



Peningkatan Literasi dan Keamanan Digital Bagi Kreator Konten di Kota Lhokseumawe

Jafaruddin^{1*}, Zahari², Masriadi³, Kamaruddin⁴, Harinawati⁵, Asmaul Husna⁶, Awaluddin Arifin⁷

^{1,2,3,4,5,6,7}Universitas Malikussaleh, Aceh Utara, Indonesia

e-mail correspondensi*: jafaruddin@unimal.ac.id

History Article	Abstract
Received: 4 March 2026 Revised: 28 March 2026 Accepted: 29 April 2026	This community service initiative aims to strengthen digital literacy and raise cybersecurity awareness among content creators and youth in Uteunkot Village, Muara Dua District, Lhokseumawe City. The location was selected as part of the 2025 community empowerment program funded through Unimal's PNBP scheme. In today's increasingly complex digital landscape, the need for strong literacy and security awareness is urgent particularly for groups that are highly exposed to online risiko. Young people and digital creators are among the most vulnerable to cyber threats such as phishing scams, social media account breaches, identity theft, and misuse of personal data. In Aceh, cases of cybercrime continue to rise and now affect not only the general public but also professionals such as teachers and journalists. This situation highlights the growing importance of community-level cybersecurity education, especially for rural youth who are active internet users and often produce digital content. The program is expected to enhance the skills and awareness of young people and content creators in safeguarding their digital presence, while also encouraging the formation of a local community that prioritizes responsible and secure online behavior. The training is delivered through an intensive two-day workshop, followed by online mentoring through a discussion group. To assess the participants' progress, the program includes pre-tests and post-tests measuring improvements in their understanding of digital security
Keyword	
<i>Training, Literacy, Digital Security, Youth, Content Creators</i>	
To cite this article: Jafaruddin, E. et al. (2026). <i>Peningkatan Literasi dan Keamanan Digital Bagi Kreator Konten di Kota Lhokseumawe</i> . Kenduri: Jurnal Pengabdian Dan Pemberdayaan Masyarakat . 6(1) 2026, 243-258. https://doi.org/10.62159/kenduri.v6i1.xxx	

PENDAHULUAN

Saat ini Indonesia sedang menghadapi tantangan serius dalam ranah keamanan digital hal ini seiring dengan melonjaknya angka pengguna internet. Ruang digital yang semakin dinamis, namun juga semakin rentan terhadap berbagai bentuk kejahatan siber, karena tingkat penggunaan internet yang sangat tinggi yang mayoritasnya generasi Milenial ndan gen Z. Tahun 2023 mencapai 215.626.156 (78,19%) baik dibandingkan tahun 2022 yaitu 210.026.769. Kondisi tersebut menjadikan Indonesia sebagai salah satu negara dengan kerentanan cybercrime tertinggi di Asia Tenggara.

Situasi tersebut diperparah oleh lemahnya literasi digital masyarakat, terutama di daerah yang belum memiliki akses edukasi keamanan digital yang memadai. Sebab di era digital saat ini, literasi digital merupakan keterampilan fundamental yang harus dimiliki oleh setiap individu. Kemampuan tersebut bukan hanya dibutuhkan bukan hanya untuk mengakses informasi di media sosial dan media online, tapi juga mampu memilah dan memilih informasi, lebih dari itu, untuk mampu melindungi akun dari serangan digital. Apalagi sekarang korban yang menjadi serangan kejahatan digital bukan hanya dari masyarakat awam saja, tapi juga menyasar dari kalangan profesional, termasuk di Aceh.

Pada awal tahun 2024 terdapat 353,3 juta koneksi seluler aktif di Indonesia, dengan angka ini setara dengan 126,8 persen dari total populasi, dari jumlah itu ada 139,0 juta identitas pengguna media sosial aktif.

Jumlah tersebut diperkirakan meningkat setiap tahun, seiring perkembangan sarana pendukung untuk berselancar di internet semakin membaik. Karena itu potensi kasus kejahatan siber juga semakin besar di era digital ini, jika pengguna internet tidak memiliki kemampuan dalam mengakses informasi. Berdasarkan data yang dihimpun pemerintah, sepanjang November 2024 hingga Januari 2025, kerugian finansial akibat kejahatan siber mencapai Rp 476 miliar dan hingga pertengahan 2025, tercatat 1,2 juta laporan penipuan digital yang masuk ke sistem pengaduan publik.

Sedangkan Aliansi Jurnalis Independen (AJI) mencatat bahwa sepanjang tahun 2023 terdapat 89 kasus serangan digital terhadap jurnalis, jumlah tertinggi dalam satu dekade terakhir. Serangan digital tersebut bukan hanya menasar jurnalis tapi juga termasuk media arus utama. Pada Desember 2023, situs Kompas.id mengalami serangan DDoS setelah mempublikasikan artikel investigasi terkait judi online. Serangan tersebut semakin meningkat pada 15 Desember 2023 setelah sebelumnya mengalami gangguan akses sehari sebelumnya. Akibat dari serangan yang berupa lalu lintas tersebut menyebabkan layanan tidak bisa diakses secara normal.

Ada dua perspektif penting dalam memahami dunia digital yaitu kemampuan berliterasi digital dan kompetensi keamanan digital sebagaimana ditekankan (O.E.C.D., 2019) dalam kerangka *digital competencies*. Semakin sering berinteraksi di internet jika tanpa dibarengi dengan kemampuan literasi digital sangat berisiko terserang. Semakin pesatnya kemajuan teknologi, dunia menghadapi tantangan yang serius dalam bentuk kejahatan siber. (A.J.I., 2023) menunjukkan bahwa serangan *ransomware* dan penipuan online meningkat 18% secara global.

