SAFEnet

MODUL PELATIHAN

HAK DIGITAL MASYARAKAT ADAT

SAFEnet

MODUL PELATIHAN

HAK DIGITAL MASYARAKAT ADAT

MODUL Hak Digital Masyarakat Adat

Editor:

Nenden Sekar Arum

Penulis:

Daeng Ipul
Natasha D. Dhanwani

Desain Sampul:

Aghnia Nurul Yasmine

Desain Tata Letak:

Eza Al Hafidz

Ilustrasi:

Aghnia Nurul Yasmine

Daftar Isi

Bagian 1: Pengantar

Teknologi digital menjadi salah satu bagian penting dalam kehidupan masyarakat zaman sekarang yang membantu dalam banyak hal, dari komunikasi, informasi, rekreasi, hingga membantu dalam hal profesi. Seluruh lapisan masyarakat menggunakan teknologi digital, tidak peduli dari mana asal dan latar belakangnya, dan salah satu penggunanya adalah kelompok masyarakat adat.

Dalam berbagai kegiatan, masyarakat adat kerap menggunakan teknologi digital guna mendukung kerja-kerja mereka. Teknologi digital digunakan untuk melakukan komunikasi, bertukar informasi, hingga merencanakan dan melakukan advokasi. Namun dalam realitanya, masih banyak kelompok masyarakat adat yang belum memahami dan mengerti tentang hak mereka dalam mengakses dan menggunakan teknologi digital. Hak yang kerap disebut sebagai hak digital ini memang masih menjadi pengetahuan baru bagi masyarakat, termasuk bagi masyarakat adat dan pendamping masyarakat adat.

Hak digital ini mencakup beragam hak, dari hak untuk mengakses internet, hak atas kebebasan berekspresi, hingga hak atas rasa aman di internet termasuk rasa aman dari kekerasan berbasis gender *online* (KBGO). Hak-hak inilah yang sering kali masih belum dipahami.

SAFEnet, sebagai organisasi yang memperjuangkan hak-hak digital, memahami kendala tersebut. Oleh karena itu, selama bertahun-tahun SAFEnet terus memperjuangkan hak digital di Indonesia dan kawasan Asia Tenggara lewat berbagai cara, mulai

dari advokasi, pendampingan korban, perluasan jaringan, hingga peningkatan kapasitas. Peningkatan kapasitas ini dilakukan lewat beragam cara, dari diskusi, *workshop*, sampai pelatihan. Tujuan utamanya adalah meningkatkan pengetahuan dan kapasitas masyarakat umum terkait hak digital.

Modul ini disusun sebagai bagian dari peningkatan pengetahuan dan kapasitas masyarakat terkait hak digital. Modul ini juga disempurnakan dengan pengetahuan tentang keamanan digital. Pengetahuan tentang keamanan digital menjadi salah satu bagian penting untuk melindungi masyarakat adat dan pendamping masyarakat adat dari ragam serangan digital yang juga adalah bentuk pelanggaran hak digital.

Selain pengetahuan tentang keamanan digital, modul ini juga dilengkapi dengan panduan dan pengetahuan tentang hak digital lainnya, seperti pengetahuan tentang hak atas akses internet, perlindungan privasi, dan tips mengurangi risiko kriminalisasi. Pengetahuan ini dianggap penting untuk diajarkan karena tingginya risiko masyarakat adat menjadi target kriminalisasi dalam beragam konflik agraria.

Modul ini disusun bersama kelompok dan pendamping masyarakat adat melalui diskusi kelompok terfokus atau FGD. Pesertanya adalah kelompok masyarakat adat dan pendamping masyarakat adat dari beberapa daerah di Indonesia seperti, Kalimantan Barat, Jawa Barat, dan Sulawesi Utara.

Modul ini disusun agar sesuai dengan kebutuhan kelompok masyarakat adat dan pendamping masyarakat adat dengan mempertimbangkan kebiasaan, kultur, dan kebutuhan kelompok masyarakat adat dan pendamping masyarakat adat.

Modul ini bertujuan agar kelompok masyarakat adat dan pendamping masyarakat adat dapat memahami hak digital mereka serta memahami cara menjaga keamanan di dunia digital dan semua aktivitas digital bisa dilakukan secara aman dan nyaman.

Denpasar, Juli 2025

Penyusun

Struktur Pelatihan
Rincian Materi per Sesi

Bagian 2: Tentang Modul

Modul ini adalah panduan bagi pelatih dan fasilitator dalam menyelenggarakan pelatihan hak digital dan keamanan digital untuk kelompok masyarakat adat dan pendamping masyarakat adat. Modul ini terdiri atas dua bagian utama:

- ***materi pelatihan***
- ***panduan teknis pelaksanaan pelatihan***

Secara garis besar, pelatihan ini dibagi ke dalam tiga tahap utama sebagai berikut.

1. **Persiapan**

Menjelaskan proses membuat konsep pelatihan; menyusun sistem ajar (kurikulum) dan materi; serta menyiapkan fasilitas, perlengkapan, dan alat-alat yang dibutuhkan.

2. **Pelaksanaan**

Menjelaskan tentang tahap-tahap (teknis) pelatihan, tujuan pelatihan, bahan ajar, waktu, cara ajar (metode) yang digunakan dalam pelatihan.

3. **Penilaian**

Menjelaskan cara memantau dan melakukan penilaian (evaluasi) sebuah pelatihan dari proses sebelum hingga selesainya pelatihan.

Materi dalam modul ini merupakan hasil pengetahuan dan pengalaman SAFEnet dalam menyelenggarakan pelatihan keamanan digital yang telah disesuaikan dengan kebutuhan kelompok masyarakat adat dan pendamping masyarakat adat.

01 | Struktur Pelatihan

Modul ini mengacu pada struktur pelatihan keamanan digital SAFEnet yang meliputi:

1. Dasar-dasar Keamanan Digital,
2. Kebersihan Perangkat,
3. Manajemen Identitas, dan
4. Komunikasi yang Aman.

Namun, khusus untuk pelatihan hak digital dan keamanan digital bagi masyarakat adat dan pendamping masyarakat adat ini, ada tiga sesi tambahan yang dimasukkan, yaitu:

Menjelaskan proses membuat konsep pelatihan; menyusun sistem ajar (kurikulum) dan materi, serta menyiapkan fasilitas, perlengkapan, dan alat-alat yang dibutuhkan.

1. Pengantar Hak Digital bagi Masyarakat Adat,
2. Komunikasi Aman di Lapangan, dan
3. Pertolongan Pertama pada Serangan Digital.

Setiap sesi dilengkapi dengan:

1. Tujuan pembelajaran tiap sesi,
2. Estimasi waktu yang diperlukan,
3. Bahan ajar dan peralatan yang dibutuhkan,
4. Metode pelaksanaan, dan
5. Tips agar sesi menarik dan interaktif.

02 | Rincian Materi Persesi

Materi 1: Pengantar Hak-hak Digital

- Pengertian Dasar Hak Digital bagi Masyarakat Adat
- Bentuk-bentuk Pelanggaran Hak Digital Masyarakat Adat
- Situasi Hak Digital di Indonesia
- Tips dan Trik dalam Perlindungan Hak Digital

Materi 2: Dasar-dasar keamanan digital

- Konsep Dasar Keamanan Digital
- Jenis dan Tren Serangan Digital
- Strategi dan Prinsip Keamanan Digital
- Data Pribadi dan Cara Melindungi Data Pribadi
- Mitigasi (Langkah-langkah Pengamanan) dari Serangan Digital

Materi 3: Kebersihan Perangkat

- Mengenali Perangkat
- Melindungi Perangkat
- Membersihkan Perangkat
- Memperkuat Perangkat

Materi 4: Mengelola Identitas Digital

- Teori dan Konsep tentang Jejak Digital
- Mendata dan Mengelola Akun-akun Digital
- Memperkuat Keamanan Akun Google

Materi 5: Komunikasi yang Aman

- Prinsip Dasar Komunikasi di Internet
- Peramban/*Browser* yang Aman
- Platform dan Aplikasi yang Lebih Aman
- Koneksi Internet yang Aman
- Cara Cek Keamanan Surel *(Email)* dan Tautan

Materi 6: Komunikasi Aman di Lapangan

- Risiko dan Ancaman Keamanan Digital saat di Lapangan
- Persiapan Sebelum ke Lapangan
- Antisipasi terhadap Serangan Digital saat di Lapangan
- Menyembunyikan Berkas Sensitif
- Komunikasi Tanpa Internet

Materi 7: Pertolongan Pertama pada Serangan Digital

Pertolongan Pertama atau Langkah Pertama yang dapat Dilakukan saat Menjadi Korban Beberapa Serangan Digital

Struktur dan urutan materi dirancang berjenjang dan saling terhubung. Materi pertama menjadi dasar untuk memahami materi berikutnya dan seterusnya. Oleh karena itu, disarankan mengikuti sesi secara berurutan, namun fleksibilitas tetap dimungkinkan sesuai dengan kebutuhan dan kemampuan peserta pelatihan.

Bagi pelatih, modul ini dapat digunakan sebagai:

- panduan mempersiapkan dan melaksanakan pelatihan secara rapi dan tertata;

- referensi untuk membuat materi dengan konteks lokal; dan
- alat bantu agar pelatihan berjalan aman, dan menyenangkan.

