

**SEMINAR DIGITAL AMAN, AMAN BERGERAK SMK ISLAMIC VILLAGE
KABUPATEN TANGERANG**

Fauyhi Eko Nugroho¹⁾, Dyas Yudi Priyanggodo²⁾, Yanuardi³⁾, Alim Hardiansyah⁴⁾
Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Tangerang

Abstrak

Pentingnya kegiatan pengenalan keamanan digital bagi siswa SMK Islamic Village. Pada saat ini teknologi yang terus berkembang saat ini banyak peluang dan ancaman yang mengintai. Mengerti dan menggunakan praktik keamanan digital yang efektif diberikan kesempatan kepada siswa-siswa untuk mempelajari tentang keamanan digital dengan melibatkan mereka dalam seminar digital aman, aman bergerak. Siswa memahami cara menjaga keamanan informasi pribadi, keluarga, lingkungan sekolah, dan informasi penting lainnya. saat disebarkan melalui platform internet. Siswa pun mengetahui cara memverifikasi keakuratan informasi. Yang beredar di dunia maya. melindungi diri mereka ketika menggunakan media internet. Mengalihkan penggunaan media internet kepada konten yang optimis dan bernilai. Di samping itu, siswa juga dapat menjaga diri mereka dari serangan online. Memastikan keamanan dan mengurangi risiko serta meningkatkan kesadaran akan keamanan. Perlunya melanjutkan pengenalan tentang keamanan digital, pada pembelajaran yang lebih mendalam mengenai etika digital, siswa akan mendapatkan pengetahuan tentang konten yang bisa dibagikan maupun yang tidak boleh dibagikan. Pada media internet, ada berbagai hal yang tidak dapat disampaikan atau dibagikan. dapat mencapai potensi maksimalnya. Baik sekolah maupun pihak-pihak terkait dapat meningkatkan keamanan dan mengurangi risiko serangan digital.

Sejarah Artikel

Submitted: 162 Agustus 2024

Accepted: 22 Agustus 2024

Published: 23 Agustus 2024

Kata Kunci

seminar, digital, teknologi, aman

PENDAHULUAN

kemajuan teknologi, berbagai permasalahan dalam kehidupan sehari-hari idealnya menjadi semakin mudah. Namun perkembangan teknologi digital juga membawa risiko yang dapat berdampak pada kehidupan penggunanya. Ini seperti pisau yang membantu Anda memotong atau menyakiti orang lain. Situasi serupa berlaku bagi kita yang memilih untuk menggunakan teknologi digital, seperti koneksi ke Internet, yang membuat berbagai layanan tersedia di jaringan virtual. Untuk meminimalkan risiko, penting untuk memahami prinsip dasar keamanan digital.

Dari permasalahan diatas kami bermaksud menyelenggarakan seminar pengabdian kepada masyarakat (PKM) yang berjudul “Digital Aman, Aman Bergerak” adalah : sebagai salah satu kewajiban dari tri darma Perguruan Tinggi.

Pelaksanaan pengabdian masyarakat ini juga bertujuan untuk mengedukasi siswa-siswi SMK Islamic Village Kabupaten Tangerang melalui seminar Digital Aman, Aman Bergerak yaitu memberikan pemahaman tentang ; Keamanan Digital Personal, Keamanan Komunikasi Digital, Digital aman saat menyampaikan pendapat di media sosial, dan jaga jejak digital dan lawan hoaks.

METODE PELAKSANAAN**Waktu dan Tempat**

Kegiatan ini akan dilaksanakan tanggal 5 Juni 2024 pada Ruang COE SMK Islamic Village, Kabupaten Tangerang. Peserta pelatihan adalah siswa-siswi SMK Islamic Village. Adapun pada kegiatan ini diikuti oleh 4 orang Dosen Universitas Muhammadiyah Tangerang serta 25 orang siswa-siswi SMK Islamic Village.

