SANISKALA : Jurnal Pengabdian Masyarakat
Vol. 1 No. 2, November 2023, Hal. 49-52
e-ISSN: 3021-8381, p-ISSN: 3021-8438
https://ejournal.unma.ac.id/index.php/saniskala

Bimbingan Teknis Menjaga Keamanan Data di Era Digital pada Siswa SMA "Waspada Ancaman Phising"

Syamsu Hidayat[1*], Astried Silvanie[2], Dwi Sidik Permanan[3], RR Aryanti Kristantini[4]
[1]Institut Bisnis dan Informatika Kosgoro 1957, Indonesia
*Korespondensi: syamsuhi3009@gmail.com

Abstract
In a digital era that is increasingly connected, cyber threats such as phishing attacks have become a pressing issue. Therefore, an introduction to phishing activity for vocational students is important. The aim is to improve students' understanding of how phishing works, teach them how to identify the signs of an attack, and provide practical cybersecurity skills. The result is students who are more aware of cyber risks, able to protect themselves from phishing attacks, and ready to face data security challenges in a complex digital world. As such, this activity plays an important role in educating the younger generation about the importance of cybersecurity and preparing them to be smart and safe users online.
Keywords: *phising, security, cyber, data*

Abstrak
Kegiatan pengenalan phishing untuk siswa SMK menjadi penting. Tujuannya adalah untuk meningkatkan pemahaman siswa tentang cara kerja phishing, mengajari mereka cara mengidentifikasi tanda-tanda serangan, dan memberikan keterampilan keamanan siber yang praktis. Hasilnya adalah siswa yang lebih sadar akan risiko siber, mampu melindungi diri mereka sendiri dari serangan phishing, dan siap menghadapi tantangan keamanan data di dunia digital yang kompleks. Dengan demikian, kegiatan ini berperan penting dalam mengedukasi generasi muda tentang pentingnya keamanan siber dan mempersiapkan mereka menjadi pengguna yang cerdas dan aman di dunia online
Kata Kunci: phising, keamanan, cyber, data

Submited: yyyy-mm-dd Accepted: yyyy-mm-dd

PENDAHULUAN

Tingginya tingkat ancaman keamanan data merupakan masalah yang menjadi pusat perhatian di era digital saat ini. Dengan pesatnya perkembangan teknologi informasi dan konektivitas online, data pribadi dan perusahaan menjadi semakin rentan terhadap serangan siber. Ancaman tersebut mencakup berbagai jenis serangan seperti serangan phishing, malware, pencurian identitas, ransomware, dan serangan DDoS (*Distributed Denial of Service*). Serangan-serangan tersebut dapat menyebabkan kerugian finansial yang sangat besar, kehilangan data berharga, dan bahkan merusak reputasi individu dan perusahaan.

Ancaman keamanan data tidak hanya berdampak pada tingkat individu, tetapi juga pada tingkat masyarakat, yang berpotensi mengganggu layanan publik, infrastruktur penting, dan bahkan keamanan nasional. Hilangnya data pribadi juga dapat mengakibatkan penyalahgunaan identitas, penipuan, dan konsekuensi sosial dan keuangan yang merugikan (Abdumalikov, 2022). Setiap orang perlu menerapkan kebiasaan menggunakan kata sandi yang kuat dan unik untuk akun mereka di era digital ini. Kata sandi yang lemah atau mudah ditebak adalah salah satu celah paling umum yang dieksploitasi oleh penjahat siber untuk mengakses akun dan mencuri data pribadi. Kata sandi yang kuat harus terdiri dari kombinasi huruf (huruf besar dan huruf kecil), angka, dan simbol, serta memiliki panjang yang cukup (Cervone, 2007). Penting untuk berhati-hati dalam membagikan informasi pribadi di media sosial atau platform online lainnya. Ini karena penjahat siber dapat dengan mudah mengumpulkan dan memanfaatkan informasi tersebut untuk membuat serangan yang lebih bertarget dan berbahaya. Informasi pribadi seperti tanggal lahir, alamat, nomor telepon, dan bahkan detail pribadi lainnya dapat