Harapannya, pelatihan ini dapat memberikan manfaat nyata dan menciptakan ruang belajar yang aman dan nyaman bagi kelompok masyarakat adat dan pendamping masyarakat adat.

Pengantar
Tahap-Tahap Persiapan
Penutup

Bagian 3: Persiapan

Pengantar

Sebelum melaksanakan pelatihan, kita perlu melakukan persiapan. Tujuannya agar pelatihan dapat berjalan lancar, tertata, dan sesuai dengan kebutuhan peserta.

Ada dua unsur penting yang harus dipersiapkan:

Sebelum masuk lebih jauh, mari pahami dulu arti kata **"pelatihan"**. Menurut Kamus Besar Bahasa Indonesia (KBBI), pelatihan berarti belajar dan membiasakan diri agar mampu (dapat) melakukan sesuatu. Artinya, dari yang tidak bisa menjadi bisa atau dari yang tidak paham menjadi paham. Contohnya, seorang balita yang belum bisa berjalan perlu latihan agar bisa berjalan dengan baik.

Kemudian, **"pelatih"** adalah orang yang memiliki kapasitas atau kemampuan untuk melatih dan sudah ahli dalam tingkat tertentu serta sudah mendapatkan sertifikasi tertentu dari sebuah lembaga.

Dalam konteks modul ini, pelatih adalah orang yang:

- telah memiliki pengetahuan keamanan digital;
- telah mengikuti pelatihan untuk pelatih (*Training of Trainers*/ ToT) dari SAFEnet; dan
- siap memfasilitasi proses belajar sesuai kebutuhan peserta.

Tahap-Tahap Persiapan

Sebelum melaksanakan pelatihan, kita perlu melakukan persiapan. Tujuannya agar pelatihan dapat berjalan lancar, tertata, dan sesuai dengan kebutuhan peserta.

Ada dua unsur penting yang harus dipersiapkan:

Konsep

Hal pertama yang perlu disiapkan saat merencanakan sebuah pelatihan adalah konsep. Konsep ini biasanya diketik dalam sebuah dokumen yang dibuat dalam bentuk Kerangka Acuan Kegiatan (KAK) atau lebih dikenal sebagai *term of reference (ToR)* dalam bahasa Inggris.

Dalam tahap ini, TOR yang dibuat harus memuat poin-poin sebagai berikut.

1. Latar Belakang

Bagian ini berisikan penjelasan kenapa harus ada pelatihan keamanan digital untuk masyarakat adat dan pendamping masyarakat adat. Pada bagian ini juga dapat diberikan informasi berupa fakta dan data.

Contohnya antara lain:

- Banyak serangan digital terhadap masyarakat adat atau pendamping masyarakat adat utamanya dalam kasus konflik agraria.
- Ancaman kriminalisasi kepada masyarakat adat atau pendamping masyarakat adat, utamanya dalam kasus konflik agraria.
- Masih kurangnya pemahaman masyarakat adat atau pendamping masyarakat adat tentang hak digital.
- Tantangan yang dihadapi oleh masyarakat adat atau pendamping masyarakat adat terkait keamanan digital.
- Menjelaskan data yang ada dari lembaga lain.

Intinya, menjelaskan dalam latar belakang kenapa penting untuk membuat pelatihan keamanan digital bagi masyarakat adat dan pendamping masyarakat adat.

2. Tujuan

Bagian ini berisikan penjelasan tentang apa saja yang ingin dicapai atau hasil yang diinginkan jika pelatihan sudah diadakan. Fokusnya adalah pada hasil pelatihan dan targetnya pada peserta

pelatihan. Pada bagian ini, dapat dibuat dalam bentuk poin-poin atau paragraf singkat.

Contoh tujuan adalah:

- Meningkatkan kesadaran masyarakat adat atau pendamping masyarakat adat tentang hak digital dan keamanan digital dasar.
- Minimal 70% peserta memahami cara melindungi akun digital dan meminimalkan risiko menjadi korban serangan digital.
- Peserta paham tentang hak digital mereka.

3. Metode

Bagian ini berisikan penjelasan tentang cara ajar atau bagaimana cara pelatihan ini dijalankan. Bagian ini juga dapat menjelaskan tentang bagaimana proses belajar yang akan digunakan dalam pelatihan.

Contoh metode yang bisa digunakan:

- Presentasi tanpa tanya-jawab (satu arah);
- Diskusi interaktif (ada bagian tanya-jawab selama presentasi);
- Tanya-jawab;
- Permainan dan simulasi;
- Praktik langsung (contohnya cara mengatur kata sandi aman), dan lainnya.

Setiap sesi dalam sebuah pelatihan yang diadakan dapat menggunakan metode yang berbeda tergantung kebutuhan peserta. Berikut ini beberapa metode yang dapat digunakan untuk pelatihan hak digital dan keamanan digital bagi masyarakat adat dan pendamping masyarakat adat:

Metode	Tujuan	Cara
Teori	Meningkatkan kesadaran peserta dari yang belum tahu menjadi tahu.	Pemateri melakukan presentasi. Pemateri menjelaskan tentang teori agar peserta dapat memahami dasar-dasar pengetahuan. Pemateri memberikan tes untuk mengukur pengetahuan.
Praktik	Menerapkan teori melalui langkah-langkah teknis.	Pemateri memandu peserta mempraktikan langsung hal yang dijelaskan dalam teori. Pemateri mengenalkan konsep dan taktik. Pada cara ini dibutuhkan perangkat, seperti laptop atau ponsel yang dimiliki peserta.

Coaching* atau *Mentoring	**Membantu peserta secara individu menyelesaikan tugas atau memahami topik tertentu.**	**Fasilitator/ pelatih menjadi pendamping langsung untuk peserta. Peserta mengerjakan beberapa tugas dan fasilitator/ pelatih melakukan penilaian secara langsung. Pelatih atau fasilitator diharapkan dapat mengerti konteks lokal, baik logat, bahasa, atau dialek untuk memudahkan komunikasi dengan peserta.**
Refleksi (Diskusi Terbuka)	**Mengajak peserta berpikir kembali tentang apa yang sudah dipelajari.**	**Diskusi santai atau berbincang dengan peserta dalam bentuk pertanyaan terbuka, seperti "Apa hal baru yang kamu pelajari hari ini?" Penyampaian respons dapat dihubungkan dengan kegiatan sehari-hari peserta agar lebih relevan.**

Simulasi	Memahami konsep dengan meniru situasi nyata secara langsung.	Seperti praktik, pemateri atau fasilitator akan memandu peserta untuk melakukan beberapa hal yang sudah dijelaskan dalam teori. Peserta memainkan peran-peran untuk berpura-pura melakukan hal atau aktivitas yang diberikan agar mengalami langsung dan lebih ingat.
Diskusi Kelompok	Melibatkan seluruh peserta dalam setiap diskusi, menciptakan kondisi agar pendapat para peserta bisa didengarkan sehingga pelatihan lebih berkesan kepada setiap peserta.	Peserta dibagi menjadi beberapa kelompok untuk berdiskusi tentang pertanyaan yang diberikan oleh fasilitator/pemateri. Perwakilan kelompok dapat diminta untuk menyampaikan hasil diskusi kepada semua peserta.

Film atau Video	**Mendorong peserta lebih bebas dalam mengungkapkan apa yang ada di pikirannya.**	**Pemateri menyediakan film dan/atau video untuk memancing diskusi kepada peserta Hal ini bisa lebih efektif daripada hanya presentasi yang membuat peserta bosan.**
Studi Kasus	**Melatih peserta untuk berpikir lebih kritis dan menganalisis kasus**	**Ambil kasus yang sering terjadi di masyarakat adat terkait tentang hak atau serangan digital dan diskusikan dalam kelompok. Analisis kasus berdasarkan teori dan konsep yang sudah disampaikan.**

4. Peserta

Bagian ini berisikan penjelasan siapa yang terlibat dalam pelatihan. Untuk pelatihan hak digital dan keamanan digital bagi masyarakat adat dan pendamping masyarakat adat, peserta ideal berjumlah 15–20 orang dengan sasaran utama adalah masyarakat adat dan pendamping masyarakat adat. Peserta yang dipilih juga

harus memenuhi syarat tertentu supaya pelatihan dapat berjalan sesuai dengan baik sesuai dengan harapan.

Syarat paling dasar untuk peserta pelatihan sebaiknya terbiasa menggunakan perangkat teknologi seperti laptop dan handphone. Mengingat mungkin sebagian besar masyarakat adat atau pendamping masyarakat adat lebih terbiasa dengan handphone, maka sebagian besar materi akan difokuskan pada materi handphone. Meski begitu, diupayakan agar peserta yang hadir adalah peserta yang terbiasa dengan perangkat laptop juga. Materi tentang kebersihan dan keamanan laptop tetap akan disampaikan dengan persentase waktu 30%--70%, dengan 70%-nya lebih banyak untuk handphone.

Catatan: Buat daftar persyaratan peserta secara tertulis sebelum seleksi agar sesuai dengan tujuan pelatihan.

5. Tempat

Bagian ini berisikan penjelasan mengenai tempat pelatihan, yaitu di mana pelatihan dilaksanakan? Contoh tempat yang dapat digunakan, contohnya di hotel, kafe, kantor, atau tempat lain.