Artinya kasus tersebut bukan hanya di Tanah Air tapi juga di negara lain. Mengingat kondisi tersebut, pelatihan literasi dan keamanan digital menjadi kebutuhan mendesak bagi pemuda dan kreator konten. Literasi digital merupakan faktor penting dalam mengurangi risiko kejahatan siber, sebagaimana ditegaskan (U.N.E.S.C.O., 2018). Mengingat kondisi ini sehingga perlu dilakukan Pelatihan Literasi dan Keamanan Digital Untuk Pemuda dan Kreator Konten di Desa Uteunkot, Kota Lhokseumawe. Kondisi ini semakin mendesak mengingat segi sosial masyarakat dari mulai desa sampai kota mulai beradaptasi dengan teknologi digital.

Namun belum memiliki literasi digital yang cukup sehingga di khawatirkan akan banyak korban penipuan berbasis digital, sehingga pelatihan ini sebagai upaya untuk meminimalisir terjadinya *cyber crime*, di kalangan konten creator. Pendidikan merupakan salah satu sektor penting dalam pembangunan nasional karena berperan dalam membentuk kualitas sumber daya manusia yang mampu menghadapi perkembangan sosial, ekonomi, dan budaya masyarakat. Dalam konteks pendidikan di Indonesia, proses pembelajaran tidak hanya diarahkan pada penguasaan pengetahuan akademik, tetapi juga pada pembentukan kemampuan berpikir kritis, kesadaran sosial, dan kemampuan peserta didik dalam memahami realitas kehidupan di lingkungan sekitarnya.

METODE PELAKSANAAN

Tahap pelaksanaan dilakukan pelatihan literasi dan keamanan Digital melalui beberapa tahapan berikut ini : Tahap persiapan pada 19 Agustus 2025; melakukan observasi terhadap keamanan digital melalui media, mengumpulkan data *cyber crime* yang terjadi dan dialami oleh masyarakat, mempersiapkan bahan pelatihan, seleksi peserta dengan menasar pemuda aktif di media sosial, konten kreator, pelaku usaha daring, dan masyarakat umum yang sering menggunakan platform digital, terdiri dari 20 peserta, mempersiapkan proveri dan tempat kegiatan.

Tahap pelaksanaan kegiatan 20 Agustus 2025; Pre test dilakukan sebelum mulai kegiatan, peserta di belikan soal melalui link (<https://forms.gle/zNkiBp7cbuGUeo55A>), untuk mengukur tingkat pemahaman peserta tentang Literasi dan keamanan digital; melalui dua tahapan pertama; peserta di bekali dengan materi keamanan digital untuk mengenalkan berbagai jenis ancaman siber yang umum dan bagaimana cara mengenalinya secara tatap muka dilanjutkan dengan sesi diskusi; Diskusi interaktif dilakukan untuk menyamakan persepsi peserta terhadap pentingnya keamanan digital; tahap kedua praktik langsung peserta melakukan pengamanan akun secara langsung (aktifkan 2FA, instal aplikasi keamanan, ubah sandi kuat, mengatur privasi akun).

Simulasi dan studi kasus disediakan simulasi penipuan digital dan praktik penanganan sederhana untuk meningkatkan kesiapsiagaan peserta dalam menghadapi skenario nyata. Distribusi e-Booklet panduan keamanan digital dengan materi yang telah dibahas diringkas dalam bentuk e-booklet berformat PDF, yang dibagikan kepada seluruh peserta untuk menjadi panduan berkelanjutan.

HASIL PEMBAHASAN

Pelaksanaan kegiatan Pengabdian ini dilakukan oleh tim pengabdian dengan sumber dana PNBP Universitas Malikussaleh tahun 2025 dengan menyelenggarakan Pelatihan Literasi dan Keamanan Digital Untuk Pemuda dan Kreator Konten di Desa Uteunkot, Kota Lhokseumawe bertempat di Di Gedung Teater Prodi Ilmu Komunikasi FISIP Unimal pada 19-20 Agustus 2025 melalui link: <https://forms.gle/zNkiBp7cbuGUeo55A> dari hasil jawaban dapat di paparkan sebagai berikut:

1. Apa yang dimaksud dengan literasi digital?

25 jawaban

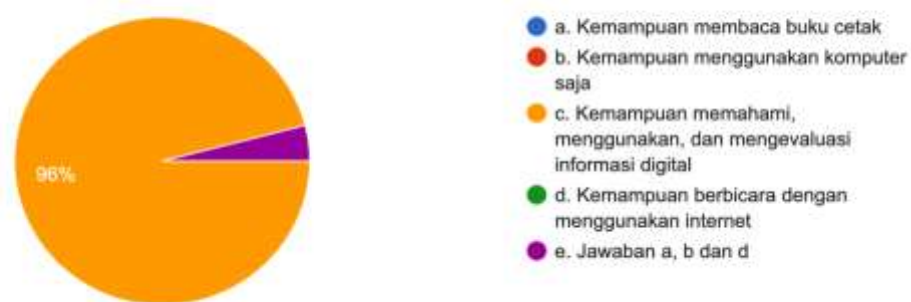


Diagram 1. Pemahaman Tentang Literasi Digital

Berdasarkan diagram 1, peserta pelatihan sangat memahami tentang literasi digital terbukti 96% menjawab literasi digital sebagai kemampuan memahami, menggunakan dan mengevaluasi informasi digital, artinya peserta pelatihan cukup memahami akan pentingnya literasi digital. Ini juga menunjukkan mayoritas peserta yang terdiri pemuda dan konten kreator memahami konsep literasi digital dengan baik. Namun, ada sekitar 4 persen peserta yang mampu menjawab dengan tepat, sehingga masih dibutuhkan penguatan materi literasi digital.

