjukkan bahwa masyarakat mulai menyadari adanya potensi *cybercrime*, namun pemahaman mengenai pola dan mekanisme terjadinya *cybercrime* masih terbatas.

Dalam kajian literasi digital, rendahnya pemahaman masyarakat terhadap keamanan digital sering menjadi faktor utama yang menyebabkan seseorang mudah menjadi korban kejahatan siber. Oleh karena itu, edukasi mengenai pola-pola *cybercrime* perlu dilakukan secara sistematis untuk meningkatkan kemampuan individu dalam mengenali potensi ancaman di ruang digital. Salah satu strategi yang dinilai efektif adalah memberikan edukasi kepada siswa di tingkat sekolah menengah, karena generasi muda merupakan kelompok yang memiliki intensitas penggunaan teknologi digital yang tinggi serta memiliki kemampuan untuk menyebarkan kembali informasi yang diperoleh kepada lingkungan keluarga. Selain itu, siswa juga sering menjadi sumber rujukan bagi orang tua dalam memahami penggunaan teknologi digital. Dengan latar belakang tersebut, tim PKM berupaya memberikan edukasi mengenai pola dan mekanisme *cybercrime* kepada siswa-siswi agar mereka memiliki pemahaman yang lebih baik mengenai proses terjadinya kejahatan siber serta mampu membagikan pengetahuan tersebut kepada keluarga masing-masing sebagai upaya pencegahan terhadap kasus serupa.

Permasalahan Mitra

Mengacu kepada Analisis Situasi, uraian permasalahan prioritas mitra yang mencakup hal-hal sebagai berikut :

1. File *apk* merupakan file ekstensi pada platform android. Dengan adanya pengiriman file *dot apk* berbahaya menyebabkan masyarakat kebingungan dalam membedakan mana file *dot apk* yang benar mana yang tidak.
2. Email resmi dari suatu perusahaan biasanya memiliki tata bahasa yang baku dan format tertentu. Namun, dengan adanya penipuan melalui pengiriman email yang mengatasnamakan perusahaan tertentu, apalagi perusahaan yang pernah dilamar, hal ini dapat menimbulkan keraguan di masyarakat dalam membedakan antara email resmi perusahaan dan email penipuan.
3. Masyarakat sering mengalami kesulitan dalam membedakan nomor telepon yang tidak dikenal, terutama ketika panggilan tersebut mengatasnamakan instansi tertentu. Pelaku kejahatan siber kerap menggunakan berbagai modus, seperti mengatasnamakan instansi resmi, teknik *social engineering* untuk memperoleh informasi pribadi korban, permintaan kode OTP yang bersifat rahasia, serta penggunaan *scare tactics* berupa ancaman atau tekanan psikologis agar korban segera mengikuti instruksi yang diberikan
4. Aplikasi yang ada seperti "Get Contact" sering dipakai untuk mengetahui nomor telepon yang tidak dikenal, tetapi dengan melakukan instalasi app tersebut pengguna juga mengizinkan app tersebut untuk mengakses kontak yang ada pada handphone app terinstal.



Solusi yang ditawarkan

Solusi yang ditawarkan bagi siswa/i adalah kemampuan untuk dapat menganalisis lebih awal bentuk-bentuk atau pola kejahatan cyber, sehingga dapat menjadi garda pertama dalam keluarga untuk mencegah timbulnya korban kejahatan cyber.

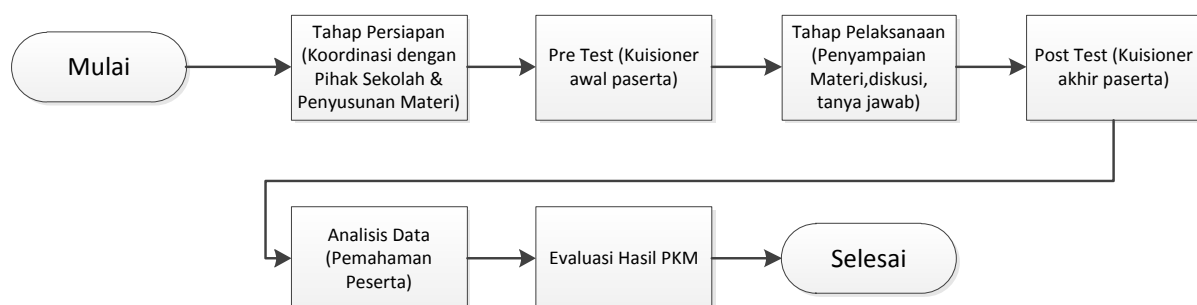
Target Luaran

Adapun target luaran dari pengabdian masyarakat (PKM) ini adalah menghasilkan dokumentasi jurnal bereputasi nasional sinta 4.