Pikirkan tempat pelatihan yang:

- Dapat menampung 15–25 orang, termasuk panitia, peserta, dan pelatih,
- Berukuran cukup luas agar penataan kursi dan meja dapat mendukung pelatihan sehingga lebih nyaman.

Pertimbangan yang dapat dipikirkan untuk menentukan tempat pelatihan:

- Apakah di tempat tersebut dapat ditata kursi dan meja berbentuk huruf U?
- Tanyakan juga kepada peserta, apakah mereka lebih nyaman duduk di kursi atau di lantai?
- Apakah tempat tersebut memiliki cahaya terang yang tidak menyilaukan?
- Apakah tempat tersebut nyaman untuk peserta?

6. Waktu

Bagian ini berisikan penjelasan mengenai hari dan tanggal pelaksanaan pelatihan. Jangan lupa tulis satuan waktu sesuai dengan daerah pelaksanaan: WIB (Waktu Indonesia Barat), WITA (Waktu Indonesia Tengah), dan WIT (Waktu Indonesia Timur).

CONTOH

Hari/Tanggal: Sabtu–Minggu, 16–17 Juni 2025
Waktu: 09.00–17.00 WIB

7. Jadwal

Bagian ini berisikan penjelasan tentang tahapan pelatihan atau bagaimana proses pelatihan tersebut berlangsung. Dengan demikian, informasi tentang jadwal dapat memberikan bayangan bagaimana proses pelatihan keamanan digital berlangsung.

Informasi yang perlu dicantumkan:

- Hari,
- Tanggal,
- Jam, dan
- Detail kegiatan setiap hari.

Informasi tentang jadwal dapat berupa tabel. Contoh informasi kegiatan adalah sebagai berikut:

No	Waktu		Durasi (Menit)	Aktivitas
Hari 1				
1	08:30	08:35	05.00	Safety Briefing
2	08:35	08:45	10.00	Pembukaan
3	08:45	09:15	30.00	Aturan Kelas dan Perkenalan
4	09:15	10:15	60.00	Pengantar Hak Digital (1)
5	10:15	10:30	15.00	Break
6	10:30	12:00	90.00	Pengantar Hak Digital (2)
7	12:00	13:00	60.00	ISHOMA
8	13:00	13:30	30.00	Penyegaran
9	13:30	14:00	30.00	Pengantar Hak Digital (3)
10	14:00	14:30	90.00	Break
11	14:30	16:00	90.00	Dasar-Dasar Keamanan Digital
12	16:00	16:30	30.00	Debrief

Hari 2				
1	08:30	09:00	30.00	Review
2	09:00	10:15	75.00	Kebersihan Perangkat (1)
3	10:15	10:30	15.00	Break
4	10:30	12:00	90.00	Kebersihan Perangkat (2)
5	12:00	13:00	60.00	ISHOMA
6	13:00	13:30	30.00	Penyegaran
7	13:30	14:45	75.00	Keamanan Akun (1)
8	14:45	15:00	15.00	Break
9	15:00	16:00	60.00	Keamanan Akun (2)
10	16:00	16:30	30.00	Debrief

Hari 3				
1	08:30	09:00	30.00	Review
2	09:00	10:15	75.00	Komunikasi yang Aman (1)
3	10:15	10:30	15.00	Break
4	10:30	11:15	45.00	Komunikasi yang Aman (2)
5	11:15	12:00	45.00	Komunikasi yang Aman di Lapangan (1)
6	12:00	13:00	60.00	ISHOMA
7	13:00	13:30	30.00	Penyegaran
8	13:30	14:15	45.00	Komunikasi yang Aman di Lapangan (2)
9	14:15	14:30	15.00	Break
10	14:30	15:30	60.00	Pertolongan Pertama Pada Serangan Digital
11	15:30	16:00	30.00	Penutupan

8. Informasi Kontak

Bagian ini berisikan penjelasan tentang siapa yang dapat dikontak jika peserta memiliki pertanyaan atau ingin berkomunikasi lebih lanjut terkait pelatihan.

Disarankan:

- Surel (*email*) resmi penyelenggara,
- Nomor ponsel aktif (bisa gunakan aplikasi aman seperti Signal), dan
- Nama penanggung jawab (bisa panitia atau fasilitator teknis).

Informasi tentang jadwal dapat berupa tabel. Contoh informasi kegiatan adalah sebagai berikut:

9. Tambahan Video

Video dibutuhkan untuk memberikan variasi dalam pelatihan sekaligus memudahkan pemberian informasi kepada peserta. Beberapa hal teknis bisa dijelaskan secara singkat dan padat lewat video.

Konten

Jika sudah selesai dalam membuat konsep, artinya sudah menjalankan satu tahap. Tahap selanjutnya dari proses persiapan pelatihan adalah menyiapkan konten atau isi pelatihan.

Konsep pelatihan ini penting dan menjadi pondasi utama yang menentukan berhasil atau tidaknya pelatihan tersebut. Berikut ini adalah bagian dari konten sebuah pelatihan.

1. Materi

Bagian ini berisikan penjelasan tentang topik-topik yang akan dipelajari selama pelatihan hak digital dan keamanan digital. Dalam pelatihan hak digital dan keamanan digital, pertanyaan yang perlu dijawab adalah, “Peserta akan belajar apa saja di pelatihan hak digital dan keamanan digital?”

Di SAFEnet, ada empat topik utama pelatihan keamanan digital.

1. Dasar-dasar Keamanan Digital
2. Kebersihan Perangkat
3. Manajemen Identitas
4. Komunikasi yang Aman.

Namun, khusus untuk pelatihan hak digital dan keamanan digital bagi masyarakat adat dan pendamping masyarakat adat, ada tiga sesi tambahan yang dimasukkan yaitu:

1. Pengantar Hak Digital bagi Masyarakat Adat;
2. Komunikasi Aman di Lapangan; dan
3. Pertolongan Pertama pada Serangan Digital.

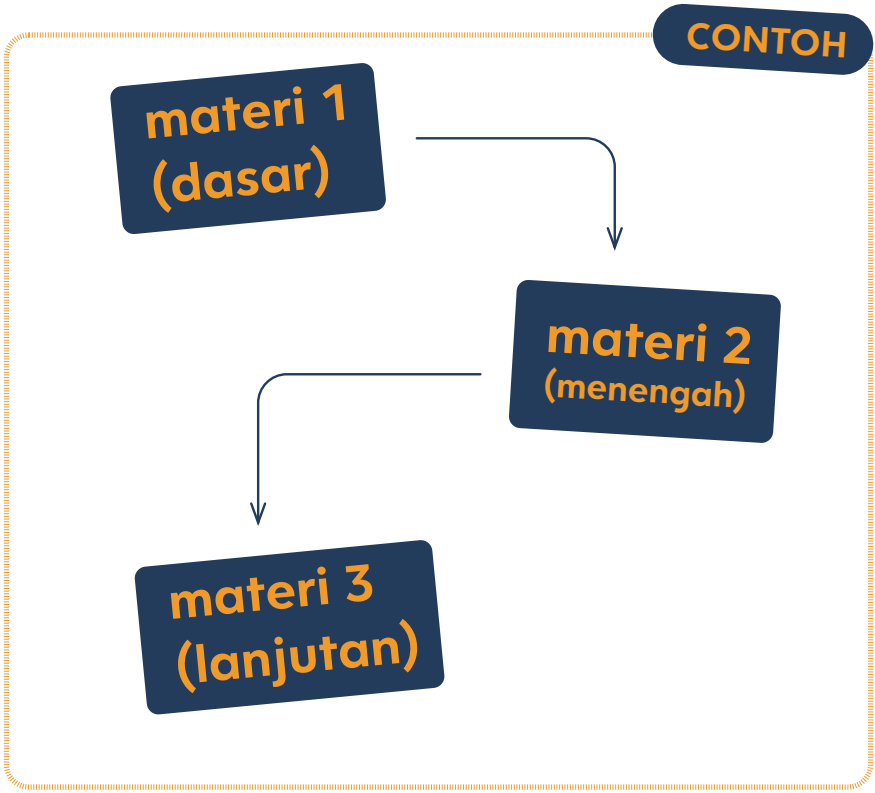
2. Struktur

Bagian ini berisikan penjelasan tentang bagaimana urutan materi yang akan disampaikan dalam pelatihan keamanan digital. Materi apa yang pertama, lalu kedua, dan seterusnya. Penting juga untuk memikirkan durasi penyampaian setiap materi yang ada.

Materi yang disampaikan harus berurutan dan tidak melompat-lompat agar tetap tersambung, terhubung, dan saling mendukung di setiap sesi.

Misalnya:

- Mulai dari materi dasar yang paling mudah, lalu ke tingkat yang sedikit sulit, setelahnya ke tingkat yang paling sulit.
- Belajar materi A terlebih dahulu lalu ke materi B karena peserta mungkin tidak akan paham materi B jika tidak belajar materi A.



3. Alur

Bagian ini berisikan penjelasan tentang teknis pelatihan atau bagaimana pelatihan akan berlangsung, yaitu urutan kegiatan seperti apa yang akan diterapkan dalam pelatihan keamanan digital dari awal hingga akhir. Contohnya adalah sebagai berikut.