2. Salah satu contoh perilaku literasi digital adalah ...

25 jawaban

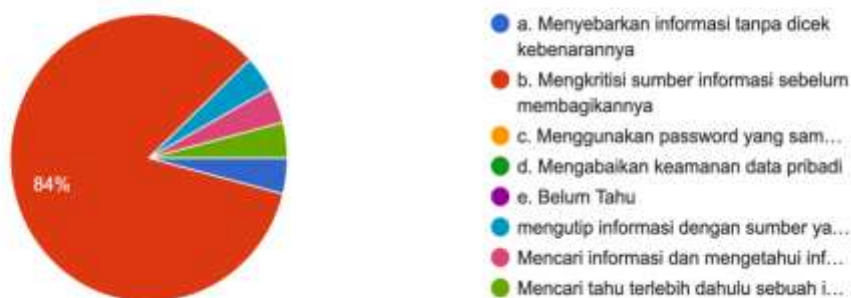


Diagram 2. Contoh prilaku Literasi Digital

Pada bagian prilaku Literasi digital, peserta pelatihan dominan (84%) menyatakan akan mengkritisi sumber informasi sebelum membagikannya, dibandingkan jawaban lain yang ditawarkan. Sikap skeptis ini yang merupakan kemampuan dari peserta sudah mampu memahami literasi digital, jadi peserta mengecek dulu informasi dan kemudian memverifikasi untuk memastikan informasi guna memastikan kebenaran informasi sebelum dikonsumsi. Ini menunjukkan bahwa sebagian besar peserta *memahami perilaku literasi digital dengan benar*, yaitu mengecek dan mengkritisi informasi sebelum menyebarkannya.

Sikap ini merupakan inti dari literasi digital mampu memilah, memverifikasi, dan memastikan kebenaran informasi. Diagram tersebut juga masih menunjukkan belum memiliki kemampuan literasi yang memadai, mereka memilih untuk menyebar informasi meskipun belum tentu benar informasi tersebut (Penyusun, 2022). Selain itu juga terdapat peserta menggunakan satu password yang sama, sehingga dengan kata lain ini mengabaikan keamanan data pribadinya. Sedangkan sebagian lainnya mengaku tidak tahu. Inilah pentingnya diadakan pelatihan tersebut.

3. Apa fungsi utama password dalam keamanan digital?

25 jawaban

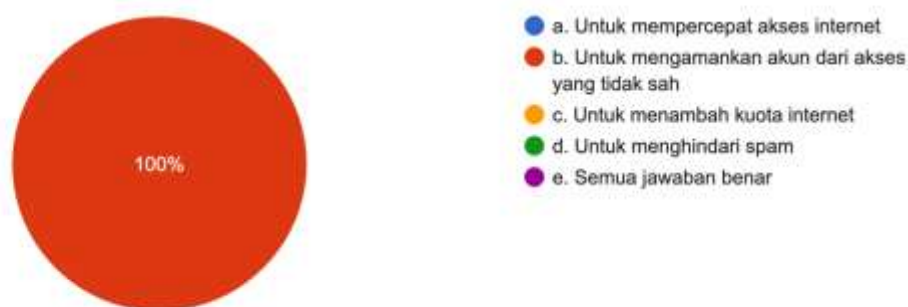


Diagram 3. Fungsi password dalam keamanan Digital

Peserta pelatihan menyatakan 100% untuk mengamankan akun dari akses yang tidak sah, sehingga peserta tidak memilih jawaban lain yang telah disediakan. Ini menunjukkan peserta sudah menerapkan prinsip keamanan digital yang baik sehingga mampu melindungi akun, kemudian dapat melindungi data pribadinya dari pencurian atau serangan orang lain. Karena password merupakan pintu pertama yang menjaga terjadi peretasan atau pun awal dari penyalagunaan akun. Ini juga menunjukkan pemahaman peserta mengenai fungsi utama *password* dalam keamanan digital sangat baik dan seragam (Budiarto & dkk, 2024).

4. Ciri-ciri berita hoaks biasanya ditandai dengan ...

25 jawaban



Diagram 4. Ciri-ciri berita hoaks

Pada pertanyaan ciri-ciri hoaks, peserta mampu mengenali dari judul. Seluruh responden (100%) sepakat bahwa ciri paling umum dari berita hoaks adalah judul yang sensasional, provokatif, dan tidak didukung sumber yang jelas. Ini menunjukkan peserta memahami karakter utama hoaks, yaitu penggunaan judul yang memancing emosi, tetapi tidak memiliki kredibilitas sumber. Tidak ada responden yang memilih opsi lain, menggunakan sumber resmi dan dapat dipercaya terdapat data dan bukti lengkap berita dari situs pemerintah (Rusdiah, 2020). Berita hoaks biasanya mudah dikenali dari judulnya yang berlebihan, bombastis, dan sering kali tidak menyebutkan sumber. Grafik ini menggambarkan kesadaran responden bahwa judul provokatif adalah indikator paling kuat dari hoaks.

