Kacanegara Jurnal Pengabdian Pada Masyarakat
ISSN: 2615-6717 (Print)
ISSN: 2657-2338 (On Line)
Terakreditasi Sinta 4 dari Kemenristekdikti No: 105/E/KPT/2022
DOI: 10.28989/kacanegara.v7i3.2106

Upaya peningkatan kesadaran keamanan data bagi guru Bahasa Inggris SMA di Kabupaten Bantul

Rianto Rianto[1,*], Iwan Hartadi Tri Untoro[2]
[1,2] Program Studi Sains Data, Universitas Teknologi Yogyakarta, Indonesia

Article Info

Article history:

Received January 31, 2024
Accepted February 16, 2024
Published Agustus 1, 2024

Kata Kunci:

Cyber-crime
Keamanan data
Smartphone

ABSTRAK

Saat ini, telepon cerdas *(smartphone)* bukan hanya alat untuk berkomunikasi, tetapi merupakan alat bantu dalam menyelesaikan pekerjaan manusia sehari-hari. Hal ini karena kemajuan teknologi yang berhasil memadukan kecanggihan telekomunikasi dan teknologi informasi dalam satu genggaman. Namun, intensitas penggunaan *smartphone* yang tinggi ini menimbulkan celah dalam keamanan data dan informasi bagi penggunanya. Pengabdian kepada Masyarakat (PKM) ini bertujuan untuk meningkatkan kesadaran pengguna *smartphone* dalam keamanan data dan informasi sehingga kejahatan dunia maya dapat diminimalkan. PKM ini termotivasi dari data hasil kuesioner mengenai kesadaran keamanan data dan informasi bagi guru Bahasa Inggris pada Sekolah Menengah Atas (SMA) di kabupaten Bantul. Sebagai tindak lanjut kemudian diadakan *Workshop on Digital Literacy: Internet & Mobile Security*. Meskipun banyak faktor yang dapat mempengaruhi terjadinya kejahatan dunia maya *(cyber-crime)*, tetapi *workshop* ini berhasil membekali peserta dengan pengetahuan dasar untuk meminimalkannya.

Corresponding Author:

Rianto Rianto,
Program Studi Sains Data,
Universitas Teknologi Yogyakarta,
Jl. Siliwangi, Jombor, Sleman, Yogyakarta, Indonesia 55285.
Email: *rianto@staff.uty.ac.id

1. PENDAHULUAN

Teknologi telekomunikasi yang kian berkembang berhasil mengubah sinyal analog menjadi sinyal digital. Dampak perkembangan teknologi komunikasi ini mampu mengubah perilaku hidup manusia di semua aspek. *Smartphone* adalah salah satu temuan teknologi di era digital yang berhasil menggeser komputer sebagai alat untuk menunjang pekerjaan manusia sehari-hari. Fleksibilitas merupakan kata kunci sehingga menyebabkan pengguna *smartphone* terus meningkat. Hal ini dikarenakan, dengan menggunakan *smartphone* seseorang dapat mengakses sumber daya internet dengan nyaman dimanapun [1].

Smartphone merupakan gabungan antara teknologi komunikasi dan teknologi informasi, sehingga memiliki sumber daya yang lebih. Didukung dengan aplikasi-aplikasi berbasis *mobile* yang terus berkembang, menjadikannya seperti asisten digital bagi pemiliknya. Kemampuan yang dimiliki *smartphone* ini bukan semata karena teknologi, tetapi juga oleh sistem pembelajaran mesin dan data yang diperoleh sehingga mengerti konteks. Agar dapat mengerti konteks, *smartphone* membutuhkan data dari penggunanya termasuk data-data yang bersifat pribadi. Hal ini tentu akan menimbulkan masalah baru yang dinamakan pelanggaran privasi [2].

Situasi tersebut mengharuskan pengguna *smartphone* memiliki pengetahuan dasar mengenai privasi data dan kejahatan dunia maya yang mungkin terjadi. Sayangnya, masih banyak pengguna *smartphone* yang tidak memperhatikan dan bahkan tidak mengetahui hal tersebut. Sebenarnya masalah ini bukan semata-mata kesalahan pengguna, tetapi memang masih banyak aplikasi *mobile* yang tidak memberikan perlindungan standar terhadap privasi penggunanya [3].

