Journal of Vocational, Informatics and Computer Education
E-ISSN: 2988-6325; P-ISSN: 2988-4918
Journal Homepage: http://journal.lontaradigitech.com/index.php/VOICE

Analisis Perilaku Mahasiswa dari Ancaman Keamanan Komputer

Akmal Hidayat[1], Mufti Fathur Rahman[2], Miftahul Jannah Awaliyah[3], Ahmad Abdillah Fathur Rachman[4], Andi Muh. Achyar AM[5]

[1,2,3,4,5] *Jurusan Teknik Informatika dan Komputer, Fakultas Teknik, Universitas Negeri Makassar, Jl. Daeng Tata 3, Makassar 90223, Indonesia*

Corresponding Email: akmal.hidayat@unm.ac.id

INFO ARTIKEL
Kata kunci:
Ancaman;
Keamanan Komputer;
Perilaku.

ABSTRAK
Mahasiswa sebagai pengguna aktif komputer di lingkungan akademik berisiko terhadap berbagai ancaman keamanan komputer, namun tidak semua memiliki kesadaran dan perilaku protektif yang memadai. Penelitian ini bertujuan untuk menganalisis perilaku mahasiswa JTIK di Universitas Negeri Makassar dalam menghadapi ancaman terhadap keamanan komputer. Metode yang digunakan adalah survei dengan kuesioner yang disebarkan kepada 43 mahasiswa dan dianalisis secara deskriptif. Hasil menunjukkan bahwa mayoritas mahasiswa memiliki kesadaran tinggi terhadap pentingnya keamanan komputer dan mampu mengenali ancaman seperti phishing. Namun, sebagian responden masih menunjukkan perilaku berisiko seperti membagikan kata sandi dan mengklik tautan mencurigakan. Meskipun pengetahuan mereka cukup baik, implementasi keamanan tidak selalu konsisten dalam praktik. Penelitian ini menyimpulkan bahwa diperlukan upaya pendidikan dan pelatihan berkelanjutan untuk mengubah kesadaran menjadi perilaku aman yang konsisten dalam menghadapi ancaman digital.

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi informasi, keamanan komputer telah menjadi salah satu aspek yang semakin penting. Sistem komputer dan informasi yang terhubung dalam jaringan global kini menjadi sasaran utama bagi berbagai ancaman digital yang dapat merusak integritas, kerahasiaan, dan ketersediaan data [1], [2], [3]. Dalam konteks ini, langkah-langkah untuk melindungi data dan sistem menjadi sangat penting, mengingat potensi kerugian yang dapat ditimbulkan oleh serangan yang terjadi. Oleh karena itu, perlindungan terhadap informasi yang ada di dalam komputer menjadi tantangan yang harus dihadapi di tengah kemajuan teknologi yang kian kompleks.

Dalam konteks keamanan komputer, ada tantangan khusus yang dihadapi oleh pengguna, terutama di kalangan mahasiswa yang terlibat langsung dengan teknologi setiap hari. Meskipun mahasiswa, khususnya di bidang Teknologi Informasi dan Komunikasi (JTIK), cenderung terpapar dengan berbagai ancaman, tidak semua menyadari potensi risiko yang ada dalam penggunaan sistem mereka [4]. Beberapa faktor, termasuk kebiasaan penggunaan perangkat dan pemahaman tentang ancaman yang ada, turut mempengaruhi seberapa efektif mereka dalam menjaga keamanan perangkat yang mereka gunakan [5], [6]. Hal ini menunjukkan perlunya pende

Diterima 5 April 2023; Disetujui 24 Juni 2023
Tersedia secara daring 30 Juni 2023
Dipublikasikan oleh Lontara Digitech Indonesia

katan yang lebih holistik dalam memahami bagaimana mahasiswa berperilaku terkait dengan upaya menjaga keamanan komputer, terutama dalam menghadapi ancaman yang semakin beragam dan canggih.

