Volume 6 Nomor 4 Desember 2022
p-ISSN : 2614-5251
e-ISSN : 2614-526X

LITERASI DIGITAL BAGI KOMUNITAS DIGITAL MARKETER PURWOKERTO DALAM UPAYA MENCEGAH ANCAMAN KEAMANAN DATA DI DUNIA SIBER

Khairunnisak Nur Isnaini[1)], Wahyu Widodo[1)]

[1)]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Purwokerto, Jawa Tengah, Indonesia

Corresponding author : Khairunnisak Nur Isnaini
E-mail : nisak@amikompurwokerto.ac.id

Diterima 27 Agustus 2022, Direvisi 25 Oktober 2022, Disetujui 25 Oktober 2022

ABSTRAK

Masalah keamanan data yang berhubungan dengan data pribadi dan data transaksi belanja online menghantui konsumen maupun pelapak (penjual online). Hal tersebut tentu mengganggu kenyamanan ketika berbelanja online karena pengguna merasa khawatir data pribadi maupun data transaksi dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Adanya kebocoran data merupakan salah satu dampak yang diakibatkan oleh kejahatan siber. Ancaman kejahatan siber akhir-akhir ini meningkat akibat sistem keamanan yang buruk dan kerentanan sistem yang parah. Adanya literasi digital bertujuan untuk upaya pencegahan ancaman keamanan informasi menjadi hal yang penting untuk disimak bagi pelapak online maupun yang berdampak kepada pembeli. Metode pelaksanaan yang digunakan adalah seminar melalui virtual meeting. Selama seminar berlangsung, peserta dapat melakukan tanya jawab dalam dua termin melalui moderator. Selain itu, setelah seminar selesai dilaksanakan peserta akan diberikan handout materi. Hasil yang diperoleh masih banyak peserta yang belum sepenuhnya mengetahui ciri-ciri tindakan yang mengancam keamanan data dan informasi. Hal ini terlihat dari hasil *pre-test* dan *post-test* yang diberikan menunjukkan angka yang signifikan terhadap penyerapan informasi yang diberikan. Bentuk evaluasi yang diperlukan adalah adanya workshop khusus mengenai sub-sub spesifik dari materi keamanan data dan informasi yang telah diberikan sebelumnya.

Kata kunci: keamanan data; kebocoran data; kejahatan siber; literasi digital.

ABSTRACT

Data security issues related to personal data and online shopping transaction the data consumers and pelapak (online sellers). This certainly disturbs the convenience when shopping online because users are worried that personal data and transaction data can be misused by irresponsible parties. The existence of data leakage is one of the impacts caused by cyber crime. The threat of cybercrime has recently increased due to poor security systems and severe system vulnerabilities. The existence of digital literacy aims to prevent information security threats, which is important for online sellers and those who have an impact on buyers. The implementation method used is a seminar through virtual meetings. During the seminar, participants can ask questions in two terms through a moderator. In addition, after the seminar is completed, participants will be given material handouts. The results obtained are that there are still many participants who do not fully understand the characteristics of actions that threaten data and information security. This can be seen from the results of the pre-test and post-test that were given showing a significant number on the absorption of the information provided. The form of evaluation that is needed is the existence of a special workshop on specific sub-subjects of data and information security materials that have been given previously.

Keywords: data security; data leakes; cyber security; digital literacy.

PENDAHULUAN

Belanja *online* adalah proses transaksi yang dilakukan konsumen menggunakan media digital berupa situs jual beli *online* maupun sosial media dalam berbelanja barang atau jasa yang disediakan oleh penjual (Harahap, 2018). Konsumen dapat dengan mudah melihat dan memilih jasa atau barang yang akan dibeli melalui berbagai macam media (Nurhayati, 2017). Menurut data yang dihimpun oleh (Cindy Mutia Annur, 2020) beberapa alasan konsumen memilih belanja online karena dianggap harga yang tertera jauh lebih murah, dapat melakukan transaksi diberbagai tempat, transaksi dianggap cepat dan praktis, adanya diskon dan promo yang

ditawarkan, dan lain sebagainya. Tentunya dalam bertransaksi *online*, konsumen maupun penjual memiliki cara atau teknik dalam menentukan alat pembayaran yang disepakati. Beberapa metode pembayaran yang digunakan dalam transaksi belanja *online* menurut (Bayu, 2020) antara lain e-wallet, transfer bank, minimarket, *paylater*, *kartudebit*, kartu kredit, dan lainnya.

