VOKATEK

E-ISSN: 2986-0105
P-ISSN : 2985-8402

VOKATEK Volume 01 Nomor 01 Januari 2023

Analisa *Clustering Phising* Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar

[1]Wahyu Hidayat M, [2] Hartini Ramli, [3]Pedang Mata Bulan Ikhram, [4]Sidrayanti, [5]Ahmad Radif Ridhawi, [6]Nur Aisyah Mukhtar, [7]Renaldy Junedy

[1234567]Universitas Negeri Makassar

Email: wahyu.hidayat@unm.ac.id[1], hartiniramli023@gmail.com [2], bulanpedang0@gmail.com [3], sidrayanti340@gmail.com [4], radiffadil5@gmail.com [5], aisyahmukhtar113@gmail.com [6], renaldydjunaeidi@gmail.com[7]

Received : 6 Januari 2023
Accepted: 27 Januari 2023
Published: 30 Januari 2023

ABSTRAK

Penelitian ini bertujuan untuk sistem sekolah mungkin memperhatikan fakta bahwa individu dan perusahaan yang menggunakan perangkat pintar semakin berisiko menjadi korban kejahatan dunia maya. Literatur tentang seberapa efektif siswa di negara maju seperti Belanda diajarkan tentang keterampilan keamanan dunia maya selama karir sekolah mereka masih langka. Meskipun materi kurikulum tersedia (Witsenboer et al., 2022). Hal ini juga bertujuan untuk menghasilkan dan meningkatkan kesadaran terhadap mahasiswa terhadap keamanan data pribadi oleh tindak *cyber crime* jenis *phising*. Hampir 42% dari modus selain *phising* yang dinyatakan dalam *website Anti-Phishing Working Group* (APWG). Dalam laporan bulanannya, mencatat ada 12.845 email baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana *phising*. Perlu adanya usaha yang dilakukan oleh para administrator jaringan dalam meningkatkan pengawasan dalam memonitoring aktivitas di jaringan. Hasil penelitian ini menunjukan bahwa sebagian besar mahasiswa menyadari pentingnya keamanan data pribadi, mahasiswa juga menyadari resiko yang nantinya akan terjadi jika kita tidak menjaga keamanan data pribadi. Namun tidak sedikit juga mahasiswa yang merasa tidak peduli dengan keamanan data pribadi mereka.

Kata Kunci: Mahasiswa, Keamanan, Data Pribadi, Phising

ABTRACT

This research aims for school systems may pay attention to the fact that individuals and companies who use smart devices are increasingly at risk of becoming victims of cybercrime. Literature on how effectively students in developed countries like the Netherlands are taught cybersecurity skills during their school careers is scarce. Although curriculum materials are available (Witsenboer et al., 2022). It also aims to produce and increase student awareness of the security of personal data by phishing-type cyber crimes. Nearly 42% of non-phishing modes stated on the Anti-Phishing Working Group (APWG) website. In its monthly report, there are 12,845 new and unique e-mails and 2,560 fake sites used as phishing tools. There needs to be effort made by network administrators in increasing supervision in monitoring activity on the network. The results of this study indicate that most students are aware of the importance of personal data security, students are also aware of the risks that will occur if we do not maintain personal data security. However, not a few students also feel that they do not care about the security of their personal data.

Keywords: Student, Security, Personal Data, Phishing

1. PENDAHULUAN

Hal yang paling melekat terhadap remaja terutama siswa ialah teknologi dimana mereka banyak menghabiskan waktu mereka untuk melakukan banyak hal di dalamnya dengan hal ini pun termasuk sosial media yang banyak menyimpan data-data pribadi mereka dan yang berhubungan dengan privasi mereka pun jadi terancam oleh peretas ilegal yang memanfaatkan hal tersebut dengan membobol keamanan biodata sosial media mereka dan memanfaatkannya untuk hal yang berbau kejahatan dan ilegalisme.

Keamanan dunia maya adalah konsep yang luas. Selain perspektif teknis, ada perspektif etika, budaya, dan politik terhadap keamanan siber. Dalam penelitian ini, fokusnya adalah pada tindakan manusia sehubungan dengan keamanan dunia maya, karena penjahat dunia maya saat ini terutama menargetkan pengguna sistem. Penelitian menunjukkan bahwa pengguna tidak memahami pemberitahuan keamanan *browser*, yang mungkin menjadi alasan pengguna tidak memperhatikannya. Ketika serangan dunia maya ditujukan untuk pengguna dalam organisasi, sistem keamanan dunia maya sering kali tersedia untuk melindungi karyawan. Sistem ini dikelola oleh pakar keamanan siber, tetapi di rumah pengguna bertanggung jawab untuk mengelola keamanan siber mereka sendiri (Witsenboer et al., 2022).

