

Waspada Kejahatan Digital: Panduan Keamanan Jaringan

Dimas Rega Hadiatullah^{1*}, Sapto Hadi Riono²

Fakultas Teknologi dan Sains, Program Studi Ilmu Komputer, Universitas PGRI Wiranegara, Kota Pasuruan, Indonesia

Email: ^{1*}reggadims@gmail.com, ²saptoenator@gmail.com

Email Corresponding Author: reggadims@gmail.com

Abstrak-Kejahatan di ruang digital semakin menjadi ancaman yang meresahkan bagi masyarakat modern. Artikel ini menjelaskan upaya pengabdian masyarakat dalam meningkatkan kesadaran akan pentingnya keamanan jaringan dan perlindungan terhadap serangan cyber. Melalui penyelenggaraan seminar dengan tema "Waspada Kejahatan di Ruang Digital", berbagai strategi dan teknik untuk mengamankan jaringan serta melindungi data dari serangan cyber telah disampaikan kepada peserta. Penekanan diberikan pada pentingnya adopsi praktik keamanan digital yang tepat dan pembaruan pengetahuan secara berkala untuk menghadapi ancaman yang terus berkembang. Artikel ini juga memberikan rekomendasi untuk peningkatan kesadaran masyarakat, pelatihan dan edukasi, kolaborasi industri, investasi dalam teknologi keamanan, audit keamanan reguler, serta kerjasama internasional dalam upaya melawan kejahatan digital. Diharapkan artikel ini dapat memberikan kontribusi positif dalam memperkuat pertahanan terhadap serangan cyber dan membangun lingkungan digital yang lebih aman bagi semua pihak.

Kata Kunci: Keamanan Jaringan, Ancaman, Digital, Hacking, Phising

Abstract-Cybercrimes pose an increasingly alarming threat to modern society. This article elucidates community engagement efforts aimed at enhancing awareness of the importance of network security and safeguarding against cyber attacks. Through the organization of a seminar titled "Vigilance Against Crimes in the Digital Space," various strategies and techniques to secure networks and protect data from cyber attacks were conveyed to participants. Emphasis was placed on the necessity of adopting appropriate digital security practices and regularly updating knowledge to confront evolving threats. The article also provides recommendations for increasing public awareness, training and education, industry collaboration, investment in security technology, regular security audits, and international cooperation in combating digital crimes. It is hoped that this article will contribute positively to strengthening defenses against cyber attacks and building a safer digital environment for all stakeholders.

Keywords: Cyber Security, Threats, Digital, Hacking, Phising

1. PENDAHULUAN

Semakin gencarnya penggunaan ponsel pintar di semua kalangan dan tidak memandang batas usia tak terkecuali para pelajar yang apalagi ditahun 2020 kemarin merebak wabah covid-19 yang mengharuskan semua pelajar menggunakan gawai untuk melangsungkan proses pendidikan diantaranya pemakaian ponsel pintar atau smartphone membuat interaksi para pelajar dengan gawainya menjadi lebih sering, hal ini mengakibatkan para pelajar tidak hanya mengakses materi pelajaran juga tetapi semakin intensif juga untuk menggunakan media sosial, permainan, aplikasi penyedia vidio yang sering kita sebut dengan ruang digital.

Penggunaan ruang digital yang sangat intensif ini banyak mengakibatkan efek buruk pada pemakainya mulai dari efek buruk kesehatan, lupa waktu dan bahkan kriminalitas Cyber yang sering berujung pada penipuan online yang meliputi Hacking, spamming, dan phising. Bagi pelajar yang mungkin asing atau baru pertama intensif menggunakan ruang digital akan sangat rentan terhadap bahaya ini karena mereka mungkin masih belum mengerti atau bahkan acuh dengan bahaya yang sedang mengancam mereka diruang digital.

Keamanan jaringan hadir untuk memberikan pengetahuan kepada para pelajar tersebut akan bahaya yang ada dalam ruang digital untuk mencegah agar terhindar, mengetahui apa itu hacking, potensi bahaya dari spamming, dan apa saja yang membuat kita terkena phising baik secara sadar maupun tidak sadar dan cara untuk mencegah dan mnanggulangnya.