Beberapa data yang biasa diminta *smartphone* antara lain lokasi, kontak, galeri, dan lain-lain. Faktor ketidaktahuan pengguna dapat menyebabkan pemberian akses penuh kepada orang lain terhadap data-data

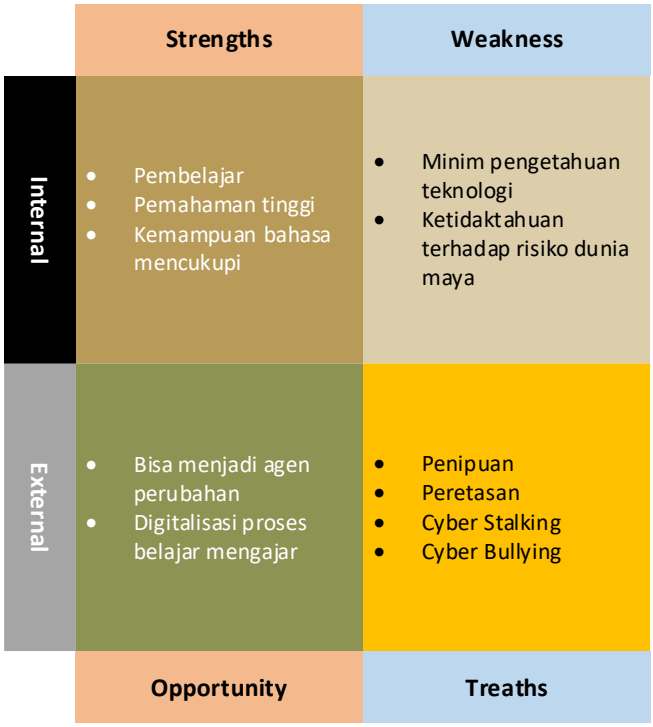
sensitif tersebut. Kejahatan paling sederhana yang sering dialami pengguna *smartphone* adalah pembajakan nomor *WhatsApp* yang merupakan aplikasi paling banyak digunakan di Indonesia [4]. Bukan hanya itu, kejahatan juga dilakukan pada aplikasi yang terhubung dengan sistem perbankan sehingga mengakibatkan kerugian finansial. Biasanya modus ini dijalankan dengan menggunakan *One Time Password* yang dikirimkan melalui *WhatsApp* [5]. Sangat banyak modus yang dilakukan oleh pelaku *cyber-crime* untuk mengelabuhi korbannya. Kasus *Cyberbullying* juga merupakan salah satu contoh kasus kejahatan dunia maya yang meningkat drastis sejak era Covid-19 pada awal tahun 2020. *Cyberbullying* lebih memanfaatkan media sosial untuk menjalankan aksi kejahatannya [6].

Selain disebabkan oleh minimnya pengetahuan, persoalan keamanan data dalam dunia maya juga dipengaruhi oleh faktor demografi yaitu jenis kelamin. Beberapa penelitian menyebutkan bahwa perempuan lebih berisiko terkena serangan siber dibandingkan dengan laki-laki. Secara keseluruhan perempuan memiliki risiko keamanan yang jauh lebih rendah dibandingkan dengan laki-laki [7]. Namun, faktor yang paling berpengaruh terhadap keamanan siber sebenarnya bukan faktor demografi, tetapi pengetahuan dan pengalaman pengguna [8].

Pengabdian kepada Masyarakat (PKM) ini termotivasi berdasarkan hasil kuesioner mengenai ketidaktahuan pengguna terhadap teknologi dan celah keamanan *smartphone* yang bisa mengakibatkan terjadinya *cyber-crime*. Motivasi ini juga dikuatkan dengan adanya beberapa kejadian mengenai pembajakan nomor *WhatsApp* yang kemudian dimanfaatkan untuk kepentingan yang tidak bertanggungjawab. Sebagai tindaklanjut, kemudian dilakukan *Workshop on Digital Literacy: Internet & Mobile Security* dengan peserta guru-guru Bahasa Inggris Sekolah Menengah Atas di kabupaten Bantul.

2. METODE

Metode analisis yang dipergunakan dalam PKM ini adalah metode SWOT [9] yang terdiri dari *Strengths* (kekuatan), *Weakness* (kelemahan), *Opportunity* (peluang), dan *Threats* (ancaman). Metode SWOT kemudian digunakan untuk menganalisis hasil *preliminary research* melalui kuisioner tentang pengetahuan keamanan data dalam internet dan *smartphone*. Hasil analisis dengan metode SWOT ditampilkan dalam Gambar 1.



Gambar 1. Analisis SWOT

Hasil analisis yang ditampilkan pada Gambar 1 menunjukkan bahwa guru-guru Bahasa Inggris SMA di Kabupaten Bantul memiliki kekuatan diantaranya adalah pembelajar, memiliki pemahaman materi yang tinggi, dan memiliki kemampuan bahasa yang mencukupi. Sebagai pembelajar tentu saja tidak ada hambatan untuk mempelajari hal yang baru termasuk teknologi. Kemampuan belajar ini juga ditopang dengan pemahaman yang tinggi terhadap materi yang sedang dipelajari. Pemahaman materi ini menjadi tinggi karena didukung kemampuan Bahasa Inggris yang memadai, karena sumber pengetahuan pada bidang teknologi internet dan *smartphone* kebanyakan menggunakan Bahasa Inggris.