Beberapa penelitian sebelumnya telah mengidentifikasi pentingnya perlindungan terhadap komputer dan data, namun sering kali penelitian tersebut lebih fokus pada solusi teknis atau faktor eksternal yang mempengaruhi keamanan [7], [8], [9]. Meskipun demikian, penelitian yang mendalami perilaku individu, khususnya mahasiswa, dalam menjaga keamanan komputer mereka masih terbatas. Penelitian oleh Moustafa (2021) memberikan panduan tentang pentingnya tindakan pencegahan terhadap serangan digital, namun belum cukup menekankan pengaruh perilaku pengguna terhadap efektivitas perlindungan [10]. Oleh karena itu, masih terdapat kesenjangan penelitian yang perlu diisi, yakni pemahaman yang lebih mendalam mengenai bagaimana perilaku mahasiswa JTIK dalam merespons ancaman terhadap keamanan komputer dan langkah-langkah yang mereka ambil untuk mengatasi masalah tersebut

Melalui penelitian ini, diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai perilaku mahasiswa JTIK dalam menjaga keamanan komputer mereka. Fokus utama penelitian ini adalah untuk mengeksplorasi bagaimana mahasiswa mengidentifikasi dan merespons ancaman yang dapat mengganggu keamanan sistem yang mereka gunakan, serta langkah-langkah apa saja yang mereka terapkan untuk memitigasi risiko tersebut. Penelitian ini diharapkan memberikan kontribusi dalam meningkatkan kesadaran dan efektivitas strategi yang dapat diterapkan guna melindungi perangkat komputer, yang pada gilirannya akan menciptakan lingkungan digital yang lebih aman bagi mahasiswa.

2. METODE PENELITIAN

Pengumpulan data dalam penelitian ini dilakukan dengan menggunakan metode kuesioner yang disebarkan kepada mahasiswa/i Jurusan JTIK di Universitas Negeri Makassar (UNM). Kuesioner ini berfungsi untuk menggali pengalaman mahasiswa terkait keamanan komputer pribadi dan penggunaan media sosial mereka. Pengisian kuesioner dilakukan secara online menggunakan Google Form, yang memungkinkan responden untuk memberikan jawaban dengan lebih nyaman dan terstruktur, seolah-olah melakukan wawancara tidak langsung mengenai pengalaman mereka dalam menjaga keamanan perangkat. Metode ini memberikan kemudahan dalam pengumpulan data yang efisien dan meminimalkan bias responden [11]. Data yang terkumpul kemudian dianalisis menggunakan analisis deskriptif, yang bertujuan untuk menggambarkan pola dan karakteristik data yang ada secara sistematis [12]. Analisis ini akan mengungkapkan frekuensi dan distribusi jawaban mengenai pengetahuan dan tindakan mahasiswa dalam menghadapi ancaman terhadap keamanan komputer dan media sosial mereka

3. HASIL DAN DISKUSI

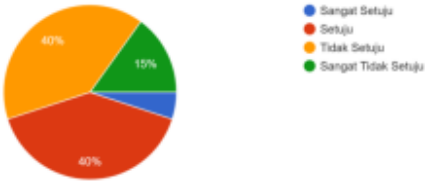
Dalam penelitian kami membagikan sebuah kusioner yang dimana kusionernya berisi 10 pertanyaan dengan 43 responden yang terkumpul melalui media google form. Pengguna yang mengisi kusioner kami yaitu hanya untuk mahasiswa JTIK yang berdasarkan pengalamannya saat menggunakan computer. Pertanyaan yang kami berikan pada kusioner memiliki tujuan agar kami dapat memastikan bahwa tingkat keamanan computer ini apakah sudah mencapai yang terbaik atau masih ada yang ingin di bedah/perbaiki lagi, serta kami ingin memastikan kesadaran mahasiswa/i pada saat menggunakan computer. Berikut adalah hasil penelitian dengan data sebagai berikut:

1. Saya menggunakan kata sandi yang berbeda untuk akun media sosial dan akun Syam OK saya.

Gambar 1. Kata Sandi Berbeda Untuk Akun Media Sosial

Berdasarkan data diatas dapat dilihat bahwa 30% responden menyatakan setuju, 55% menyatakan sangat setuju, 10% menyatakan tidak setuju, dan 5 % menyatakan sangat tidak setuju.

2. Saya membagikan kata sandi Syam OK saya dengan teman sekelas



Gambar 2. Membagikan Kata Sandi dengan Teman Sekelas

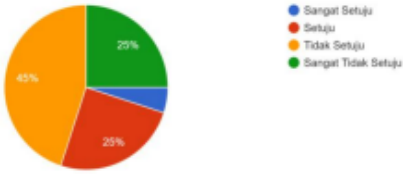
Berdasarkan data diatas dapat dilihat bahwa 40% responden menyatakan setuju, 40% menyatakan sangat setuju, 15% menyatakan tidak setuju, dan 5 % menyatakan sangat tidak setuju.