Prosedur Pelaksanaan

Peserta seminar mendapatkan pengetahuan tentang prinsip-prinsip keamanan digital untuk melindungi data personal dan jejak digital. Para peserta seminar yang didampingi oleh tim dosen dari Dosen Universitas Muhammadiyah Tangerang ini berkesempatan untuk berdiskusi langsung mengenai langkah-langkah hal penting yang harus diperhatikan dalam keamanan digital ini meliputi perlindungan pribadi yang meliputi asset digital dan identitas pribadi. perlindungan asset digital sangat erat kaitannya dengan akun-akun digital kita yang meliputi akun media sosial, akun belanja, akun toko digital dan akun-akun penting lainnya.

HASIL DAN PEMBAHASAN**Kemanan Digital Personal**

Siswa di SMK Islamic Village Tangerang akan mendapatkan manfaat dari seminar ini dengan materi presentasi yang baik. Selama seminar ini, siswa diajarkan tentang Prinsip kemanan digital, agar dalam penggunaan teknologi digital siswa dapat meminimalisir resiko kejahatan digital.

Tak lupa dari team pemateri menjelaskan ancaman ancaman yang sering terjadi seperti : Baiting, Pretexting, Phishing, Spear dan phishing. Untuk itulah pengguna device harus sadar akan bahaya yang mengancam data mereka. berikut tips pencegahannya :

- jangan mengklik tautan yang mencurigakan.
- periksa kembali sumber situs yang ingin dibuka.
- hindari percakapan dengan orang asing.
- Hindari download dokumen dari sumber yang tidak dikenal
- anggap saja seluruh tawaran hadiah itu palsu
- tolak request email atau pesan dari orang yang tidak dikenal
- selalu ingat akan risiko kehilangan informasi penting

Dan di ajarkan pula cara pengamanan pada :

- Cek Keamanan e-Mail
- Perkuat Pilihan Password
- Gunakan Password Manager
- Pasang Gembok 2FA
- Privasi / Sekuriti WhatsApp
- Pasang Anti Virus
- Pasang VPN

Keamanan Komunikasi Digital

Bicara tentang keamanan dunia digital tak lepas dari kemanan digital. keamanan digital menjadi sangat penting dengan semakin bertambahnya pengguna internet di Indonesia. Hal penting yang harus diperhatikan dalam keamanan digital ini meliputi perlindungan pribadi yang meliputi asset digital dan identitas pribadi. perlindungan asset digital sangat erat kaitannya dengan akun-akun digital kita yang meliputi media sosial, akun belanja, akun toko digital dan akun-akun penting lainnya.

Data jumlah serangan siber januari-Agustus 2019/2020 dari pusat Operasi Keamanan Siber Nasional yang dirilis oleh Kompas Tekno 20 Oktober 2020 sebagai berikut :



Data Jumlah Serangan Siber Januari - Agustus 2019/2020

(Sumber : <https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi>)

Digital Aman Saat Unjuk Rasa

Teknologi digital dan perangkat elektronik merupakan beberapa komponen penting dalam melakukan aktivitas saat ini, tidak hanya dalam kehidupan sehari-hari saja, bahkan dalam aksi protes atau unjuk rasa yang pernah dilakukan, teknologi digital menjadi pemicu, membuat aksi semakin meluas dan aksi bisa mendapatkan perhatian di media-media mainstream. Sebagai contoh, aksi protes yang dilakukan di hongkong pada Juni 2019, teknologi bahkan menjadi salah satu penyebab mobilisasi dan memiliki representasi yang menyedihkan sebagai mekanisme penindasan, melalui kampanye pemerintah terhadap pengunjung rasa, aksi ini semakin meluas dan didengar oleh aktivis-aktivis lain didalam hongkong dan diluar hongkong berkat masifnya pemberitaan aksi di berrbagai sosial media.