Di samping memiliki kekuatan yang cukup, para guru juga memiliki kelemahan yaitu minimnya pengetahuan teknologi dan faktor ketidaktahuan risiko di dunia maya. Kelemahan tersebut perlu diselesaikan

ISSN: 2615-6717 (Print), 2657-2338 (On-Line)

karena sebenarnya ada peluang yang lebih besar yaitu sebagai agen perubahan serta peningkatan digitalisasi proses belajar mengajar. Selain itu, terdapat ancaman yang nyata dalam dunia maya yang disebut dengan *cyber-crime* yang saat ini mulai dimanfaatkan untuk penipuan, peretasan, *bullying*, dan lain-lain [10].

Berdasarkan hasil analisis SWOT yang ditampilkan dalam Gambar 1, kemudian dilakukan *Workshop on Digital Literacy: Internet & Mobile Security* yang dilaksanakan di SMA Negeri 1 Bantul Jl. Kh Wahid Hasyim, RT.03/RW.08, Jetis, Palbapang, Bantul, Daerah Istimewa Yogyakarta 55713. *Workshop* ini diikuti oleh guru-guru Bahasa Inggris se-Kabupaten Bantul yang tergabung dalam Musyawarah Guru Mata Pelajaran (MGMP) Bahasa Inggris. Materi *workshop* disesuaikan dengan kebutuhan dan tidak membahas terlalu teknis karena *background* peserta bukan dari lingkungan Teknologi Informasi. Penekanan materi lebih kepada penyadaran dan meminimalkan perilaku pengguna yang dapat menyebabkan kehilangan data misalnya *logout* untuk mengakhiri sesi *login*, melakukan *rolling password* berkala, tip dan trik membuat *password*, *update* sistem operasi, dan lain sebagainya. Pada akhir sesi *workshop* peserta harus mengikuti *post-test* untuk mengetahui pemahaman peserta terkait dengan keamanan data dan *cyber-crime*.

3. HASIL DAN PEMBAHASAN

Maraknya pencurian data oleh pihak yang tidak bertanggungjawab melalui dunia maya tentu sangat meresahkan pengguna internet dan *smartphone*. Tindakan tersebut sebenarnya merupakan pelanggaran hukum dalam bidang Teknologi Informasi dan pelanggaran hak asasi manusia [11]. Hukum di Negara Kesatuan Republik Indonesia sebenarnya sudah mengatur hal tersebut dengan adanya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Badan Siber dan Sandi Negara (BSSN) [12]. Namun, sejumlah materinya belum mampu merespon berbagai tantangan pemanfaatan teknologi internet saat ini [13]. Oleh sebab itu pengetahuan mengenai keamanan data dan *cyber-crime* harus ditingkatkan baik secara individu ataupun organisasi. Dampak *workshop* ini juga bisa lebih luas karena peserta bisa berbagi kepada teman sejawat, komunitas, dan keluarganya. Hal ini sesuai dengan hasil analisis SWOT pada bagian *opportunity* yaitu sebagai agen perubahan untuk kesadaran keamanan data [14].

Hasil survei awal yang sudah dilakukan untuk mengetahui perilaku pengguna *smartphone* di kalangan guru-guru Bahasa Inggris SMA di Kabupaten Bantul ditampilkan dalam Tabel 1.

Tabel 1. Hasil survei awal

No.	Key	Value	Keterangan
1	*Password* kombinasi (angka, huruf, dan karakter) lebih aman.	75%	setuju
2	Saat *smartphone* terhubung internet berarti ada peluang pihak lain untuk mengakuisisi *smartphone* kita.	70%	setuju
3	Peluang terjadinya penyadapan informasi di *wireless* layanan publik lebih besar	80%	setuju
4	Selalu *logout* setiap kali selesai menggunakan sistem terautentikasi agar keamanan data terjaga.	81%	setuju
5	*Rolling password* perlu dilakukan agar *password* tidak mudah ditebak.	77%	setuju
6	Pesan dari nomor yang tidak dikenal patut dicurigai	97%	setuju
7	Membuka pesan di *smartphone* saat bangun tidur atau menjelang istirahat adalah tindakan yang tidak bijak.	89%	setuju
8	*Block number* atau *report number* dapat dimanfaatkan jika ada pengiriman pesan yang mencurigakan dari nomor tersebut.	90%	setuju
9	Penggunaan *biometric security* seperti *fingerprint* lebih efektif untuk mengunci aplikasi.	80%	setuju
10	Membuat *backup data* merupakan tindakan yang bijaksana.	85%	setuju