Di sisi lain, masalah-masalah keamanan data yang berhubungan dengan data pribadi dan data transaksi belanja online menghantui konsumen maupun pelapak (penjual online). Hal tersebut tentu mengganggu kenyamanan ketika berbelanja *online* karena pengguna merasa khawatir data pribadi maupun data transaksi dapat disalah gunakan oleh pihak yang tidak bertanggungjawab. Kekhawatiran pengguna tentu beralasan, menurut (Pusparisa, 2020a) di Tahun 2020 terdapat 90 juta data pengguna yang dicuri dari Tokopedia, 10 juta data dari Bukalapak, dan beberapa lainnya dari e-commerce Bhinneka. Terlebih lagi menurut (Pusparisa, 2020b) data yang dicuri tersebut diperjual belikan oleh oknum yang tidak bertanggungjawab. Data dari Tokopedia dan Bukalapak dijual pada kisaran harga lebih dari 70 juta rupiah dan data dari Bhinneka dijual dalam kisaran harga lebih dari 10 juta rupiah. Sedangkan data-data tersebut berisi data pribadi yang mencakup data transaksi seperti nomor induk kependudukan, alamat rumah, no handphone, dan nomor rekening.

Adanya kebocoran data seperti yang telah diuraikan pada paragraf sebelumnya merupakan salah satu dampak yang diakibatkan oleh kejahatan siber. Ancaman kejahatan siber akhir-akhir ini meningkat akibat sistem keamanan yang buruk dan kerentanan sistem yang parah (Tangkary, Hartono, & Amelia, 2018) Kejahatan siber sendiri dapat diartikan sebagai tindakan kejahatan menggunakan komputer yang terjadi di dunia siber (John Reimon Batmetan; Ahnes Montoh; I Gusti Ayu Mirahyanti, 2018). Tentunya aktivitas ilegal tersebut merugikan para penjual dan pembeli, kerugian materiil maupun non materiil. Saat ini, (Rahayu, Ruqoyah, Berliana, Pratiwi, & Saputra, 2021) memang terdapat aturan dan hukum yang berlaku di Indonesia namun penegakan hukum untuk pelaku cybercrime masih minim sehingga kejahatan di dunia maya masih sering terjadi dan terulang kembali.

Komunitas Digital Marketer Purwokerto merupakan tempat bagi masyarakat yang memiliki *passion* dan niat untuk menggiatkan produksi dan distribusi barang atau jasa bahkan UMKM sebagai upaya untuk meningkatkan taraf hidup yang lebih baik. Tantangan yang dihadapi oleh para anggota Komunitas Digital Marketer Purwokerto ini yaitu masih minimnya pengetahuan dan keahlian tentang perlindungan keamanan data bagi pelapak (penjual online) sehingga memberikan celah kelemahan pada aktivitas siber dan dimanfaatkan oleh pihak yang tidak bertanggungjawab.

Pentingnya menambah ilmu pengetahuan dan wawasan khususnya terkait perlindungan keamanan data bagi pelapak (penjual online) perlu ditingkatkan. Hal tersebut merupakan hal dasar yang perlu dipahami terutama untuk melindungi data pribadi pelanggan yang ditanggalkan atau tersimpan melalui aplikasi, sosial media maupun e-commerce yang digunakan oleh pelapak online. Tujuannya agar para pembeli atau konsumen merasa aman berbelanja online di toko yang mereka pilih karena merasa yakin jika toko online yang dipilih adalah toko yang trusted (dapat dipercaya) dalam menyimpan informasi data pembeli.