memberikan penjahat siber wawasan yang cukup untuk merancang serangan seperti phishing yang lebih meyakinkan (Rifiyanti, 2020). Penting untuk memahami betapa rentannya kita terhadap serangan-serangan ini dan pentingnya mengambil langkah proaktif dalam menjaga keamanan data pribadi. Pelatihan dan sosialisasi tentang praktik keamanan siber adalah kunci untuk melindungi diri kita sendiri dan komunitas kita dari ancaman yang terus berkembang di dunia digital ini. Dengan memahami tingkat ancaman yang tinggi ini, kita dapat menggali lebih dalam tentang cara-cara untuk melindungi data pribadi dan perusahaan, serta mengambil tindakan yang diperlukan untuk mengurangi risiko yang terkait dengan serangan siber (Suteja et al., 2021).

Dalam hal tersebut, penting bagi siswa SMK perlu memiliki akses ke pelatihan keamanan siber yang relevan. Pelajaran tentang ancaman siber, teknik serangan, dan cara melindungi diri harus diintegrasikan ke dalam kurikulum mereka. Berdasarkan latar belakang tersebut, tim dosen – dosen dari Fakultas Ilmu Komputer, program studi Teknik Informatika Institut Bisnis dan Informatika mengadakan kegiatan pengabdian masyarakant (abdimas) yang bertajuk bimbingan teknis menjaga keamanan data di era digital pada siswa smk: waspada ancaman Phising. Kegiatan ini bertujuan memberikan pemahaman kepada para siswa tentang potensi konsekuensi dari serangan phishing, baik untuk diri mereka sendiri maupun untuk perusahaan tempat mereka bekerja nantinya. Hal ini akan membuat mereka lebih berkomitmen untuk menjaga keamanan data. Kegiatan ini diadakan di SMK Perguruan Cikini, Jagakarsa dengan para peserta adalah para siswa dari jurusan Teknik Jaringan Komputer (TKJ)

METODE

Kegiatan ini dilakukan berupa bimbingan teknis yang secara aktif melibatkan siswa dalam diskusi, simulasi serangan phishing, dan latihan pengenalan. Hal ini dilakukan untuk memberikan pengalaman praktis yang lebih mendalam. Langkah – Langkah kegiatan yang dilakukan digambarkan pada diagram berikut ini:

Gambar 1. Langkah – Langkah pelaksanaan kegiatan abdimas

Metode pelaksanaan bimbingan teknis mengacu pada pendekatan praktis dalam pembelajaran keamanan data. Artinya, para siswa tidak hanya diberikan teori-teori tentang keamanan data, tetapi mereka juga dilibatkan dalam kegiatan-kegiatan yang memberikan pengalaman praktis dalam menjaga keamanan data. Untuk mengevaluasi hasil dari bantuan teknis, para siswa diberikan skenario keamanan data atau masalah yang perlu diselesaikan. Hal Ini meliputi simulasi serangan, insiden keamanan, atau memecahkan masalah nyata yang melibatkan keamanan data.

HASIL DAN PEMBAHASAN

Kegiatan diawali dengan sambutan dari ketua abdimas dan kepala jurusan TKJ dan dilanjutkan dengan pemaparan materi awal tentang pengenalan phising dan cara kerjanya.

Gambar 2. Pemberian materi oleh dosen IBIK 57

Phishing adalah bentuk serangan siber yang digunakan oleh penjahat siber untuk mencuri informasi sensitif seperti kata sandi, nomor kartu kredit, atau informasi pribadi dengan menyamar sebagai entitas tepercaya. Penjahat siber mencoba memancing (phishing) informasi ini dari korbannya dengan menipu atau merayu mereka. Phishing bekerja dengan menipu korban untuk percaya bahwa mereka berurusan dengan entitas yang sah, seperti perusahaan, bank, atau situs web layanan online (Bhavsar et al., 2018). Selanjutnya pemberian materi tentang pengenalan tanda-tanda serangan Phishing dan cara menanganinya.

Gambar 3. Pemaparan pengenalan tanda-tanda Phishing dan cara menanganinya.