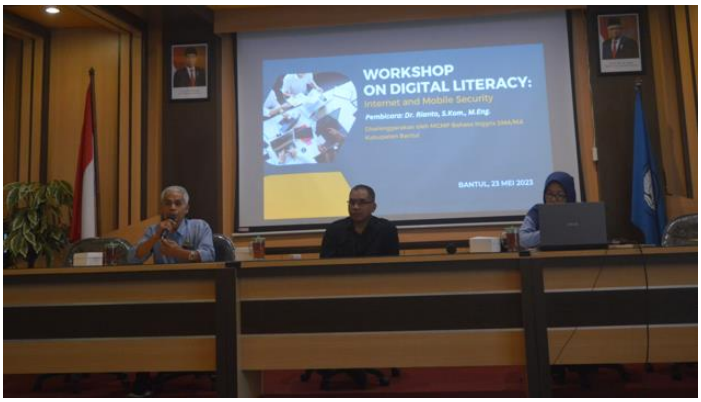
Data yang ditampilkan pada Tabel 1 menunjukkan bahwa sebagian besar peserta memanfaatkan *smartphone* untuk kepentingan *messenger* dan media sosial. Sebenarnya tidak ada yang salah dari penggunaan *smartphone* di media sosial, hanya saja lingkungan keamanannya harus mendukung seperti *update* sistem operasi dan aplikasi, *password*, dan pengetahuan harus selalu ditambah. Hasil survei juga menunjukkan bahwa tidak semua peserta rajin melakukan *update* sistem operasi maupun aplikasi yang digunakan. Hal ini tentu sangat rentan karena *patching security hole* dilakukan dengan cara *update* [15].

Dalam konteks pembuatan *password* juga masih ditemukan kelemahan yaitu pembuatan *password* ataupun *Personal Identification Number* (PIN) dengan berformat tanggal. Hal ini sesuai dengan hasil penelitian yang pernah dilakukan bahwa pembuatan *password* dipengaruhi oleh bahasa dan identitas [16]. Selain itu juga masih banyak yang membuat *password* tanpa menggunakan kombinasi angka, karakter, maupun huruf besar dan huruf kecil. Kerentanan ini tentu saja mudah dimanfaatkan oleh *cracker* untuk melakukan *brute force attack* demi mendapatkan *password* [17]. Kasus lain adalah tidak pernah melakukan *rolling password* ataupun tidak mengganti *password* yang diberikan oleh admin sekolah ataupun admin aplikasi, padahal *password* yang diberikan *default* semua sama. Hal ini membuka peluang bagi oknum yang tidak bertanggungjawab untuk

melakukan pencurian ataupun perusakan data. Di samping itu masih banyak peserta menggunakan *password* yang sama untuk seluruh aplikasi yang memerlukan *login*. "Lupa" merupakan jawaban standar sebagai alasan kenapa satu *password* untuk semua aplikasi. Tentu saja yang dimaksud dalam hal ini bukan *Single Sign On* (SSO) seperti yang dimiliki oleh *Google*, *Facebook*, ataupun *Instagram*. Peserta juga tidak ada yang mempergunakan *password manager* untuk mendokumentasikan *username* dan *password*. Temuan-temuan tersebut jika dikategorikan masuk ke dalam lemahnya kesadaran akan pentingnya keamanan dan keselamatan informasi dari serangan ataupun peretasan data [18]. Salah satu yang menyebabkan hal ini adalah pengalaman pengguna yang lebih melihat kejahatan secara aktual, sehingga kejahatan di dunia maya belum diperhatikan [19].

Masalah-masalah yang diidentifikasi melalui survei tersebut muncul karena kurangnya pengetahuan mengenai tata kelola keamanan data sebagai akibat minimnya peserta dalam *upgrade* pengetahuan teknologi. Hal ini dapat diketahui dari data hasil survei yang menyatakan hanya sekitar 15% peserta yang mencari tambahan pengetahuan dalam hal keamanan data dan *cyber-crime* melalui seminar, *workshop*, ataupun sumber pengetahuan lainnya. Meskipun jarang melakukan tambahan pengetahuan peserta masih bijak dalam menggunakan media sosial. Survei terkait aktivitas *sharing* data-data sensitif sangat tidak sering dilakukan dalam media sosial. *Sharing* data di media sosial sangat riskan karena informasi yang didapat selanjutnya dapat digunakan untuk melakukan tindakan kejahatan [20]. Sebagai contoh, *upload* dokumen yang memuat tanggal lahir, pasti akan digunakan oleh *cracker* untuk meretas PIN ataupun *password* yang kemungkinan besar berformat tanggal.

Workshop on Digital Literacy: Internet & Mobile Security dilaksanakan pada tanggal 23 Mei 2023 mulai pukul 13.30 WIB sampai dengan selesai diikuti kurang lebih 54 peserta. *Workshop* ini dibuka oleh kepala sekolah SMA Negeri 1 Bantul yang dalam sambutannya menyampaikan bahwa MGMP bukan hanya membahas mengenai bidang studi yang diampu tetapi juga harus diisi materi lain yang lebih bermanfaat seperti pada *workshop* ini. Dokumentasi Pembukaan *Workshop* dapat dilihat pada Gambar 2.