Menjaga kredibilitas dan kepercayaan konsumen adalah hal yang wajib diperhatikan oleh penjual/pelapak online. Seiring maraknya kasus yang terjadi, pelapak online tentu perlu memiliki cara-cara khusus agar tetap dipercaya sebagai penjual yang memiliki integritas dalam menjaga kerahasiaan dan keutuhan data pribadi pembeli. Saat ini, belum banyak para pelapak online termasuk komunitas *digital marketer* yang mengetahui cara-cara tersebut bahkan mempraktikkannya dalam aktivitas jual belinya. Tentu ini menjadi masalah serius dan perlu segera mendapatkan informasi dan arahan yang tepat untuk dapat mencegah aktivitas ilegal yang dapat merugikan pembeli dan berdampak juga bagi penjual.

Salah satu yang sering terjadi dan seringkali penjual tidak menyadarinya adalah aktivitas *inadvertent threats*. *Inadvertent threats* merupakan aktivitas kebocoran data yang diakibatkan oleh kelalaian manusia maupun tindakan yang disengaja, contohnya kelemahan sistem yang mengakibatkan terjadinya *configuration error improper encryption* bahkan adanya peluang ancaman cyber espionage (tindakan mata-mata) dan sabotase (Delpiero, Reynaldi, Ningdiah, & ..., 2021). Meskipun tidak dapat dipungkiri selain adanya *inadvertent threats* terdapat ancaman lain yang belum banyak disadari oleh penjual online seperti *phising*, ancaman *malware*, serangan DDoS, dan *Hacking* (Tangkary et al., 2018). Adanya peluang dalam penyalahgunaan data pribadi dapat diartikan bahwa terdapat kelemahan sistem, pengawasan, dan evaluasi sehingga dapat

merugikan kedua belah pihak (Situmeang, 2021).

Berdasarkan uraian contoh permasalahan di atas dan peluang terjadinya penyalahgunaan data pribadi dari orang dalam maupun pihak ketiga di kemudian hari, maka isu literasi digital khususnya terkait pengamanan data pribadi pelapak atau penjual online serta cara-cara pencegahannya dari aktivitas ilegal perlu diangkat ke permukaan. Sehingga dikemudian hari diharapkan semua penjual atau pelapak online memiliki kecakapan dalam menentukan penanganan permasalahan tersebut.

METODE

Pelaksanaan kegiatan pengabdian masyarakat ini dilaksanakan secara virtual meeting melalui Zoom. Metode pelaksanaan secara garis besar terbagi menjadi tiga yaitu pra-pelaksanaan, pelaksanaan, dan pasca-pelaksanaan.

Tahap pra-pelaksanaan terbagi menjadi beberapa aktivitas antara lain:

a. Membuat bahan materi berupa *file* presentasi singkat dan *handout* bagi para peserta.
b. Melakukan kerjasama dengan mitra pengabdian sebagai bentuk kesepakatan dalam membuat seminar literasi digital
c. Memastikan persiapan ruang virtual dengan media *online meeting* dan jaringan internet yang memadai sesuai dengan jumlah peserta.

Tahap pelaksanaan terbagi menjadi beberapa aktivitas antara lain:

a. Presentasi dilaksanakan dalam satu sesi berisi materi-materi meliputi *cyber security awareness* yang disampaikan oleh ketua pengabdian.
b. Sesi tanya jawab dengan peserta dalam dua termin memuat masing-masing dua pertanyaan yang akan dijawab oleh ketua pengabdian (dosen) maupun anggotanya.
c. Membagikan soal pre-test sebelum pemaparan materi dan post-test pada akhir sesi.
d. Membagikan presensi online sebagai bukti keikutsertaan peserta.

Tahap pasca-pelaksanaan dilakukan evaluasi terhadap seluruh kegiatan dan memberikan *follow up* agar kegiatan dapat berjalan optimal.