Salah satu pilar globalisasi adalah penggunaan komunikasi yang merupakan pilar utama hubungan internasional dengan menggunakan kemajuan teknologi informasi. Dalam perkembangannya, kemajuan teknologi informasi telah mendorong negara-negara untuk meliberalisasi sektor komunikasi sehingga mendorong kompetisi dan globalisasi komunikasi dan pada akhirnya telah menstimulasi kemajuan ekonomi (Rosadi, 2016). Era modern sekarang, orang-orang tidak bisa lepas dari yang namanya internet dan gadget. Di tambah, saat ini orang-orang berlomba memperbanyak akun jejaring sosial mereka untuk mencari kepopuleran seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Untuk mendapat berita ter-update orang-orang juga bisa menjumpai berbagai macam artikel baik dalam maupun luar negeri melalui sebuah laman web ataupun di jejaring sosial juga. Pastinya orang-orang membuka *web browser* dulu agar bisa pergi ke berbagai jejaring sosial semacam itu. Setiap orang pasti memiliki akun jejaring sosial lebih dari satu. Selain itu, sosial media juga digunakan untuk lahan berbisnis misalnya *online shop*. Kegiatan ini sangat mudah dan menguntungkan karena tidak membutuhkan modal dan hanya tinggal memposting barang jualan. Untuk pembayarannya bisa lewat rekening, COD, *market*, dll.

Tidak tau sampai kapan serangan phising akan dilancarkan sebagai kejahatan siber. Karena para hacker-hacker itu terus memunculkan ide-ide baru untuk merusak kegiatan di internet. Dan sayangnya di setiap tahunnya kasus seperti ini semakin bertambah banyak dan korban yang terjaring juga tidak bisa hanya dihitung dengan jari. Mereka mencari uang dengan cara yang mudah. Namun tak selamanya mereka melakukan itu karena uang. Biasanya mereka hanya ingin bersenang-senang atau ingin mengintip kegiatan sang pemilik akun. Jika beruntung, mereka juga bisa mendapat uang sekaligus melihat-lihat isi akun pengguna yang mereka serang untuk bersenang-senang. Bila hanya orang biasa yang mereka serang mungkin masalah tidak akan terlalu besar. Bagaimana jika yang mereka serang adalah orang yang penting atau pun orang yang berpengaruh di dunia ini. Kasus itu pasti sudah sering terjadi. Orang-orang yang memiliki kuasa tertinggi beberapa juga melakukan kejahatan tetapi ia hanya menjadi bagian penyuruh untuk sang hacker. Selanjutnya hacker-hacker itu yang melaksanakan perintah untuk menyerang. Hal-hal itu sudah wajar terjadi apalagi saat masa masa kampanye berpolitik ataupun contohnya pada saat dua perusahaan yang awalnya menjalin hubungan yang baik tiba-tiba salah satu perusahaan merasa kecewa karena saat pembagian hasil tidak memenuhi sepakat yang tercantum sebelumnya. Maka muncullah ide ide berbuat kecurangan. Mereka akan memanfaatkan hacker sebagai sarana penghancur sang lawan. Mereka menyuruh sang hacker untuk diam-diam mencuri data keuangan perusahaan musuh dan kemudian memanipulasi data tersebut sebaik mungkin. Lalu pada akhirnya semua uang hasil kerja sama mereka menjadi milik perusahaan yang menyewa hacker tadi semua. Pastinya si hacker tadi mendapat keuntungan beberapa persen.

Untuk itulah masih ada banyak orang baik di dunia ini yang mau menciptakan alat pendeteksi atau aplikasi untuk mencegahnya. Para peneliti maupun pembuat aplikasi itu biasanya merupakan orang-orang yang pernah mengalami serangan phising. Mereka tidak terima dan kemudian memutuskan untuk membalaskan dendamnya dengan sebuah aplikasi *anti phishing*. Maka dari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan phising (Wibowo & Fatimah, n.d.).

2. METODE PENELITIAN

Penelitian ini dilakukan dengan metode penelitian kuantitatif. Survei dilakukan dengan cara mengumpulkan data hasil survei mahasiswa jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar. Penelitian ini dilakukan dengan pembagian kuesioner penelitian.