1. Pembukaan & Perkenalan
2. Pemaparan Materi
3. ISHOMA (Istirahat, Sholat, Makan)
4. Diskusi Kelompok
5. Evaluasi & Refleksi Harian

Alur harus dibuat secara detail dan spesifik, tidak hanya gambaran atau bayangan saja. Mirip dengan pembuatan jadwal, namun lebih kepada konsep urutan proses kegiatan berlangsung.

4. Presentasi

Bagian ini berisikan penjelasan tentang bentuk materi yang akan disampaikan dalam pelatihan. Bagaimana cara menyampaikan materi kepada peserta?

Rekomendasi yang dapat dilakukan adalah sebagai berikut.

- Membuat presentasi menggunakan aplikasi PowerPoint, Canva, atau Keynote.
- Presentasi bisa dicetak dan dibagikan kepada peserta untuk jadi pegangan selama pelaksanaan kegiatan.
- Dalam presentasi, gunakanlah visual lebih banyak daripada teks.

- Hindari menyalin langsung dari buku panduan atau referensi.
- Gunakan gambar, ilustrasi, atau video untuk menjelaskan istilah sulit.
- Tambahkan contoh kasus nyata dari serangan digital atau pelanggaran hak digital pada masyarakat adat atau pendamping masyarakat adat.

5. Bahan Ajar

Bagian ini berisikan penjelasan tentang teknis pelatihan atau bagaimana pelatihan akan berlangsung, yaitu urutan kegiatan seperti apa yang akan diterapkan dalam pelatihan keamanan digital dari awal hingga akhir. Contohnya adalah sebagai berikut.

Sesi	Alat Bantu yang dibutuhkan
Perkenalan	Spidol, Kertas A4
Diskusi Kelompok	Kertas *flip chart* (kertas panjang abu-abu/ putih), kertas tempel (*sticky note*), karton *metaplan*, selotip kertas
Praktik	Laptop/HP
Permainan	Tali Rafia

Bahan ajar (alat-alat apa saja yang dibutuhkan) ini dapat diketahui setelah kita mengetahui dan memikirkan alur.

6. Interaksi

Bagian ini berisikan penjelasan tentang cara membuat pelatihan menjadi kegiatan yang menyenangkan bagi peserta. Setiap pelatihan yang diadakan pasti melelahkan. Karena itu, penting untuk berpikir kreatif dalam membuat kegiatan pelatihan yang tidak membosankan bagi peserta. Selain menjadi kegiatan yang menyenangkan, pelatihan juga harus membuat semua peserta terlibat dalam berpartisipasi dan berkontribusi untuk membuat suasana menjadi aman dan nyaman.

Pelatih/pemateri/fasilitator dapat mencoba memancing peserta dengan pertanyaan-pertanyaan terbuka, misalnya:

- Dalam sehari berapa jam kalian mengakses internet?
- Pernahkah berada di situasi tidak ada sinyal internet?
- Ada yang punya pengalaman akun Facebook atau WhatsApp-nya menghilang?
- Adakah yang punya pengalaman mendapatkan tautan *phishing*?

7. Pemantauan

Bagian ini berisi penjelasan tentang tindakan atau kegiatan yang dilakukan untuk mengukur perkembangan kemampuan peserta dari yang tidak tahu menjadi tahu, ataupun dari yang pemahamannya salah menjadi paham konsep dengan tepat. Kegiatan yang dinamakan pemantauan (*monitoring*) ini dilakukan

sebelum, selama, dan setelah pelaksanaan pelatihan.

- Kegiatan pengukuran pemahaman yang dilakukan sebelum pelatihan dapat berupa kegiatan peserta mengisi tes, dinamakan *pre-test*.
- Kegiatan pengukuran pemahaman yang dilakukan selama pelatihan dapat berupa permainan yang berguna mengingat kembali (*review*) materi yang sudah dibahas.
- Kegiatan pengukuran pemahaman yang dilakukan setelah pelatihan dapat berupa kegiatan peserta mengisi tes, dinamakan *post-test*.

Dalam kegiatan pemantauan, pelatih harus melihat perkembangan peserta dari sebelum, selama, dan sesudah pelatihan. Jika ada perubahan, dapat dikatakan bahwa peserta telah berkembang. Jika tidak ada perubahan, evaluasi terhadap pelatihan harus dilakukan. Kegiatan melihat ada atau tidaknya perubahan ini disebut sebagai pemantauan. Kegiatan pemantauan ini dapat dilakukan setiap hari selama pelatihan berlangsung dan melibatkan seluruh peserta.

Target capaian dari *pre-test* dan *post-test*

Dalam pelaksanaan *pre-test* dan *post-test*, tentu ada harapan yang ingin dicapai dalam setiap proses pelatihan.

Tujuan *pre-test* adalah sebagai berikut.

- Mendapatkan informasi tentang perangkat (alat-alat digital) yang biasa digunakan oleh para peserta.
- Informasi kemampuan awal peserta terkait keamanan digital.
- Informasi pemahaman peserta yang masih harus diperbaiki.

Semua informasi tersebut bisa didapatkan secara menyeluruh sebelum peserta mengikuti pelatihan.

Tujuan dari *post-test* adalah sebagai berikut.

- Ada perubahan atau peningkatan kapasitas pada peserta serta ada umpan balik dari peserta untuk meningkatkan kualitas pelatihan.
- Mendapatkan informasi mengenai metode pelatihan dan materi yang cocok bagi peserta.

Semua informasi tersebut bisa didapatkan secara menyeluruh setelah peserta mengikuti pelatihan.

Daftar Contoh Kasus atau Visual yang Berkaitan

Untuk mendukung materi dan presentasi agar lebih maksimal, pelatih dapat mempersiapkan terlebih dahulu studi kasus yang berkaitan dengan pemenuhan hak digital atau teori keamanan digital yang sering terjadi pada masyarakat adat dan pendamping masyarakat adat. Menggunakan studi kasus dalam pelatihan hak digital dan keamanan digital akan membantu peserta menjadi lebih paham karena ada contoh langsung.

Contoh kasus:

- Kriminalisasi pada masyarakat adat yang menolak tambang di daerahnya, atau
- Komentar buruk pada unggahan yang menolak pembangunan di lahan masyarakat adat.

Selain studi kasus, dapat pula menggunakan visual berupa ilustrasi, gambar, ataupun visual gerak yang menggambarkan lebih lanjut tentang teori keamanan digital yang dibahas.

8. Logistik

Bagian terakhir dalam tahap persiapan adalah menyediakan perlengkapan dan peralatan kebutuhan pendukung pelatihan, disebut sebagai logistik. Jika konsep adalah pondasi bangunan dan konten adalah bangunan itu sendiri, maka logistik adalah interior di dalam bangunan.

Jadi, agar bangunan dapat nyaman digunakan, kita butuh interior untuk mendukung bangunan tersebut. Sebaik apa pun persiapan kita tentang konsep dan konten, hasil baiknya tergantung pada seberapa siap kita mempersiapkan perlengkapan dan peralatan.

Ada istilah dalam bahasa Inggris, *"the devil is in the detail"* yang artinya 'detail yang kecil dan sederhana bisa sangat berpengaruh bagi hal yang lebih besar'. Detail yang dimaksud di sini adalah kebutuhan pendukung untuk menyokong konsep dan konten agar pelaksanaan pelatihan keamanan digital bagi komunitas dapat berhasil dengan baik.

Berikut ini adalah daftar logistik yang harus dipersiapkan untuk pelatihan keamanan digital.

Alat tulis kantor (ATK)

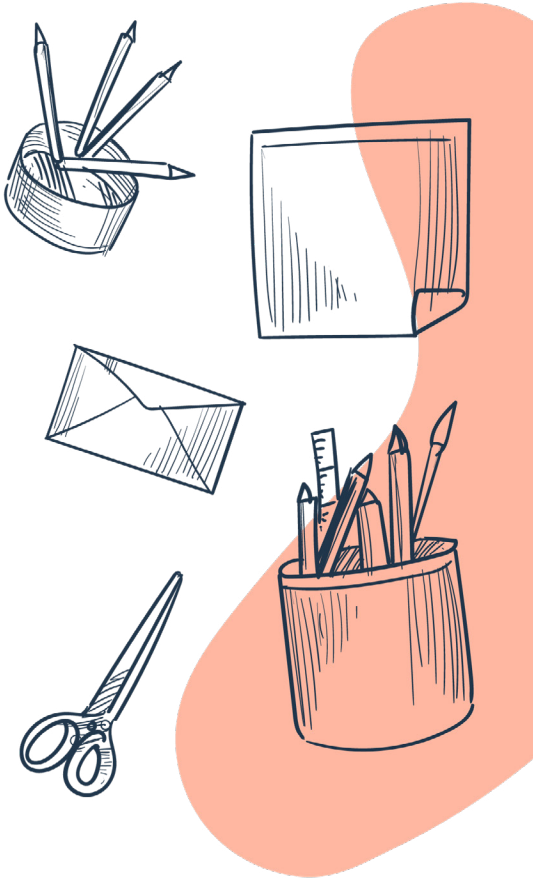
Siapkan alat-alat tulis yang dibutuhkan untuk pelaksanaan pelatihan. Selain jenisnya, perlu dipikirkan jumlah alat tulis yang dibutuhkan.

