Bonding Relations Journal
Volume 2; Nomor 2; Tahun 2025; Halaman 34-38
https://bemj.e-journal.id/BRJ/index

Peningkatan Kesadaran Keamanan Siber Di Era Digital: Mengedukasi Bahaya Scam Dan Ransomware

Fernanda
Universitas Mulia
Email: fernanda@students.universitasmulia.ac.id

Riyayatsyah
Universitas Mulia
Email: riyayatsyah@universitasmulia.ac.id

Haerullah
Universitas Mulia
Email: haerullah@universitasmulia.ac.id

Abstrak

Di era digital yang semakin maju, masyarakat dihadapkan pada berbagai ancaman siber yang dapat merugikan secara finansial, psikologis, maupun sosial. Tiga di antaranya yang paling sering terjadi adalah scam (penipuan online) dan ransomware (serangan peretas yang menyandera data) yang menyasar berbagai kalangan, termasuk pelajar dan masyarakat umum. Rendahnya literasi digital dan kesadaran akan keamanan siber menjadi faktor utama tingginya angka korban. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan pemahaman dan kewaspadaan masyarakat terhadap tiga bentuk ancaman digital tersebut melalui pendekatan edukatif dan tanya jawab. Metode yang digunakan meliputi sosialisasi interaktif, diskusi kelompok, dan simulasi kasus nyata yang dilakukan di lingkungan sekolah, komunitas pemuda, dan organisasi masyarakat. Hasil kegiatan menunjukkan peningkatan signifikan dalam pengetahuan peserta mengenai jenis-jenis scam, cara kerja ransomware, serta dampak negatif dari judi online. Peserta juga menunjukkan pemahaman yang lebih baik terkait langkah-langkah pencegahan, seperti penggunaan autentikasi ganda, pemeliharaan keamanan perangkat, dan pelaporan aktivitas mencurigakan. Melalui kegiatan ini, diharapkan tercipta komunitas yang lebih tanggap terhadap risiko siber dan mampu menjadi agen literasi digital di lingkungan masing-masing.

Kata Kunci: Literasi Digital, Scam, Ransomware, Bahaya Ancaman Siber

1. PENDAHULUAN

Perkembangan teknologi digital telah membawa berbagai kemudahan dalam kehidupan sehari-hari. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman keamanan siber, seperti scam (penipuan online), ransomware (perangkat lunak perusak dan pemeras) yang menjadi ancaman nyata bagi masyarakat umum dari berbagai usia. Terutama generasi muda dan kelompok rentan digital / orang tua yang ada di lingkungan Organisasi CB Triple S Samarinda, mereka masih memiliki kesadaran yang rendah terhadap bahaya dan cara pencegahan terhadap keamanan siber.

Untuk meningkatkan kesadaran masyarakat khususnya anggota Organisasi CB Triple S Samarinda, maka mereka perlu di bekali pemahaman dan kesadaran mengenai keamanan siber serta memberikan edukasi mengenai dampak dan pencegahan kejahatan digital.

Pengabdian masyarakat ini menawarkan solusi berupa kegiatan edukatif, preventif dan penanganan yang ditujukan untuk membekali masyarakat dengan pengetahuan dan keterampilan dasar dalam menghadapi ancaman scam dan ransomware. Solusi yang ditawarkan mencakup:

a. Sosialisasi dan Penyuluhan Interaktif
   Memberikan penjelasan sederhana dan mudah dipahami mengenai:
   1) Definisi scam dan ransomware.
   2) Cara kerja dan contoh kasus nyata.
   3) Ciri-ciri umum dari penipuan digital dan perangkat lunak berbahaya.
b. Pelatihan Deteksi Dini dan Pencegahan
   Melatih peserta untuk:
   1) Mengenali pesan, situs, dan aplikasi berbahaya.
   2) Menggunakan kata sandi yang kuat dan autentikasi dua faktor.
   3) Mendeteksi file atau email mencurigakan sebelum dibuka.
c. Prosedur Pelaporan
   Memberikan informasi tentang bagaimana dan ke mana harus melapor apabila kita mengalami serangan siber yang merugikan kita secara materi.
d. Pendampingan Pasca Kegiatan
   Memberikan arahan dan konsultasi lanjutan untuk pertanyaan seputar keamanan siber melalui komunikasi online seperti *Whatsapp*, maupun konsultasi langsung.

Dengan dilaksanakan kegiatan edukasi ini, diharapkan anggota organisasi memiliki kesadaran lebih tinggi terhadap ancaman keamanan siber, Anggota organisasi dapat melindungi diri sendiri dan keluarga dari risiko ancaman digital.(Parulian et al., 2021), dan turunnya angka korban scam & ransomware serta terciptanya budaya penggunaan teknologi yang aman, bijak, dan produktif di dalam organisasi.

