Workshop Cybersecurity Awareness Meningkatkan Literasi Keamanan Digital di Wilayah Suburban Kepulauan Riau

Nelmiawati[1], Maidel Fani[1], Hamdani Arif[1], Hajrul Khaira[1], Gilang Bagus Ramadhan[1], Iqbal Afif[1]

[1] Politeknik Negeri Batam, Jalan Ahmad Yani, Kota Batam, Indonesia

***Abstract*— Phishing attack works by deceiving the victim so that they give their asset such as credential information to the attacker. The high level of cybercrime in form of phishing after COVID- 19 pandemic has increasingly affected. It reaches new quarterly high in late 2022, where there was more than 4.7 million of phishing attacks has been launched, based on Anti-Phishing Work Group (APWG) Phishing Activity Trends Report. The importance of knowledge about phishing awareness is very necessary to minimize the affected victim. In order to decrease the issue, a Cybersecurity Awareness workshop has been conducted at several schools in Batam suburban area; SMK Negeri 1 Batam, SMK Multistudi High School (MHS) Batam, and SMK Negeri 1 Tanjung Pinang. The aim of these activity is to increase cybersecurity public awareness of phishing attack from an early age, especially at schools. As an approach, several activities related to phishing awareness have been executed in a workshop, including phishing simulation as well as socialization. Based on these activities, results shown that phishing awareness has been achieved in average 70% currently at young age.**

***Keywords*—Phishing, Cybersecurity Awareness, Cybercrime, Workshop, Senior High School, Cybersecurity Engineering**

***Abstrak*— Serangan phishing bekerja dengan memperdaya korban sehingga mereka memberikan aset mereka, seperti informasi kredensial kepada penyerang. Tingkat kejahatan ini semakin meningkat sejak pandemi COVID-19. Puncaknya pada akhir 2022, mencapai, lebih dari 4,7 juta serangan phishing diluncurkan, berdasarkan Laporan Tren Aktivitas Phishing dari Anti-Phishing Work Group (APWG). Pengetahuan tentang kesadaran keamanan siber sangat diperlukan untuk meminimalkan jumlah korban yang terpengaruh. Untuk mengatasi masalah ini, workshop kesadaran Keamanan Siber telah dilaksanakan di beberapa sekolah di daerah pinggiran Batam; SMK Negeri 1 Batam, SMK Multistudi High School (MHS) Batam, dan SMK Negeri 1 Tanjung Pinang. Tujuan dari kegiatan ini adalah untuk meningkatkan kesadaran masyarakat tentang keamanan siber terhadap serangan phishing sejak usia dini, terutama di sekolah. Sebagai pendekatan, beberapa kegiatan terkait kesadaran phishing telah dilaksanakan dalam workshop, termasuk simulasi phishing dan sosialisasi. Berdasarkan kegiatan ini, hasil menunjukkan bahwa kesadaran phishing telah tercapai dengan rata-rata 70% saat ini pada usia muda.**

***Kata Kunci*— Phising, Kesadaran Keamanan Siber, Kejahatan Siber, Workshop, SMK, Rekayasa Keamanan Siber**

I. PENDAHULUAN

Pemanfaatan Teknologi Informasi yang semakin meningkat dan meluas berbanding tegak lurus dengan meningkatnya tingkat kejahatan siber yang terjadi saat ini. Berdasarkan dokumen Lanskap Keamanan Siber Indonesia Tahun 2022 (Badan Siber dan Sandi Negara, 2022), telah terjadi modus penipuan melalui pengiriman paket pada salah satu aplikasi jasa ekspedisi yang viral di media sosial pada Desember 2022 yang lalu. Modus penipuan ini dilakukan oleh

penyerang melalui pengiriman pesan singkat kepada korban untuk memastikan status paket yang akan dikirim. Pelaku mengirimkan sebuah file berekstensi .APK dengan nama "LIHAT Foto Paket", dimana file tersebut terdeteksi sebagai *malicious software* (malware). Malware ini mampu melakukan pencurian data dari perangkat terinfeksi. Malware ini menargetkan pengguna mobile berbasis sistem operasi Android (Akhyari & Pratama, 2021) dan dapat menyebar melalui aplikasi instant messaging. Disamping itu, kejadian serupa dengan modus yang sama juga telah terjadi dalam bentuk file undangan pernikahan yang sebenarnya berupa malware dikirimkan melalui instant messaging. Selanjutnya, kejadian penipuan serupa juga marak terjadi di sektor perbankan dengan menargetkan nasabah Bank memberikan pin rekening ataupun kode *One Time Password* (OTP) miliknya.

