

Analisa Kewaspadaan Generasi Z terhadap Keamanan Pribadi

Ade Mulyana¹, Egi Adithia Pradana^{2*}, Melani Faliana Putri³

^{1,2,3}Institut Bisnis dan Informatika Kesatuan, Bogor

Jl. Ranggagading No.1 Bogor, Jawa Barat

email: ademulyana@ibik.ac.id¹, egiadithia@ibik.ac.id², melanifaliana@ibik.ac.id³

* Penulis korespondensi

Diajukan: 20 Mei 2024

Direvisi: 3 Juni 2024

Diterima: 3 Juni 2024

Dipublikasikan: 31 Juli 2024

Abstract

Information security is one of the important things about information technology. The two are interrelated, so if one is not maintained, then the result is a leak of data or important information. Especially in the current era of globalisation, data is a very important "gold mine," because the data that is unguarded is an easy target for data thieves. On the other hand, in the current era, the use of information technology is increasing, especially with the increasing number of social media platforms and public services from both the government and the state. With these things, of course, people are becoming more intense in socialising and gathering digitally. This research uses a quantity survey method. The survey was conducted on several social media, which are often used by many people, especially by generation Z. This is based on research conducted by Nicolle Merrill regarding the use of social media for social research, "Using an exploratory online survey distributed through online social networks as an example. Based on this research, Gen Z, as a generation known as the digital generation, must pay more attention to personal and environmental digital security, be more alert, and not be easily tempted by unreasonable offers made on social media or communication media such as email or chat applications. Thus, it can be concluded that Generation Z, as a generation known as the digital generation, is already concerned about personal security, which includes the security of social media accounts and threats that might attack them.

Keyword: Information Security, Digital, Generation Z, Social Media, Awareness

Abstrak

Keamanan informasi merupakan hal penting dari teknologi informasi, keduanya saling terkait sehingga apabila tidak dijaga maka hasilnya adalah kebocoran data atau informasi penting. Data adalah "tambang emas" yang sangat penting, karena data yang tidak dijaga merupakan sasaran empuk bagi pencuri data. Disisi lain penggunaan teknologi informasi semakin tinggi terutama dengan semakin banyaknya platform media sosial, layanan publik dari pemerintah maupun negara, hal tersebut tentunya orang semakin intens untuk bersosialisasi dan berkumpul secara digital. Tujuan penelitian ini mengetahui kadar kewaspadaan generasi Z terkait keamanan dan kebiasaan menjaga data diri di media sosial. Metode survei kuantitas dilakukan di media sosial yang sering digunakan oleh generasi Z, hal ini berdasarkan penelitian Nicolle Merril tentang penggunaan media sosial untuk riset sosial, "Using an exploratory online survey distributed through online social networks as an example. Gen z sebagai generasi yang dikenal sebagai generasi digital harus lebih memperhatikan keamanan digital personal maupun lingkungan, bersikap lebih waspada serta tidak mudah tergiur akan tawaran kurang masuk akal yang dilakukan di media sosial maupun media komunikasi seperti email maupun aplikasi chat. Dengan demikian, disimpulkan bahwa generasi z sebagai generasi digital sudah memiliki kepedulian terhadap keamanan pribadi yang mencakup keamanan akun media sosial dan ancaman-ancaman yang mungkin dapat menyerang.

Kata Kunci: Keamanan Informasi, Digital, Generasi Z, Media Sosial, Kewaspadaan

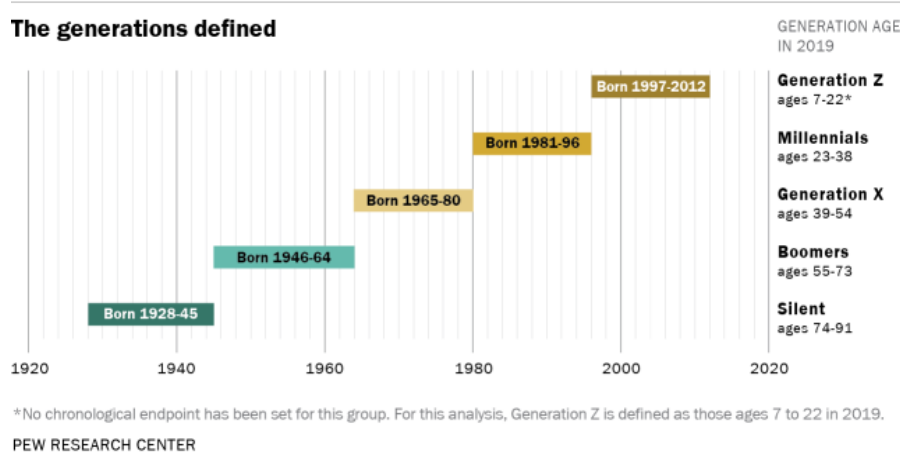
1. PENDAHULUAN

1.1. Latar Belakang

Keamanan informasi merupakan salah satu hal penting dari teknologi informasi, keduanya saling terkait sehingga bila salah satu tidak dijaga maka hasilnya adalah kebocoran data atau informasi penting, terutama di era globalisasi seperti saat ini, data adalah "tambang emas" yang sangat penting, karena data yang tidak dijaga merupakan sasaran empuk bagi para pencuri data.