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

a. Sistem Keamanan Data Pribadi

Keamanan data sangat diperlukan dalam sebuah perangkat, agar data-data yang diperlukan tidak dicuri atau dihapus oleh oknum-oknum tidak bertanggungjawab. Jika dilihat secara sederhana, keamanan data adalah tindakan yang perlu dilakukan oleh suatu perusahaan atau individu untuk melindungi ekosistem teknologi informasi. Adanya keamanan data ini, perusahaan atau individu tidak perlu khawatir lagi apabila terjadi pelanggaran keamanan. Karena biar bagaimanapun, data merupakan dokumen penting yang terkadang berisikan informasi pribadi. Jika data data berhasil dicuri, bukan tidak mungkin dokumen tersebut akan digunakan untuk tindakan-tindakan kriminal.

b. Phising

Perkembangan teknologi informasi dan komunikasi (ICT) di dunia sangat dirasakan manfaatnya dalam berbagai sektor industri, perbankan maupun Usaha Kecil Menengah (UKM). Sektor-sektor tersebut merasakan manfaat efisiensi dan efektivitas dalam segi operasional maupun peningkatan layanan terhadap pengguna. Namun perkembangan tersebut memunculkan tantangan baru dengan munculnya berbagai tindak kriminal berbasis siber (*cybercrime*) oleh pihak-pihak yang berusaha mengeksploitasi kelemahan sistem dan kesadaran pengguna terhadap sistem informasi. Salah satu bentuk *cybercrime* yang dilakukan oleh para frauder adalah phising (Radiansyah & Priyadi, 2016).

Phising adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi (nama, usia, alamat), data akun (username dan password), dan data finansial (informasi kartu kredit, rekening). Istilah resmi phising adalah *phishing*, yang berasal dari kata fishing yaitu memancing. Kegiatan phising memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan kejahatan.

c. Peningkatan Keamanan Data Pribadi

Kebocoran data ialah resiko yang berhubungan dengan keamanan dan data pribadi. Penggunaan komunikasi digital tidak terlepas dari penggunaan big data. Hal ini dikarenakan dunia saat ini tidak lepas dari peran data karena semua dibangun di atas sebuah fondasi data. Saat ini, sejumlah besar data yang dikumpulkan dan dihasilkan setiap hari menawarkan berbagai peluang analitis bagi organisasi untuk mengungkap informasi yang bermanfaat untuk operasinya (Munawar et al., 2022).

Keamanan digital adalah hal utama yang perlu anda pikirkan sebelum benar benar mulai untuk menyerahkan data Anda ke internet. Sebenarnya, internet tidak selalu buruk, tapi bertindak dan menggunakannya dengan bijak akan memberikan manfaat seperti:

1. Menjaga Kerahasiaan Privasi
   Data yang bersifat sensitif biasanya privat, alias hanya Anda saja yang seharusnya tahu atau orang-orang serta pihak tertentu seperti institusi pemerintahan atau organisasi pendidikan. Nah, dengan menjaga keamanan digital, nantinya Anda mampu menjaga kerahasiaan data diri Anda termasuk email, password, nama ibu, dan nomor identitas.
2. Menghindari Ancaman Kejahatan Siber
   Kejahatan Siber ada banyak macamnya dan pencurian data serta penyalahgunaan data adalah salah satu di antara banyaknya jenis kejahatan siber. Dengan menyadari pentingnya menjaga keamanan digital, Anda bisa terhindar dari ancaman tersebut dan bisa online dengan nyaman.

3.2 Hasil Penelitian

a. Peserta

Kuesioner dibagikan kepada 30 mahasiswa dari Jurusan Teknik Informatika dan Komputer Universitas Negeri Makassar. Responden berusia rata-rata 19 tahun dari rentang usia 18 sampai 20 tahun. Pembagian jenis kelamin adalah 43,3% perempuan dan 56,7% laki laki. Tabel 1 menunjukkan karakteristik partisipan.

b. Hasil Analisis Kuantitatif

Tabel 1. Demografi partisipan dalam penelitian kuesioner

Karakteristik	Total
Banyak Sampel	30
Jenis Kelamin : Laki-laki Perempuan	 13 17
Usia : 18 19 20	 5 22 3
Rata-rata Usia	19

Tabel 2. Hasil perbandingan

Item	Ya	Tidak
Saya menggunakan kata sandi yang berbeda untuk akun media sosial dan akun sekolah saya	24	6
Saya membagikan *password* akun media sosial atau sekolah saya pada teman kelas	9	21
Saya menggunakan kombinasi huruf, angka, dan simbol pada *password* akun sosial dan sekolah saya	27	3
Saya membiarkan laptop/ipad/*smartphone* saya tidak terkunci saat saya belajar dikelas	10	20
Saya tidak mengklik link, thumbnail ataupun tautan pada *email*, hanya jika itu berasal dari orang yang saya kenal	24	6
Jika email dari pengirim yang tidak dikenal terlihat menarik, saya klik tautan di *email*	10	20
Saya tidak membuka link, thumbnail, ataupun tautan pada *email* jika pengirimnya tidak saya kenal	24	6
Saya dapat mengetahui mana *email phishing*	15	15
Saya mendownload semua file yang saya butuhkan untuk tugas saya pada komputer kampus	23	7
Saya mengunjungi semua *website* yang saya inginkan saat menggunakan internet kampus	20	10
Saya memperhatikan *security* akses sebelum memasuki sebuah web	22	8
Saya dapat mengetahui yang mana *website phishing*	20	10
Saya secara berskala memeriksa pengaturan privasi pada akun media sosial saya	22	8