5. Salah satu cara melindungi data pribadi di media sosial adalah ...

25 jawaban



Diagram 5. Cara melindungi data Pribadi di Media sosial

Pada pertanyaan cara melindungi data pribadi di media sosial salah satunya menggunakan sumber resmi dan dapat di percaya menempati (76%) dan (16%) terdapat data dan bukti yang lengkap. Grafik ini menunjukkan peserta memahami data pribadi berkaitan dengan informasi yang dikonsumsi dan dibagikan, tapi masih ada (4%) yang sulit secara tepat tentang cara melindungi data pribadi, sehingga yang memilih opsi ini menunjukkan adanya miskonsepsi.

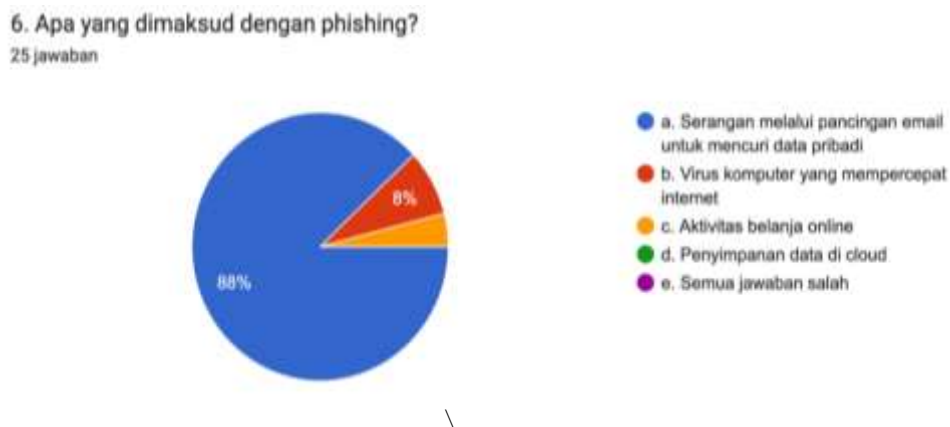
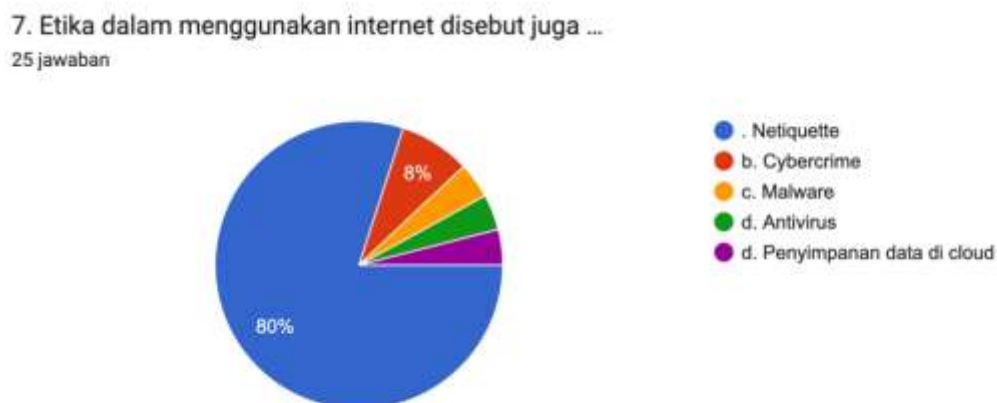


Diagram 6. Pemahaman tentang Phising

Pemahaman peserta tentang phishing sangat baik, ditunjukkan oleh dominasi jawaban benar (88%) yaitu serangan melalui pancingan email untuk mencuri data pribadi. Lalu ada 8% menyatakan virus komputer yang mempercepat internet (Cybersecurity, 2022). Secara keseluruhan ada 12 persen yang masih memiliki miskonsepsi tentang istilah phishing, sehingga edukasi tambahan bermanfaat untuk menegaskan bahwa phishing adalah tindakan penipuan melalui pancingan informasi, biasanya lewat email maupun pesan palsu lainnya.



Digram 7. Etika dalam berinternet

Peserta pelatihan (80%) menjawab etika dalam berinternet sebagai *Netiquette* dan (8%) menjawab *Cybercrime* sehingga perlu penjelasan dalam pelatihan agar peserta seluruhnya memahami etika dalam berinternet. Namun, masih terdapat 8% peserta yang menjawab “Cybercrime, yang menunjukkan adanya kesalahpahaman antara konsep etika berinternet (*Netiquette*) dan kejahatan siber (*Cybercrime*). Miskonsepsi ini penting untuk diperhatikan karena kedua istilah memiliki makna dan ruang lingkup yang berbeda (Nasrullah, 2021).

8. Contoh penggunaan literasi digital dalam perkuliahan adalah ...

25 jawaban



Diagram 9. Pemahaman tentang Resiko Wi-Fi publik tanpa pengamanan

Peserta sebagian besar (64%) menyatakan risiko menggunakan wi-fi publik tanpa pengamanan mengakibatkan data pribadi bisa di curi, selain itu kecepatan internet semakin lambat menjawab (32%). Kesadaran peserta mengenai ancaman pencurian data sudah cukup tinggi (64%). Diagram tersebut menggambarkan 36% peserta yang belum memahami bahwa risiko utama Wi-Fi publik adalah keamanan, bukan performa atau baterai perangkat. Untuk itulah dalam pelatihan literasi digital tersebut menekankan bahaya Wi-Fi publik tanpa enkripsi (Informatika Republik Indonesia, 2023). Cara mengamankan diri, seperti menggunakan VPN, HTTPS, dan menghindari login akun penting di jaringan publik.