Disisi lain pada era sekarang penggunaan teknologi informasi semakin tinggi terutama dengan semakin banyaknya platform media sosial, layanan publik baik dari pemerintah maupun negara, dengan hal-hal tersebut tentu saja orang semakin intens untuk bersosialisasi dan berkumpul secara digital.

Generasi Z atau yang lebih dikenal Gen Z adalah generasi yang lahir pada tahun 1997 sampai ke 2012 berdasarkan penelitian yang dilakukan oleh Pew Research.



Gambar 1. Klasifikasi umur antar generasi

Milenial adalah pionir digital, namun Gen Z adalah generasi digital sejati, Pola Pikir Generasi Z: Gen Z cepat mengadopsi saluran komunikasi baru dan lebih memilih komunikasi digital yang real-time, transparan, dan kolaboratif, (Jenkins, Ryan, (APJII, 2024) (We Are Social, 2024) (Komalasari, 2018) (Maulana, 2022), 2019).

Penelitian ini bertujuan untuk mengetahui kadar kewaspadaan dari generasi Z terkait dengan keamanan dan kebiasaan dalam menjaga data diri di media sosial sehingga bisa dapat menjadi acuan di masa depan.

1.2. Penetrasi Internet

Dari survei terkait penetrasi internet di Indonesia yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) 18 Desember 2023 sampai ke 19 Januari 2024, bahwa pengguna internet terbesar adalah Gen Milenial dengan prosentase sebesar 93,17 % disusul oleh gen Z sebesar 87,02% (APJII, 2024, "Survei Penetrasi Internet Indonesia 2024")

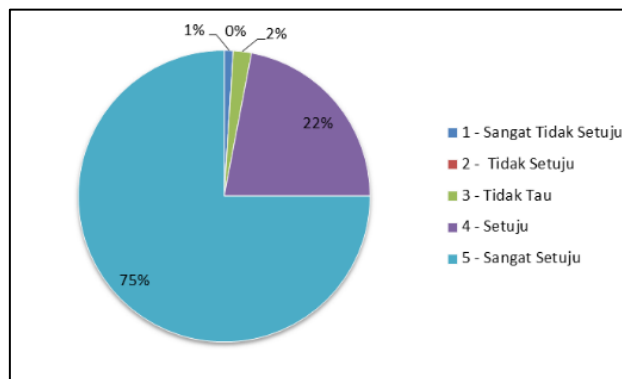
2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode survei kuantitas, survei dilakukan di beberapa media sosial yang sering digunakan oleh banyak orang terutama oleh generasi Z, hal ini berdasarkan penelitian yang dilakukan oleh Nicolle Merril tentang penggunaan media sosial untuk riset sosial, "Using an exploratory online survey distributed through online social networks as an example, the author gathers data on the use of social media in international higher education recruiting and outreach." (Merril, Nicolle, Emerald Group Publishing Limited, 2011), penelitian ini menggunakan media sosial seperti Twitter dan Facebook dikarenakan mayoritas anak muda menggunakan internet untuk media sosial sebesar (84,37% (Badan Pusat Statistik, 2023), sedangkan platform media sosial terbesar saat ini adalah Youtube sebesar 100%, kemudian Whatsapp sebesar 83,4% (We Are Social, Digital 2024 April Global Statshot Report, April 2024) dan pengguna terbesar dari email, pengunjung *brand website* serta yang paling aktif melakukan digitalisasi kehidupan adalah gen Z (We Are Social, Digital 2024 April Global Statshot Report, April 2024)

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Berdasarkan survei kuantitas yang dilakukan di beberapa media sosial yang sering digunakan oleh generasi Z, didapatkan hasil sebagai berikut (Gambar 2).



Gambar 2. Diagram 1 Pentingnya menjaga data pribadi

Diagram di atas menunjukkan bahwa rata-rata dari jumlah jawaban yang diberikan terhadap pertanyaan yang diajukan, responden menyetujui terkait pentingnya menjaga keamanan data pribadi seperti biodata, rekening, media sosial, dan lainnya. Hal ini dapat diketahui karena 75% dari total 100 responden atau sama dengan 75 responden memberikan nilai 5 (sangat setuju). Sementara 22% dari total 100 responden atau sama dengan 22 responden memberikan nilai 4 (setuju). Dengan demikian dapat disimpulkan bahwa 97 dari 100 responden menyetujui bahwa keamanan data pribadi seperti biodata, rekening, media sosial, dan yang lainnya sangat penting untuk dijaga kerahasiaannya.