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian masyarakat berlangsung pada Hari Sabtu, 18 Juni 2022 pukul 09.00-10.30 WIB melalui media Zoom Meetings dengan skema Webinar Series. Webinar Series ini diberi tajuk "Waspada Terhadap Ancaman Siber yang Mengancam Data Pribadi" yang dipimpin oleh moderator Ibu Faridatun Nida, S.S., M.A. Pengabdian masyarakat ini ditujukan untuk para komunitas atau pegiat digital marketer dari berbagai platform yang tersedia saat ini. Para peserta webinar yang hadir dalam sesi ini berjumlah 20 orang.

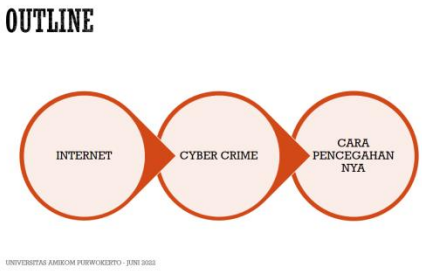
Pada tahap awal tim pengabdian mengecek keseluruhan persiapan pelaksanaan pertemuan daring diantaranya materi yang akan disampaikan, *form pre-test dan post-test*, *link* presensi *online* dan koneksi internet narasumber serta moderator. Tidak hanya tiga hal tersebut, persiapan juga dilakukan oleh operator memastikan semua peserta telah hadir di ruang virtual.

Webinar Series ini terbagi menjadi tiga sesi yaitu sesi pertama materi yang disampaikan oleh saya sendiri Khairunnisak Nur Isnaini, M.Kom. dengan judul "Ancaman Keamanan Data di Dunia Siber dan Cara Pencegahannya" kemudian dilanjutkan oleh narasumber kedua dan di akhiri dengan sesi tanya jawab. Sebelum memulai kegiatan webinar, peserta diminta untuk mengisi form Pre-test yang digunakan untuk mengukur pengetahuan awal tentang kejahatan siber. Pre-test yang diberikan berisi 5 soal pertanyaan. Pada tabel 1, berikut daftar pertanyaan yang diberikan kepada peserta.

Tabel 1. Daftar pertanyaan

No	Item pertanyaan
1	Apakah Anda tahu tentang Kejahatan Siber (Cyber Crime) ?
2	Di bawah ini manakah arti dari kejahatan siber
3	Manakah yang termasuk kejahatan siber di dunia e-commerce ataupun financial technology?
4	Manakah yang termasuk bentuk kejahatan siber secara umum, kecuali..
5	Manakah yang termasuk cara untuk mengamankan data dari kejahatan siber dalam lingkup e commerce maupun financial technology (dapat memilih lebih dari 1)

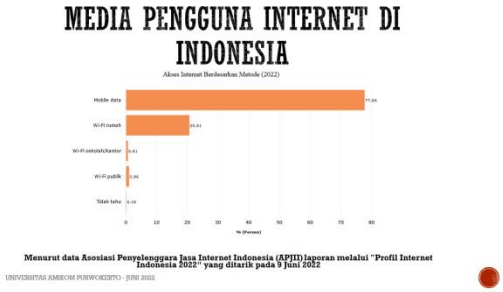
Kegiatan webinar diawali dengan pembukaan oleh moderator yang kemudian dilanjutkan dengan memaparkan inti materi yang terdiri dari tiga materi utama yaitu internet, cyber crime, dan cara pencegahannya yang dapat dilihat pada gambar 1.



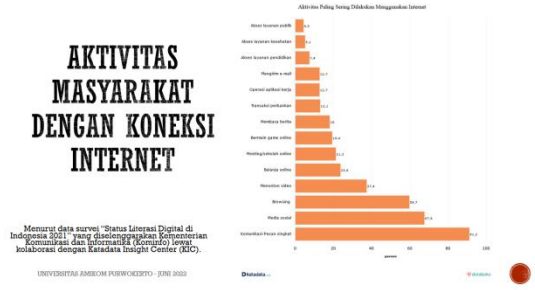
Gambar 1. Outline materi secara keseluruhan

Awal materi narasumber menyampaikan informasi terkait penggunaan internet, media yang digunakan dalam mengakses internet, dan beragam aktivitas masyarakat yang memanfaatkan konektivitas dengan internet yang dapat dilihat pada gambar 2 hingga 4.