10. Aplikasi two-factor authentication (2FA) digunakan untuk ...

25 jawaban

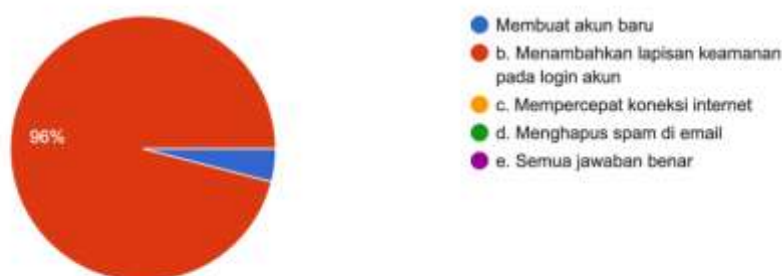


Diagram 10. Pemahaman tentang Aplikasi 2FA

Peserta pelatihan memahami Aplikasi two-factor authentication (2FA) untuk menambah lapisan keamanan pada login akun.

ANALISIS HASIL PRE-TEST

Dari jawaban peserta pada hasil pre-test dengan 10 pertanyaan, menunjukkan bahwa peserta sudah mengenal konsep dasar literasi digital, namun pemahaman peserta terkait keamanan digital masih rendah. Dari grafik tersebut menunjukkan 96% peserta mampu mendefinisikan literasi digital, tetapi hanya sebagian lainnya peserta yang memahami phishing, keamanan kata sandi, dan perlindungan privasi. Temuan ini sejalan dengan penelitian global mengenai kesenjangan literasi keamanan digital (DataReportal, 2024). Setelah mengikuti kegiatan pelatihan, kepada peserta diberikan posttest sebagai umpan balik dari kegiatan pelatihan ini, tujuannya adalah untuk mengukur tingkat pemahaman yang dimiliki peserta, berikut link posttest. Berikut data yang diperoleh berdasarkan hasil posttest terhadap peserta pelatihan

1. Literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga ...

20 jawaban

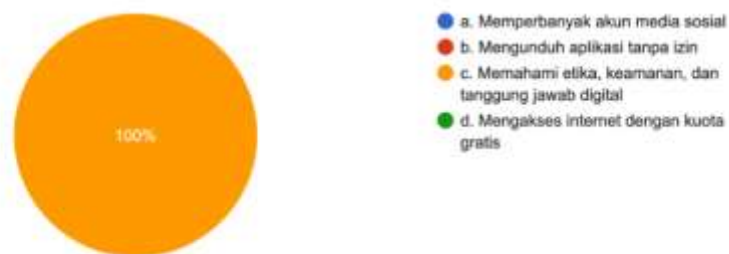


Diagram 11. Pemahaman tentang Literasi Digital

Pemahaman peserta pelatihan tentang literasi digital 100% memahami etika, keamanan dan tanggung jawab digital.

2. Salah satu langkah kritis dalam mengecek kebenaran informasi digital adalah ...

20 jawaban

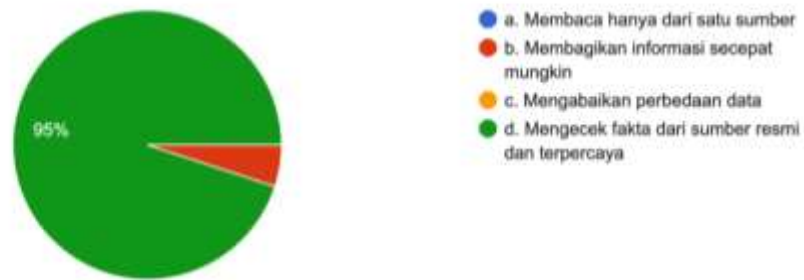


Diagram 12. Langkah mengecek kebenaran informasi digital

3. Menggunakan password yang kuat artinya ...

20 jawaban



Diagram 13. Arti menggunakan password kuat

Peserta pelatihan memahami bahwa menggunakan kombinasi angka dan huruf, angka dan symbol merupakan password yang kuat.

4. Bagaimana cara aman mengakses informasi di internet?

20 jawaban

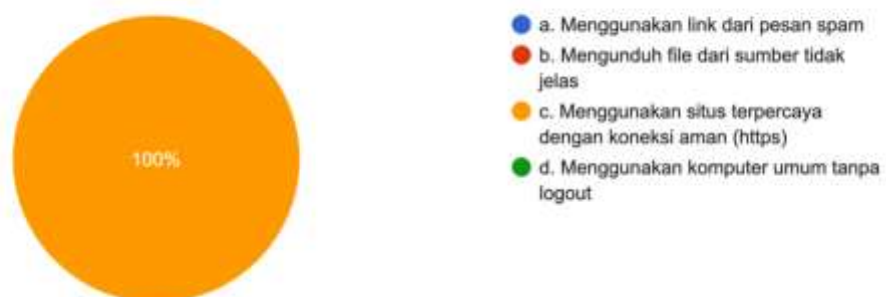


Diagram 14. Cara Aman mengakses internet

Sementara peserta menyatakan menggunakan situs terpercaya dengan koneksi aman (https) sebagai cara aman untuk mengakses informasi di internet (100%).

5. Apa yang dimaksud dengan jejak digital?

20 jawaban



Diagram 15. Jejak Digital

Berkaitan dengan jejak digital (100%) peserta menyatakan semua aktivitas online yang terekam dan dapat ditelusuri.