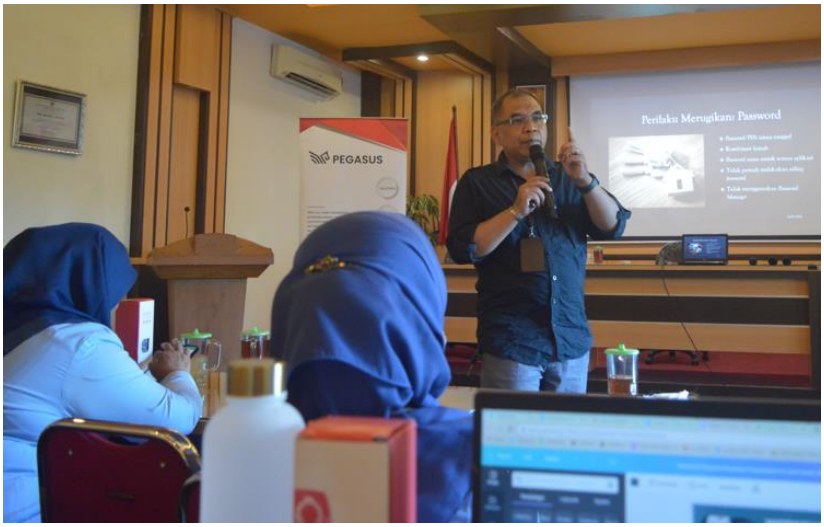


Gambar 2. Pembukaan *Workshop* oleh Kepala Sekolah

Antusiasme peserta dalam mengikuti materi *workshop* juga tampak nyata ditandai dengan banyaknya pertanyaan yang disampaikan oleh peserta. Aktivitas tersebut merupakan modal positif untuk menumbuhkan kesadaran dalam keamanan internet dan *smartphone*. Hal ini sesuai dengan *strength* bahwa peserta *workshop* adalah pembelajar yang cepat memahami hal-hal baru. Selain bertanya, para peserta juga aktif menjawab pertanyaan yang diberikan oleh narasumber. Antusiasme peserta Workshop dapat dilihat pada Gambar 3 dan Gambar 4.

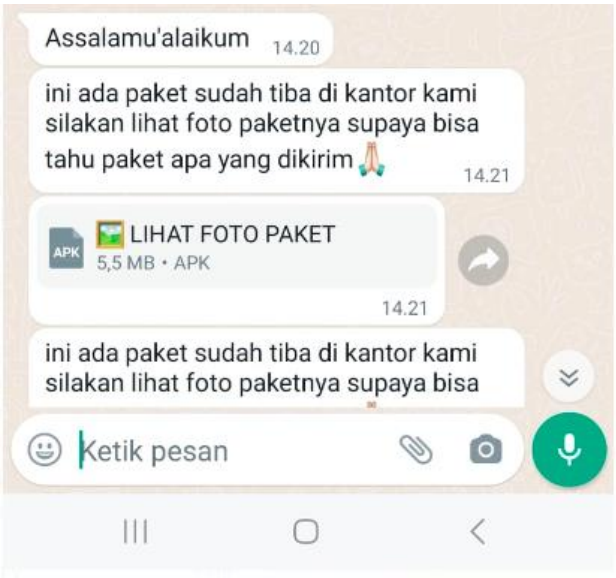
Gambar 3. Antusiasme Peserta *Workshop*

ISSN: 2615-6717 (Print), 2657-2338 (On-Line)



Gambar 4. Sesi tanya jawab dalam *workshop*

Dalam *workshop* ini juga dibahas studi kasus mengenai peserta yang mengalami pembajakan nomor *WhatsApp*. Peserta tersebut mendapat pesan berupa pengiriman paket dari nomor yang tidak dikenal. Sebenarnya jika dicermati pesan tersebut sudah terasa janggal berdasarkan alasan: 1) nomor pengirim tidak dikenal; 2) format file yang dikirim adalah file APK. Contoh pesan tersebut ditampilkan dalam Gambar 5.



Gambar 5. Modus penipuan dengan *WhatsApp*

Poin nomor satu tentang nomor yang tidak dikenal ini masuk akal karena kiriman datang dari kurir yang bekerja pada perusahaan ekspedisi yang nomornya tidak disimpan. Namun, pada poin dua seharusnya penerima pesan curiga andai saja mengenal format file standar yang sering digunakan misalnya JPG untuk gambar atau PDF untuk dokumen. File yang dikirim tersebut adalah file *Android Package Kit* (APK) yaitu sebuah paket *software* yang berfungsi untuk mendistribusikan aplikasi kepada pengguna sistem operasi Android [21]. Jika penerima membuka file tersebut maka akan terjadi proses instalasi ke *smartphone* target dan selanjutnya nomor *WhatsApp* target akan diakuisisi oleh penyerang.