METODE KEGIATAN

Pengabdian Kepada Masyarakat (PKM) ini dilaksanakan bekerja sama dengan SMA Santo Thomas 4 Binjai yang berlokasi di Jl. Ikan Tenggiri No. 21, Dataran Tinggi, Kecamatan Binjai Timur, Binjai, Sumatera Utara 20351. Kegiatan ini dilaksanakan pada tanggal 10 Juni 2024 dengan sasaran peserta yaitu siswa/i kelas XI A. Jumlah peserta yang mengikuti kegiatan ini sebanyak 38 orang siswa. Program pengabdian ini bertujuan untuk memberikan pengetahuan dan pemahaman kepada para siswa sesuai dengan materi yang disampaikan dalam kegiatan PKM.

Metode kegiatan PKM ini dilaksanakan melalui beberapa tahapan, yaitu tahap persiapan, pelaksanaan, dan evaluasi. Pada tahap persiapan dilakukan koordinasi dengan pihak sekolah serta penyusunan materi penyuluhan. Tahap pelaksanaan dilakukan dengan metode penyampaian materi, diskusi, dan tanya jawab kepada siswa. Instrumen yang digunakan dalam kegiatan ini berupa materi presentasi serta kuesioner sederhana untuk mengetahui pemahaman peserta sebelum dan sesudah kegiatan. Selanjutnya, data yang diperoleh dianalisis secara deskriptif untuk melihat peningkatan pemahaman peserta terhadap materi yang disampaikan.



Gambar 1. Diagram Alir Pelaksanaan PKM

HASIL DAN PEMBAHASAN

Sebelum melakukan presentasi kepada siswa/i terlebih dahulu dilakukan pre-test dengan memberikan kuesioner yang berisi pertanyaan tentang materi untuk mengukur pengetahuan tentang Cyber Crime. Mitra yang merupakan pihak sekolah akan dipandu oleh tim PKM untuk mengikuti kegiatan dan penjelasan dari pemateri. Pemberian materi akan dilakukan dengan tujuan agar siswa-siswi memiliki pengetahuan tentang cyber crime sehingga dapat mengantisipasinya. Selain itu siswa-siswi akan menjadi agen dalam mengantisipasi cyber crime di lingkungan keluarga dan masyarakat sekitarnya.

Beberapa pertanyaan pre-testnya meliputi :

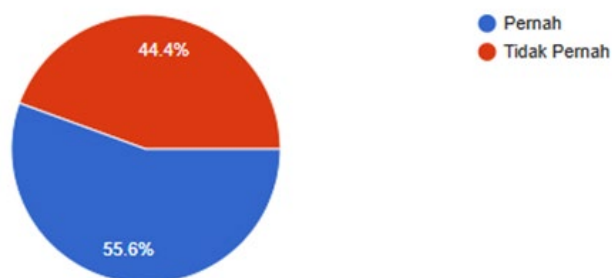
1. Apakah Keluarga Anda Pernah Menjadi Korban Kejahatan Cyber (Cyber Crime) ?

Tabel 1. Hasil Pre Test Pertanyaan 1

No	Jawaban
1	Pernah



2	Pernah
3	Pernah
4	Pernah
5	Pernah
6	Tidak Pernah
7	Tidak Pernah
8	Tidak Pernah
9	Tidak Pernah
10	Pernah
11	Tidak Pernah
12	Tidak Pernah
13	Tidak Pernah
14	Pernah
15	Pernah
16	Pernah
17	Tidak Pernah
18	Tidak Pernah
19	Pernah
20	Pernah
21	Pernah
22	Tidak Pernah
23	Pernah
24	Pernah
25	Pernah
26	Tidak Pernah
27	Tidak Pernah



Gambar 2. Hasil Pre-Test Pertanyaan 1

2. Jenis Kejahatan Apa yang keluarga anda pernah alami ?

Tabel 2. Hasil Pre Test Pertanyaan 2

No	Jawaban
1	Penipuan lewat telepon
2	Penipuan lewat telepon
3	Penipuan lewat telepon
4	Penipuan
5	Mengaku sebagai keluarga
6	Tidak ada
7	Tidak ada
8	Tidak ada
9	tidak ada
10	Penipuan melalui telepon
11	Tidak ada
12	Tidak ada
13	Tidak pernah
14	Penipuan
15	Ditelepon penipu
16	Penipuan
17	Tidak pernah
18	Tidak ada
19	telepon penipuan
20	telepon penipuan
21	Penipuan (Mengaku Keluarga)
22	Tidak pernah
23	Penipuan ttg saudara saya ditangkap,
24	Penipuan
25	Nomor panggilan yang tidak dikenal
26	Tidak pernah
27	Tidak pernah