2. METODE KEGIATAN PKM

Pengabdian masyarakat ini menggunakan pendekatan edukatif partisipatif, yaitu metode yang melibatkan peserta secara aktif dalam proses pembelajaran melalui ceramah, tanya jawab, demonstrasi, dan diskusi. Kegiatan ini menargetkan komunitas organisasi CB. Triple S dengan rentang usia 25 sampai 40 tahun keatas.

Bonding Relations Journal
Volume 2; Nomor 2; Tahun 2025; Halaman 34-38
https://bemj.e-journal.id/BRJ/index

3. HASIL DAN PEMBAHASAN

Pengabdian masyarakat pengabdian ini dilaksanakan pada tanggal 8 Agustus 2025, bertempat di markas Organisasi CB Triple S yang berlokasi di Jalan Abdul Wahab Syahrani, Komp. Ruko Syahrani Centre No. 30 RT.14, Gunung Kelua, Samarinda Ulu.

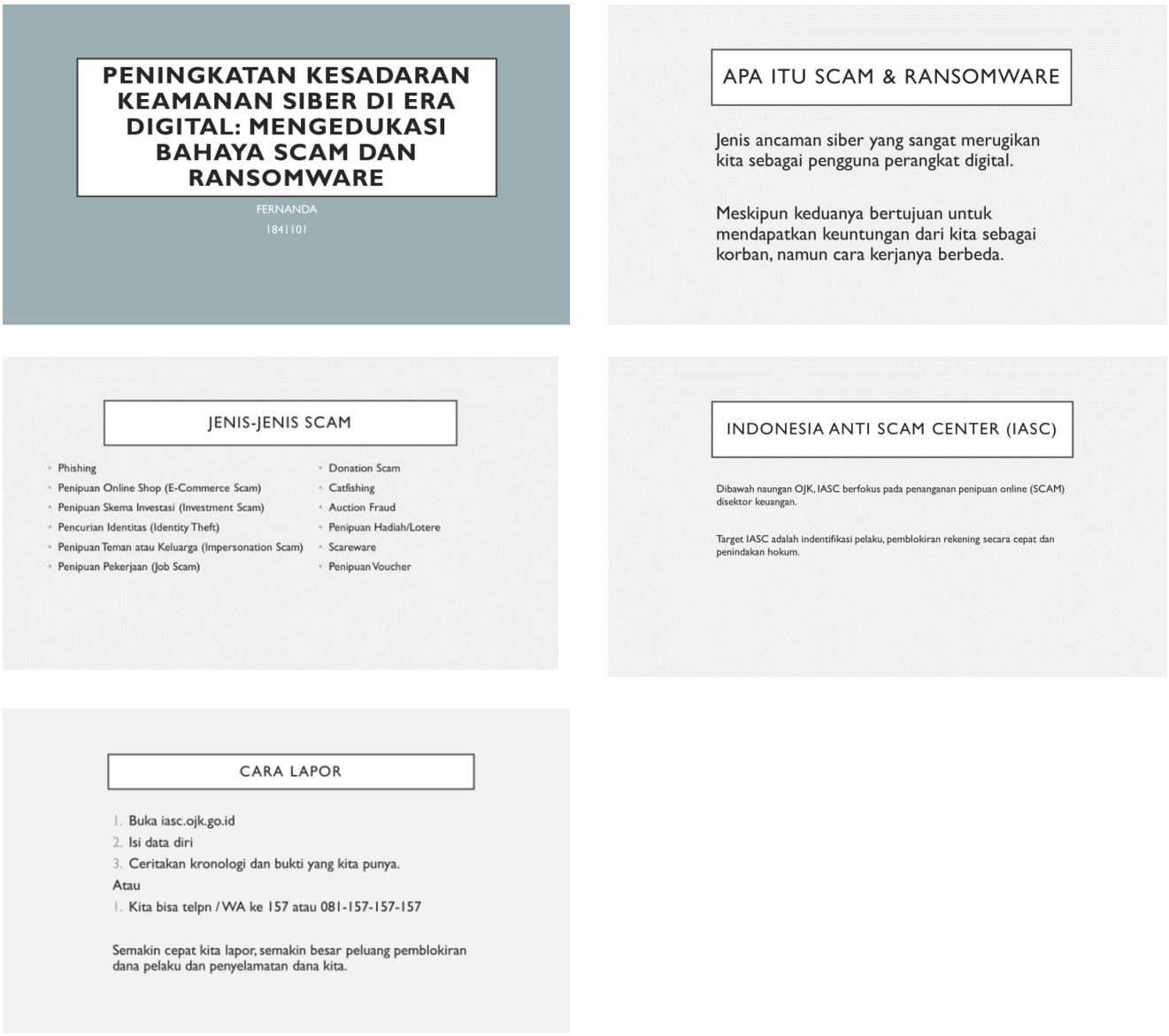
Guna mencegah potensi anggota organisasi menjadi korban kejahatan siber. Pengabdian masyarakat ini dilaksanakan karena belum pernah dilakukan dan belum ada yang edukasi rata-rata anggota organisasi terhadap bahaya kejahatan siber yang sedang mengintai.