Dalam *workshop* ini juga dibahas teknik mitigasi untuk mengantisipasi hal tersebut ataupun langkah apa yang harus dilakukan jika terkena serangan tersebut. Sebagai langkah antisipasi peserta kemudian diminta untuk melakukan *update* aplikasi *WhatsApp*, mengaktifkan PIN, dan mengaktifkan autentikasi dua faktor. Hal ini sebagai langkah antisipasi untuk mengurangi risiko pembajakan nomor *WhatsApp* dan *Message Forwarding*. *Message forwarding* merupakan sebuah teknik untuk menyadap pesan yang dikirimkan melalui *WhatsApp*. Jika pada aplikasi *WhatsApp* terpasang PIN dan autentikasi dua faktor, maka setiap ada penambahan *device* aplikasi akan menanyakan kedua hal tersebut. Jika penyerang tidak berhasil menemukan autentikasinya maka penambahan *device* untuk penyadapan informasi akan terhambat [22].

Sesi *workshop* diakhiri dengan *post-test* pengisian kuesioner untuk melihat tingkat kesadaran peserta terkait dengan keamanan data di dunia digital. Hasil kuesioner peserta *workshop* ditampilkan dalam Tabel 2 berikut.

Tabel 2. Hasil *post-test* peserta *workshop*

No.	Key	Awal	Akhir	Keterangan
1	*Password* kombinasi (angka, huruf, dan karakter) lebih aman.	75%	87%	setuju
2	Saat *smartphone* terhubung internet berarti ada peluang pihak lain untuk mengakuisisi *smartphone* kita.	70%	82%	setuju
3	Peluang terjadinya penyadapan informasi di *wireless* layanan publik lebih besar	80%	91%	setuju
4	Selalu *logout* setiap kali selesai menggunakan sistem terautentikasi agar keamanan data terjaga.	81%	90%	setuju
5	*Rolling password* perlu dilakukan agar *password* tidak mudah ditebak.	77%	89%	setuju
6	Pesan dari nomor yang tidak dikenal patut dicurigai	97%	98%	setuju
7	Membuka pesan di *smartphone* saat bangun tidur atau menjelang istirahat adalah tindakan yang tidak bijak.	89%	93%	setuju
8	*Block number* atau *report number* dapat dimanfaatkan jika ada pengiriman pesan yang mencurigakan dari nomor tersebut.	90%	96%	setuju
9	Penggunaan *biometric security* seperti *fingerprint* lebih efektif untuk mengunci aplikasi.	80%	87%	setuju
10	Membuat *backup data* merupakan tindakan yang bijaksana.	85%	94%	setuju

Berdasarkan data yang ditampilkan pada Tabel 2 dapat diketahui bahwa level kesadaran peserta *workshop* terhadap keamanan data dalam dunia digital sudah baik. Terkait dengan *password* kombinasi, peserta sudah memiliki kesadaran karena sebagian aplikasi yang diperuntukkan bagi guru-guru sudah mewajibkan *password* memiliki kombinasi huruf, angka, dan karakter. Namun, sebenarnya kekuatan *password* bukan terletak dari kombinasi dengan karakter, tetapi lebih pada persyaratan panjang minimum dan kekuatan minimum. Persyaratan kelas karakter hanya berkontribusi sedikit perbaikan pada keamanan efektif [23].

Kasus lain yang menarik dalam *workshop* ini adalah pemanfaatan *biometric security* yang biasanya menggunakan *fingerprint* pada *smartphone*. Kasus ini memunculkan dua pendapat yaitu: 1) aman dan tidak aman. Dikatakan aman karena *fingerprint* seseorang adalah *unique* atau tidak ada yang sama di seluruh dunia, tetapi 2) bisa tidak aman karena dalam kondisi tidak sadar ibu jari bisa diarahkan seseorang untuk membuka aplikasi. Penggunaan *fingerprint* bersifat otentik, akurat, dan dapat diandalkan dalam *smartphone*, sehingga menjadi pilihan utama untuk mengamankannya [24]. Mengenai poin nomor 2, sudah banyak penelitian yang dikembangkan untuk mengantisipasi hal tersebut misalnya ditambah dengan sensor-sensor lain, meskipun masih banyak pekerjaan lain yang harus ditambahkan [25]. Namun, pada intinya sistem keamanan dengan *biometric security* terbukti lebih akurat. Sebagian peserta juga berpendapat bahwa penggunaan *fingerprint* untuk autentikasi memperbesar peluang untuk lupa *password* karena tidak pernah menginput *password* ketika masuk aplikasi. Solusi untuk hal ini sebenarnya adalah dengan menggunakan *password manager*, sehingga semua data tentang autentikasi aplikasi dapat disimpan dengan aman dan pemegang cukup menghafal satu *password master* untuk bisa masuk ke dalam *password manager* [26].