Gambar 3. Hasil Pre-Test Pertanyaan 2

3. Langkah apa yang keluarga anda lakukan untuk mengantisipasi kejahatan cyber ?

Tabel 3. Hasil Pre Test Pertanyaan 3

No	Jawaban
1.	Mengabaikan
2.	Menipunya kembali
3.	Memblokir kontak
4.	Tidak ada
5.	Jangan mudah percaya dengan orang lain
6.	Mengabaikan dan memblokir no tersebut
7.	Jangan gampang percaya pada org lain, pastikan terlebih dahulu
8.	Mengantisipasi nomor baru
9.	Jangan mudah percaya dengan orang lain
10.	mematikan telepon dan memblokir nomor tersebut
11.	memblokir serta mematikan nomor yang melakukan telepon tersebut
12.	Tidak di tanggapin atau nipu balik lagi
13.	Mengantisipasi nomor baru
14.	Tidak memperdulikannya karna saudara saya saat itu ada di rumah
15.	Memasuk nomor ke daftar hitam
16.	Blokir nomornya

Dari pre-test yang dilakukan didapati bahwa kejahatan cyber sudah pernah mencoba masuk dalam lingkungan keluarga siswa/i. Oleh sebab itu PKM dengan topik “Pemahaman Terhadap Pola Kejahatan Cyber Sebagai Langkah Awal Antisipasi Tindak Penipuan” dirasa tepat dilakukan.

Presentasi dilakukan dengan menyajikan data dan fakta yang terjadi di lapangan dengan menjelaskan tujuan, populasi dan jenis-jenis kejahatan cyber.

Pemahaman Terhadap Pola Kejahatan Cyber Sebagai Langkah Awal Antisipasi Tindak Penipuan



Manutur P Siregar, ST, M.Kom
Abwabul Jinan, S.Kom, M.Kom
Windi Saputri Simamora, S. Kom., M. Kom
Siti Sarah Harahap, S.Kom, M.Kom

Gambar 4. Slide Presentasi Utama



Gambar 5. Materi Slide Presentasi

Presentasi menjelaskan tentang 6 jenis kejahatan cyber yang meliputi: *Phising*, *Identity Theft*, *Cyberstalking*, *Spam*, *OTP Fraud* dan Pinjol Ilegal. Pemahamannya meliputi pola, bagaimana cara mengidentifikasinya serta apa yang dilakukan jika kita atau salah satu dari keluarga kita mengalami kejadian sebagai korban *cyber crime*.



Gambar 6. Aktivitas Presentasi



Gambar 7. Tanya Jawab dengan siswa/i



Gambar 8. Sesi Foto

Solusi permasalahan dari analisis situasi untuk menyelesaikan permasalahan yang dihadapi di uraikan sebagai berikut:

1. Memastikan Aktif fitur pemblokiran install aplikasi dari sumber yang tidak dikenal, serta hanya melakukan instalasi aplikasi dari Google Play Store
2. Memeriksa domain url dari link perusahaan, format penulisan email serta domain email yang digunakan oleh pengirim.
3. Memastikan teknik komunikasi penelepon apakah seperti bersumber dari instansi yang terpercaya atau tidak.
4. Memastikan pemberian izin atau blokir terhadap fitur-fitur yang akan digunakan aplikasi pihak ke-3.

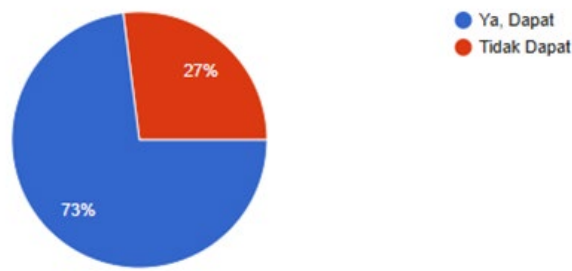
Setelah dilakukan presentasi, maka dilakukan lagi post-test untuk mengetahui tingkat pemahaman siswa/i terhadap materi yang diberikan. Beberapa pertanyaan yang ditanyakan ke siswa/i yakni :