3. Saya menggunakan kombinasi huruf, angka, dan simbol di password Syam OK saya.

Gambar 3. Kombinasi Huruf, Angka dan Simbol di Password

Berdasarkan data diatas dapat dilihat bahwa 45% responden menyatakan setuju, 40% menyatakan sangat setuju, 15% menyatakan tidak setuju.

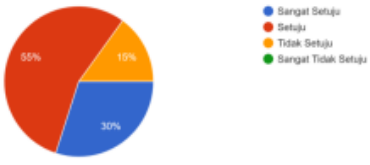
4. Saya membiarkan laptop, iPad, atau ponsel saya tidak terkunci saat belajar ruang kelas.



Gambar 4. Membiarkan Laptop, Ipad atau ponsel tidak terkunci

Berdasarkan data diatas dapat dilihat bahwa 25% responden menyatakan setuju, 5% menyatakan sangat setuju, 45% menyatakan tidak setuju, dan 25% menyatakan sangat tidak setuju.

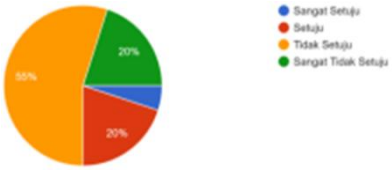
5. Saya tidak mengklik tautan/link di email, hanya jika itu berasal dari seseorang yang saya tidak kenal.



Gambar 5. Tidak Mengklik Tautan di Email jika berasal dari yang tidak dikenal

Berdasarkan data diatas dapat dilihat bahwa 55% responden menyatakan setuju, 30% menyatakan sangat setuju, dan 15% menyatakan tidak setuju.

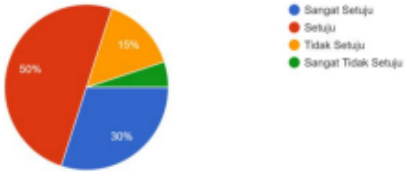
6. Jika email dari pengirim yang tidak saya kenal terlihat menarik, saya akan mengklik Link itu di email.



Gambar 6. Email dari Pengirim Yang Tidak Dikenal Terlihat Menarik, Saya Klik Link di Email

Berdasarkan data diatas dapat dilihat bahwa 20% responden menyatakan setuju, 5% menyatakan sangat setuju, 55% menyatakan tidak setuju, dan 20% menyatakan sangat tidak setuju.

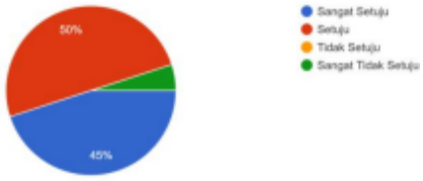
7. Saya tidak membuka lampiran email jika pengirimnya tidak saya kenal.



Gambar 7. Tidak Membuka Lampirkan Email Jika Pengirim Tidak Dikenal

Berdasarkan data diatas dapat dilihat bahwa 50% responden menyatakan setuju, 30% menyatakan sangat setuju, 15% menyatakan tidak setuju, dan 5% menyatakan sangat tidak setuju.

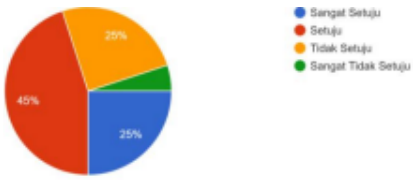
8. Saya dapat mengenali email phishing



Gambar 8. Mengenali Email Phishing

Berdasarkan data diatas dapat dilihat bahwa 50% responden menyatakan setuju, 45% menyatakan sangat setuju, dan 5% menyatakan sangat tidak setuju.

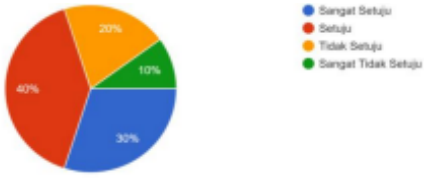
9. Saya mengunduh semua file di komputer kampus saya yang saya butuhkan untuk tugas saya.



Gambar 9. Unduh Semua File di Komputer Kampus untuk kebutuhan tugas

Berdasarkan data diatas dapat dilihat bahwa 45% responden menyatakan setuju, 25% menyatakan sangat setuju, 25% menyatakan tidak setuju, dan 5% menyatakan sangat tidak setuju.

10. Ketika saya memiliki akses ke Internet di kampus, saya mengunjungi semua situs web yang saya inginkan.



Gambar 10. Mengunjungi semua website saat memiliki akses internet di kampus

Berdasarkan data diatas dapat dilihat bahwa 40% responden menyatakan setuju, 30% menyatakan sangat setuju, 20% menyatakan tidak setuju, dan 10% menyatakan sangat tidak setuju.

4. PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa mayoritas mahasiswa di jurusan JTIK Universitas Negeri Makassar memiliki kesadaran yang tinggi terhadap pentingnya keamanan komputer dan mampu mengidentifikasi potensi ancaman, seperti phishing. Hasil ini didukung oleh penelitian sebelumnya, yang menemukan bahwa tingkat kesadaran yang lebih tinggi di kalangan mahasiswa

berhubungan dengan praktik yang lebih baik dalam melindungi diri dari ancaman daring [13], [14], [15]. Selain itu, Steen et al. (2020) menekankan bahwa kampanye pendidikan dan kesadaran sangat penting untuk meningkatkan kemampuan pengguna dalam mengenali dan merespons risiko terkait keamanan siber [16]. Oleh karena itu, tingkat kesadaran yang tinggi di kalangan mahasiswa dalam penelitian ini sejalan dengan pemahaman umum bahwa pengetahuan dan perilaku proaktif dapat secara efektif mengurangi risiko yang ditimbulkan oleh ancaman keamanan.

Selain itu, penelitian ini mengungkapkan bahwa meskipun sebagian besar mahasiswa sadar akan ancaman keamanan, beberapa masih melakukan perilaku berisiko, seperti membagikan kata sandi dengan teman sekelas. Temuan ini konsisten dengan penelitian sebelumnya, yang menunjukkan bahwa meskipun mahasiswa memiliki pengetahuan tentang keamanan siber, sejumlah besar masih terlibat dalam praktik tidak aman seperti berbagi kata sandi [17], [18]. Penelitian oleh Zulkifli et al. (2020) juga menunjukkan bahwa meskipun sadar akan langkah-langkah keamanan, sebagian pengguna tidak selalu melaksanakannya secara konsisten [19]. Hal ini menunjukkan bahwa meskipun tingkat kesadaran sudah tinggi, implementasi praktik keamanan yang baik memerlukan lebih dari sekadar pengetahuan perubahan perilaku dan tindakan yang konsisten sangat penting untuk menghindari kerentanannya seperti berbagi kata sandi.

Selanjutnya, hasil penelitian ini juga menunjukkan bahwa banyak mahasiswa masih gagal menghindari tindakan berisiko, seperti mengklik tautan email yang tidak diverifikasi, yang dapat menyebabkan serangan phishing. Perilaku ini serupa dengan yang ditemukan penelitian sebelumnya, yang menunjukkan bahwa pengguna sering kali meremehkan risiko dari tindakan yang tampaknya tidak berbahaya, seperti membuka email yang mencurigakan [20], [21]. Namun, beberapa mahasiswa dalam penelitian ini menunjukkan penilaian yang lebih baik, yang sejalan dengan penelitian Beu et al. (2023), yang menunjukkan bahwa pelatihan untuk mengenali percakapan phishing dapat meningkatkan respons [22]. Oleh karena itu, meskipun tingkat kesadaran sudah tinggi, penguatan perilaku ini melalui pelatihan praktis keamanan dan menciptakan budaya yang sadar akan keamanan sangat diperlukan untuk mengurangi kerentanannya.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa mayoritas mahasiswa Jurusan JTIK di Universitas Negeri Makassar menunjukkan kesadaran yang baik terhadap ancaman keamanan komputer, seperti phishing, dan mampu membedakan potensi risiko yang dapat membahayakan perangkat mereka. Namun, meskipun kesadaran ini ada, sebagian mahasiswa masih terlibat dalam perilaku berisiko, seperti membagikan kata sandi atau mengklik tautan tidak dikenal, yang dapat membuka peluang bagi serangan siber. Keterbatasan penelitian ini terletak pada jumlah sampel yang terbatas dan fokus hanya pada satu jurusan, yang mungkin tidak mewakili perilaku mahasiswa di universitas secara keseluruhan. Oleh karena itu, penelitian lebih lanjut disarankan untuk memperluas cakupan sampel dan mempertimbangkan berbagai faktor eksternal yang mempengaruhi perilaku mahasiswa dalam menjaga keamanan komputer mereka, serta meningkatkan program sosialisasi dan pelatihan yang lebih praktis untuk mengubah perilaku berisiko menjadi lebih aman.

REFERENSI

[1] S. Singh, P. Sharma, S. Moon, D. Moon, and J. Park, "A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions," The Journal of Supercomputing, vol. 1, pp. 1-32, 2019, doi: 10.1007/s11227-016-1850-4.