Perkirakan jumlah kebutuhan sesuai dengan

- jumlah peserta,
- jumlah sesi, dan
- jenis metode.

Jenis alat tulis yang dimaksud adalah

- kertas *flipchart*,
- kertas karton,
- pensil/pulpen,
- amplop,
- lem kertas,
- *double tape*
- selotip kertas,
- spidol papan tulis,
- spidol warna warni,
- *sticky note,*
- kertas karton,
- pin peserta,
- gunting,
- dan lain-lain.



9. Analisis risiko

Penting bagi kita mempunyai daftar atau hasil analisis risiko dalam bentuk narasi dan tulisan, terutama terkait tentang lokasi pelatihan. Risiko adalah ancaman atau dampak yang mungkin ada jika terjadi bahaya. Analisis risiko yang dimaksud pada bagian logistik adalah terkait lokasi pelatihan.

- Apakah lokasi pelatihan memiliki tingkat keamanan yang baik?
- Apakah lingkungan sekitar lokasi pelatihan menerima identitas peserta?
- Bagaimana masyarakat lokal memandang aktivitas pelatihan dan pesertanya?

Contoh Analisis Resiko:

- Jika dalam daftar peserta pelatihan ada kelompok masyarakat adat yang terkenal keras menentang pembangunan industri atau proyek strategis pemerintah dan bahkan bergesekan dengan aparat, penting untuk menilai apakah tempat pelaksanaan pelatihan rawan dari pemantauan aparat atau tidak.

- Pertimbangkan kemungkinan sebaiknya pelatihan dilaksanakan dalam kondisi *incognito mode* atau mode bersembunyi. Artinya, pelatihan sebaiknya tidak diungkap ke publik atau minimal hanya diberitahukan kepada orang terdekat, seperti keluarga atau orang kantor.

- Jadi, pada dasarnya analisis risiko adalah daftar ancaman yang mungkin membahayakan keamanan peserta dalam pelatihan.

10. Anggaran

Jelaskan secara detail dan spesifik berapa biaya yang dibutuhkan untuk menyelenggarakan pelatihan tersebut. Biaya yang dibutuhkan adalah total pengeluaran untuk pembelian atau pembiayaan fasilitas pendukung pelatihan.

Contohnya:

- biaya sewa tempat,
- biaya penginapan,
- biaya konsumsi selama kegiatan (makan berat dan camilan),
- transportasi keberangkatan dan transportasi kepulangan,
- honor narasumber,
- honor fasilitator,
- biaya pengetik-pencatat,
- biaya-biaya lain yang dibutuhkan dalam pelatihan.

Besaran biaya dapat mengikuti standar organisasi dan juga menyesuaikan standar donor atau lembaga pemberi dana.

11. Akomodasi

Pelatihan akan dilaksanakan di satu tempat tertentu dengan mengundang peserta dari beragam wilayah. Perlu untuk mempertimbangkan soal akomodasi peserta. Umumnya, akomodasi disiapkan satu kamar untuk satu orang agar setiap peserta punya privasi serta merasa lebih nyaman.

Pertimbangkan juga kemungkinan ada peserta yang akan datang membawa anaknya yang mungkin masih kecil dan tidak bisa ditinggal. Kemungkinan ini tentu berpengaruh pada biaya konsumsi, utamanya konsumsi di luar waktu pelatihan seperti makan siang dan makan malam.

12. Ruangan atau tempat

Pada umumnya pelatihan yang diadakan oleh SAFEnet membutuhkan ruangan yang memungkinkan meja-kursi diatur dalam posisi huruf U. Bentuk ini dipilih karena lebih fleksibel bagi

fasilitator dan pelatih untuk bergerak dan mendekati peserta.

Hal-hal berikut ini perlu juga untuk diperhatikan.

- Ukuran ruang cukup untuk 20–25 orang.
- Kursi dan meja untuk 10–15 peserta dapat diatur dalam pola huruf U.
- Sisa ruang yang cukup luas untuk meja panitia, serta tempat untuk menggelar kegiatan penyegaran.

13. Daftar Periksa

Agar memudahkan untuk memeriksa dan memastikan semua kebutuhan dapat terpenuhi, kita bisa menggunakan tabel yang berisi daftar periksa.

Berikut ini contoh daftar periksa persiapan pelatihan keamanan digital.

No	Tahapan/Bahan	Nama Penanggung Jawab	Sudah/Belum
1.	Kerangka Acuan Kerja (KAK)		
2.	Undangan		
3.	Lokasi		
4.	Alat Pelatihan Kertas A4 Kertas flipchart Spidol Permanen Spidol Warna Warni Proyektor Laptop Kertas Tempel Buku Catatan Daftar Hadir Selotip Kertas Dan seterusnya		
5..	Materi Presentasi		

Penutup

Dalam modul ini, pelatih diharapkan tidak hanya mengikuti secara spesifik apa yang sudah disusun. Pelatih diharapkan memiliki sisi kreatif untuk membuat konsep, konten, dan logistik sesuai kebutuhan masyarakat adat dan pendamping masyarakat adat di daerah. Sebelum melaksanakan pelatihan, penting untuk mempelajari konteks lokal agar lebih relevan/lebih terhubung dengan komunitas masyarakat adat dan pendamping masyarakat adat.

Bagian 4: Pelaksanaan

Pengantar

Pada tahap pelaksanaan kegiatan akan dijelaskan tentang bagaimana proses atau langkah-langkah pelaksanaan kegiatan setelah melakukan persiapan. Berhasil atau tidaknya sebuah pelatihan dapat dilihat pada saat pelaksanaan ini.

Alur dan struktur sebuah pelatihan hak digital dan keamanan digital dapat berbeda-beda, sesuai kebutuhan peserta dan kemampuan masyarakat adat dan pendamping masyarakat adat. Tentunya, lembaga yang mengadakan pelatihan juga memiliki kontrol dalam menentukan alur dan struktur pelatihan hak digital dan keamanan digital.

Berdasarkan pengalaman SAFEnet, dalam menyelenggarakan pelatihan keamanan digital, proses pelaksanaan biasanya dibagi menjadi dua hari dengan penyesuaian durasi dan metode penyampaian sesuai dengan situasi yang ada. Namun, mengingat pelatihan ini ditambahkan dengan materi lain, seperti pengantar hak digital, komunikasi yang aman di lapangan, dan pertolongan pertama pada serangan digital, maka waktu pelatihan akan ditambah satu hari, totalnya adalah tiga hari.

Struktur dasar pelatihan terdiri atas:

- Pembukaan dan Perkenalan,
- Pemaparan Materi,
- Diskusi,

Setiap sesi harus dirancang agar interaktif agar tidak membosankan. Komunikasi dua arah, partisipasi aktif, dan penggunaan studi kasus nyata sangat dianjurkan.

Pembukaan dan Perkenalan

Pengantar

Dalam sesi ini, fasilitator dan peserta akan mengenal satu sama lain dan menyepakati aturan kelas secara partisipatif. Peserta juga akan melihat kembali jadwal, proses, dan alur pelatihan serta menyampaikan harapannya.

Tujuan

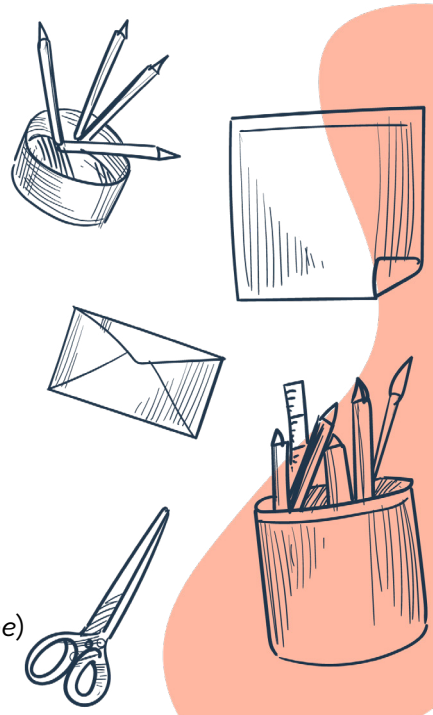
Fasilitator memastikan seluruh peserta dapat melakukan hal-hal berikut ini.

- Mengetahui alur kegiatan selama pelatihan.
- Mengenal satu sama lain, terutama nama, lembaga, dan pengalaman.
- Membagi harapan yang ingin dicapai setelah mengikuti pelatihan.

Topik

- Penjelasan tentang jadwal, aturan, dan etika di kelas.
- Penyusunan kesepakatan kelas selama kegiatan.
- Perkenalan profil diri dan lembaga masing-masing.
- Penyampaian harapan tentang pelatihan.

Bahan Ajar



- Proyektor dan layar
- Materi presentasi
- Kertas *flipchart*
- Kertas ukuran A4 kosong
- Spidol permanen
- Spidol warna-warni
- Buku tulis
- Pulpen
- Karton/*metaplan*
- Selotip kertas (*masking tape*)

Waktu

- 30 menit.

Metode

- Presentasi
- Diskusi
- Menggambar

Proses

- Fasilitator membuka kegiatan, menyapa peserta dan menjelaskan tujuan diadakannya pelatihan.

