



Peningkatan Kesadaran dan Kewaspadaan Terhadap Ancaman Cybercrime Bagi Masyarakat di Era Digital

Yessica Siagian¹, Arridha Zikra Syah², Novica Irawati^{3*}

Program Studi Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Royal, Kisaran, Indonesia

email: ¹yessiegt@ymail.com, ²azsyra@gmail.com, ^{3*}novicairawati11@gmail.com

Email Coressponding Author: novicairawati11@gmail.com

Abstrak-Abstrak Pada kegiatan pengabdian masyarakat di desa Cengkring Kabupaten Batubara ini mengkaji pentingnya peningkatan kesadaran dan kewaspadaan terhadap ancaman *cybercrime* di era digital. Dengan kemajuan teknologi yang pesat dan adopsi luas internet, risiko terhadap kejahatan siber semakin meningkat. Banyak individu dan organisasi tidak sepenuhnya menyadari metode dan dampak *cybercrime*, yang menciptakan celah keamanan. Kegiatan ini menyoroti kebutuhan mendesak untuk edukasi dan pelatihan yang lebih baik tentang praktik keamanan digital. Melalui kolaborasi antara pemerintah, sektor swasta, dan masyarakat, serta inisiatif kesadaran yang proaktif, diharapkan dapat mengurangi kerentanan terhadap ancaman siber dan menciptakan lingkungan digital yang lebih aman. Hal ini menunjukkan bahwa pendekatan interaktif dan fokus pada isu-isu aktual seperti keamanan *cyber* sangat efektif dalam meningkatkan kesadaran dan kesiapan terhadap ancaman digital.

Kata Kunci: Cybercrime, Teknologi, Masyarakat

Abstract-Abstract In this community service activity in Cengkring village, Batubara Regency, it examines the importance of increasing awareness and vigilance against the threat of *cybercrime* in the digital era. With the rapid advancement of technology and the widespread adoption of the internet, the risk of *cybercrime* is increasing. Many individuals and organizations are not fully aware of the methods and impact of *cybercrime*, which creates security gaps. This activity highlights the urgent need for better education and training on digital security practices. Through collaboration between governments, the private sector, and the community, as well as proactive awareness initiatives, it is hoped that it can reduce vulnerability to cyber threats and create a safer digital environment. This shows that an interactive approach and focus on actual issues such as cybersecurity is very effective in increasing awareness and readiness against digital threats.

Keywords: Cybercrime, Technology, Society

1. PENDAHULUAN

Maraknya kasus penipuan online serta berita hoaks menjadi latar belakang utama penyelenggaraan kegiatan sosialisasi pentingnya kesadaran terhadap ancaman *cybercrime*. Sosialisasi ini bertujuan untuk meningkatkan kesadaran masyarakat tentang bahaya penipuan online dan hoaks, serta membekali mereka dengan pengetahuan dan strategi untuk melindungi diri dari ancaman tersebut (Hafid et al. 2023). Dalam era digital saat ini, peningkatan kesadaran dan kewaspadaan terhadap ancaman *cybercrime* menjadi semakin penting. Beberapa faktor yang mendasari kebutuhan ini meliputi: Pertumbuhan Teknologi dan Digitalisasi: Kemajuan teknologi dan peningkatan penggunaan internet di seluruh dunia telah mengubah cara kita berinteraksi, bekerja, dan berbelanja. Dengan meningkatnya ketergantungan pada teknologi digital, risiko terjadinya kejahatan siber juga meningkat. Evolusi Ancaman *Cybercrime*: Ancaman *cybercrime* semakin canggih dan beragam. Dari serangan phishing yang mencoba mencuri data pribadi hingga ransomware yang dapat mengunci data penting, pelaku kejahatan siber terus mengembangkan metode untuk mengeksploitasi kelemahan sistem dan individu. Kurangnya Pengetahuan dan Kesadaran: Banyak orang masih kurang memahami bagaimana melindungi diri mereka secara efektif di dunia maya. Kurangnya pengetahuan tentang langkah-langkah keamanan yang sederhana, seperti penggunaan kata sandi yang kuat dan perlindungan terhadap perangkat, dapat membuat mereka menjadi sasaran empuk bagi pelaku kejahatan siber. Dampak Ekonomi dan Sosial:



Cybercrime dapat memiliki dampak yang signifikan terhadap individu dan organisasi, termasuk kerugian finansial, kerusakan reputasi, dan gangguan operasional. Kesadaran yang lebih tinggi dapat membantu memitigasi risiko dan mengurangi potensi kerugian. Perlunya Edukasi dan Pelatihan: Masyarakat memerlukan edukasi dan pelatihan tentang cara melindungi diri dari ancaman siber. Program pelatihan yang efektif dapat meningkatkan kemampuan individu untuk mengidentifikasi potensi ancaman dan meresponsnya dengan tepat. Peran Pemerintah dan Sektor Swasta: Pemerintah dan sektor swasta memiliki peran penting dalam meningkatkan kesadaran dan kewaspadaan terhadap *cybercrime*. Ini termasuk inisiatif kebijakan, pelatihan, dan penyuluhan yang bertujuan untuk melindungi masyarakat dari ancaman siber. Dengan latar belakang ini, penting bagi semua pihak, termasuk individu, organisasi, dan pemerintah, untuk bekerja sama dalam meningkatkan kesadaran dan kewaspadaan terhadap ancaman *cybercrime*. Upaya kolektif ini akan membantu menciptakan lingkungan digital yang lebih aman dan lebih terlindungi bagi semua pengguna teknologi.

2. KERANGKA TEORI

2.1 Cybercrime

Cybercrime merupakan sebuah tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer berupa internet sebagai alat kejahatan utamanya, dan merupakan bentuk aktifitas kejahatan yang melanggar hukum (Asnawi et al. 2023). *Cybercrime*, atau kejahatan siber, merujuk pada berbagai aktivitas ilegal yang dilakukan dengan menggunakan komputer, jaringan komputer, atau internet. Kejahatan ini melibatkan berbagai bentuk aktivitas yang merugikan, baik itu terhadap individu, perusahaan, atau negara. Berikut beberapa contoh umum dari *cybercrime*:

1. Hacking: Akses tanpa izin ke sistem komputer atau jaringan untuk mencuri, merusak, atau memanipulasi data.
2. Phishing: Teknik penipuan yang digunakan untuk mendapatkan informasi sensitif seperti kata sandi atau nomor kartu kredit dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik.
3. Malware: Perangkat lunak berbahaya yang dirancang untuk merusak, mengakses, atau mencuri data dari komputer atau jaringan. Contoh malware termasuk virus, worm, trojan, dan ransomware.
4. Ransomware: Jenis malware yang mengenkripsi data pada komputer korban dan menuntut tebusan untuk mengembalikan akses ke data tersebut.
5. Identity Theft: Pencurian informasi pribadi seseorang untuk digunakan secara ilegal, misalnya untuk membuka rekening bank atau melakukan pembelian tanpa izin.
6. DDoS Attacks: Distributed Denial of Service attacks, yang melibatkan pengiriman lalu lintas internet yang sangat besar ke server atau jaringan untuk membuat layanan atau situs web menjadi tidak tersedia.
7. Online Fraud: Penipuan yang dilakukan melalui internet, termasuk penjualan barang palsu, investasi palsu, atau skema Ponzi.

Cybercrime dapat menyebabkan kerugian finansial, merusak reputasi, dan bahkan menimbulkan ancaman keamanan nasional. Karena sifatnya yang terus berkembang, upaya untuk mencegah dan menangani kejahatan siber memerlukan kombinasi dari teknologi canggih, kebijakan keamanan, dan kesadaran serta pendidikan yang baik bagi pengguna (Informasi, Mandiri, and Ii n.d.).

2.2 Teknologi

Secara etimologis, kata teknologi berasal dari dua kata yaitu *techn* yang berarti kerajinan, dan *logia* (*logos*) yang berarti ilmu atau teori Menurut Kamus Besar Bahasa Indonesia (KBBI) teknologi adalah metode ilmiah untuk mencapai tujuan praktis; ilmu pengetahuan terapan; 2 keseluruhan sarana untuk menyediakan barang-barang yang diperlukan bagi kelangsungan dan kenyamanan hidup manusia (Change et al. 2021). Teknologi adalah penerapan ilmu pengetahuan dan keahlian dalam menciptakan alat, sistem, atau metode yang digunakan untuk memecahkan masalah dan



memenuhi kebutuhan manusia. Teknologi mencakup berbagai bidang, mulai dari perangkat elektronik seperti komputer dan ponsel, hingga teknik rekayasa seperti jembatan dan mesin, serta sistem yang lebih kompleks seperti internet dan kecerdasan buatan. Teknologi seringkali dikaitkan dengan inovasi dan kemajuan, karena ia berfungsi untuk meningkatkan efisiensi, produktivitas, dan kualitas hidup. Teknologi juga berperan penting dalam berbagai aspek kehidupan sehari-hari, termasuk komunikasi, transportasi, kesehatan, pendidikan, dan banyak lagi.