6. Salah satu cara menghindari serangan malware adalah ...

20 jawaban

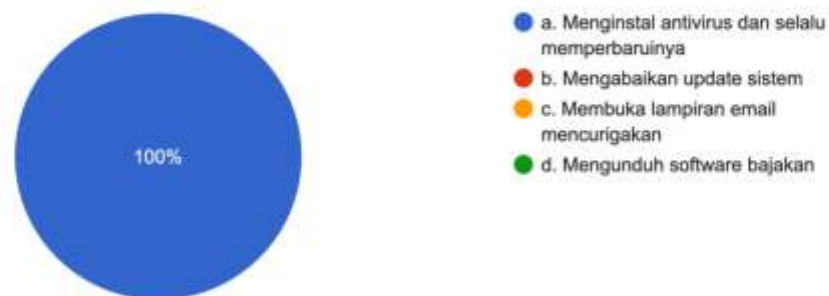


Diagram 16. Cara Menghindari serangan malware

Bagi peserta salah satu cara menghindari serangan malware adalah dengan menginstal antivirus dan selalu memperbaruinya menempati jawaban (100%).

7. Mengutip informasi dari internet untuk tugas kuliah sebaiknya ...

20 jawaban

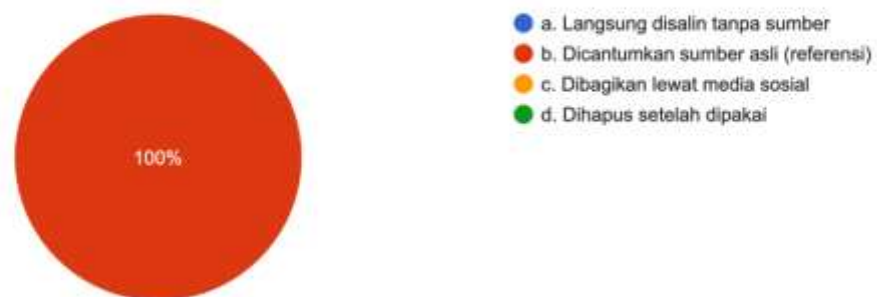


Diagram 17. Pengutipan Sumber

8. Etika dalam berdiskusi di forum online termasuk ...

20 jawaban

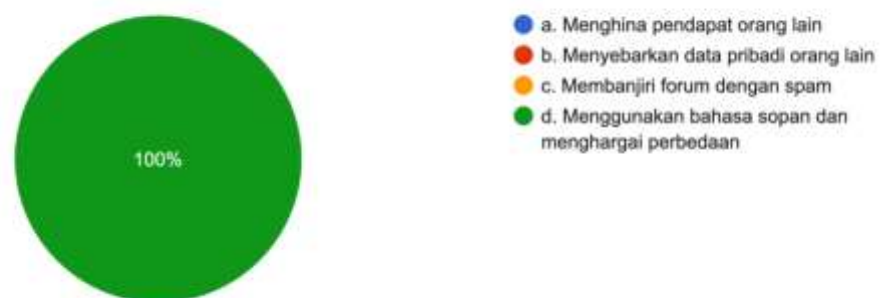


Diagram 18. Etika dalam diskusi forum Online

9. Fungsi utama VPN dalam keamanan digital adalah ...

20 jawaban

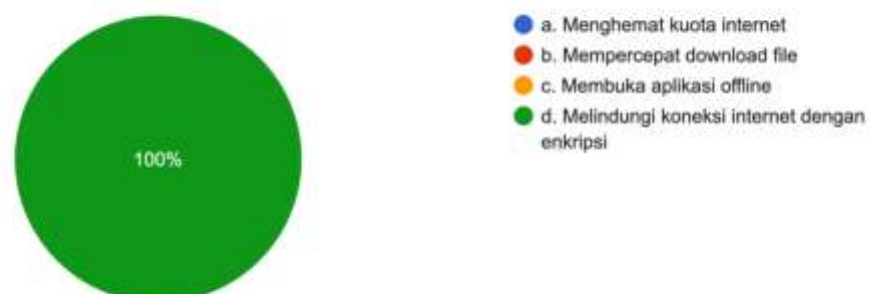


Diagram 19. Fungsi Utama VPN dalam Keamanan Digital

Peserta pelatihan memahami fungsi utama VPN dalam keamanan digital untuk melindungi koneksi internet dengan enkripsi dengan total jawaban (100%).

10. Jika menerima email mencurigakan yang meminta data pribadi, maka langkah tepat adalah ...
20 jawaban



Diagram 20. Email mencurigakan dan langkah mengatasinya

Peningkatan Pemahaman Pasca Pelatihan (Post-test)

Pemahaman peserta menunjukkan peningkatan signifikan tentang literasi dan keamanan digital setelah mengikuti pelatihan selama dua hari, berdasarkan hasil post-test yang diisi yang dibagikan melalui google form. Seluruh peserta (100%) mampu mengidentifikasi ciri phishing, kemudian sudah mampu membuat password kuat yang terdiri kombinasi huruf kapital, simbol dan angka, serta memahami pengaturan privasi digital. Hal ini mendukung temuan UNESCO bahwa pembelajaran berbasis praktik mampu meningkatkan kompetensi digital dengan cepat. Peserta juga mampu memahami dengan baik dengan metode penyampaian materi yang disertai dengan praktik langsung dan memudahkan mereka untuk mengingatnya (A.P.J.I.I., 2023).