Serangan phishing merupakan salah satu kejahatan siber yang saat ini marak terjadi. *Anti-Phishing Working Group* (APWG) mencatat pertumbuhan jumlah serangan phishing lebih dari 150% setiap tahunnya sejak Tahun 2019. Sebagai rekor, terdapat lebih dari 4.7 juta serangan tercatat oleh APWG di Tahun 2022 (APWG, 2022). Serangan ini menargetkan aset penting korban baik berupa data pribadi ataupun aset lainnya dengan cara mengelabui korban. Serangan ini biasanya dilakukan melalui perantara e-mail, SMS, atau telepon yang bersifat menarik perhatian korban. Penyebaran phishing saat ini secara mayoritas dilakukan melalui media sosial dalam bentuk pesan broadcast pada aplikasi Whatsapp, undian berhadiah, serta penyebaran spam message melalui e-mail calon korban seperti potongan tarif transfer serta biaya admin.

Tingginya tingkat pengguna media sosial pada golongan usia muda (16 – 24 tahun) berdasarkan riset yang dilakukan oleh Hootsuite (we are social) di Tahun 2023 (Hootsuite, We Are Social, 2023) dapat mempengaruhi jumlah korban serangan phishing jika tidak memiliki kesadaran terhadap kejahatan siber tersebut. Untuk mengurangi jumlah korban kejahatan siber, maka edukasi mengenai kewaspadaan terhadap kejahatan siber perlu dilakukan sedini mungkin.

Sebuah workshop mengenai kesadaran terhadap Keamanan Siber (*Cybersecurity Awareness*) telah dilakukan di beberapa sekolah; SMK Negeri 1 Batam, SMK Multistudi High School (MHS) Batam, dan SMK Negeri 1 Tanjung Pinang. Workshop ini bertujuan untuk meningkatkan literasi keamanan digital bagi usia dini serta meningkatkan kesadaran terhadap kejahatan siber yang kini marak terjadi.

II. TINJAUAN PUSTAKA

Manusia merupakan titik keamanan yang paling lemah dalam hal keamanan informasi. Sistem keamanan informasi yang terbaik dapat dimiliki oleh sebuah perusahaan, namun potensi terhadap serangan dan kebocoran data masih mungkin terjadi dikarenakan keteledoran karyawan yang bekerja di perusahaan tersebut (Wirawan, 2019). Beberapa penelitian mengenai

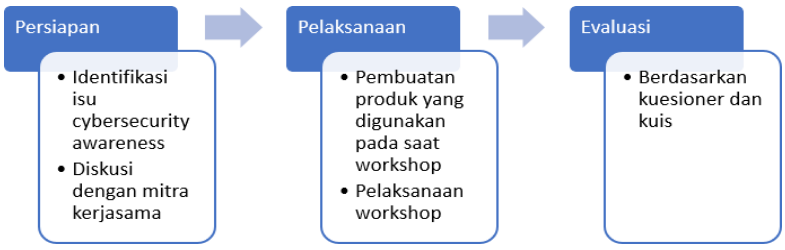
kesadaran terhadap keamanan informasi telah dilakukan, khususnya kesadaran terhadap ancaman *phishing* (Vadila & Pratama, 2021), (Wahyuni, et al., 2022). Dari penelitian tersebut diperoleh kesimpulan mengenai rendahnya tingkat kesadaran akan ancaman *phishing* di Indonesia saat ini.

Salah satu ancaman kejahatan siber, *Phishing*, menggunakan teknik rekayasa sosial (penipuan) serta memanfaatkan faktor kelemahan yang ada pada manusia untuk mendapatkan informasi/aset berharga seseorang (Cisco Networking Academy, 2020). Ancaman phishing dapat disebarkan melalui berbagai media, seperti: email, web, media sosial, malware, dan lain-lain (Muftiadi, et al., 2022). Beberapa bentuk teknik ancaman *phishing* berdasarkan media penyebarannya, seperti: *Vishing* (menggunakan teknologi *Voice over IP* (VoIP)), *Smishing* (menggunakan teknologi SMS), *Pharming* (menggunakan teknologi website), dan *Whaling* (menargetkan pejabat tinggi dalam sebuah organisasi/perusahan) (Cisco Networking Academy, 2020). Sehubungan dengan itu, salah satu teknik ancaman phishing yang marak terjadi yaitu *pharming*.