2.3 Masyarakat

Masyarakat adalah kelompok individu yang hidup bersama dalam suatu wilayah dan berinteraksi satu sama lain berdasarkan norma dan aturan sosial yang berlaku. Ini mencakup struktur sosial, budaya, dan hubungan yang saling mempengaruhi.

Community dalam bahasa Yunani adalah “persahabatan”. Sebagai refleksi dari arti kata tersebut, Aristoteles mengemukakan bahwa manusia yang hidup bersama dalam masyarakat karena mereka menikmati ikatan yang saling bekerja sama, untuk memenuhi kebutuhan dasar mereka dan untuk menemukan makna kehidupan. Masyarakat dalam konteks pemberdayaan masyarakat adalah masyarakat atau *community* dalam bahasa Inggris atau juga komunitas. Secara etimologis “community” berasal dari *kommunitat* yang berakar pada *comunete* atau *comman* (Simões 1995).

3. METODE PELAKSANAAN

Pengabdian kepada masyarakat dengan tema “Peningkatan Kesadaran dan Kewaspadaan Terhadap Ancaman *Cybercrime* Bagi Masyarakat di Era Digital” ini dilaksanakan di desa Cengkring Pekan Kabupaten Batubara. Isi dari materi yang disampaikan mencakup pengenalan *cyber crime*, karakteristik *cyber crime*, berbagai macam modus kejahatan *cyber crime*, dan cara menghindari kejahatan *cyber crime*.

Dalam melakukan kegiatan pengabdian ini, metode kegiatan yang digunakan adalah sosialisasi, *pre-test*, dan *post-test* pada masyarakat desa Cengkring Kabupaten Batu Bara. Sosialisasi materi dilakukan oleh tim dosen STMIK Royal Kisaran mengenai apa itu *cyber crime*, bagaimana cara melindungi diri dari kejahatan *cyber crime*, dan memberikan contoh-contoh kasus *cyber crime* yang sering terjadi pada masyarakat. Tujuan dari penyampaian materi ini adalah agar masyarakat dapat memahami konsep dan bahaya dari *cyber crime*. *Pre-test* bertujuan untuk menentukan sejauh mana masyarakat memahami kejahatan *cyber crime* sebelum materi disampaikan secara keseluruhan, dimana tim dosen akan memberikan tes awal kepada masyarakat. *Post-test* bertujuan untuk mengukur sejauh mana pengetahuan siswa setelah diberikan sosialisasi mengenai *cyber crime*.

Dengan menggunakan metode yang terstruktur dan akurat, diharapkan kegiatan ini dapat memberikan kontribusi yang signifikan bagi dunia Pendidikan dan masyarakat dalam menggunakan sosial media. Kegiatan pengabdian ini dilaksanakan melalui tahapan-tahapan yang dapat dilihat pada Gambar 1 dibawah ini.





EVALUASI

Gambar 1. Tahapan Kegiatan

Tahap pertama dilakukan survey ke lokasi dan mengadakan pertemuan dengan kepala desa Cengkring. Pertemuan tersebut membahas tentang keinginan dari STMIK Royal melakukan kegiatan pengabdian kepada masyarakat tentang adanya kejahatan-kejahatan cyber yang marak terjadi di kalangan masyarakat. Tahap kedua yaitu perumusan masalah. Masalah pada hasil survei menunjukkan kurangnya pengetahuan dan ketrampilan para masyarakat desa. Selain itu kurangnya pemahaman tentang pentingnya menggunakan media online baik itu media sosial, website resmi, ataupun portal-portal online pengelolaan administrasi. Jika dalam penggunaan media tersebut tidak benar dan kurang hati-hati dalam penyampaian informasinya maka akan menimbulkan celah-celah kejahatan online. Langkah ketiga yaitu penyiapan materi. Materi disesuaikan dengan tujuan kegiatan pengabdian kepada masyarakat. Materi meliputi perkembangan teknologi informasi, kejahatan di dunia maya (*cybercrime*), jenis-jenis *cybercrime*, dampak *cybercrime*, penanggulangan *cybercrime* serta sanksi hukuman jika terlibat dalam kasus *cyber crime* Survey selanjutnya di akhir Kegiatan dilakukan tahapan Evaluasi melalui post untuk mengukur pemahaman peserta atas materi yang disampaikan.