Terlepas dari semua permasalahan tersebut, *workshop* yang dilakukan ini berhasil mengubah *mindset* peserta untuk peduli terhadap keamanan data khususnya di dunia maya. Setidaknya peserta sudah mulai melakukan *update* aplikasi maupun sistem operasi baik untuk *smartphone* maupun komputernya. Terkait dengan *update* pengetahuan dan pemahaman mengenai risiko keamanan siber memang tidak berbanding lurus dengan kecelakaan yang terjadi. Terbukti dari jumlah peserta yang mengikuti *workshop* ini baru dua orang yang pernah mengalami kejadian pembajakan nomor *WhatsApp*. Namun, hal tersebut tidak bisa dijadikan alasan untuk tidak melakukan *update* pengetahuan, karena perkembangan teknologi akan sebanding lurus dengan modus baru dalam kejahatan siber [27].

4. KESIMPULAN

Workshop yang dilaksanakan sebagai bentuk PKM ini menyimpulkan beberapa hal terkait dengan keamanan data dan kejahatan siber yang sering terjadi di era digital saat ini. Beberapa poin yang disimpulkan adalah sebagai berikut:

1. Pengetahuan mengenai keamanan data bagi seseorang tidak terkait langsung dengan kejahatan siber yang menimpa seseorang. Hal ini dapat diidentifikasi dari sebagian besar peserta *workshop* yang belum memiliki pengetahuan mendasar mengenai keamanan data tetapi tidak mengalami kecelakaan terkait dengan kejahatan siber seperti pembajakan nomor *WhatsApp*.
2. Meskipun tidak terkait secara langsung, tetapi peningkatan pengetahuan mengenai keamanan data secara otomatis akan menumbuhkan kesadaran untuk lebih waspada dalam memanfaatkan teknologi

ISSN: 2615-6717 (Print), 2657-2338 (On-Line)

khususnya *smartphone*.

3. Peserta *workshop* yang menerima materi pengetahuan dasar mengenai keamanan data dan kejahatan siber, pada akhirnya bisa menjadi agen perubahan tentang kesadaran keamanan data bukan hanya untuk pribadi tetapi juga keluarga, komunitas, organisasi, dan institusi tempat mereka bekerja.

Pada masa mendatang *workshop* ini bisa dilanjutkan dengan materi mengenai *password manager* yang sangat dibutuhkan untuk pengelolaan *password*. Hal ini sangat krusial karena belum dimanfaatkannya *password manager*, seseorang akan takut untuk membuat *password* dengan kombinasi dan panjang *password* yang kuat.

DAFTAR PUSTAKA

[1] T. Li *et al.*, "Smartphone App Usage Analysis: Datasets, Methods, and Applications," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 2, pp. 937–966, 2022, doi: 10.1109/COMST.2022.3163176.

[2] M. Hatamian, "Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers," *IEEE Access*, vol. 8, pp. 35429–35445, 2020, doi: 10.1109/ACCESS.2020.2974911.

[3] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice," *IEEE Access*, vol. 6, pp. 9390–9403, Jan. 2018, doi: 10.1109/ACCESS.2018.2799522.

[4] A. Yudhana, I. Riadi, R. Yudhi Prasongko, A. Dahlan, J. Ahmad Yani Tamanan, and J. Soepomo, "Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 7, no. 1, pp. 43–48, Jan. 2022, doi: 10.30591/JPIT.V7I1.3639.

[5] R. Aditama, "Penegakan Hukum Cyber Crime Terhadap Tindak Pidana Pencurian Uang Nasabah Dengan Cara Pembajakan Akun Internet Banking Lewat Media Sosial," *Wajah Hukum*, vol. 5, no. 1, pp. 118–125, Apr. 2021, doi: 10.33087/WJH.V5I1.360.

[6] A. I. Yuladi and R. Indrayani, "Analisis dan Perbandingan Tools Forensik menggunakan Metode NIST dalam Penanganan Kasus Kejahatan Siber," *Jurnal Teknologi Terpadu*, vol. 9, no. 2, pp. 95–100, Dec. 2023, doi: 10.54914/JTT.V9I2.636.

[7] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks," *Educ Inf Technol (Dordr)*, vol. 27, no. 4, pp. 4729–4752, May 2022, doi: 10.1007/S10639-021-10806-7/TABLES/7.

[8] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[9] M. F. Rozi and M. P. Utami, "Perencanaan Strategis Penerapan Teknologi Informasi Menggunakan Metode Analisis SWOT Proses Bisnis Unit IT," *Decode: Jurnal Pendidikan Teknologi Informasi*, vol. 3, no. 1, pp. 74–81, Feb. 2023, doi: 10.51454/DECODE.V3I1.139.