Gambar 2. Perkembangan pengguna internet di Indonesia

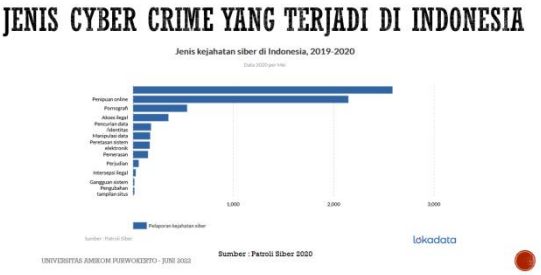


Gambar 3. Media yang digunakan dalam mengakses internet



Gambar 4. Aktivitas masyarakat dengan koneksi internet

Sub materi kedua materi yang disampaikan antara lain teori singkat dan pemahaman tentang ruang siber, cyber crime, dan data dari jenis cyber crime yang terjadi di Indonesia sepanjang tahun 2019-2020. Data tersebut dapat dilihat pada gambar 5.



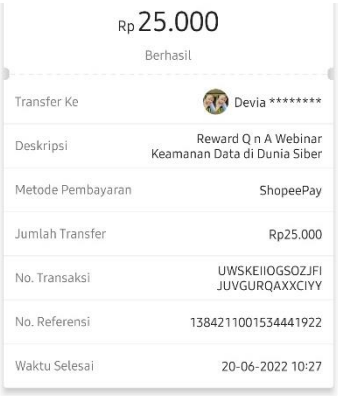
Gambar 5. Aktivitas masyarakat dengan koneksi internet

Sub materi terakhir merupakan puncak materi yaitu jenis-jenis cyber crime yang menyerang pegiat online marketer baik menggunakan sosial media ataupun e commerce. Narasumber memberikan beberapa gambaran jenis cyber crime pada ruang lingkup E-Commerce.

Gambar 6. Jenis-jenis cyber crime dalam ruang lingkup E-Commerce

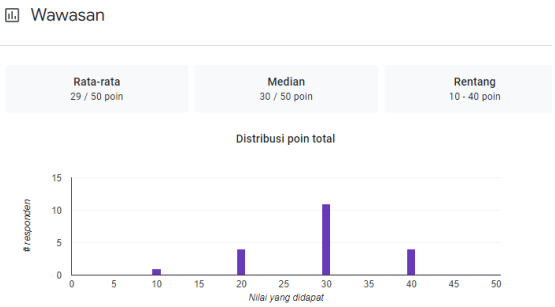
Sebelum menuju akhir sesi, materi terakhir yang disampaikan adalah cara pencegahan aktivitas cyber crime di sektor e commerce di antaranya tidak tergiur testimoni maupun harga murah dan waspada terhadap metode pembayaran yang tidak lazim. Selain itu, disampaikan juga cara aman menangkis kejahatan cyber crime di dunia financial technology antara lain tidak menggunakan akses internet umum dan merahasiakan PIN atau kode akses ataupun kode OTP.

Pada akhir sesi pelaksanaan pengabdian, tim membagikan presensi untuk di isi oleh peserta. Presensi ini digunakan sebagai isian data untuk pembuatan sertifikat digital. Selain itu, tim juga mencatat pertanyaan yang ditanyakan dan narasumber memberikan reward atas pertanyaan yang diajukan yaitu saldo dompet digital. Salah satu yang beruntung mendapatkan reward sebesar 25.000 seperti pada gambar 7.



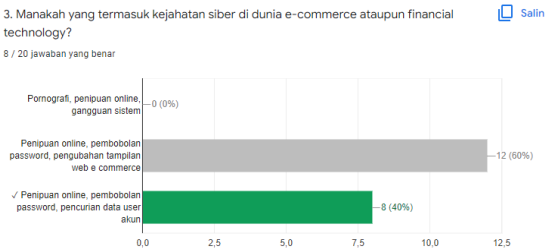
Gambar 7. Pemberian reward kepada peserta yang beruntung

Selain informasi umum jalannya kegiatan webinar yang menjadi hasil kegiatan, peningkatan pengetahuan para peserta juga menjadi hal yang penting untuk diinformasikan. Berdasarkan hasil pre-test yang telah dilakukan pada awal sesi sebelum webinar pada gambar 8.