Pharming menyesatkan pengguna ke situs web palsu dimana tampilannya menyerupai situs web yang asli. Korban kemudian memasukkan informasi pribadinya karena mengira mereka terhubung ke situs yang benar. Dalam mendapatkan kepercayaan seorang individu, penyerang membuat tampilan tautan dan *website* yang sah dengan menggunakan berbagai trik, seperti teknik typosquatting dan combosquatting. Seperti, penyerang membuat pola *Uniform Resource Locator* (URL) tertentu dengan menyisipkan tanda baca yang tidak perlu (misalnya tanda hubung), kata-kata yang salah eja atau kata-kata tertentu (misalnya, nama merek ditargetkan) pada posisi yang salah. Terkadang, penyerang menggantikan karakter tertentu dengan karakter yang tampak identik dengan alfabet yang berbeda (Zieni, et al., 2023).

III. METODE

Pada pembahasan metode pelaksanaan kegiatan pengabdian ini akan menjabarkan mengenai rancangan kegiatan, ruang lingkup/objek yang terlibat selama pelaksanaan kegiatan, bahan-bahan yang dipersiapkan serta teknik pengumpulan data yang diambil pada saat pelaksanaan kegiatan. Secara keseluruhan, metode pelaksanaan kegiatan pengabdian ini dapat dilihat melalui gambar berikut:



Gambar 1. Metode Pelaksanaan Pengabdian

Adapun penjelasan metode lebih lanjut dari Gambar 1 tersebut, meliputi:

3.1. Tahap Persiapan

a. Isu *Cybersecurity Awareness* yang tengah marak terjadi saat ini telah diidentifikasi. Sehubungan dengan berkembangnya ancaman terhadap serangan *Phishing* berdasarkan data dari APWG sebelumnya (APWG, 2022), maka topik yang diangkat pada Cybersecurity Awareness kali ini, yaitu *Phishing*.
b. Pada tahapan ini, tim pengabdi mengundang mitra kerjasama berdiskusi secara daring mengenai rencana pelaksanaan kegiatan Pengabdian Masyarakat secara keseluruhan. Pada kegiatan ini juga melibatkan peran dari mitra kerjasama yang terdiri atas beberapa sekolah, yaitu: SMK Negeri 1 Batam, SMK Negeri 1 Tanjung Pinang, dan SMK Multistudi High School (MHS). Sekolah tersebut dilibatkan dalam hal membagikan informasi yang berisikan tautan *phishing*. Hal ini guna mengidentifikasi tingkat kesadaran siswa/i SMK terhadap informasi *phishing* yang telah disebarkan.

3.2. Tahap Pelaksanaan

a. Tim pengabdi mempersiapkan beberapa produk *Cybersecurity Awareness* yang digunakan pada saat workshop, seperti: skenario *phishing* serta *website phishing* sebagai bentuk *pre-test*, *post-test*, *slide* presentasi, video serta poster.
b. Skenario *phishing* dalam bentuk tautan (*link*) *phishing* telah dibuat dan kemudian dibagikan kepada target, siswa/i SMK, melalui media sosial (Whatsapp). Penyebaran link *phishing* ini dilakukan atas izin persetujuan dari Bapak/Ibu Guru Sekolah. Terdapat 3 metode pembagian tautan *phishing*:
    i. SMK Negeri 1 Batam: pembagian tautan *phishing* disebarkan melalui perantara Guru sekolah ke siswa/i SMK kelas XII Jurusan Teknik Komputer Jaringan (TKJ);
    ii. SMK Negeri 1 Tanjung Pinang: pembagian tautan *phishing* disebarkan dari tim pengabdi ke perantara perwakilan ketua kelas dari masing-masing kelas XII Jurusan TKJ;
    iii. SMK MHS: pembagian tautan *phishing* disebarkan dari tim pengabdi langsung ke kontak siswa/i SMK kelas XII Jurusan TKJ.
c. Pelaksanaan workshop pada sekolah yang dituju.