Hasil post-test juga menunjukkan 95 persen peserta menyatakan mengabaikan atau melaporkan sebagai spam jika menerima email yang mencurigakan yang meminta data pribadi. Dari jumlah itu, hanya (5%) yang menyatakan mengunduh lampiran untuk memeriksa isinya. Dari pelatihan yang dilakukan peserta merasakan antusias untuk mengikuti dari awal sampai akhir kegiatan sebagai tindak lanjut maka dibuat rencana tindak lanjut yang akan dilakukan oleh tim pelaksana pengabdian dengan di dukung oleh peserta dan pemerintahan Gampong Uteunkot Cunda Lhokseumawe.

Perbandingan Pre-test dan Post-test

Hasil pre-test dan post-test menunjukkan terjadinya peningkatan paling signifikan pada pemahaman phishing, dari 88% (pre-test) menjadi 100% (post-test). Pemahaman sangat penting untuk kalangan pemuda dan konten creator, karena selama ini yang menjadi korban bukan hanya dari kalangan biasanya tapi juga kalangan profesional. Begitu juga dengan pemahaman jejak digital, kemudian pentingnya menjaga keamanan akun, dan kemampuan mengidentifikasi *malware* juga mengalami peningkatan dari peserta. Hasil ini konsisten dengan penelitian yang menegaskan bahwa simulasi ancaman siber efektif meningkatkan kesadaran keamanan digital (Livingstone & Helsper, 2010).

Selama sesi praktik, seluruh peserta berhasil: (1) mengaktifkan *two-factor authentication* (2FA) pada akun email maupun media sosial, (2) mengganti kata sandi lama dengan kombinasi huruf kapital dan kecil, angka, dan simbol, lalu (3) menerapkan pengaturan privasi lanjutan pada berbagai platform media sosial dan (4) mengenali ciri-ciri tautan phishing dan email mencurigakan.

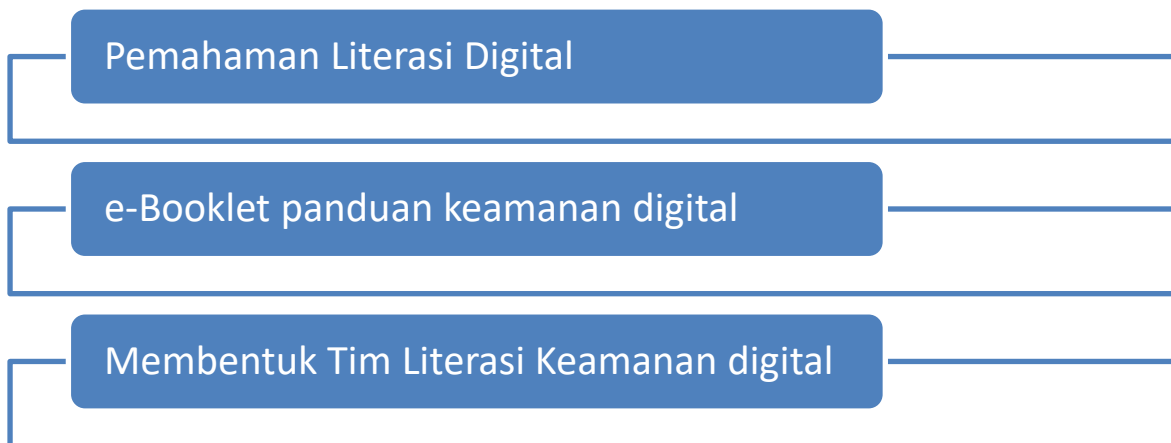
Penegasan Hubungan Temuan dan Teori

Temuan pelatihan mendukung teori literasi digital UNESCO dan model kompetensi digital *Organisation for Economic Co-operation and Development* (OECD), yang menekankan bahwa literasi digital mencakup aspek perlindungan diri dan kemampuan evaluatif di ruang digital. Kompetensi ini kemampuan menemukan, mengevaluasi dan menggunakan informasi digital, memodifikasi konten, perlindungan data pribadi, menggunakan teknologi untuk memecahkan masalah digital serta keterampilan literasi digital. Peningkatan kemampuan dalam memahami literasi dan keamanan digital pasca pelatihan menunjukkan bahwa metode pembelajaran berbasis konteks lokal mampu menjembatani kesenjangan literasi digital masyarakat. Peserta dapat menemukan langsung persoalan yang disampaikan dengan mengangkat contoh kasus yang dekat dengan mereka.

Dampak Sosial dan Rencana Tindak Lanjut

Pelatihan ini mampu meningkatkan literasi dan kesadaran keamanan digital peserta. Hal ini terlihat dari adanya peningkatan skor post-test, atau adanya perubahan perilaku keamanan digital yang dapat diamati dari peserta. Kemudian meningkatnya kemampuan peserta dalam menerapkan strategi proteksi digital secara mandiri terjadap semua akun yang dimiliki. Keselarasan antara kebutuhan peserta dan konten pelatihan merupakan salah satu faktor keberhasilan program edukasi digital. Selain itu, pelatihannya ini bukan hanya meningkatkan pemahaman individual peserta, tetapi juga mendorong terbentuknya kelompok kecil “Komunitas Sadar Keamanan Digital” di Desa Uteunkot, yang diharapkan dapat membagikan pengetahuan kepada pemuda yang lainnya.

Kelompok ini dibentuk agar dapat transfer pengetahuan kepada peserta dapat dilakukan secara berkelanjutan. Hal ini sebagaimana disarankan oleh berbagai lembaga keamanan digital internasional. Panitia pelaksana bersama perangkat gampong melanjutkan kegiatan melalui penyusunan modul keamanan digital berbasis lokal berdasarkan komitmen MoU yang sudah ditandatangani. Lalu pendampingan daring melalui grup diskusi serta penyediaan materi tutorial keamanan digital secara berkala via media sosial. Kendati demikian juga terdapat kendala yang dihadapi dalam pelatihan ini seperti ketidakstabilan jaringan internet saat sesi praktik, perbedaan tingkat kemampuan peserta, serta keterbatasan perangkat yang digunakan sebagian peserta. Kendala ini menjadi catatan untuk penyelenggaraan pelatihan lanjutan dengan pendekatan yang lebih adaptif (Anwar, 2018).