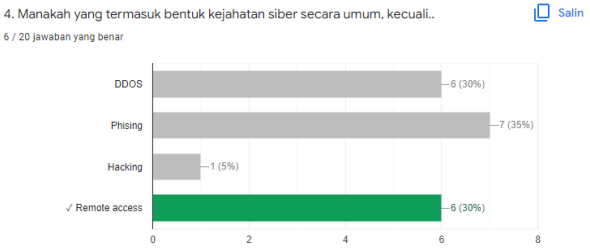
Gambar 8. Rangkuman hasil secara umum

Terlihat bahwa peserta masih banyak yang belum mengerti dan memahami tentang kejahatan siber dan cara penanganannya. Terlebih jika melihat secara spesifik pada beberapa item pertanyaan, peserta telah mengetahui tentang kejahatan siber namun secara arti maupun penyebutan jenis ataupun tindakannya masih tergolong belum memahami. Hal ini dapat terlihat pada hasil pre-test di gambar 9 hingga 11.



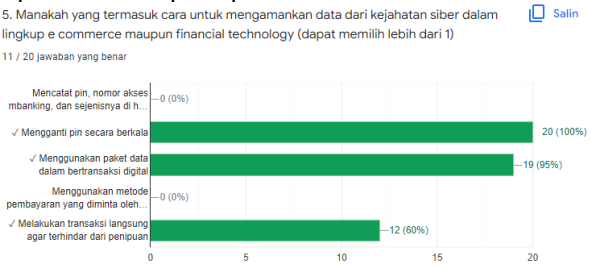
Gambar 9. Rangkuman jawaban pertanyaan tentang kejahatan siber di dunia e-commerce

Pada gambar 9 terlihat sebanyak 60% jawaban peserta masih keliru dan belum tepat dalam memahami kejahatan siber yang tergolong pada ruang lingkup e commerce. Pada dasarnya, kejahatan siber ini tidak terbatas pada ruang lingkup tersebut. Namun peserta juga cukup memahami jika gangguan sistem bukan tergolong pada kejahatan siber di ruang lingkup e commerce.



Gambar 10. Rangkuman jawaban pertanyaan tentang jenis kejahatan siber

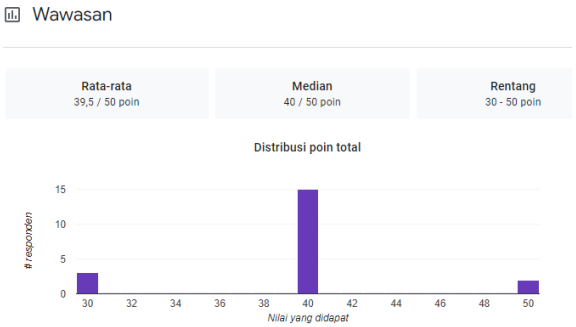
Pada gambar 10 terlihat sebanyak 30% saja peserta yang memahami tentang bentuk kejahatan siber dengan tepat. Sisanya, masih banyak yang terjebak dengan jawaban salah yang dimunculkan. Hal ini menandakan bahwa istilah-istilah pada ruang lingkup kejahatan siber belum cukup diketahui dan dipahami oleh para peserta.



Gambar 11. Rangkuman jawaban pertanyaan tentang cara penanganan kejahatan siber

Pada gambar 11 terlihat bahwa hampir semua peserta dapat memahami cara penanganan kejahatan siber dengan mengganti pin secara berkala dan menggunakan paket data pribadi untuk bertransaksi digital. Namun, beberapa peserta masih banyak yang belum *aware* terhadap pemilihan transaksi yang dilakukan secara langsung untuk meminimalisir tindak kejahatan siber.