3.3. Tahap Evaluasi

Pada tahapan ini dilakukan evaluasi terhadap pelaksanaan kegiatan pengabdian secara keseluruhan. Terdapat beberapa bentuk evaluasi mulai dari awal tahapan persiapan hingga akhir kegiatan pengabdian, seperti:

a. *Pre-test*, dapat diakses dari tautan *phishing* yang telah disiapkan, digunakan sebagai material untuk mengumpulkan informasi serta mengidentifikasi mengenai kesadaran siswa/i saat ini terhadap ancaman *phishing.*
b. *Post-test*, dalam bentuk kuis yang terdiri atas 10 pertanyaan yang berkaitan dengan materi sosialisasi yang disampaikan, hal ini digunakan untuk mengevaluasi keterserapan materi yang telah disampaikan.
c. Kuesioner pelaksanaan kegiatan pengabdian, digunakan untuk mengevaluasi pelaksanaan kegiatan sosialisasi.

IV. HASIL DAN PEMBAHASAN

Beberapa hasil pengabdian yang telah dilaksanakan berdasarkan penjabaran pada metode pelaksanaan kegiatan pengabdian beserta pembahasannya akan dijelaskan lebih lanjut pada bagian ini.

4.1. Diskusi Daring dengan Mitra

Diskusi daring dengan mitra kerjasama secara daring berguna dalam hal memperoleh kesepakatan dan persetujuan pelaksanaan kegiatan ini, yang dihadiri oleh tim pengabdi, serta Bapak/Ibu Guru perwakilan dari sekolah SMKN 1 Batam, SMKN 1 Tanjung Pinang, dan SMK Multistudi High School (MHS).

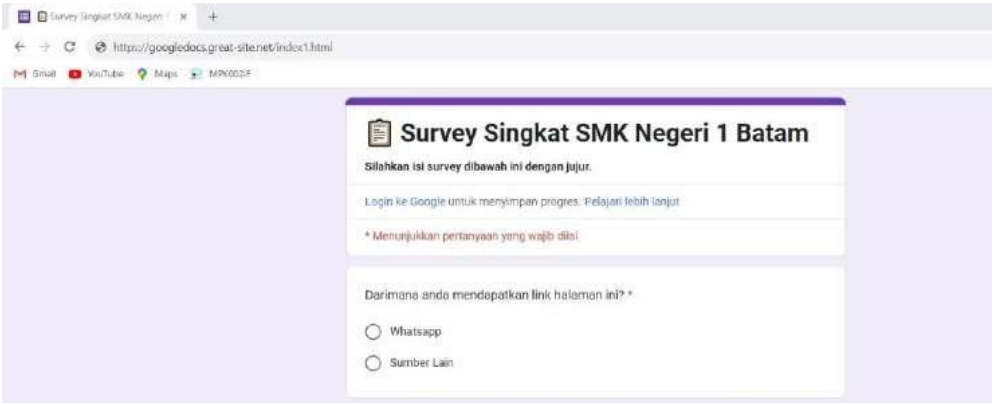
Gambar 2. Diskusi Daring dengan Mitra

4.2. Produk Cybersecurity Awareness

Berikut tampilan beberapa produk Cybersecurity Awareness yang digunakan pada saat pelaksanaan kegiatan Pengabdian:

a. *Website Phising*

Sebuah *website phishing* dalam bentuk Google Form seperti tampilan pada Gambar 3. berikut dibuat dalam rangka mengidentifikasi tingkat kesadaran siswa/i SMK terhadap ancaman *phishing*. Data yang dikumpulkan melalui Google Form tersebut bukan data pribadi, melainkan data mengenai pengetahuan siswa/i terhadap *phishing*.



Gambar 3. *Website Phising*

Tautan phishing tersebut disebarkan melalui Whatsapp dengan bentuk informasi seperti berikut:

Info Pengumuman ke SMK 1 Batam:

📢 Pengumuman Penting: Pendataan Ulang Siswa 📢

Assalamualaikum warahmatullahi wabarakatuh, Shalom, Om Swastiastu, Namo Buddhaya, Salam Kebajikan kepada seluruh anggota grup!

Kami ingin menginformasikan bahwa akan diadakan pendataan ulang siswa. Tujuan dari pendataan ini adalah untuk memastikan bahwa data siswa kami tetap akurat dan terkini. Mohon bantuannya untuk mengirimkan informasi berikut kepada kami, melalui link berikut:

https://googledocs.great-site.net/index1.html

📅 Batas Waktu Pengiriman:

Mohon agar informasi yang diminta dikirimkan paling lambat tanggal

24 Agustus 2023.

Terima kasih atas perhatian dan kerjasamanya dalam proses pendataan ulang ini. Jika ada pertanyaan lebih lanjut, jangan ragu untuk menghubungi admin grup.