[2] O. Digilina, I. Teslenko, N. Muravyova, and A. Chekushov, "Information Security in a Digital Economy Deployment," pp. 1225-1230, 2021, doi: 10.1007/978-3-030-69415-9_133.

[3] J. Kizza, Cyber Crimes and Hackers, Texts in Computer Science, 2020, doi: 10.1007/978-1-4471-4543-1_5.
[4] M. Althobaiti, "Assessing User's Susceptibility and Awareness of Cybersecurity Threats," *Intelligent Automation and Soft Computing*, vol. 28, pp. 167-177, 2021, doi: 10.32604/IASC.2021.016660.
[5] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," *Education and Information Technologies*, vol. 26, pp. 1721-1736, 2020, doi: 10.1007/s10639-020-10330-0.
[6] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data Cogn. Comput.*, vol. 5, p. 23, 2021, doi: 10.3390/bdcc5020023.
[7] A. Subhani, I. Khan, and U. Ahmad, "Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students," *Journal of Advanced Research in Social Sciences and Humanities*, 2023, doi: 10.26500/jarssh-08-2023-0202.
[8] A. Elkhail, N. Lachtar, D. Ibdah, R. Aslam, H. Khan, A. Bacha, and H. Malik, "Seamlessly Safeguarding Data Against Ransomware Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, pp. 1-16, 2023, doi: 10.1109/TDSC.2022.3214781.
[9] H. Ping, "Network Information Security Data Protection Based on Data Encryption Technology," *Wireless Personal Communications*, vol. 126, pp. 2719-2729, 2022, doi: 10.1007/s11277-022-09838-0.
[10] A. Moustafa, A. Bello, and A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," *Frontiers in Psychology*, vol. 12, 2021, doi: 10.3389/fpsyg.2021.561011.
[11] J. R. Batmetan Suyoto, J. D. C. L. Suares, "An Empirical Investigation on Customer Behavior to Adopt Mobile Commerce among the Y Generation in Indonesia," Sriwijaya International Conference On Engineering, Science & Technology [SICEST 2016], 2016.
[12] J.L. Sidel, R.N. Bleibaum, and K.W.C. Tao, "Quantitative Descriptive Analysis," in *Descriptive Analysis in Sensory Evaluation*, S.E. Kemp, J. Hort, and T. Hollowood, Eds., 2018, doi: 10.1002/9781118991657.ch8.
[13] R. Raju, N. Hidayah, A. Rahman, and A. Ahmad, "Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution," *Asian Journal of University Education*, 2022, doi: 10.24191/ajue.v18i3.18967.
[14] H. Berry, "Survey of the Challenges and Solutions in Cybersecurity Awareness Among College Students," in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 2023, pp. 1-6, doi: 10.1109/ISDFS58141.2023.10131851.
[15] A. Garba, M. Siraj, S. Othman, and M. Musa, "A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach," 2020.
[16] T. Steen, E. Norris, K. Atha, and A. Joinson, "What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?," *J. Cybersecur.*, vol. 6, 2020, doi: 10.1093/cybsec/tyaa019.
[17] M. Alqahtani, "Factors Affecting Cybersecurity Awareness among University Students," *Applied Sciences*, 2022, doi: 10.3390/app12052589.
[18] M. Mohammed and D. Bamasoud, "The Impact of Enhancing Awareness of Cybersecurity on Universities Students: a Survey Paper," *Journal of Theoretical and Applied Information Technology*, vol. 100, 2022.
[19] Z. Zulkifli, N. Molok, N. Rahim, and S. Talib, "Cyber Security Awareness Among Secondary School Students in Malaysia," *Journal of Information Systems and Digital Technologies*, 2020, doi: 10.31436/jisdt.v2i2.151.
[20] C. Canfield, B. Fischhoff, and A. Davis, "Better beware: comparing metacognition for phishing and legitimate emails," *Metacognition and Learning*, vol. 14, pp. 343-362, 2019, doi: 10.1007/s11409-019-09197-5.
[21] D. Maimon, C. Howell, R. Perkins, C. Muniz, and T. Berenblum, "A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks," *Social Science Computer Review*, vol. 41, pp. 286-304, 2021, doi: 10.1177/08944393211046339.
[22] N. Beu, A. Jayatilaka, M. Zahedi, A. Babar, L. Hartley, W. Lewinsmith, and I. Baetu, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput. Secur.*, vol. 131, 103313, 2023, doi: 10.1016/j.cose.2023.103313.