Berikut ini dokumentasi pelaksanaan pengabdian kepada Masyarakat:

Gambar 1. Penyampaian materi

Bonding Relations Journal
Volume 2; Nomor 2; Tahun 2025; Halaman 34-38
https://bemj.e-journal.id/BRJ/index

Materi yang diberikan adalah terkait edukasi terhadap ancaman siber seperti Scam dan Ransomware. Berikut adalah pembahasan materi dari pengabdian kepada Masyarakat



Gambar 2. Bahan Materi

4. KESIMPULAN DAN SARAN

Kesimpulan

Dengan semakin meningkatnya perkembangan era digital seperti saat ini kesadaran dan edukasi untuk meningkatkan pemahaman tentang bahaya serangan siber adalah investasi yang penting untuk melindungi diri kita dan data yang kita miliki dari berbagai macam ancaman siber yang terus berevolusi. Sebab ancaman siber saat ini semakin kompleks, Era digital telah membawa banyak kemudahan, namun juga diiringi dengan peningkatan risiko keamanan siber. Ancaman seperti scam dan ransomware menjadi

semakin canggih dan merajalela, menargetkan individu maupun organisasi.

Kesadaran adalah kunci pertahanan pertama sebab pertahanan teknis saja tidak cukup. Kesadaran dan pemahaman kita tentang berbagai bentuk ancaman siber, modus operandi pelaku, dan konsekuensi dari serangan siber merupakan lapisan pertahanan yang paling fundamental dan efektif. Kemudian untuk memerangi ancaman ini, edukasi yang berkelanjutan dan komprehensif sangatlah penting. Edukasi harus mencakup tentang:

1) Mengenali Tanda-tanda Awal, Mengajarkan cara mengidentifikasi email phishing, tautan mencurigakan, pesan teks penipuan, atau tawaran yang terlalu bagus untuk menjadi kenyataan.
2) Praktik Keamanan Dasar, Mendorong penggunaan kata sandi yang kuat dan unik, autentikasi dua faktor (2FA), serta berhati-hati dalam berbagi informasi pribadi secara online.
3) Tindakan Pencegahan Ransomware, Edukasi tentang pentingnya backup data secara rutin, penggunaan antivirus yang mutakhir atau terupdate, dan tidak membuka lampiran email dari sumber yang tidak dikenal.
4) Prosedur Pelaporan, Memberikan informasi tentang bagaimana dan ke mana harus melaporkan insiden siber jika terjadi.

Saran

Berikut adalah beberapa saran yang diberikan bagi pemateri apabila akan membawakan presentasi tentang keamanan siber ini secara berkelanjutan:

1) Jika memungkinkan tunjukkan secara singkat dan langsung bagaimana sebuah *scam* dan *ransomware* terjadi atau bagaimana proses awal mula terjadinya serangan siber yang menyerang data pribadi atau file penting kita dan cara penanganan secara langsung agar membuat peserta dapat memahami lebih dalam terkait ciri-ciri awal mula serangan tersebut terjadi dan cara penanganan awalnya.
2) Pastikan penjelasan mengenai *scam*, *ransomware*, atau konsep teknis lainnya disampaikan dengan bahasa yang mudah dipahami oleh semua kalangan, tanpa latar belakang teknis. Jika harus menggunakan istilah teknis, jelaskan dengan analogi yang sederhana.
3) Memastikan pengawalan berkelanjutan untuk menghidarkan dan meminimalisir serangan siber menyerang anggota organisasi.

5. vDAFTAR PUSTAKA

AnNisyaNursabilah, N. (2025, July). *View of Perlindungan Hukum Bagi Korban Tindak Pidana Cyber Scam Serta Dampaknya Bagi Korban Sebagai Bentuk Viktimisasi Sekunder*. https://journal.lpkd.or.id/index.php/Humif/article/view/1912/2300

Kajian Stratejik Ketahanan Nasional Jurnal Kajian Stratejik Ketahanan Nasional, J., Badan Siber dan Sandi Negara Dalam Strategi Badan Siber dan Sandi Negara Dalam, S., Apri Sudarmadi, D., Josias Simon Runturambi, A., Apri, D., Josias Simon, A., Badan Siber dan Sandi Negara Dalam Menghadapi Ancaman Siber di Indonesia, S., & Kajian Stratejik, J. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Article 7 Ketahanan Nasional*, *2*(2). https://doi.org/10.7454/jkskn.v2i2.10028

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, *1*(2), 85–92. https://ejournal.upi.edu/index.php/TELNECT/article/view/40866