- Fasilitator membuka kegiatan, menyapa peserta dan menjelaskan tujuan diadakannya pelatihan.
- Peserta memberi waktu kepada perwakilan hotel atau tempat pelaksanaan kegiatan untuk memberikan *safety briefing* atau penjelasan tentang keamanan hotel dan proses evakuasi bila terjadi bencana.
- Fasilitator menjelaskan jadwal dan alur pelatihan sesuai jadwal yang dibuat (2–3 hari) dan/atau yang sudah dibagikan dalam KAK.
- Fasilitator membuat aturan kelas bersama peserta. Aturan kelas ini berfungsi untuk menjaga agar kelas menjadi ruang aman dan nyaman bagi semua orang.
- Materi aturan kelas bisa berbeda-beda, tetapi sebagai acuan, aturan kelas minimal berisi hal-hal berikut:

* **tepat waktu di semua sesi;**
* **saling menghormati, termasuk bila ada perbedaan pendapat;**
* **tanpa kekerasan *(do no harm)* baik dalam bentuk fisik, verbal, atau seksual;**
* **menghormati privasi, bila peserta akan mengambil gambar pastikan orang yang ada di dalam foto tidak keberatan untuk difoto dan mungkin disebarluaskan di kanal media sosial;**
* **menjaga kebersihan *(clean desk policy)*, bersihkan meja dari semua sampah atau catatan kecil yang diambil saat pelatihan.**

- Peserta diminta aktif untuk menyampaikan apabila ada keberatan dan seterusnya.

- Peserta memberikan tanggapan mengenai kesepakatan atau aturan kelas yang dibahas bersama untuk mendapatkan kesepakatan bersama.

- Setelah ada aturan kelas, peserta dapat berdiskusi tentang kotak pandora. Kotak pandora adalah hal-hal yang harus dilakukan jika ada pelanggaran terkait aturan/kesepakatan kelas. Lebih mirip seperti konsekuensi yang cenderung terkesan menyenangkan namun untuk pelanggaran yang bersifat ringan. Bentuk konsekuensi bisa dengan bernyanyi, berjoget, dan sebagainya. Pastikan bentuk konsekuensi ini tidak menyakiti peserta, baik secara fisik maupun mental.

- Peserta perlu diingatkan ada tindak lanjut penanganan apabila terjadi kekerasan, terutama kekerasan seksual. Hal ini termasuk pelanggaran berat dan tidak bisa menggunakan kotak pandora. Sebagai acuan penanganan, penyelenggara bisa menerapkan SOP Kekerasan Seksual untuk mendapatkan skema penanganan yang jelas.

- Penyelenggara bisa menggunakan SOP yang disediakan SAFEnet dan diinformasikan kepada peserta secara singkat.

- Setelah membahas aturan kelas dan kotak pandora, fasilitator meminta para fasilitator, pemateri, dan peserta mengenalkan diri termasuk latar belakang lembaga masing-masing. Ada beberapa metode perkenalan yang dapat digunakan. Berikut contoh-contoh metode perkenalan yang bisa digunakan.

* **Menggambar diri**, setiap orang menggambar sesuatu (benda, hewan, bunga, atau apapun) yang mewakili dirinya. Setiap orang punya waktu 5 menit menggambar. Setiap orang kemudian maju untuk menjelaskan gambar tersebut kepada peserta lain.
* **Peserta menuliskan tiga kata** yang menggambarkan diri mereka di kertas/post-it (tanpa nama). Kertas dikumpulkan, lalu dibacakan secara acak. Peserta saling menebak itu siapa.
* **Peserta menunjukkan atau menyebutkan satu benda favorit mereka** yang mereka bawa dan menjelaskan alasannya. Setiap peserta punya waktu dua menit untuk menjelaskan benda favorit tersebut.

- Fasilitator menutup sesi jika semua orang sudah memperkenalkan diri maupun peserta lain, lalu mengantarkan untuk sesi selanjutnya kepada pemateri.

Pengenalan Sistem Pasangan

- Untuk mendekatkan peserta dan memperlancar pelatihan, salah satu metode yang bisa digunakan adalah membuat sistem pasangan *(buddy system)*. Dalam metode ini, setiap orang yang ikut dalam pelatihan, termasuk fasilitator dan pemateri, akan memiliki pasangan masing-masing. Artinya, pasangan adalah dua orang yang saling mengingatkan. Jika jumlahnya ganjil, maka mungkin akan ada salah satu pasangan yang berjumlah tiga orang.
- Pasangan ini akan menjadi pengingat dan penjaga satu sama lain selama berlangsungnya pelatihan agar peserta tidak tertinggal. Misalnya, ketika sudah waktunya memulai

sesi, tetapi satu peserta belum ada, maka pasangannya wajib mengontak dan mengingatkan. Begitu pula jika peserta itu sakit atau berhalangan, maka pasangannya harus tahu.

- Salah satu cara menentukan pasangan adalah dengan cara mengundi. Setiap orang diminta menulis namanya di post it lalu diundi siapa akan berpasangan dengan siapa.

Pengantar Hak-hak Digital

Pengantar

Hak-hak digital masyarakat adat tidak jauh berbeda dengan hak masyarakat secara keseluruhan. Di dalamnya mencakup (1) Akses ke Teknologi, (2) Perlindungan dari segala bentuk eksploitasi, (3) Hak untuk Menentukan Nasib Sendiri dalam ruang digital, (4) Penggunaan Internet dalam Perjuangan Hak-hak Asasi Manusia. Dalam bagian ini, fasilitator pelatihan akan memberikan beberapa pemaparan konsep-konsep hak digital. Namun dalam pelatihan ini, fasilitator juga akan mengeksplorasi beberapa persoalan sehari-hari terkait pelanggaran hak digital yang dirasakan oleh masyarakat adat.

Tujuan

Tujuan dari sesi ini, peserta diharapkan dapat:

- Memahami pentingnya hak digital bagi masyarakat adat;
- Mengetahui bentuk-bentuk pelanggaran hak digital;
- Mengeksplorasi bersama contoh pelanggaran hak digital masyarakat adat; dan
- Mengeksplorasi tip dan trik dalam perlindungan hak digital.

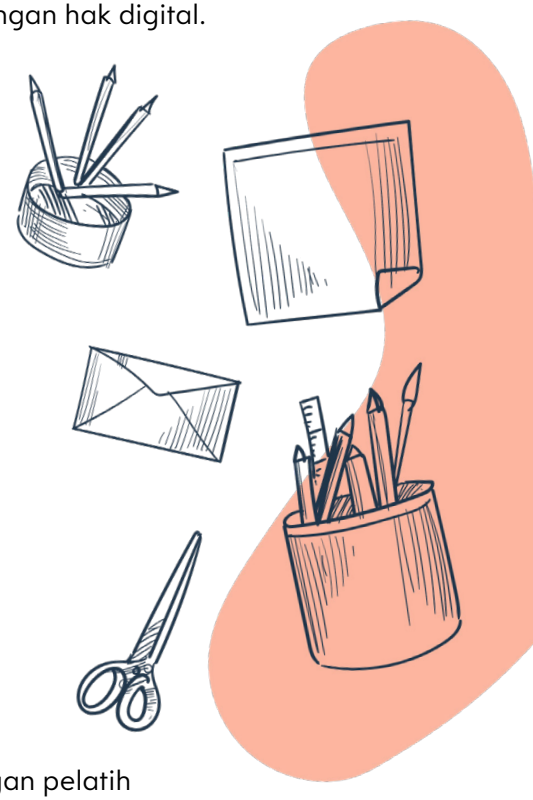
Topik

Pokok bahasan utama dari sesi ini adalah:

- Pengertian dasar hak digital bagi masyarakat adat,
- Bentuk-bentuk pelanggaran hak digital masyarakat adat,
- Situasi hak digital di indonesia, dan
- Tip dan trik dalam perlindungan hak digital.

Bahan Ajar

- Slide presentasi
- Layar
- Proyektor
- Kertas *flipchart*
- Kertas simulasi
- Kertas tempel
- Spidol



Waktu

- 180 menit

Metode

- Presentasi
- Tanya-jawab peserta dengan pelatih
- Analisis dan diskusi kelompok

Proses

Alur Sesi

Secara garis besar, alur sesi ini terdiri atas:

* **60 menit pengantar dan belanja masalah internet;**
* **30 menit penjelasan materi;**
* **30 menit diskusi kelompok;**
* **40 menit tip menghindari ancaman kriminalisasi;**
* **20 menit tip bagaimana untuk mengatakan "tidak".**

60 Menit Pengantar dan Belanja Masalah yang Berkaitan dengan Internet

- **Pelatih memulai sesi dengan menyapa kabar peserta dan pertanyaan pemancing terkait topik sesi. Misalnya, "Apa kabar pagi ini? Siapa yang sudah mengunggah *(upload)* Facebook?" Beri waktu lima menit untuk peserta menjawab pertanyaan tersebut.**
- **Pelatih menayangkan film berjudul "komunikasi" mengenai masyarakat adat yang menggunakan berbagai cara komunikasi dalam perlawanan. Di dalam video yang dibuat oleh Life Mosaic ini dijelaskan tentang masalah internet dan hak internet. Pelatih juga dapat menayangkan film lain yang relevan.**
- **Pelatih kemudian menanyakan persoalan-persoalan yang dihadapi setiap hari tentang internet. Cari setidaknya dua peserta untuk menjawab masing-masing pertanyaan tersebut.**