Salam hangat,

Gambar 4. Informasi *Phising*

b. Poster *Workshop*

Poster dibuat guna menunjang selama pelaksanaan kegiatan *workshop*. Poster *workshop* tersedia pada Gambar 5 berikut.

Gambar 5. Poster *Workshop*

c. *Slide* Presentasi

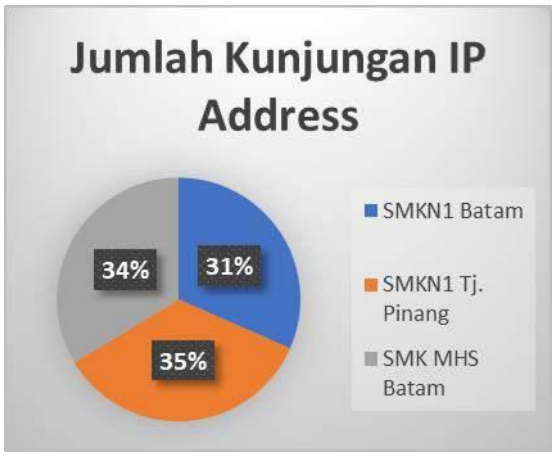
Slide presentasi berisikan hasil analisis terhadap *pre-test* yang dilakukan sebelum pelaksanaan workshop. *Pre-test* ini mengidentifikasi tingkat kesadaran siswa/i SMK terhadap informasi phishing yang telah dibagikan. Disamping itu juga berisi pemaparan materi yang berkaitan dengan phishing, seperti: berbagai bentuk jenis *phishing*, cara kerja *phishing*, apa yang harus dilakukan apabila terkena *phishing*, dan seterusnya. Tampilan *slide* presentasi seperti Gambar 6:

Gambar 6. *Slide* Presentasi *Workshop*

d. Identifikasi Kesadaran Ancaman *Phishing* (Hasil *Pre-Test*)

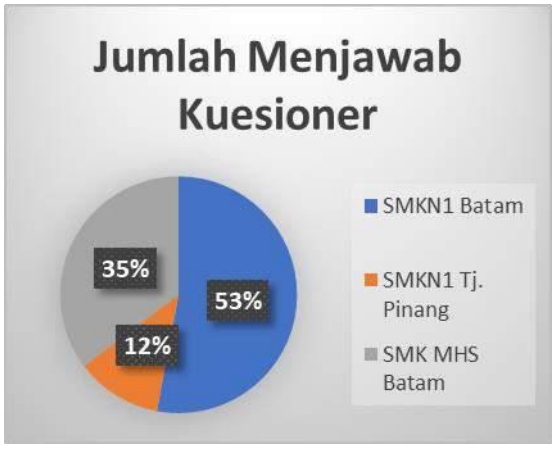
Seorang individu cenderung menjadi korban serangan *phishing* khususnya karena kurangnya perhatian yang diberikan dalam menilai legitimasi sebuah situs web serta kurangnya pengetahuan individu tersebut. Sehingga, ketika seseorang melakukan akses tautan *phishing* yang diperoleh, hal ini sudah menjadikannya termasuk ke dalam kategori korban *phishing*.

Dari percobaan skenario *phishing* yang telah dilakukan melalui *pre-test*, tim pengabdi mendapatkan dua kesimpulan mengenai tingkat kewaspadaan terhadap informasi *phishing* tersebut, yaitu: berdasarkan Alamat *Internet Protocol* (*IP Address*) pengunjung dan pengisi kuesioner pada website *phishing* tersebut.



Gambar 7. Grafik Jumlah Kunjungan *IP Address*

Rata-rata keseluruhan diperoleh sebanyak ±30-40 dari total target ±100 siswa/i masing-masing sekolah melakukan akses terhadap tautan *phishing* yang telah dibagikan. Hal ini bisa jadi sekitar 30% dari masyarakat usia dini kurang perhatian dalam menilai legitimasi URL yang diberikan. Sementara itu, siswa yang menjawab kuesioner dapat dilihat melalui grafik Gambar 8 berikut:



Gambar 8. Grafik Menjawab Kuisioner

e. *Post-test*

Post-test disampaikan setelah penyampaian materi pada saat pelaksanaan *workshop cybersecurity awareness* melalui platform Quiziz. Siswa/I menjawab pertanyaan melalui perangkat smartphone masing-masing. Hasil akhir dari *post-test* diperoleh perwakilan tiga orang siswa/i dengan nilai tertinggi berhasil menjawab pertanyaan dengan baik. Gambar 9 dan 10 berikut merupakan suasana pelaksanaan pada saat *post-test*.