2. KERANGKA TEORI

Guna untuk mencegah bahaya yang ada didalam ruang digital, sosialisasi pengetahuan tentang bahaya dalam ruang digital perlu diberikan kepada pelajar yang dilakukan dalam acara seminar dengan seluruh warga SMKN 1 Wonorejo Kab. Pasuruan. Sebagai gambaran, SMKN 1 Wonorejo adalah sekolah yang ada di kecamatan Wonorejo Kabupaten Pasuruan yang akses dari pusat kota cukup jauh menempuh waktu kurang lebih satu jam perjalanan dengan kendaraan bermotor, hal ini cukup menjadi gambaran bahwa jarak yang jauh dari pusat kota menjadi faktor belum pahamnya pelajar disekolah tersebut tentang bahaya yang ada dalam ruang digital.

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalahgunaan informasi Internet of Things, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer(Munawar et al., 2020).

Edukasi Siber adalah sebuah pengenalan akan cybercrime dan bahayanya. Edukasi siber lebih lagi ditujukan untuk memberikan manfaat informasi tentang cybercrime keseluruhan baik, bahayanya, jenis-jenisnya, dan modusnya(Agung et al., 2023).

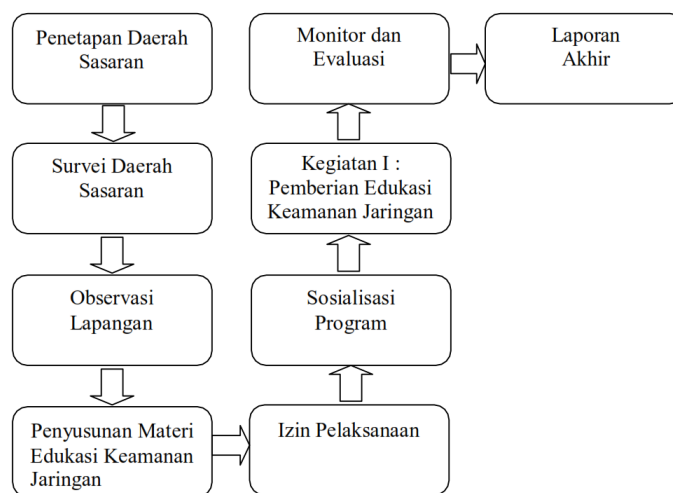
Sistem informasi adalah sebagai suatu integrasi antar komponen untuk mengumpulkan, menyimpan dan pemrosesan data. Data tersebut kemudian digunakan untuk menyediakan informasi, berkontribusi pada pengetahuan serta produk digital yang memfasilitasi pengambilan keputusan (Hadiatullah, 2023)

Phising adalah merupakan sebuah metode untuk melakukan penipuan dengan cara mencuri atau mengambil data pribadi korban melalui situs atau website palsu. Kata *Phising* sendiri berasal dari istilah dalam bahasa Inggris *Fishing* yang punya arti “memancing”, istilah “memancing” digunakan untuk menarik korban agar memasukkan informasi pribadi miliknya dengan maksud tertentu, *Phising* sendiri sering disebarkan pelaku melalui *e-mail* korban, *e-mail* digunakan untuk menyebarkan situs palsu bertujuan untuk menarik korban yang dituju oleh pelaku (Putra Y, 2021).

Spamming adalah tindakan mengirim surat elektronik secara acak kepada banyak pengguna baik itu bermuatan konten negatif yang bertujuan untuk memancing atau hanya sekedar beriklan, akibat dari tindakan ini adalah pemenuhan kotak masuk perpesanan atau bisa memperlambat performa dari perangkat komputer penerima pesan (Putra, 2016).