3.2. Pembahasan

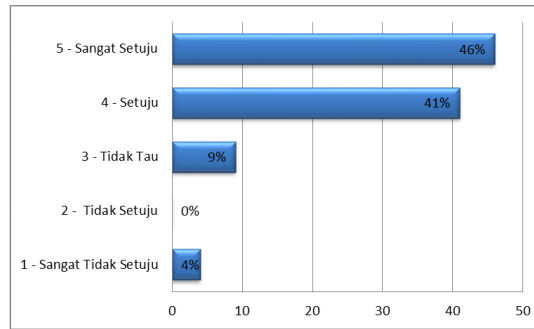
3.2.1. Profil Informan

Menurut Moeleong (dalam Khosiah, dkk., 2017: 143), informan adalah orang yang dimanfaatkan untuk memberikan informasi tentang situasi dan kondisi latar penelitian. Sementara Bungin (dalam Nurdiansyah & Rugoyah, 2021: 159) mengungkapkan bahwa informan adalah orang yang diwawancarai, dimintai informasi oleh pewawancara, yang diperkirakan menguasai dan memahami data, informasi, ataupun fakta dari suatu objek penelitian. Dari kedua definisi di atas dapat disimpulkan bahwa informan adalah orang yang diwawancarai dan dimintai informasi tentang situasi dan kondisi latar penelitian.

Informan pada penelitian ini adalah generasi z, yaitu pada batas usia 12 - 27 tahun pada tahun 2024. Informan tidak dibatasi dalam bidang pekerjaan, etnis, dan lainnya. Namun, informan pada penelitian ini merupakan generasi z yang memiliki dan menggunakan media sosial di dalam kehidupannya sehari-hari.

3.2.2. Kepedulian Pengguna dengan *Password* atau Kata Sandi yang Rumit

Berdasarkan survei kuantitas yang dilakukan dengan penyebaran kuesioner melalui beberapa media sosial dengan kurun waktu selama 14 (empat belas) hari atau 2 (dua) minggu dan jumlah responden sebanyak 100 orang serta jumlah pertanyaan sebanyak 14 (empat belas) pertanyaan yang diajukan kepada responden melalui Google Form, didapatkan hasil bahwa rata-rata keseluruhan responden memiliki tingkat kepedulian terhadap pentingnya penggunaan *password* atau kata sandi yang rumit. Hal ini dapat dilihat melalui diagram yang menunjukkan hasil jawaban setiap responden dalam bentuk persentase berikut (Gambar 3).

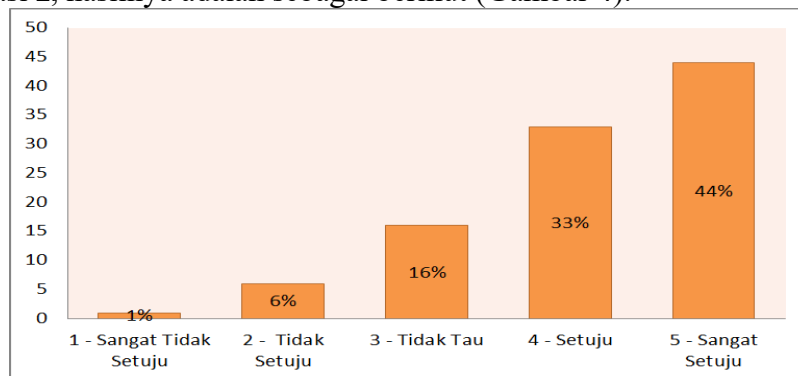


Gambar 3. Diagram Kepedulian pengguna terhadap kata sandi yang rumit

Pada diagram di atas tampak bahwa 46% dari total 100 responden atau sama dengan 46 responden sangat setuju terhadap pentingnya penggunaan kata sandi yang rumit untuk menjaga keamanan data pribadi. Sementara 41% dari total 100 responden atau sama dengan 41 responden setuju terhadap pentingnya penggunaan kata sandi yang rumit, dan hanya 4% dari total 100 responden atau sama dengan 4 responden yang sangat tidak setuju terkait pentingnya penggunaan kata sandi yang rumit. Hal ini menunjukkan bahwa total 87% dari total 100 responden atau sama dengan 87 responden menyetujui dan memiliki kepedulian yang tinggi terkait pentingnya penggunaan kata sandi yang rumit untuk menjaga keamanan data pribadi pada media sosial yang digunakan.

3.2.3. Pentingnya Kombinasi *Password* atau Kata Sandi 8 Karakter

Yamin, dkk. (2023: 43) mengungkapkan bahwa *password* atau kata sandi adalah serangkaian karakter yang digunakan untuk mengautentikasi pengguna pada sistem komputer. Dalam bidang komputer *password* atau kata sandi adalah deretan karakter yang dimasukkan untuk mendapatkan akses terhadap *file*, aplikasi, atau sistem komputer. *Password* atau kata sandi yang kuat merupakan kombinasi huruf kecil, huruf besar, angka, dan karakter khusus yang panjangnya minimal 8 karakter (Komalasari, 2018: 142). Dengan demikian dapat diketahui bahwa *password* atau kata sandi yang sebaiknya digunakan terdiri dari deretan karakter kombinasi yang panjang minimalnya adalah 8 karakter. Berdasarkan hasil survei terkait pentingnya kombinasi *password* atau kata sandi 8 karakter yang dilakukan kepada 100 responden generasi z, hasilnya adalah sebagai berikut (Gambar 4).