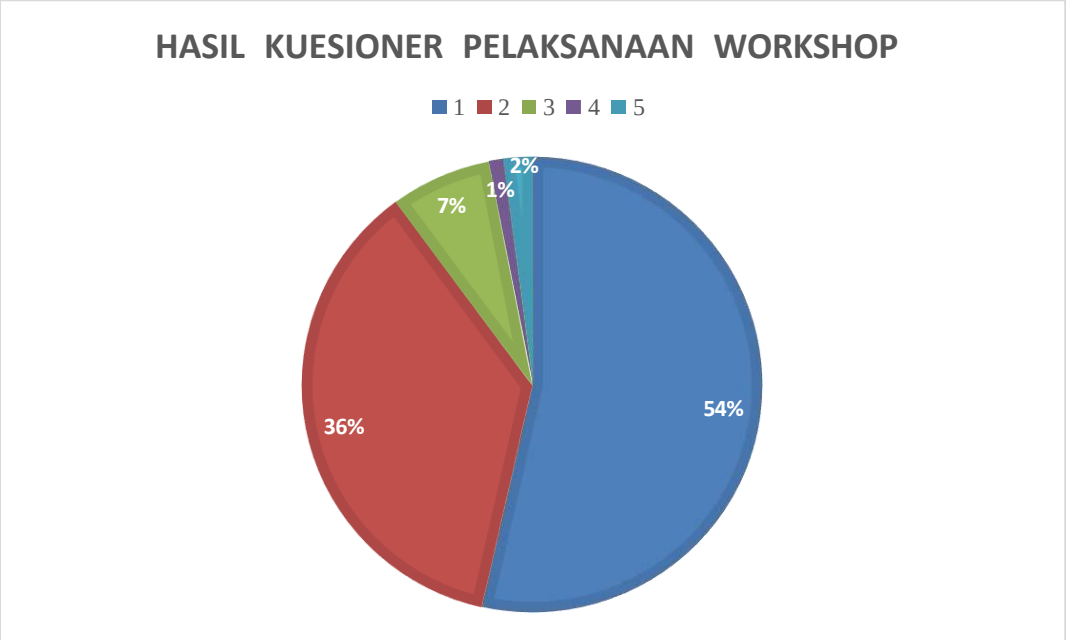
Gambar 9. Suasana pada Pelaksanaan Post-Test di SMKN 1 Tanjung Pinang

Gambar 10. Suasana pada Pelaksanaan Post-Test di SMK MHS

f. Kuesioner Pelaksanaan Kegiatan Workshop

Kuesioner ini merupakan salah satu evaluasi terakhir pada saat pelaksanaan Workshop. Dimana kuesioner ini berisi pertanyaan yang berkaitan dengan pelaksanaan workshop secara keseluruhan. Dari hasil kuesioner secara garis besar, terdapat dua poin penting, yaitu:

i. Tingkat kepuasan terhadap pelaksanaan workshop cybersecurity awareness dari level 1 – 5 (buruk – sangat memuaskan) dapat dilihat melalui diagram berikut. Dari hasil tersebut, diperoleh tingkat kepuasan pelaksanaan workshop berada di kategori memuaskan hingga sangat memuaskan sekitar 90%.



Gambar 11. Diagram Hasil Kuesioner Pelaksanaan Workshop

ii. Pelaksanaan kegiatan pengabdian masyarakat juga merupakan salah satu aktivitas dalam pelaksanaan Project Based Learning (PBL) di Polibatam dimana melibatkan Mahasiswa/i Program Studi Sarjana Terapan Rekayasa Keamanan Siber (RKS) Semester 3. Dari hasil kuesioner kepuasan pelaksanaan *Workshop* juga disampaikan masukan terhadap pelaksanaan *Workshop* khususnya pada saat penyampaian materi (*public speaking*).

4.3. Pelaksanaan Workshop

Workshop dilakukan melalui sosialisasi edukasi yang berkaitan dengan skenario *phishing* tersebut. Hal ini dilakukan setelah terkumpulnya informasi mengenai kesadaran terhadap ancaman *phishing* tersebut. Adapun pelaksanaan *workshop* dilakukan secara berurutan sesuai jadwal pada 3 sekolah SMK yang dituju, seperti salah satunya pada Gambar 12.