1. Jika terjadi kejahatan cyber di lingkungan keluarga anda. Dapatkah anda mendeteksinya secara dini ?

Tabel 4. Hasil Post Test Pertanyaan 1

No	Jawaban
1	Ya, Dapat
2	Tidak Dapat
3	Ya, Dapat

4	Ya, Dapat
5	Ya, Dapat
6	Ya, Dapat
7	Ya, Dapat
8	Ya, Dapat
9	Ya, Dapat
10	Tidak Dapat
11	Ya, Dapat
12	Ya, Dapat
13	Tidak Dapat
14	Ya, Dapat
15	Ya, Dapat
16	Ya, Dapat
17	Ya, Dapat
18	Ya, Dapat
19	Ya, Dapat
20	Ya, Dapat
21	Ya, Dapat
22	Ya, Dapat
23	Ya, Dapat
24	Ya, Dapat
25	Tidak Dapat
26	Tidak Dapat
27	Ya, Dapat
28	Ya, Dapat
29	Tidak Dapat
30	Ya, Dapat
31	Ya, Dapat
32	Ya, Dapat
33	Tidak Dapat
34	Ya, Dapat
35	Tidak Dapat
36	Tidak Dapat
37	Tidak Dapat



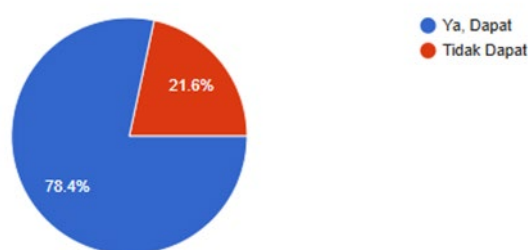
Gambar 9. Hasil Post Test Pertanyaan 1

2. Apakah anda dapat melakukan aksi nyata jika salah satu keluarga anda menjadi korban kejahatan cyber ?

Tabel 5. Hasil Post Test Pertanyaan 2

No	Jawaban
1	Ya, Dapat
2	Tidak Dapat
3	Ya, Dapat
4	Ya, Dapat
5	Ya, Dapat
6	Ya, Dapat
7	Tidak Dapat
8	Ya, Dapat
9	Ya, Dapat
10	Tidak Dapat
11	Ya, Dapat
12	Ya, Dapat
13	Ya, Dapat
14	Ya, Dapat
15	Ya, Dapat
16	Ya, Dapat
17	Ya, Dapat
18	Ya, Dapat
19	Ya, Dapat
20	Ya, Dapat
21	Tidak Dapat
22	Ya, Dapat
23	Ya, Dapat

24	Ya, Dapat
25	Ya, Dapat
26	Ya, Dapat
27	Ya, Dapat
28	Ya, Dapat
29	Tidak Dapat
30	Ya, Dapat
31	Ya, Dapat
32	Ya, Dapat
33	Tidak Dapat
34	Ya, Dapat
35	Ya, Dapat
36	Tidak Dapat
37	Tidak Dapat



Gambar 10. Hasil Post Test Pertanyaan 2

3. Apakah Anda tertarik dengan topik Cyber Crime ?

Tabel 6. Hasil Post Test Pertanyaan 3

No	Jawaban
1	Tertarik
2	Tertarik
3	Tertarik
4	Tertarik
5	Tertarik
6	Tertarik
7	Tertarik
8	Tertarik
9	Tertarik

10	Tertarik
11	Tertarik
12	Tertarik
13	Tertarik
14	Tertarik
15	Tertarik
16	Tertarik
17	Tertarik
18	Tertarik
19	Tertarik
20	Tertarik
21	Tertarik
22	Tertarik
23	Tertarik
24	Tertarik
25	Tertarik
26	Tertarik
27	Tertarik
28	Tertarik
29	Tertarik
30	Tertarik
31	Tertarik
32	Tertarik
33	Tertarik
34	Tertarik
35	Tertarik
36	Tertarik
37	Tertarik



Gambar 11. Hasil Post Test Pertanyaan 3

KESIMPULAN DAN SARAN

Kesimpulan

Dengan pengabdian kepada masyarakat ini, berdasarkan jawaban yang diberikan oleh siswa/i maka sebanyak 73% dapat mendeteksi secara dini kejahatan *cyber* dan sebanyak 78,4% dapat melakukan aksi nyata jika salah satu keluarga anda menjadi korban kejahatan *cyber* serta 100% siswa tertarik untuk belajar lebih dalam lagi tentang topik *cybercrime*.