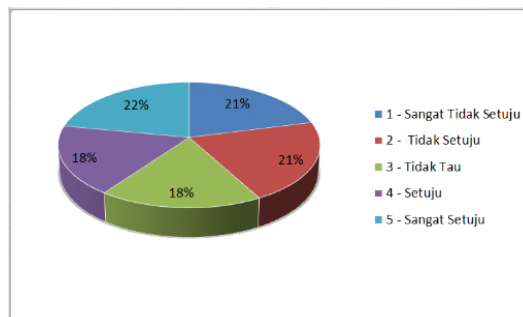


Gambar 4. Diagram Pentingnya kombinasi *password* atau kata sandi 8 karakter

Pada diagram di atas dapat dilihat bahwa 44% dari 100 responden atau sama dengan 44 responden sangat setuju bahwa kata sandi yang kuat merupakan kata sandi yang merupakan kombinasi dari 8 karakter, dan 33% dari 100 responden atau sama dengan 33 responden juga setuju dengan hal tersebut. Berdasarkan hasil survei, hanya 1% dari 100 responden atau sama dengan 1 responden yang sangat tidak setuju terhadap pentingnya kombinasi kata sandi 8 karakter. Dengan demikian dapat disimpulkan bahwa 77% dari 100 responden atau sama

dengan 77 responden generasi z sudah memiliki kepedulian dan pengetahuan terkait pentingnya penggunaan kata sandi yang kuat untuk media sosial yang digunakannya.

3.2.4. Kerumitan Kombinasi *Password* atau Kata Sandi

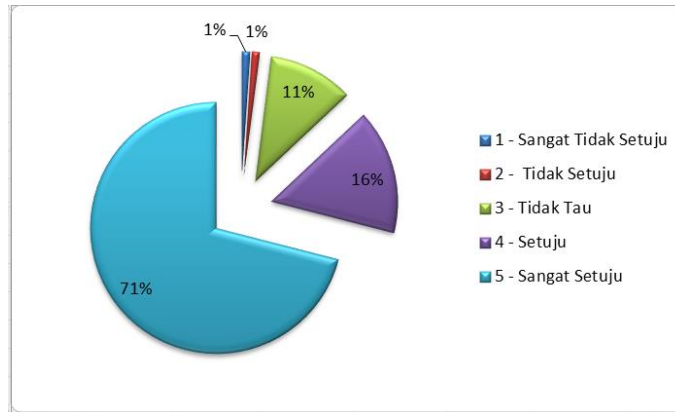


Gambar 5. Kerumitan kombinasi *password* atau kata sandi

Berdasarkan hasil survei yang telah dilakukan, dapat dilihat pada diagram 4 bahwa 42% atau sama dengan 42 responden yang merupakan penggabungan dari 21% (21 responden) yang sangat tidak setuju dan 21% (21 responden) yang tidak setuju menyatakan tidak setuju bahwa kombinasi *password* atau kata sandi itu merepotkan. Sementara 40% atau sama dengan 40 responden yang merupakan penggabungan dari 22% (22 responden) yang sangat setuju dan 18% (18 responden) yang setuju bahwa kombinasi *password* atau kata sandi itu merepotkan. Dengan demikian dapat diketahui bahwa sebagian generasi z sebagai pengguna media sosial menganggap bahwa kombinasi *password* atau kata sandi adalah hal yang tidak merepotkan dan sebagian lagi menganggap sebaliknya. Oleh karena itu, kesadaran terkait pentingnya kerumitan *password* yang dapat menjaga keamanan data pribadi harus lebih ditanamkan kepada generasi z yang saat ini sangat fasih terhadap media sosial.

3.2.5. Keamanan Akun Media Sosial

Sinaga (2020: 3) mengungkapkan bahwa keamanan adalah kondisi yang menunjukkan keadaan bebas dari bahaya maupun ancaman. Sementara menurut Wardani (dalam Syahindra, dkk., 2022: 165), keamanan adalah bagian penting dalam proses tata kelola teknologi informasi guna mengurangi celah ancaman pada aset yang meliputi kerahasiaan, keutuhan dan ketersediaannya. Dari kedua definisi diatas dapat disimpulkan bahwa keamanan adalah bagian penting dalam proses tata kelola teknologi informasi guna terciptanya kondisi atau keadaan bebas dari bahaya maupun ancaman. Keamanan sangat dibutuhkan dalam berbagai aspek kehidupan termasuk pada penggunaan media sosial. Keamanan media sosial merupakan suatu kondisi aman dari laman atau aplikasi dalam jaringan sosial. Keamanan akun media sosial menjadi hal yang krusial bagi generasi z. Hal ini dapat dilihat pada diagram 5 yang menunjukkan data bahwa 71% atau sama dengan 71 responden sangat setuju dan 16% atau sama dengan 16 responden setuju bahwa akun media sosial harus diamankan dari pihak-pihak yang tidak bertanggung jawab.