Materi ini disajikan dengan cara yang menarik dan interaktif, dengan contoh-contoh konkret dan studi kasus nyata untuk memberikan pemahaman yang mendalam tentang ancaman phishing dan cara melindungi diri dari serangan tersebut. Selain itu, simulasi dan latihan langsung membantu siswa untuk mempraktikkan pengetahuan yang mereka pelajari, sehingga mereka dapat merasa lebih siap untuk menghadapi ancaman phishing di dunia nyata.

Kegiatan selanjutnya adalah sesi tanya jawab yang disambut antusias oleh para siswa. Diskusi secara interaktif terjadi antara peserta dengan para pemateri dengan memberikan kesempatan kepada para siswa untuk mengajukan pertanyaan dan berbicara tentang pengalaman dan pemahaman mereka tentang keamanan siber. Selanjutnya kegiatan diakhiri dengan kesimpulan dan saran – saran atas kegiatan yang telah berlangsung.

KESIMPULAN DAN SARAN

Pengenalan dan pemahaman tentang phishing merupakan langkah yang sangat penting dalam mengedukasi siswa-siswi SMK tentang ancaman siber di era digital. Melalui seminar atau lokakarya interaktif, para siswa dapat memperoleh pemahaman yang mendalam tentang cara kerja phishing dan cara melindungi diri mereka sendiri dari serangan ini. Dengan meningkatkan kesadaran dan keterampilan keamanan siber para siswa, mereka dapat menjadi lebih siap dalam menghadapi ancaman siber dan melindungi data pribadi mereka di dunia online yang semakin kompleks. Kegiatan ini disarankan untuk terus dilanjutkan dalam upaya sosialisasi dan pendidikan keamanan siber secara teratur. Hal ini dapat mencakup materi tambahan, pengingat tentang praktik keamanan, dan peringatan tentang ancaman siber terbaru. Diharapkan pula pada kesempatan yang akan datang dapat berkolaborasi dengan perusahaan atau organisasi yang relevan dalam menyelenggarakan kegiatan ini untuk memberikan perspektif praktis tentang keamanan siber di dunia kerja.

DAFTAR PUSTAKA

Abdumalikov, G. (2022). *Profound Importance of Cyber security in the Field of Business*. *c*, 43–46. https://media.neliti.com/media/publications/408257-profound-importance-of-cyber-security-in-a2668cec.pdf

Cervone, H. F. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (Vol. 7, Issue 2). https://doi.org/10.1353/pla.2007.0017

Rifiyanti, H. (2020). Meningkatkan Kualitas Informasi dalam Bersosial Media Melalui Media Internet di Kampus IBI KOSGORO, Kota Jakarta. *Jurnal Pengabdian Teratai*, *1*(2), 255–270. https://doi.org/10.55122/teratai.v1i2.144

Suteja, E., N, E. K., & Raharjo, S. (2021). Mengurangi Kejahatan Cyber Menggunakan Teknik Demilitarized Zone (Dmz) Dan Firewall Rules (Studi Kasus : Laboratorium Basis Data IST AKPRIND). *Jurnal JARKOM*, *09*(01), 71–80.

Abdumalikov, G. (2022). *Profound Importance of Cyber security in the Field of Business*. *c*, 43–46. https://media.neliti.com/media/publications/408257-profound-importance-of-cyber-security-in-a2668cec.pdf

Cervone, H. F. (2007). Computer Network Security and Cyber Ethics (review). In *portal: Libraries and the Academy* (Vol. 7, Issue 2). https://doi.org/10.1353/pla.2007.0017

Rifiyanti, H. (2020). Meningkatkan Kualitas Informasi dalam Bersosial Media Melalui Media Internet di Kampus IBI KOSGORO, Kota Jakarta. *Jurnal Pengabdian Teratai*, *1*(2), 255–270. https://doi.org/10.55122/teratai.v1i2.144

Suteja, E., N, E. K., & Raharjo, S. (2021). Mengurangi Kejahatan Cyber Menggunakan Teknik Demilitarized Zone (Dmz) Dan Firewall Rules (Studi Kasus : Laboratorium Basis Data IST AKPRIND). *Jurnal JARKOM*, *09*(01), 71–80.