* **Bagaimana keadaan sosial/ekonomi/politik di wilayah kalian (masalah sosial sehari-hari dan juga persoalan masuknya proyek negara, perusahaan, konflik)?**
* **Untuk apa saja internet dibutuhkan di rumah dan di kampung?**
* **Berapa uang yang dikeluarkan ketika mengakses internet sehari-hari? Berapa sering membeli paket internet?**
* **Dari mana uang untuk internet itu berasal? apa yang mereka jual/korbankan untuk membayar kebutuhan/keinginan untuk mengakses internet?**
* **Apa saja yang diakses? Siapa (anak, ibu, bapak) mengakses apa?**
* **Apakah pernah mengalami penipuan ketika menggunakan internet?**
* **Dimana internet paling dekat bisa diakses? Dengan cara seperti apa?**
* **Siapa yang memberikan akses internet di kampung?**
* **Provider (penyedia internet) apa yang digunakan?**
* **Apakah ada bisnis internet baru yang dilakukan oleh elite di kampung atau pihak militer?**

- **Pelatih kemudian melanjutkan dengan pertanyaan berikut ini.**

  * **Bagaimana jika internet yang digunakan mendadak putus di kampung mereka?**

  * **Bagaimana jika mereka dilaporkan orang lain yang tidak suka terhadap foto/tulisan yang diunggah (di-*upload*) di Facebook?**

  * **Bagaimana jika akun WhatsApp mereka diambil alih (di-*hack*) orang lain?**

  * **Bagaimana jika foto dan tanda tangan mereka disebarluaskan oleh perusahaan/negara untuk menyatakan ketersetujuan mereka atas masuknya proyek di kampung/wilayah marga mereka?**

  * **Pelatih menjelaskan bahwa kejadian-kejadian di atas menunjukkan pentingnya pemenuhan, perlindungan, dan penghormatan terhadap hak-hak digital.**

30 MENIT PENJELASAN MATERI

- **•Pelatih menjelaskan pengertian materi utama sebagai berikut:**

* **Pengertian tentang hak, yaitu sesuatu yang dimiliki setiap orang dan bebas untuk digunakan maupun tidak digunakan. Contohnya, hak untuk hidup, hak atas tanah, hak atas lingkungan, makan, dan belajar.**

* **Hak asasi manusia adalah hak dasar yang dimiliki setiap orang sejak lahir, misalnya hak untuk hidup yang layak.**

* **Hak-hak digital adalah hak asasi manusia yang berlaku di dunia digital. Contohnya, hak untuk bisa menggunakan internet, hak untuk bekerja di internet, dan semacamnya.**

* **Hak-hak digital terdiri atas hak untuk mengakses internet, hak untuk bebas berekspresi, dan hak atas rasa aman di internet.**

* **Hak untuk mengakses internet terkait dengan layanan dan konten.**

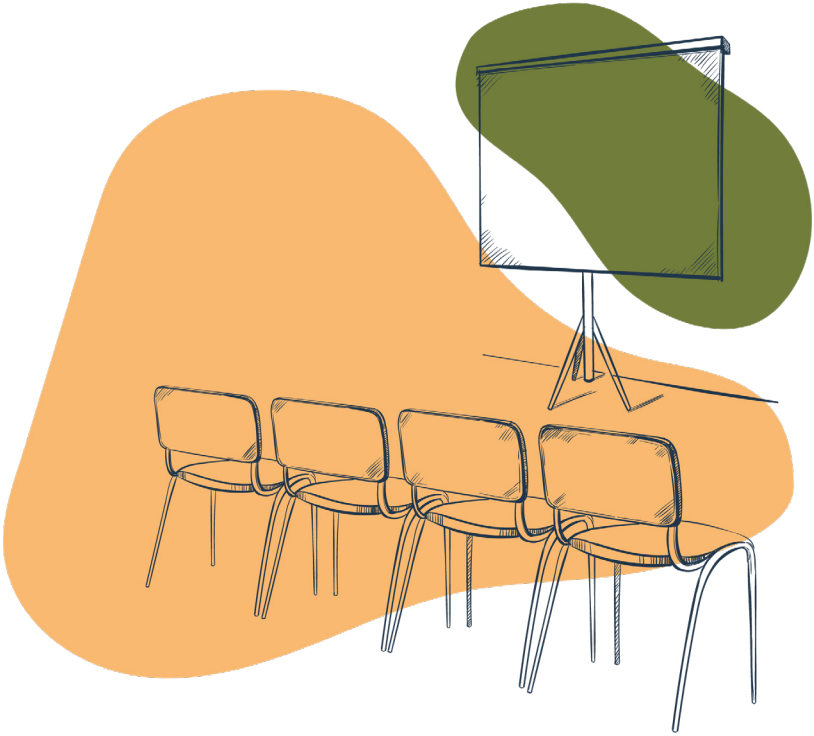
* **Hak untuk bebas berekspresi termasuk ekspresi politik, gender, budaya, dan lain-lain**

* **Hak atas rasa aman termasuk hak melindungi privasinya, hak untuk melindungi data-data pribadinya, juga hak bebas dari teknologi yang membeda-bedakan.**

* **Pelatih menjelaskan bentuk-bentuk pelanggaran hak-hak digital, seperti pemutusan akses internet, kriminalisasi terhadap ekspresi, serangan digital, dan kekerasan berbasis gender.**

* **Pelatih menunjukkan data hasil pemantauan SAFEnet selama tahun 2024.**

* **Pelatih mempersilakan peserta untuk bertanya tentang materi yang sudah dijelaskan. Fokusnya untuk memperdalam pengetahuan peserta tentang hak-hak digital.**



30 Menit Diskusi Kelompok

- **Pelatih membagi peserta ke dalam tiga kelompok dengan cara berhitung 1, 2, 3 secara berurutan. Peserta yang menyebut angka 1 masuk kelompok 1, peserta yang menyebut angka 2 masuk kelompok 2, dan seterusnya.**
- **Peserta berdiskusi dalam kelompok selama 20 menit untuk membahas pertanyaan kunci, "apa saja pelanggaran hak-hak digital yang dialami di daerah masing-masing?"**
- **Hasil diskusi dicatat dalam kertas *flipchart* yang dibagi dalam empat kolom yaitu akses internet, kebebasan berekspresi, serangan digital, dan KBGO.**
- **Setelah diskusi kelompok selesai, setiap peserta akan presentasi masing-masing 7 menit untuk menyampaikan hasil diskusi kelompok.**
- **Pelatih menyimpulkan setelah semua kelompok selesai presentasi dengan menekankan pentingnya hak-hak digital bagi masyarakat adat.**

40 Menit Tip Menghindari Ancaman Kriminalisasi

Satu pelatihan kecil tentang cara menuliskan fakta yang baik ketika terjadi sebuah permasalahan di kampung/desa (misal, masuknya tambang, masuknya perusahaan perkebunan, dan lainnya) di sosial media mereka. Di sini peserta akan diajak untuk menentukan di wilayah mana, ada masalah apa, dan bagaimana menuliskan masalah itu ke publik (internet) dengan cara-cara yang aman sehingga terhindar atau lebih resisten terhadap ancaman kriminalisasi.

- **Pelatih membagi peserta ke dalam tiga kelompok dengan cara berhitung 1, 2, 3 secara berurutan. Peserta yang menyebut angka 1 masuk kelompok 1, peserta yang menyebut angka 2 masuk kelompok 2, dan seterusnya.**

- **Pelatih menyediakan sebuah peta kampung/desa//wilayah marga yang telah dibuatnya, yang di dalamnya terdapat persoalan yang telah dituliskan dalam kertas *flipchart*.**

- **Pelatih meminta peserta untuk menuliskan bagaimana biasanya mereka menuliskan post Facebook atau di sosial media setiap terjadi masalah di wilayah dalam peta, pada kertas simulasi post baru Facebook. Selain itu juga foto seperti apa yang diambil oleh para peserta.**

- **Setelah menuliskan simulasi post baru di Facebook mengenai masalah yang mereka hadapi, peserta mempresentasikan tulisannya ke publik (kelompok peserta lainnya)**

- **Kelompok peserta lain diminta memberi komentar bagian mana yang baik dan mana yang cukup rentan mendapatkan ancaman dari simulasi post peserta yang sedang presentasi**

- **Setelah semua kelompok selesai mempresentasikan hasil simulasi post-nya, pelatih akan memberi kesimpulan dari hasil presentasi serta tip dan trik bagaimana menulis/membuat post yang baik di sosial media sehingga terhindar dari ancaman kriminalisasi.**

20 Menit Tip Bagaimana untuk Mengatakan “Tidak”

Satu pelatihan kecil tentang cara mengatakan “tidak” bagi siapa pun yang ingin mengambil data/informasi kampung/desa/marga ataupun individu. Ini merupakan hal genting karena semakin banyak perusahaan/negara mengambil data di dalam sebuah komunitas. Data yang diambil antara lain adalah peta wilayah marga, KTP, tanda tangan, foto, video, dan bahkan rekaman wawancara.