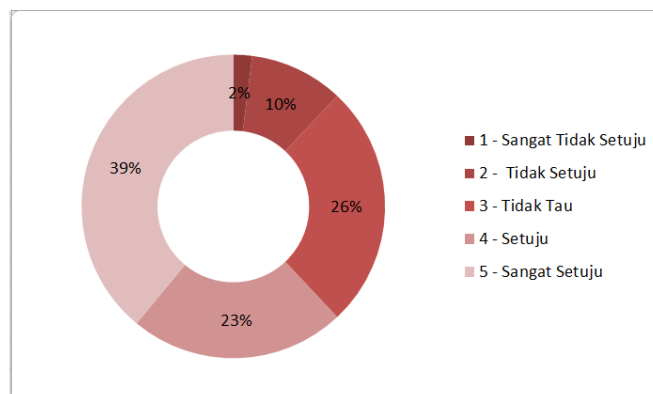


Gambar 6. Diagram Keamanan akun media sosial

Selain itu, dapat dilihat juga pada pada diagram 5 bahwa hanya 1% atau sama dengan 1 responden yang sangat tidak setuju, 1% atau sama dengan 1 responden yang tidak setuju bahwa akun media sosial harus diamankan. Sementara sisanya tidak tahu bahwa akun media sosial harus diamankan. Dengan demikian dapat disimpulkan bahwa hampir keseluruhan responden telah memiliki tingkat kewaspadaan terkait keamanan akun media sosial yang tinggi.

3.2.6. Pembaruan Keamanan Akun Media Sosial

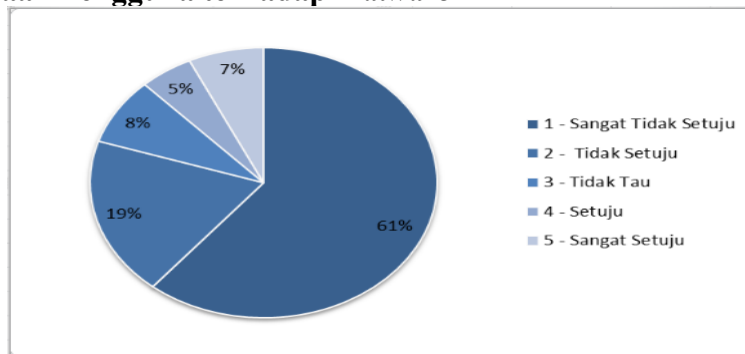
Pembaruan merupakan proses, cara, perbuatan membarui (KBBI IV). Sementara keamanan adalah bagian penting dalam proses tata kelola teknologi informasi guna terciptanya kondisi atau keadaan bebas dari bahaya maupun ancaman, dan media sosial merupakan laman atau aplikasi yang memungkinkan pengguna dapat membuat dan berbagi isi atau terlibat dalam jaringan sosial. Sehingga dapat disimpulkan bahwa pembaruan keamanan akun media sosial merupakan proses atau cara membarui kondisi aman dari laman atau aplikasi dalam jaringan sosial sehingga kondisi aman tersebut dapat tetap terjaga eksistensinya. Oleh karena itu, pembaruan keamanan akun media sosial harus dilakukan secara rutin oleh pengguna akun media sosial. Hasil survei yang berkaitan dengan kesadaran pentingnya pembaruan keamanan akun media sosial dapat dilihat pada diagram 6 berikut.



Gambar 7. Diagram Pembaruan akun media sosial

Pada diagram di atas dapat dilihat bahwa 62% dari 100 responden menyetujui bahwa pembaruan keamanan akun media sosial harus dilakukan secara rutin, dan hanya 12% dari 100 responden yang tidak menyetujui hal tersebut. Sehingga dapat disimpulkan bahwa generasi z yang menggunakan akun media sosial telah menyadari akan pentingnya pembaruan keamanan akun media sosial secara rutin agar akun media sosial tidak dapat diretas oleh pihak-pihak yang tidak bertanggung jawab.

3.2.7. Kewaspadaan Pengguna terhadap *Malware*

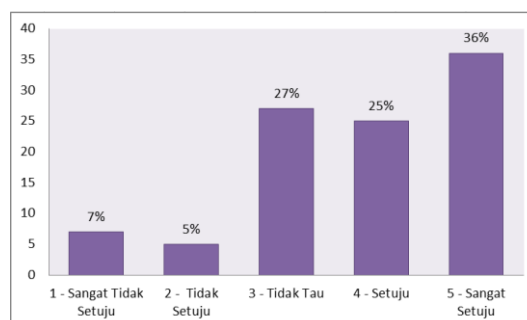


Gambar 8. Diagram Kewaspadaan pengguna terhadap *malware*

Malware merupakan suatu *software* yang dibuat untuk tujuan tertentu dengan mencari celah keamanan sistem (Adenansi & Novaria, 2017: 38). Selain itu, *malware* juga dapat diartikan sebagai perangkat lunak yang sengaja dirancang untuk mencuri data, memanipulasinya, dan mendapatkan akses penuh ke server yang terinfeksi (Prayitno, dkk., 2022: 53). Dari kedua pengertian di atas, maka dapat disimpulkan bahwa *malware* merupakan perangkat lunak yang sengaja dibuat untuk mencari celah keamanan dan mencuri data. Oleh karena itu, *malware* merupakan salah satu ancaman keamanan pengguna media sosial. *Malware* dapat dikirimkan oleh orang yang tidak bertanggung jawab dalam berbagai bentuk, salah satunya adalah dalam bentuk *file*. Dengan demikian, pengguna harus lebih waspada terhadap *file-file* yang dikirimkan oleh orang yang tidak dikenal. Hasil survei terkait hal ini dapat dilihat pada diagram 7 di atas. Pada diagram di atas dapat disimpulkan bahwa 80% dari 100 responden atau sama dengan 80 responden setuju bahwa pengguna tidak seharusnya membuka *file-file* yang dikirimkan oleh orang-orang yang dikenal. Hal ini menunjukkan bahwa generasi z telah memiliki tingkat kewaspadaan dan pengetahuan yang cukup terkait *malware*.