Bagan 11. Rencana Tindak Lanjut

Pemahaman, Panduan dan Tim Literasi

Dari hasil evaluasi menunjukkan masih terdapat peserta yang kesulitan membedakan informasi valid dan konten manipulative, karena itu dibutuhkan tindak lanjut dari pelatihan tersebut untuk meningkatkan kembali pemahaman literasi digital kepada peserta melalui sesi pendalaman materi, terutama pada aspek pencarian informasi. Bentuk dari keberlanjutan program, tim pengabdian menyusun *e-booklet* yang sederhana tentang keamanan digital berisi panduan praktis mengenai pengelolaan password, pengaturan privasi, deteksi phishing, dan perlindungan data pribadi untuk dibagikan kepada peserta nantinya melalui grup media sosial (Susilo et al., 2019).

Peserta juga dapat berkonsultasi dengan tim pengabdian melalui grup WhatsApp. Diharapkan peserta yang sudah mengikuti pelatihan tersebut dapat membentuk Tim Literasi Keamanan Digital di tingkat desa untuk menular pengetahuan yang dimiliki (Maskun, 2014). Tim ini berfungsi sebagai agen edukasi lokal yang memberikan penyuluhan, melakukan pendampingan, serta melaporkan potensi insiden digital seperti penipuan online.



Gambar 1. Alur Kegiatan Pengabdian



Gambar 2. Pemaparan dan simulasi materi Keamanan Digital (20 Agustus 2025)



Gambar 3. Diskusi Interaktif peserta pelatihan (20 Agustus 2025)



Gambar 4. Pemaparan Materi Keamanan Digital (20 Agustus 2025)

KESIMPULAN

Pelatihan ini diharapkan kepada para peserta memiliki pengetahuan dan wawasan dalam keamanan digital, ditengah maraknya cybercrime, para peserta diharapkan mampu menererapkan prinsip keamanan digital dan menjadi cakap digital. Pelatihan ini terselenggara berkat dukungan LPPM, tim pelaksana dan peserta yang telah mengikuti pelatihan harapannya kegiatan ini akan terus berlanjut. Untuk itu sebagai bahan masukan agar dapat dilaksanakan pelatihan berikutnya dengan membekali peserta pelatihan modul/ebooklet kemanan digital

UCAPAN TERIMAKASIH

Pengabdian ini terselenggara berkat dukungan dari semua pihak untuk itu pada kesempatan ini kami ingin mengucapkan terimakasih kepada Bapak Rektor Universitas Malikussaleh Prof. Dr. Ir. Herman Fithra, M.T., IPM., ASEAN Eng; Ketua LLPM Universitas Malikussaleh Prof. Dr. Ir. Mawardati, M.Si; Dekan Fakultas Ilmu Sosial dan Ilmu Politik; Teuku Zulkarnaen, S.E., M.M., Ph.D; Pemerintahan Gampong Uteunkot Cunda, Peserta Pelatihan serta Tim pelaksana Pengabdian.

DAFTAR PUSTAKA

- A.J.I. (2023). *Laporan kekerasan terhadap jurnalis 2023*. Aliansi Jurnalis Independen.
- A.P.J.I.I. (2023). *Survei Internet Indonesia 2023: Tabap 1*. Asosiasi Penyelenggara Jasa Internet Indonesia. <https://survei.apjii.or.id>
- Anwar, M. (2018). Cybersecurity Awareness Among Youth. In *Telematics and Informatics*.
- Budiarto, H., & dkk. (2024). Indeks masyarakat digital Indonesia. In *Badan Pengembangan SDM Komunikasi dan Digital*.
- Cybersecurity, E. U. A. (2022). *Cybersecurity skills framework*. Publications Office of the European Union.
- DataReportal. (2024). *Laporan Digital 2024 – Indonesia*.
- Informatika Republik Indonesia, K. K. (2023). *Laporan Tahunan Keamanan Siber Nasional 2023*. Kemenkominfo.
- Livingstone, S., & Helsper, E. (2010). Balancing Opportunities and Risks in Teenagers' Use of the Internet. In *New Media & Society*.
- Maskun. (2014). *Kejahatan siber (cyber crime): Suatu pengantar (Cetakan ke-2)*. Kencana Prenada Media Group.
- Nasrullah, R. (2021). *Literasi digital: Isu, risiko, dan etika*. Kencana.
- O.E.C.D. (2019). *How's life in the digital age? Opportunities and risks of the digital transformation*. OECD Publishing. <https://doi.org/10.1787/9789264311800-en>
- Penyusun, T. (2022). *Modul literasi digital untuk perguruan tinggi* (E. Ningtyas (Ed.)). AJI Indonesia.
- Rusdiah, R. (Ed.). (2020). *Data and cyber security: Technology, use cases & governance*. Perkumpulan Basis Data Indonesia.
- Susilo, M. E., Afifi, S., & Yustitia, S. (2019). *Mengurai hoaks merajut persatuan*. LPPM UPN Veteran Yogyakarta.
- U.N.E.S.C.O. (2018). *Digital Literacy Global Framework*. UNESCO Publishing.