Dalam Melakukan aksi protes, seorang atau kelompok aktivis sangat mungkin menjadi sasaran pelacakan digital oleh penegak hukum pada perangkat elektronik mereka. Berbagai sumber menunjukkan Peningkatan penggunaan alat pelacakan digital oleh lembaga penegak hukum; memo khusus dikeluarkan ketika polisi amerika serikat melakukan pengawasan aksi protes masyarakat amerika sebagai buntut tewasnya George Floyd oleh salah satu anggota kepolisian AS ketika melakukan penangkapan. Memo internal yang diperoleh BuzzFeed News menunjukkan DEA (Drugs Enforcement Agency) mulai memata-matai pemrotes pada saat aksi protes dilakukan.

Mereka yang terlibat dalam aksi atau protes damai dapat menjadi sasaran penggeledahan atau penangkapan, gerakan dan asosiasi mereka dipetakan, atau menjadi target pengawasan dan penindasan. Penting bahwa dalam demokrasi, warga negara menggunakan hak mereka untuk berkumpul secara damai, dan para demonstran harus menyadari beberapa tindakan pencegahan yang dapat mereka ambil untuk menjaga diri mereka sendiri dan data mereka tetap aman.

Saat ini, penting sekali memiliki praktik yang baik dalam hal keamanan digital, karena saat ini informasi adalah salah satu aset yang paling berharga. Data atau informasi yang ada pada anda, baik di ponsel maupun di perangkat elektronik lainnya harus di berikan perlindungan, banyak terjadi serangan-serangan digital pada aktivis pada saat mereka melakukan aksinya, Serangan digital adalah segala bentuk gangguan secara tidak sah terhadap

aset dan atau identitas digital target, baik secara kasar maupun halus, dengan cara menguasai, mencuri, menyadap, atau menyebarluaskan data-data pribadi target.

Hasil riset dari safenet menunjukkan serangan digital relatif naik pada saat ada momentum tertentu. Empat tahun terakhir, misalnya, puncak serangan itu terjadi ketika ada gerakan nasional menolak revisi UU KPK (2019), pengesahan UU Cipta Kerja (2020), pelaksanaan Tes Wawasan Kebangsaan (TWK) pada staf KPK (2021), dan wacana perpanjangan periode jabatan Presiden Joko Widodo (2022)

Secara sederhana, bentuk serangan digital bisa dibagi menjadi dua berdasarkan metode dan tujuannya, yaitu serangan kasar (hard attack) atau serangan secara teknis (technical attack) dan serangan halus (soft attack) atau serangan secara psikologis (psychological attack) Meskipun demikian, satu serangan juga kadang bisa memenuhi dua kriteria sekaligus, yaitu serangan secara kasar dan halus. Misalnya Zoom Bombing yang dilakukan dengan cara masuk ke dalam sebuah kegiatan pertemuan Zoom, di mana dia menggunakan identitas palsu untuk masuk dan kemudian mengganggu jalannya kegiatan.

Jaga Jejak Digital

Merawat jejak digital adalah proses mengontrol dan mengelola informasi yang diterbitkan di internet tentang diri kita. Hal ini penting karena informasi yang di terbitkan di internet dapat digunakan oleh berbagai pihak, seperti Perusahaan, kampanye politik, atau bahkan penipu. Dengan merawat jejak digital, kita dapat memastikan bahwa informasi yang diterbitkan di internet tentang diri kita akurat, professional, dan mencerminkan identitas kita yang sebenarnya.

Selain itu, melawan hoaks adalah hal penting untuk dilakukan dalam era digital saat ini. Hoaks adalah informasi yang tidak benar atau tidak sah yang disebar luaskan melalui internet, yang dapat menimbulkan kerugian bagi individu tau Masyarakat. Melawan hoaks dapat dilakukan dengan mengecek keabsahan informasi sebelum menyebarkanluaskannya, serta menyebarkan informasi yang akurat dan terpercaya.

Kedua hal ini sangat penting untuk dilakukan agar kita dapat menjaga reputasi kita di dunia maya dan menghindari kerugian yang mungkin timbul dari penyebaran informasi yang tidak bener. Selain itu, merawat jejak digital dan melawan hoaks juga dapat membantu membangun Masyarakat yang lebih baik dan lebih memiliki kemampuan berfikir kritis dengan pendekatan literasi digital.