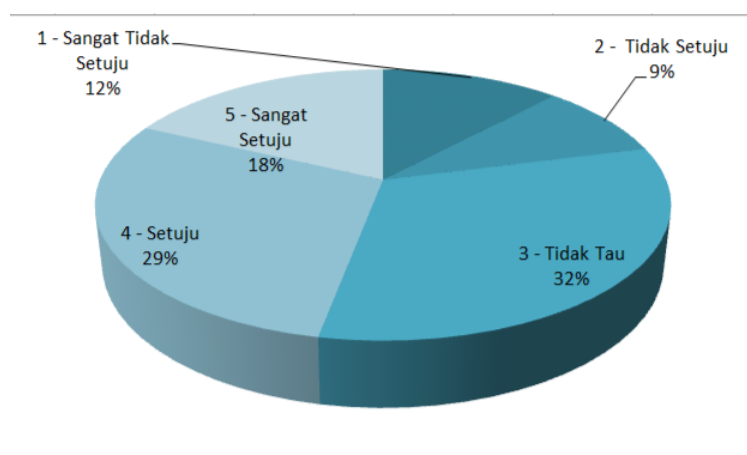
3.2.8. Penggunaan Fitur Keamanan *2FA*

2FA atau yang dikenal dengan *Two Factor Authentication* merupakan proses keamanan sistem informasi di mana dua cara identifikasi digabungkan untuk meningkatkan kemungkinan bahwa suatu entitas, umumnya pengguna komputer, adalah pemegang yang sah dari entitas tersebut (Allen & Pickup dalam (Maulana, 2020: 23)). Berdasarkan definisi tersebut, dapat diketahui bahwa *2FA* dapat meningkatkan keamanan akun media sosial yang digunakan oleh generasi z. Oleh karena itu, penggunaan *2FA* terus meningkat seiring perkembangan waktu. Hal ini dapat dilihat pada diagram 8 yang menunjukkan bahwa sebanyak 61% dari 100 responden atau sama dengan 61 responden menyetujui bahwa *2FA* merupakan salah satu solusi keamanan terhadap akun media sosial yang digunakan oleh generasi z saat ini. Akan tetapi, masih terdapat 27 responden (27%) yang belum mengetahui fitur *2FA*, sehingga perlu adanya sosialisasi lebih mendalam terkait penggunaan fitur *2FA* terhadap generasi z yang menggunakan media sosial.



Gambar 9. Diagram Penggunaan fitur keamanan *2FA*

3.2.9. Pengaruh Fitur Keamanan 2FA terhadap Keamanan Akun Media Sosial

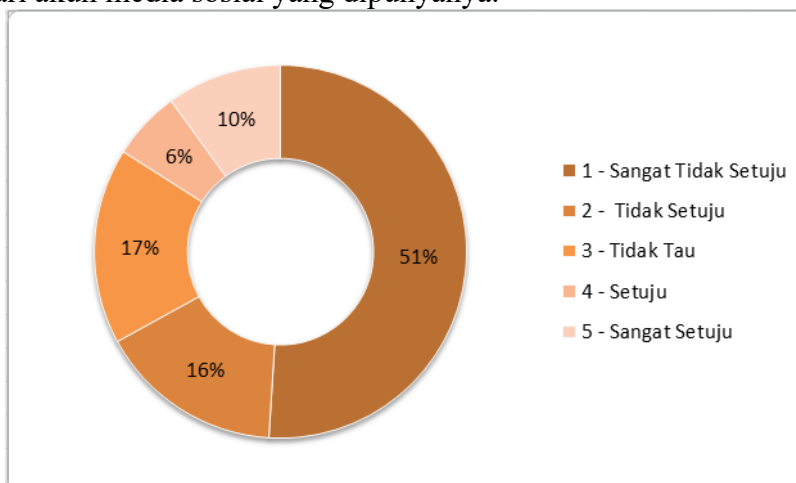


Gambar 10. Diagram Pengaruh fitur keamanan 2FA terhadap keamanan akun media sosial

Pada diagram diatas menunjukkan hasil yang positif terkait kepedulian generasi z selaku pengguna media sosial terhadap fitur keamanan 2FA. Namun, ternyata sebanyak 32% dari 100 responden atau sama dengan 32 responden tidak mengetahui pengaruh dari fitur keamanan 2FA terhadap keamanan akun media sosial yang dipunyanya. Oleh karena itu diperlukannya sosialisasi lebih mendalam terkait pengaruh fitur keamanan 2FA terhadap keamanan akun media sosial kepada generasi z.