Hacking atau peretasan merupakan sebuah aktivitas menyusup atau menerobos masuk ke dalam aplikasi atau sistem pada perangkat keras seperti komputer dan smartphone. Aktivitas penyusupan ini belum tentu merupakan tindakan jahat karena tergantung dari untuk apa tujuannya (Habibi & Liviani, 2020)

3. METODE PELAKSANAAN



Gambar 1. Kerangka Kegiatan Pelaksanaan

Dari tahap diatas dideskripsikan : (1) Penetapan daerah sasaran: Pada penetapan daerah sasaran sesuai dengan data hasil observasi dan wawancara dengan Kepala SMKN 1 Wonorejo Kab. Pasuruan (2) Survei daerah sasaran: Dari data yang didapat, tim meninjau lokasi pengabdian (3) Observasi Lapangan ; Observasi dilakukan dengan pengambilan langsung dilokasi (4) Penyusunan materi : Menyusun materi tentang ancaman dan kejahatan diruang digital sekaligus cara mencegahnya (5) Izin pelaksanaan : Melakukan perizinan dari SMKN 1 Wonorejo Kab. Pasuruan. (6) Sosialisasi Program: Sosialisasi tentang kegiatan yang akan diadakan (7) Pelaksanaan kegiatan: Melaksanakan kegiatan berbasis seminar keamanan jaringan yang berjudul Waspada Kejahatan Diruang Digital (8) Monitor dan Evaluasi: Dilakukan saat kegiatan berlangsung dan pasca kegiatan (9) Laporan akhir : Penyusunan laporan akhir. hasil serta pembahasan dari topik pengabdian, yang bisa di buat terlebih dahulu. Bagian ini juga merepresentasikan penjelasan yang berupa penjelasan, gambar, tabel dan lainnya.

3.1. Penetapan Daerah Sasaran

Dalam menetapkan sasaran, dilakukan proses observasi dan wawancara kepada kepala SMKN 1 Wonorejo Kab. Pasuruan. Dalam observasi dan wawancara didapatkan bahwa minimnya kesadaran akan ancaman diruang digital

3.2. Penyusunan Materi

Materi disusun berdasarkan referensi artikel dan jurnal juga tentang pengetahuan umum bagaimana ancaman diruang digital, macam-macam kejahatan diruang digital, dan cara mencegah dan menanggulangi kejahatan diruang digital

3.3. Pelaksanaan kegiatan

Kegiatan sosialisasi ini dikemas dalam kegiatan seminar yang pesertanya dihadiri oleh warga SMKN 1 Wonorejo, baik dari siswa dewan guru ataupun tenaga pendidikan dari SMKN 1 Wonorejo. Pada awal pelaksanaan kegiatan kuisioner dibagikan kepada peserta yang sifatnya sebagai *pre-test* untuk mengetahui berapa tingkat kesadaran yang dimiliki oleh

peserta terhadap ancaman diruang digital, kemudian diberikanlah materi oleh pemateri tentang keamanan jaringan, waspada kejahatan diruang digital, setelah materi diberikan diadakan sesi tanya jawab antara pemateri dan peserta, setelah rangkaian pemberian materi diberikan dilakukan pembagian kuisioner kembali sebagai *post-test* untuk mengetahui sejauh mana peningkatan kesadaran akan ancaman diruang digital

3.4. Monitor Dan Evaluasi

Monitor dilaksanakan dengan kuisioner yang dibagikan kepada peserta pada saat kegiatan berlangsung. Evaluasi dilakukan setelah kegiatan selesai dilaksanakan dengan kuisioner yang juga dibagikan kepada peserta.

4. HASIL DAN PEMBAHASAN

Pada pelaksanaan kegiatan, pertama adalah pembagian kuisioner atau biasa disebut pre-test, dilakukan dengan tujuan agar peserta pengabdian bisa diukur pengetahuan atau seberapa banyak peserta mengetahui tentang ancaman diruang digital, setelah itu dilaksanakan kegiatan yang dikemas dalam seminar tentang ancaman diruang digital. Diakhir kegiatan kembali dibagikan kuisioner atau yang biasa disebut post-test untuk mengukur sejauh mana pengetahuan yang didapat oleh peserta setelah mengikuti kegiatan ini, selain itu juga terdapat wawancara dengan salah satu peserta kegiatan tentang pendapatnya setelah mengikuti kegiatan ini

Dari hasil pelaksanaan kegiatan pengabdian ini didapatkan peningkatan pengetahuan dan kewaspadaan yang diperoleh peserta, dari hasil pre-test menunjukkan 47% peserta masih belum memahami dan memiliki tingkat kewaspadaan rendah terhadap kejahatan dunia digital, setelah mengikuti kegiatan ini, dari hasil post-test menunjukkan 97% Peserta sudah memahami dan memiliki tingkat kewaspadaan yang tinggi terhadap kejahatan dunia digital.