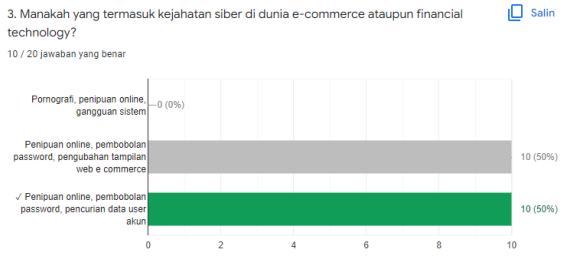
Perbandingan peningkatan pengetahuan tentang kejahatan siber dan cara penanganannya terlihat jelas pada hasil *post-test* yang dikerjakan oleh peserta. Perbandingan tersebut sangat terlihat pada hasil wawasan *form google* yang dapat dilihat pada gambar 12.



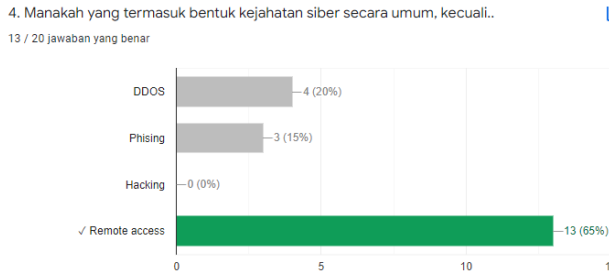
Gambar 12. Rata-rata wawasan pada *form post-test*

Pada gambar 8, mula-mula rerata wawasan peserta pada poin 29/50 dan setelah mendapatkan informasi dari webinar yang telah diselenggarakan, rerata wawasan meningkat menjadi 39,5/50.

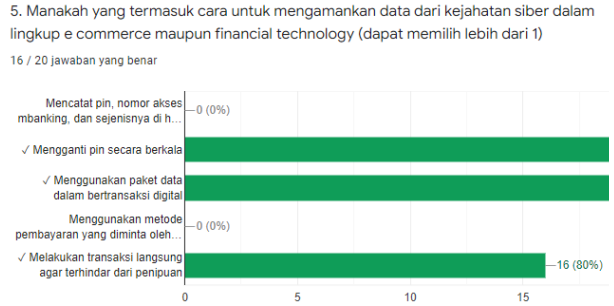
Hasil lain terlihat pada beberapa hasil jawaban peserta yang mayoritas telah memahami konsep tentang kejahatan siber, jenis atau bentuknya, dan cara penanganannya.



Gambar 13. Hasil *form post-test* tentang jenis aktivitas kejahatan siber



Gambar 14. Hasil *form post-test* tentang bentuk kejahatan siber



Gambar 15. Hasil *form post-test* tentang cara penanganan kejahatan siber

Hasil evaluasi yang diperoleh adalah masih banyak peserta yang belum memahami aktivitas-aktivitas kejahatan melalui internet. Selain itu, banyak dari peserta juga masih mengalami kebingungan dalam mengatasi hal-hal buruk seperti bocornya data pada akun *mobile banking* atau sosial media. Hal ini diperkuat dengan pertanyaan yang diajukan oleh salah satu peserta tentang cara penanganan pengguna jika akun mobile banking dibobol oleh *hacker* atau terindikasi aktivitas yang mencurigakan. Bentuk tindak lanjut kegiatan ini adalah adanya *workshop* hingga praktik mengenai cara atau tindakan yang perlu dilakukan untuk mencegah aktivitas kejahatan di dunia siber pada akun sosial media ataupun *mobile banking* milik pengguna.

Kendala yang dihadapi pada pelaksanaan pengabdian salah satunya yaitu koneksi internet yang kurang stabil hal ini dikarenakan peserta webinar menyimak materi dari domisili tempat tinggalnya masing-masing sehingga tidak dapat diprediksi kekuatan sinyal internetnya. Namun para peserta tetap antusias mendengarkan paparan materi hingga akhir sesi dan tanya jawab. Kepuasan peserta terlihat pada sesi diskusi ketika pertanyaan-pertanyaan berhasil menjawab permasalahan yang dialami.