3.2.10. Kepedulian Pengguna terhadap Keamanan Password atau Kata Sandi

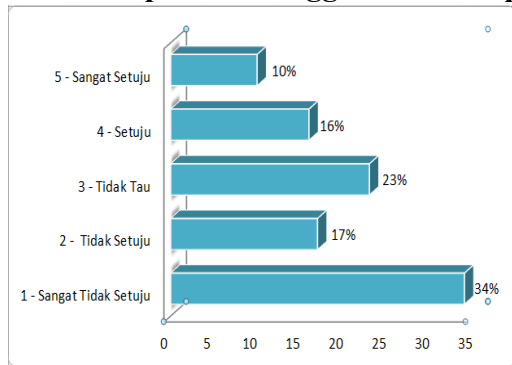
Password atau kata sandi merupakan hal yang sangat krusial bagi akun media sosial. Jika *password* atau kata sandi suatu akun tersebar maka data-data pada akun tersebut otomatis akan ikut tersebar. Oleh karena itu, perlunya kesadaran pengguna terhadap keamanan *password* atau kata sandi dari akun media sosial yang dipunyanya.



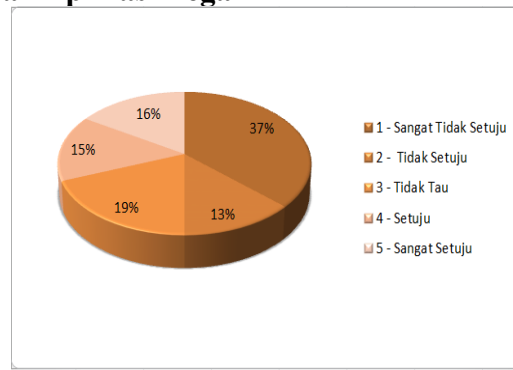
Gambar 11. Diagram Kepedulian pengguna terhadap keamanan password atau kata sandi

Berdasarkan hasil survei yang dilakukan, dapat dilihat pada diagram diatas yang menunjukkan bahwa sebanyak 67% dari 100 responden atau sama dengan 67 responden tidak menyetujui bahwa *password* atau kata sandi boleh dibagikan ke relasi. Data ini sudah menunjukkan bahwa generasi z telah mempunyai kepedulian sebagai pengguna media sosial terhadap keamanan *password* atau kata sandi.

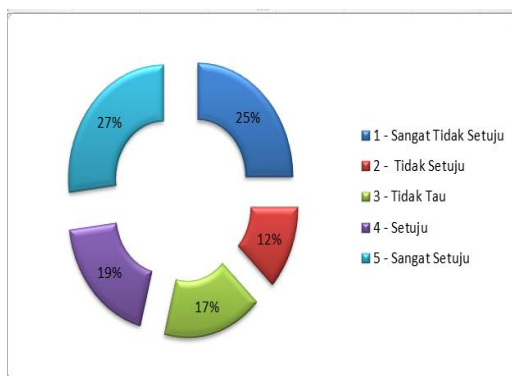
3.2.11. Kewaspadaan Pengguna terhadap Situs dan Aplikasi Ilegal



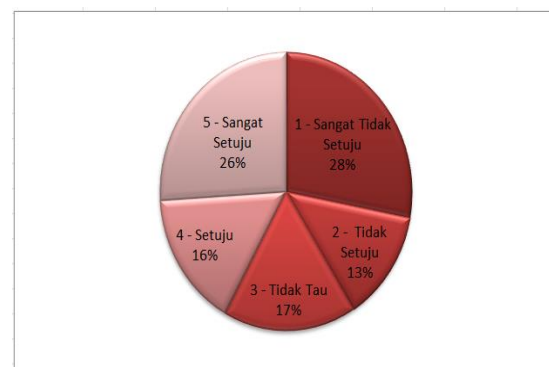
Gambar 12. Diagram Tingkat kewaspadaan Pengguna terhadap situs *torrent*



Gambar 13. Diagram Tingkat kewaspadaan pengguna terhadap *streaming* ilegal



Gambar 14. Diagram Tingkat kewaspadaan pengguna terhadap aplikasi bajakan



Gambar 15. Diagram Tingkat kewaspadaan pengguna terhadap aplikasi ilegal

Berbagai virus dan *malware* yang menyerang akun media sosial dapat berasal dari situs maupun aplikasi ilegal. Oleh karena itu, perlunya kewaspadaan pengguna akun media sosial terhadap situs dan aplikasi ilegal. Berdasarkan hasil survei yang dapat di lihat pada diagram 11, diagram 12, diagram 13, dan diagram 14 yang menunjukkan bahwa lebih dari 50% dari 100 responden tidak pernah membuka situs *torrent* dan *streaming* ilegal, namun pernah mengunduh aplikasi bajakan dan ilegal. Dengan demikian dapat disimpulkan bahwa tingkat kewaspadaan generasi z sebagai pengguna akun media sosial masih harus ditingkatkan pada penggunaan aplikasi ilegal atau dan aplikasi bajakan yang dapat membahayakan keamanan data pribadi yang tersimpan pada akun media sosial.