Saran

Perlu dilakukan identifikasi terhadap berbagai jenis serangan siber melalui kegiatan edukasi kepada masyarakat dengan memberikan contoh modus yang sering terjadi, seperti phishing, spam email, penipuan melalui kode OTP, dan teknik *social engineering*. Selain itu, masyarakat perlu diberikan panduan praktis untuk mengenali tanda-tanda serangan siber, melakukan verifikasi terhadap informasi yang diterima, serta menjaga kerahasiaan data pribadi agar dapat mengurangi risiko menjadi korban kejahatan digital.

UCAPAN TERIMA KASIH

Terima kasih tim Pengabdian Kepada Masyarakat (PKM) sampaikan kepada Universitas Satya Terra Bhinneka dan LPPM Universitas Satya Terra Bhinneka karena pengabdian ini didanai oleh Hibah Internal Universitas Satya Terra Bhinneka dan sebagai tempat para dosen menerapkan tri darma perguruan tinggi serta kepada SMA Santo Thomas 4 Binjai Sumatera Utara sebagai tempat Pengabdian Kepada Masyarakat (PKM).

DAFTAR PUSTAKA

- Al-Dhaqm, A., Razak, S. A., Ikuesan, R. A., Kebande, V. R., & Siddique, K. (2020). A Review of Mobile Forensic Investigation Process Models. *IEEE Access*, 8, 173359–173375. <https://doi.org/10.1109/ACCESS.2020.3014615>
- Djibu, M. A. (2025). Transformasi Digital dan Keamanan Siber: Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia. *Judge: Jurnal Hukum*, 5(1), 10–20.
- Hartati, C. S., & Muhammad, A. (2022). Combating Cybercrime and Cyberterrorism in Indonesia. *Jurnal Hubungan Internasional*, 11(2), 235–248.
- Indradjaja, M. A. P., Suseno, S., & Atmaja, B. A. (2024). Implementasi Penyidikan Terhadap Tindak Pidana Siber dalam Perspektif Perbandingan Hukum: Indonesia Dan Inggris Raya. *Jurnal Ilmiah Penegakan Hukum*, 11(2), 150–162.
- Karim, A., Azam, S., Shanmugam, B., Kannoopatti, K., & Alazab, M. (2019). A Comprehensive Survey for Intelligent Spam Email Detection. *IEEE Access*, 7, 168261–168295. <https://doi.org/10.1109/ACCESS.2019.2954791>
- Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, 8, 125140–125148. <https://doi.org/10.1109/ACCESS.2020.3007867>
- Nasution, M. (2025). Cyberstalking Crime in the Perspective of Islamic Criminal Law. *Jurnal Mercatoria*, 18(1), 33–44.
- Pratama, D. (2025). Perlindungan Hukum Terhadap Korban Kejahatan Cybercrime di Indonesia. *De Juncto Delicti: Journal of Law*, 3(1), 45–58.
- Rahman, A. (2024). Penegakan Hukum Pidana Terhadap Perkembangan Cyber Crime di Indonesia. *The Juris*, 8(2), 77–88.
- Saputra, R. (2021). Eksistensi Keamanan Siber Terhadap Tindakan Cyberstalking dalam Sistem Pertanggungjawaban Pidana Cybercrime. *Syntax Literate: Jurnal Ilmiah Indonesia*, 6(9), 4210–4220.
- Sharma, P., & Gillanders, J. (2022). Cybersecurity and Forensics in Connected Autonomous Vehicles: a Review of the State-of-the-Art. *IEEE Access*, 10, 108979–108996. <https://doi.org/10.1109/ACCESS.2022.3213843>



- Silalahi, R. S., Mulyadi, M., & Trisna, W. (2025). Analisis Hukum Tindak Pidana Cyber Data Breach di Era Digital. *SIBATIK Journal*, 4(1), 120–130.
- Siregar, H. (2024). Globalisasi Digital dan Cybercrime: Tantangan Hukum dalam Menghadapi Kejahatan Siber Lintas Batas. *Jurnal Hukum Sasana*, 10(1), 95–106.
- Sitompul, F., Manik, A. P. P., & Sihotang, R. (2023). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Hukum Indonesia. *Jaksa: Jurnal Kajian Ilmu Hukum dan Politik*, 2(3), 101–110.
- Waliadin. (2024). Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia. *Jurnal Thengkyang*, 7(1), 55–65.