[10] C. Berlian, "Kejahatan Siber yang Menjadi Kekosongan Hukum," *JOURNAL EQUITABLE*, vol. 5, no. 2, pp. 19–20, Apr. 2020, doi: 10.37859/JEQ.V5I2.2532.

[11] S. M. Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI*, vol. 27, no. 1, pp. 38–52, Mar. 2021, doi: 10.47268/sasi.v27i1.394.

[12] A. Haryanto and S. M. Sutra, "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal*, vol. 7, no. 1, pp. 56–69, Apr. 2023, doi: 10.34010/GPSJOURNAL.V7I1.8141.

[13] A. M. Rohmy, T. Suratman, and A. I. Nihayaty, "UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi," *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam*, vol. 7, no. 2, pp. 309–339, Aug. 2021, doi: 10.54471/DAKWATUNA.V7I2.1202.

[14] J. Maulindar and D. Hartanti, "Pelatihan Perlindungan Data Pribadi dan Keamanan Siber Untuk Siswa SMK Negeri 2 Surakarta," *Madaniya*, vol. 4, no. 4, pp. 1851–1856, Nov. 2023, doi: 10.53696/27214834.652.

[15] M. A. Zein, U. Y. K. S. Hediyanto, and A. Almaarif, "Security Hardening Sistem Operasi Virtual Private Server pada Instansi Pendidikan XYZ Berdasarkan NIST SP 800-123," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 8, no. 1, pp. 230–241, Feb. 2023, doi: 10.29100/JIPI.V8I1.3438.

[16] M. Grobler, M. A. P. Chamikara, J. Abbott, J. J. Jeong, S. Nepal, and C. Paris, "The importance of social identity on password formulations," *Pers Ubiquitous Comput*, vol. 25, no. 5, pp. 813–827, Oct. 2021, doi: 10.1007/S00779-020-01477-1/METRICS.

[17] R. Verma, N. Dhanda, and V. Nagar, "Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms," *Lecture Notes in Networks and Systems*, vol. 376, pp. 513–522, 2022, doi: 10.1007/978-981-16-8826-3_44/COVER.

[18] M. E. Gharieb, "Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah Al-Mukarramah- Saudi Arabia,"

International Journal of Computer Science & Network Security, vol. 21, no. 8, pp. 360–368, 2021, doi: 10.22937/IJCSNS.2021.21.8.45.

[19] L. F. Chaparro *et al.*, "Quantifying Perception of Security through Social Media and Its Relationship with Crime," *IEEE Access*, vol. 9, pp. 139201–139213, 2021, doi: 10.1109/ACCESS.2021.3114675.

[20] U. S. Yadav, B. B. Gupta, D. Peraković, F. J. G. Peñalvo, and I. Cvitić, "Security and Privacy of Cloud-Based Online Online Social Media: A Survey," *EAI/Springer Innovations in Communication and Computing*, pp. 213–236, 2022, doi: 10.1007/978-3-030-90462-3_14/COVER.

[21] R. Mateless, D. Rejabek, O. Margalit, and R. Moskovitch, "Decompiled APK based malicious code classification," *Future Generation Computer Systems*, vol. 110, pp. 135–147, Sep. 2020, doi: 10.1016/J.FUTURE.2020.03.052.

[22] S. Jarecki, M. Jubur, H. Krawczyk, N. Saxena, and M. Shirvanian, "Two-factor Password-authenticated Key Exchange with End-to-end Security," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 3, p. 17, Apr. 2021, doi: 10.1145/3446807.

[23] J. Tan, L. Bauer, N. Christin, and L. F. Cranor, "Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1407–1426, Oct. 2020, doi: 10.1145/3372297.3417882.

[24] D. Afah, A. Gautam, S. Misra, A. Agrawal, R. Damaševičius, and R. Maskeliūnas, "Smartphones Verification and Identification by the Use of Fingerprint," *Lecture Notes in Networks and Systems*, vol. 292, pp. 365–373, 2022, doi: 10.1007/978-981-16-4435-1_35/COVER.

[25] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *EURASIP J Image Video Process*, vol. 2021, no. 1, pp. 1–28, Dec. 2021, doi: 10.1186/S13640-021-00548-4/TABLES/5.

[26] W. Yudha Aditama, I. Rosianal Hikmah, D. Febriyan Priambodo, P. Siber dan Sandi Negara, K. Bogor, and P. Korespondensi, "Analisis Komparatif Keamanan Aplikasi Pengelola Kata Sandi Berbayar Lastpass, 1Password, dan Keeper Berdasarkan ISO/IEC 25010," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 4, pp. 857–864, Aug. 2024, doi: 10.25126/JTIIK.20231036544.

[27] M. R. Habibi and I. Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, vol. 23, no. 2, pp. 400–426, Dec. 2020, doi: 10.15642/ALQANUN.2020.23.2.400-426.