4. SIMPULAN

Berdasarkan penelitian ini, 97 dari 100 responden yang merupakan generasi z menyetujui bahwa keamanan data pribadi seperti biodata, rekening, media sosial, dan yang lainnya sangat penting untuk dijaga kerahasiaannya. Pernyataan tersebut dapat diperkuat dengan beberapa hasil survei yang dilakukan menunjukkan 87 dari 100 responden menyetujui dan memiliki kepedulian yang tinggi terkait pentingnya penggunaan kata sandi yang rumit untuk menjaga keamanan data pribadi pada media sosial yang digunakan, 77 dari 100 responden generasi z memiliki kepedulian dan pengetahuan terkait pentingnya penggunaan kata sandi yang kuat untuk media sosial yang digunakannya, 87 dari 100 responden setuju bahwa akun media sosial harus diamankan dari pihak-pihak yang tidak bertanggung jawab, dan 62 dari 100 responden menyetujui bahwa pembaruan keamanan akun media sosial harus dilakukan secara rutin. Generasi z selaku responden dari penelitian ini tidak hanya memiliki kepedulian terhadap

keamanan akun media sosial yang dipunyanya saja, namun generasi z selaku responden juga memiliki kepedulian terhadap gangguan atau ancaman yang mungkin dapat menyerang keamanan akun media sosial yang dipunyanya. Hal ini dapat diperkuat dengan hasil survei yang dilakukan menunjukkan 80 dari 100 responden atau sama dengan 80 responden setuju bahwa pengguna tidak seharusnya membuka *file-file* yang dikirimkan oleh orang-orang yang dikenal, 67 dari 100 responden tidak menyetujui bahwa *password* atau kata sandi boleh dibagikan ke relasi, dan lebih dari 50 dari 100 responden tidak pernah membuka situs *torrent* dan streaming ilegal. Dengan demikian, dapat disimpulkan bahwa generasi z sebagai generasi yang dikenal sebagai generasi digital sudah memiliki kepedulian terhadap keamanan pribadi yang mencakup keamanan akun media sosial dan ancaman-ancaman yang mungkin dapat menyerang. Namun, generasi z tetap harus memperhatikan keamanan digital personal maupun lingkungan, bersikap lebih waspada serta tidak mudah tergiur akan tawaran-tawaran kurang masuk akal yang dilakukan di media sosial maupun media komunikasi seperti email maupun aplikasi *chat*.

DAFTAR PUSTAKA

- Adenansi, R., & Novaria, L. (2018). Kesadaran akan keamanan penggunaan username dan password. *Tematik - Jurnal Teknologi Informasi dan Komunikasi*, Vol 5 (2), 141-152.
- APJII. (2024). *Survei Penetrasi Internet Indonesia*. Jakarta: APJII.
- Jenkins, Ryan. (2019). *The Generation Z Guide: The Complete Manual to Understand, Recruit, and Lead the Next Generation*. Ryan Jenkins, LLC.
- Komalasari, R. (2018). Kesadaran akan Keamanan Penggunaan Username dan Password. *TEMATIK*, 141-152.
- Khosiah., Hajrah., & Syafril. (2017). Persepsi Masyarakat terhadap Rencana Pemerintah Membuka Area Pertambangan Emas di Desa Sumi Kecamatan Lambu Kabupaten Bima. *Jurnal Ilmu Sosial dan Pendidikan*, 1(2), 141-149.
- Maulana, C. (2022). Rancang Bangun Sistem Informasi Pemesanan Barang Menggunakan Two Factor Authentication.
- Nurdiansyah, F., & Rugoyah, H.S. (2021). Strategi *Branding* Bandung Giri Gahana Golf Sebelum dan Saat Pandemi Covid-19. *Jurnal Purnama Berazam*, 2(2), 153-171.
- Prayitno, D., Santoso, N.A., & Kurniawan, R.D. (2022). Systematic Literature Review: Implementasi Metode Statis Dan Dinamis Pada Analisa Malware. *Simetris - Jurnal Teknologi Dan Sains Terapan*, 53-57.
- Pradana, E. A., Mursidayanti, S., & Putry, A. A. (2023). Rancang Bangun Media Praktikum Mata Kuliah Sistem Operasi Dengan Kernel Virtual Machine Server Terintegrasi Dengan Sistem Akademik. *Indo-Math Edu Intellectuals Journal*, 1237-1248.
- R, S. M. (2023). Implementasi Two-Factor Authentication (2FA) Dengan Aplikasi Authy dalam Sistem Informasi untuk Meningkatkan Keamanan Akses Pengguna.
- Sadikin, N., & Mahardika, M. S. (2024). Implementasi Keamanan Server Domain Controller Active Directory Domain Services terhadap Berbagai Threat dan Attack. *Jurnal Maklumatika*, 11(1), 12–21. Retrieved from <https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/254>

Sinaga, A.S. (2020). *Keamanan Komputer*. Solok: Insan Cendekia Mandiri.

Syahindra, I.P.S., Primasari, C.H., & Irianto, A.B.P. (2022). Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi XYZ Menggunakan Indeks KAMI dan ISO 27005 : 2011. *Jurnal Teknoinfo*, 16(2), 165-182

Yamin, M., Malethi, T.T., Monica., Jodhika., & Natali, S. (2023). Evaluasi Risiko pada Penggunaan *Password* yang Lemah: Analisis Kasus Penggunaan *Password* Umum. *Jurnal Ilmiah Multidisiplin Ilmu Komputer*, 41-48.

We Are Social. (2024). *Digital 2024 April Global Statshot*. We Are Social.