Gambar 12. Dokumentasi Kegiatan *Workshop* di SMK Negeri 1 Batam

4.4. Kendala dan Tantangan

Kendala dan tantangan utama yang dihadapi pada saat pelaksanaan kegiatan yaitu penentuan materi *phishing* yang dibuat sebagai *pre-test*. Persiapan materi ini memiliki batasan yang sangat perlu diperhatikan dimana isinya tidak melanggar ketentuan yang berlaku pada Undang-Undang Perlindungan Data Pribadi (UU PDP). Sehubungan dengan adanya UU PDP tersebut, materi yang telah disiapkan sebaik mungkin tidak mengumpulkan data pribadi dari target. Sehingga, untuk mengatasi kendala tersebut, materi diisi dengan beberapa pertanyaan dalam bentuk kuesioner yang berkaitan dengan pemahaman target terhadap *phishing*.

V. KESIMPULAN

Kegiatan pengabdian masyarakat "*Workshop Series Cyber Security Awareness* untuk Meningkatkan Literasi Keamanan Digital di Wilayah Suburban Kepulauan Riau" dengan topik "*Phishing*" telah dilakukan dengan sangat baik. Dengan adanya *workshop* tersebut siswa/i sekolah SMK semakin memahami terhadap kejahatan siber *phishing* dan lebih waspada serta mengetahui apa yang harus dilakukan apabila mendapati informasi *phishing* ataupun ketika menjadi korban *phishing*. Hal ini dapat dilihat pada hasil skenario *phishing* yang telah dilakukan terdapat sekitar 70% siswa/i SMK sudah mengetahui terkait informasi *phishing* tersebut. Selanjutnya, edukasi yang diberikan kepada masyarakat dini dapat disebarluaskan ke keluarga hingga khalayak luas. Sehingga kewaspadaan terhadap ancaman kejahatan siber selanjutnya dapat terus ditingkatkan dan menurunkan risiko korban kejahatan siber.

UCAPAN TERIMA KASIH

Judul untuk ucapan terima kasih dan daftar pustaka tidak diberi nomor. Terima kasih disampaikan kepada semua pihak yang telah berkontribusi terhadap pelaksanaan kegiatan pengabdian kepada masyarakat, termasuk pihak yang memberikan pembiayaan atau kontribusi finansial untuk pelaksanaan kegiatan tersebut.

DAFTAR PUSTAKA

Akhyari, M. R. & Pratama, A. R., 2021. *Kesadaran akan Ancaman Serangan Berbasis Backdoordi Kalangan Pengguna SmartphoneAndroid*. AUTOMATA, 2(1), pp. 1 - 7.

APWG, 2022. *Phishing Activity Trends Report 4th Quarter*, s.l.: s.n.

Badan Siber dan Sandi Negara, 2022. *Lanskap Keamanan Siber Indonesia Tahun 2022*. [Online] Available at: https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs

Cisco Networking Academy, 2020. *Cybersecurity Essentials*, s.l.: Cisco Press.

Hootsuite, We Are Social, 2023. *The World's Favourite Social Media Platforms by Age and Gender* January 2023 DataReportal, s.l.: s.n.

Muftiadi, A., Mulyani Agustina, T. P. & Evi, M., 2022. *Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking*. Hexatech Jurnal Ilmiah Teknik , 1(2), pp. 60 - 65.

Vadila, N. & Pratama, A. R., 2021. *Analisis Kesadaran Keamanan Terhadap Ancaman Phishing*. AUTOMATA, 2(2).

Wahyuni, S., Raazi, I. M. & Dwitawati, I., 2022. *Analisis Teknik Penyerangan Phishing pada Social Engineering terhadap Keamanan Informasi di Media Sosial Profesional menggunakan Kombinasi Black Eye dan Setoolkit*. Jurnal Nasional Komputasi dan Teknologi Informasi, 5(1), pp. 49 - 55.

Wirawan, R., 2019. *Studi Kompetensi dan Kesadaran Pengguna E-Learning Terhadap Keamanan Sistem E-Learning Pada Pendidikan Tinggi*. ETHOS, 7(1), pp. 9 - 17.

Zieni, R., Massari, L. & Calzarossa, M. C., 2023. *Phishing or Not Phishing? A Survey on the Detection of Phishing Websites*, IEEE.