KESIMPULAN DAN SARAN

Sangat penting bagi siswa sekolah menengah atas untuk mengikuti kegiatan seminar ini. Pada zaman teknologi yang terus berkembang. Kehadiran kemajuan yang signifikan pasti membawa peluang sekaligus potensi ancaman. memberikan perhatian yang cukup pada pengembangan kualitas pendidikan.

Memahami dan melaksanakan langkah-langkah keamanan cyber yang efektif. Dengan mengikuti ini di lingkungan sekolah, Murid memahami langkah-langkah yang perlu diambil untuk menjaga keamanan informasi pribadi mereka, keluarga, lingkungan sekolah, dan informasi penting lainnya. saat disebarkan di platform online. Siswa juga memiliki pengetahuan tentang cara memverifikasi keakuratan data. yang dapat ditemukan di internet. Siswa memiliki kesadaran tentang risiko yang ada di media internet dan cara yang tepat dalam menggunakannya.

Untuk mengubah teks tersebut menjadi parafrase, dapat diungkapkan sebagai berikut: "Media internet dapat diarahkan untuk menyajikan konten yang memberikan dampak positif dan bernilai." Di samping itu, murid dapat menjaga diri mereka dari serangan siber. Mengatur potensi ancaman dan meningkatkan pemahaman tentang keamanan. Perlu dilanjutkan

pengenalan mengenai keamanan siber. Agar siswa dapat memiliki pemahaman yang lebih mendalam mengenai etika digital serta mengetahui tindakan apa yang dapat mereka lakukan dalam berbagi informasi secara online.

Hal-hal yang tidak dapat disebarkan melalui media online, dapat mengembangkan potensi mereka secara maksimal dan mencapai kesuksesan. Seminar ini yang tepat membantu siswa memperoleh pengetahuan dan keterampilan yang diperlukan dalam dunia kerja dan kehidupan sehari-hari. Dalam pelatihan ini, siswa diberikan panduan dan dukungan yang diperlukan untuk meraih tujuan mereka. Dengan adanya seminar ini, setiap siswa memiliki kesempatan yang sama untuk meraih keberhasilan dan menjadi sumber daya yang berharga bagi Masyarakat, selain itu, pihak-pihak di lingkungan sekolah juga dapat meningkatkan tingkat keamanan dan mengurangi kemungkinan terjadinya serangan cyber.

REFERENSI

- Anggono, A., & Riskiyadi, M. (2021). *Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka*
- Cakrawala, Apa Itu Cyber security? Mengapa Cyber security Kini Makin Penting? <https://infokomputer.grid.id/read/122710604/apa-itu-cyber-security-mengapa-cyber-security-kini-makinpenting?page=all> (Diakses tanggal 2 November 2021)
- Banyumurti, Indroyatno, D. (2018). *Kebijakan Cyber Security Dalam Perspektif Multi Stakeholder*.
- Dasep Lukiman, Cyber security: Apa Itu Cyber security?, <https://wakool.id/blog/582-cyber-security-apa-itucyber-security> (Diakses tanggal 2 November 2021)
- Garo Pane, C. G. (2021). Edukasi Kepada Siswa Sma Negeri 1 Mimika Untuk Mengatasi Ancaman Media Online Pada Data Pribadi. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, 1(2), 412–418. <https://doi.org/10.24002/konstelasi.v1i2.4166>
- Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, 1(2), 68–81. <https://doi.org/10.22437/pampas.v1i2.9574>
- Rahmadi, G., & Pratama, A. R. (2020). Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia. *Automata*, 1(2), 7. Retrieved from <https://journal.uui.ac.id/AUTOMATA/article/view/15399>
- Salim, S. C. (2017). Analisis Cyber Security pada Instagram untuk mengukur customer trust. (227), 1–23.
- Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review. *Jurnal Manajemen Dan Organisasi (JMO)*, 12(3), 239–251.