Saya memikirkan dampak negatif sebelum memposting sesuatu pada media sosial	27	3
Saya memposting apapun yang saya inginkan tentang universitas saya	13	7
jika saya mengalami hal aneh saat *online*, saya membagikannya pada orang tua saya	12	8

4. KESIMPULAN DAN SARAN

Hasil dari penelitian kami telah menunjukkan mahasiswa JTIK sudah banyak mengetahui dan sadar betapa pentingnya keamanan data pribadi dan betapa berbahayanya tindakan phising terhadap data pribadi mereka ini juga menunjukkan betapa besarnya kesadaran mahasiswa terhadap pentingnya sebuah data.

Pada zaman era modern sekarang ini dimana informasi data adalah hal yang sangat berharga maka banyak juga ancaman yang harus dihadapi untuk menjaga keamanan informasi tersebut. Tidak hanya kesadaran, peningkatan terhadap sistem keamanan data digital juga harus diperhatikan begitu pula dengan tindak kejahatan *cybercrime* lainnya yang dapat mengancam keamanan data informasi orang orang.

REFERENSI

Bahri, A., Sahribulan, S., & Hidayat, W. (2022). PELATIHAN PENGEMBANGAN WEBSITE SEKOLAH BAGI GURU DAN TENAGA PENDIDIK DI SEKOLAH DASAR KABUPATEN TAKALAR. *Community Development Journal: Jurnal Pengabdian Masyarakat*, *3*(3), 1426-1431.

Firlansyah, A., Risal, A. A. N., Adiba, F., & Kaswar, A. B. (2020). Clustering Produksi Perikanan Budidaya Laut Berdasarkan Provinsi Menggunakan Algoritma K-means. *Journal of Embedded Systems, Security and Intelligent Systems*, *2*(1), 58-63.

Isma, A., Rakib, M., Marhawati, Surianto, D. F., & M Miftach Fakhri. (2023). Pelatihan Pembuatan Bakso Sayur Bernilai Gizi Tinggi Sebagai Alternatif Peluang Usaha Bagi Ibu Rumah Tangga. TEKNOVOKASI : Jurnal Pengabdian Masyarakat, 1(1), 51–57. Retrieved from. https://journal.unm.ac.id/index.php/TEKNOVOKASI/article/view/15

Munawar, Z., Widhiantoro, D., Putri, N. I., & Komalasari, R. (2022). Keamanan, Data Pribadi Pada Metaverse. 9(2), 10.

Radiansyah, I., & Priyadi, Y. (2016). ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING. 7(1), 14.

Rizal, M., Hadis, M. S., Angriawan, R., & Arifin, A. (2020). Evaluasi Kinerja Bluetooth Pada Modul ESP32 Di Lingkungan Line Of Sight. *J. Embed. Syst. Secur. Intell. Syst*, *1*, 42-47.

Rosadi, S. (2016). IMPLIKASI PENERAPAN PROGRAM E-HEALTH DIHUBUNGKAN DENGAN PERLINDUNGAN DATA PRIBADI. Arena Hukum, 9(3), 403–420. https://doi.org/10.21776/ub.arenahukum.2016.00903.6.

Rustam, S. (2018). ANALISA CLUSTERING PHISING DENGAN K-MEANS DALAM MENINGKATKAN KEAMANAN KOMPUTER. ILKOM Jurnal Ilmiah, 10(2), 175– 181. https://doi.org/10.33096/ilkom.v10i2.309.175-181.

Ulfah, A. N., Lizarti, N., Sudyana, D., Anam, M. K., & Asnal, H. (2021). Pelatihan Secure Computer User Untuk Meningkatkan Kesadaran Siswa Terhadap Keamanan Data dan Informasi. 2(1), 8.

Wibowo, M. H., & Fatimah, N. (n.d.). ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME. 1, 5.

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. Computers & Education, 186, 104536. https://doi.org/10.1016/j.compedu.2022.104536.

Zulkiplih, S., & Parenreng, J. M. (2020). Pengembangan Aplikasi Pariwisata Sulawesi Barat Berbasis Android. *Journal of Embedded Systems, Security and Intelligent Systems*, *1*(1), 48-56.