Berisi hasil dari pengabdian yang dilakukan dijelaskan sesuai dengan alur tawaran solusi dilaksanakan; (1) Deskripsi dari apa yang telah dilakukan, (2) diikuti ada foto dokumentasi (bukan foto bersama), (3) penjelasan lanjutan. (4) Setiap Gambar atau Tabel dirujuk pada paragraf sebelum atau sesudahnya. (Gambar 1, Tabel 1, ...), (5) Monitoring dan Evaluasi; Monitoring: apa yang dilakukan saat kegiatan dilakukan (bisa bentuk wawancara, lebih tepat observasi), Bisa langsung ke evaluasi jika kegiatan dilakukan dalam sekali waktu. Hasil tes atau angket mohon jelaskan disini, khususnya persentase peningkatan yang terjadi sebelum atau sesudah kegiatan, (6) Kendala yang Dihadapi atau Masalah Lain yang Terekam Disertai saran solusi.

Hasil dan Pembahasan harus ada di bagian ini, dengan Font Size 10 dan jenis huruf Cambria. Ilustrasi hasil penelitian dapat berupa grafik/tabel/gambar yang diberi keterangan secukupnya agar mudah dimengerti. Dalam naskah, nomor kutipan secara berurutan dalam tanda kurung siku, juga tabel angka dan angka secara berurutan seperti yang ditunjukkan pada Tabel 1 dan Gambar 2.

Tabel 1. Presentase kesadaran peserta tentang kejahatan dunia digital

Presentase	Sebelum Kegiatan	Sesudah Kegiatan
Tidak Menyadari	63%	7%
Menyadari	37%	93%
Total	100%	100%



Gambar 2. Foto pelaksanaan kegiatan seminar keamanan dalam jaringan Waspada Ancaman Ruang Digital

5. SIMPULAN DAN SARAN

Menyoroti pentingnya kesadaran akan risiko kejahatan cyber yang semakin meresahkan. Dalam kegiatan ini, telah dibahas beragam strategi dan teknik untuk mengamankan jaringan serta melindungi data dari serangan cyber. Para peserta diingatkan akan pentingnya mengadopsi praktik keamanan digital yang tepat dan terus memperbarui pengetahuan mereka untuk menghadapi ancaman yang terus berkembang di ruang digital. Perlu adanya kampanye yang lebih luas untuk meningkatkan kesadaran masyarakat akan risiko kejahatan digital. Hal ini dapat dilakukan melalui seminar, workshop, dan kampanye publik lainnya.

DAFTAR PUSTAKA

- Agung, A., Hafrida, H., & Erwin, E. (2023). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS: Journal of Criminal Law*, 3(2), 212–222. <https://doi.org/10.22437/pampas.v3i2.23367>
- Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam*, 23(2), 400–426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>
- Hadiatullah, D. R. (2023). Employee Presence Design Based on Near Field Communication (Nfc). *Jurnal Komputer Dan Informatika*, 11(1), 7–13. <https://doi.org/10.35508/jicon.v11i1.9852>
- Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, 02(01), 14–20.
- Putra, E. N. (2016). Pengiriman E-Mail Spam Sebagai Kejahatan Cyber Di Indonesia. *Jurnal Cakrawala Hukum*, 7(2), 169–182. <https://doi.org/10.26905/idjch.v7i2.1906>
- Putra Y, V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurist-Diction*, 4(6), 2525. <https://doi.org/10.20473/jd.v4i6.31857>