4. HASIL

Hasil evaluasi dari kegiatan sosialisasi tersebut menunjukkan bahwa peserta lebih memahami pentingnya berhati-hati saat memberikan dan menyebarkan informasi di dunia siber, termasuk informasi pribadi dan berita. Dengan adanya kegiatan sosialisasi ini Para peserta dapat mengetahui cara menjaga data privasi aman dan konsekuensi jika mengabaikannya. Tujuan dari sosialisasi yang dilakukan adalah untuk meningkatkan kesadaran peserta tentang pentingnya menjaga keamanan data. Dengan sosialisasi, peserta diharapkan lebih berhati-hati saat menggunakan data pribadi. Dengan adanya wadah komunitas yang kuat, informasi dan pemahaman tentang keamanan data di dunia siber akan tersebar dengan lebih efektif dan dapat memberikan manfaat dalam menciptakan lingkungan yang lebih aman (Syaddan 2024). Berikut ini adalah dokumentasi dari kegiatan sosialisasi yang di lakukan di desa Cangkring Kabupaten Batu Bara, dimulai dari pembukaan dengan kata sambutan yang di berikan oleh Bapak kepala Desa Cengkring Kabupaten Batu Bara serta ketua kegiatan sosialisasi yaitu ibu Yessica Siagian S.Kom, M.Kom yang juga memberikan materi yang disampaikan. Hal tersebut dapat dilihat seperti gambar di bawah ini.





Jurnal Pengabdian Kepada Masyarakat Mitra Kreasi Cendekia

Vol 2, No 2, Juli 2024, Hal. 164-169

ISSN 2985-7430 (Media Online)

<https://ejournal.mitrakreasicendekia.com/index.php/mkc>

Gambar 2. Pemberian Kata Sambutan

Penyampaian materi mengenai keamanan data di dunia siber diperlihatkan pada Gambar 3. Para peserta sosialisasi turut memperhatikan dengan sungguh-sungguh mengenai materi yang disampaikan dan suasana saat acara berlangsung dengan hikmat.



Gambar 3. Penyampaian Materi

Kegiatan terakhir dilakukan foto bersama setelah peserta mengikuti sosialisasi dan melakukan pretest dan posttest. Kegiatan foto bersama dapat dilihat pada gambar 4 di bawah ini.



Gambar 4. Kegiatan Foto Bersama Setelah sosialisasi berlangsung

5. KESIMPULAN

Berdasarkan hasil pelaksanaan kegiatan pengabdian kepada masyarakat yang telah dilaksanakan, dapat ditarik kesimpulan bahwa masyarakat peserta yang mengikuti kegiatan sosialisasi mendapatkan pemahaman yang lebih dalam tentang cyber crime, jenis-jenisnya, serta fungsinya dalam kehidupan sehari-hari dan juga kegiatan pengabdian kepada masyarakat ini berhasil memberikan informasi dan pemahaman tentang bahaya cyber crime bahkan hingga sosial media dalam kemajuan era teknologi saat ini. Akhirnya peserta juga memahami jenis dan cara mengatasi kejahatan cyber crime serta perlindungan dan dampak hukum dari kejahatan ini.

DAFTAR PUSTAKA

Asnawi, Asnawi et al. 2023. "Sosialisasi Literasi Kejahatan Dunia Maya (Cyber Crime) Pada Generasi Milenial Di Desa Kelapian." *Indonesian Collaboration Journal of Community Services (ICJCS)* 3(3): 218–28.



Jurnal Pengabdian Kepada Masyarakat Mitra Kreasi Cendekia

Vol 2, No 2, Juli 2024, Hal. 164-169

ISSN 2985-7430 (Media Online)

<https://ejournal.mitrakreasicendekia.com/index.php/mkc>

- Change, Global et al. 2021. “No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title.” *Paper Knowledge . Toward a Media History of Documents* 3(2): 6.
- Hafid, Muhammad et al. 2023. “Tantangan Menghadapi Kejahatan Cyber Dalam Kehidupan Bermasyarakat Dan Bernegara Muhammad.” *Pendidikan Tambusai* 7(2): 9548–56.
- Informasi, Fakultas Teknologi, Universitas Nusa Mandiri, and Cengkeh Ii. “CYBERCRIME PADA PENGGUNAAN DAN Daffa Alfiansyah.” (5).
- Simões. 1995. “No 主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析Title.” *Analytical Biochemistry* 11(1): 78. <http://link.springer.com/10.1007/978-3-319-59379-1%0Ahttp://dx.doi.org/10.1016/B978-0-12-420070-8.00002-7%0Ahttp://dx.doi.org/10.1016/j.ab.2015.03.024%0Ahttps://doi.org/10.1080/07352689.2018.1441103%0Ahttp://www.chile.bmw-motorrad.cl/sync/showroom/lam/es/>.
- Syaddan, Syaddan. 2024. “Sosialisasi Keamanan Data Di Dunia Siber Untuk Meningkatkan Kewaspadaan SMK 1 Negeri Tarakan Terhadap Ancaman Cybercrime.” *Archive: Jurnal Pengabdian Kepada Masyarakat* 3(2): 289–99.