SIMPULAN DAN SARAN

Kegiatan webinar ini telah menambah ilmu pengetahuan dan wawasan para pegiat *online marketer* ataupun komunitas UMKM pada umumnya tentang jenis-jenis kejahatan di dunia siber dan cara pencegahannya. Selain itu, peserta webinar semakin waspada terhadap aktivitas sehari-hari yang berhubungan dengan internet terutama pada saat melakukan transaksi *online*.

Saran yang dapat diberikan adalah meluasnya informasi tentang kejahatan siber dan cara pencegahannya yang dikemas dalam bentuk webinar series ataupun workshop berkelanjutan yang diisi oleh beberapa narasumber pada sub topiknya masing-masing.

UCAPAN TERIMAKASIH

Ucapan terima kasih kami haturkan kepada mitra pengabdian masyarakat yaitu Komunitas Digital Marketer Purwokert telah menjadi peserta webinar. Selain itu, kami haturkan juga kepada LPPM Universitas Amikom Purwokerto yang telah mendukung pendanaan dan terlaksananya kegiatan ini.

DAFTAR RUJUKAN

Bayu, D. J. (2020). Jumlah Pengguna Internet di Indonesia Capai 196,7 Juta. Retrieved

January 5, 2021, from https://databoks.katadata.co.id/datapublish/2020/11/11/jumlah-pengguna-internet-di-indonesia-capai-1967-juta

Cindy Mutia Annur. (2020). Ragam Alasan Konsumen Pilih Berbelanja Online. Retrieved November 9, 2021, from Katadata.co.id website: https://databoks.katadata.co.id/datapublish/2020/11/11/ragam-alasan-konsumen-pilh-berbelanja-online

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & ... (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Reserach and Debat Society*, *9*(1). Retrieved from http://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509

Harahap, D. A. (2018). Perilaku Belanja Online Di Indonesia: Studi Kasus. *JRMSI - Jurnal Riset Manajemen Sains Indonesia*, *9*(2), 193–213. https://doi.org/10.21009/jrmsi.009.2.02

John Reimon Batmetan; Ahnes Montoh; I Gusti Ayu Mirahyanti, T. R. (2018). Analisa Penyebab Terjadinya Cybercrime (Study Kasus: Yhummy Online Shop). *Jurnal Keamanan Komputer*, *1*(1). https://doi.org/10.31219/osf.io/da7sw

Nurhayati, N. (2017). Belanja “Online” Sebagai Cara Belanja Di Kalangan Mahasiswa (Studi Kajian Budaya Di Universitas Malikussaleh, Lhokseumawe, Aceh). *Aceh Anthropological Journal*, *1*(2), 1–22. https://doi.org/10.29103/aaj.v1i2.1140

Pusparisa, Y. (2020a). Bocornya Puluhan Juta Data Pengguna E-Commerce Indonesia. Retrieved November 9, 2021, from Katadata.co.id website: https://databoks.katadata.co.id/datapublish/2020/05/12/bocornya-puluhan-juta-data-pengguna-e-commerce-indonesia

Pusparisa, Y. (2020b). Data Pengguna E-Commerce Dijual Puluhan Juta Rupiah. Retrieved November 9, 2021, from Katadata.co.id website: https://databoks.katadata.co.id/datapublish/2020/05/12/data-pengguna-e-commerce-dijual-puluhan-juta-rupiah

Rahayu, S. K., Ruqoyah, S., Berliana, S., Pratiwi, S. B., & Saputra, H. (2021). Cybercrime dan dampaknya pada teknologi e-commerce. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(3), 632–637. https://doi.org/10.52362/jisamar.v5i3.478

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Jurnal Sasi*, *27*(1), 38–52. https://doi.org/10.47268/sasi.v27i1.394

Tangkary, S., Hartono, H., & Amelia, R. (2018). Keamanan Siber untuk e-Commerce. In D. B. U. I. Banyumurti (Ed.), *Seri Literasi Digital*. Retrieved from www.literasidigital.id