- **Pelatih menanyakan pengalaman-pengalaman peserta dan meminta peserta untuk menceritakannya, setidaknya tiga peserta.**
- **Di sini, pelatih memberikan tip apa saja yang perlu ditanyakan oleh komunitas ketika ada yang ingin mengambil data di kampung/desa. Pertanyaan-pertanyaan yang dapat ditanyakan adalah sebagai berikut.**

* **Siapa yang mengambil data, apakah komunitas mengenalnya?**
* **Dokumen surat izin seperti apa yang dibawa?**
* **Apa saja yang ingin didapatkan?**
* **Di mana data akan digunakan atau disebarluaskan?**
* **Untuk kepentingan yang seperti apa?**
* **Apa saja resiko dari memberikan dan penyebarluasan data itu?**
* **Apa ada dokumen berisi semua detail yang ditanyakan yang dapat ditandatangani kedua belah pihak dan disimpan oleh komunitas?**

- **Pelatih kemudian menyatakan bahwa jika peserta/komunitas/masyarakat tidak puas dengan jawaban-jawaban yang diberikan oleh mereka yang memiliki niat untuk mengambil data di dalam kampung/desa/komunitas, mereka memiliki hak untuk mengatakan "tidak".**

- **Selain pertanyaan-pertanyaan yang dapat diajukan, pelatih juga memberikan tip untuk mengetahui apabila ada orang yang mengambil foto/video/rekaman suara dengan cara tersembunyi.**

- **Dengan ini, bagian "Pengantar Hak Digital" selesai, pelatih dapat memberikan kesimpulan dari seluruh materi Hak Digital.**

Dasar-dasar Keamanan Digital

Pengantar

Pada sesi ini, peserta akan mempelajari teori dasar tentang keamanan digital, prinsip, dan strategi menerapkan keamanan digital dasar secara sederhana. Dalam pelatihan ini, pelatih akan memberikan pembekalan yang kebanyakan berupa teori untuk meningkatkan kesadaran tentang maraknya serangan digital dan strategi untuk meningkatkan keamanan digital secara personal maupun kelembagaan.

Tujuan

Tujuan dari sesi ini adalah peserta diharapkan dapat:

- Memahami konsep keamanan digital, termasuk data, jenis, dan target serangan digital;
- Memahami strategi mengurasi risiko serangan digital; dan
- Memahami konsep dari keamanan digital.

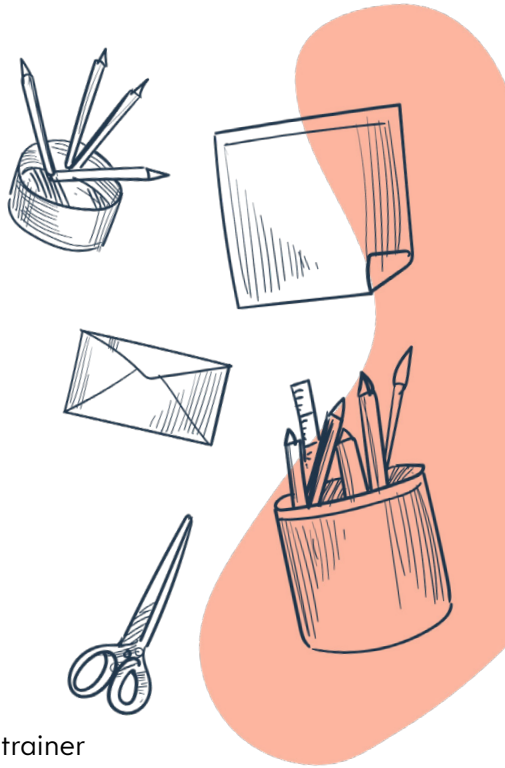
Topik

Pokok bahasan utama dari sesi ini adalah:

- Konsep dasar keamanan digital;
- Jenis dan tren serangan digital;
- Strategi dan prinsip keamanan digital;
- Data pribadi dan cara melindungi data pribadi; dan
- Mitigasi (langkah-langkah pengamanan) dari serangan digital.

Bahan Ajar

- *Slide* (salindia) presentasi
- Layar
- Proyektor
- Kertas *flipchart*
- Kertas tempel
- Spidol



Waktu

- 90 menit.

Metode

- Presentasi
- Tanya-jawab peserta dengan trainer
- Analisis dan diskusi kelompok

Proses

Alur Sesi

Secara garis besar, alur sesi ini terdiri atas:

* **10 menit pengantar;**
* **30 menit penjelasan materi;**
* **30 menit diskusi kelompok;**
* **20 menit presentasi kelompok**

10 Menit Pengantar

- **Pelatih akan membuka sesi dan menyapa peserta.**
- **Pelatih bertanya kepada peserta mengenai pengalaman berinternet dan menggunakan gadget sehari-hari. Contoh pertanyaan, "Dalam sehari berapa jam menggunakan internet? Untuk apa saja?" atau "Apakah teman-teman pakai media sosial setiap hari? Apa saja yang dipakai?", dan pertanyaan sejenisnya.**

30 Menit Penjelasan Materi

- **Pelatih akan menjelaskan tentang apa itu serangan digital dan bagaimana karakteristik serta bahayanya serangan digital sebagai berikut.**

  * **Bisa terjadi dalam 24 jam, tanpa mengenal waktu.**
  * **Pelakunya bisa dari mana saja dan sulit untuk diketahui. Berbeda dengan serangan fisik yang kadang pelakunya masih mudah untuk dikenali, serangan digital benar-benar bisa menyembunyikan siapa pelakunya.**
  * **Tujuan serangan bisa apa saja, bisa bermotif ekonomi, bisa juga bermotif politis.**
  * **Makin tak terlihat, makin berbahaya.**
  * **Dampak tidak bisa diukur, bisa berdampak pada fisik, ekonomi, atau psikologi korban.**
  * **Bentuknya sangat beragam. Bisa dalam bentuk serangan yang menyasar teknis, bisa juga serangan yang menyasar psikologi korban.**

- **Pelatih akan menjelaskan jenis, contoh serangan digital yang ada di laporan tahunan SAFEnet. Pada dasarnya, serangan digital itu dibagi menjadi dua bentuk, yaitu serangan yang menggunakan kemampuan teknis (serangan kasar), atau serangan yang tidak menggunakan kemampuan teknis dan lebih menyerang psikologis korban (serangan halus). Contoh serangan kasar antara lain sebagai berikut.**

    * ***Phishing***: pemancingan melalui tautan berbahaya, baik lewat pesan singkat maupun surel *(email).*
    * **Penyadapan**: menyadap komunikasi kedua belah pihak.
    * **Peretasan**: penguasaan atau bahkan pengambilalihan aset digital korban.
    * **DDoS *Attack***: serangan yang membanjiri peladen (server) target dengan bot sehingga tidak dapat diakses.
    * ***Robocall***: panggilan dari nomor tidak dikenal yang dilakukan berulang-ulang.
    * **SMS *Masking*** : pengiriman pesan atas nama target serangan dengan isi pesan yang justru bertentangan dengan apa yang dimaksud oleh target.

- **Contoh serangan halus adalah sebagai berikut.**

  * ***Doxing***: pengungkapan data-data pribadi target serangan untuk tujuan merusak nama baik atau menjatuhkan kredibilitas.
  * ***Trolling***: penyerbuan membabi buta pada unggahan target serangan dengan tujuan demoralisasi atau mengacaukan situasi.
  * **Impersonasi**: pembuatan akun tiruan target serangan yang mengunggah hal-hal bertentangan dengan kampanye atau sikap target serangan.
  * **Kriminalisasi**: pemidanaan terhadap target serangan untuk menekan atau meneror.

- **Pelatih akan memaparkan data serangan digital yang dapat diambil dari laporan pemantauan situasi hak digital SAFEnet. Tekankan bahwa jumlah insiden serangan digital meningkat setiap tahun dan biasanya bersifat politis.**

- **Pelatih menanyakan apakah peserta pernah menjadi korban serangan digital semacam penipuan atau scam, phishing, dan sejenisnya? Bagaimana mereka menyelesaikan masalah tersebut? Minta peserta untuk cerita secara singkat terkait hal tersebut.**

-

- **Pelatih menjelaskan strategi dan prinsip keamanan digital kepada peserta. Strategi tersebut adalah sebagai berikut.**

  * **Mengurangi jejak digital** dengan mengurangi aktivitas atau pengungkapan data pribadi melalui media digital. Dalam kehidupan sehari-hari, misalnya, mengurangi jejak digital dapat dilakukan dengan tidak mengunggah tanggal lahir, nama ibu kandung, alamat rumah, dan semacamnya. Contoh lain, ketika berada di lapangan untuk menginvestigasi, kita tidak perlu mengungkapkan perjalanan kita secara detail mulai dari boarding sampai investigasi di lapangan.

  * **Mengendalikan sejauh mana data kita dapat diakses** atau siapa saja yang dapat mengakses data tersebut. Strategi ini antara lain berupa mengatur sejauh mana sebuah aplikasi di ponsel kita dapat mengakses data-data termasuk kontak, isi pesan, kamera, dokumen, dan lain-lain. Bisa juga bentuknya adalah mengatur siapa saja yang dapat melihat unggahan kita di Instagram, Twitter, Facebook, dan lain-lain.

  * **Melindungi aset-aset digital** kita dengan langkah tertentu agar tidak dengan mudah diakses atau dikuasai orang lain. Praktiknya dapat berupa pembuatan kata sandi yang lebih kompleks agar lebih kuat, menerapkan autentikasi dua langkah (2FA), atau mengenkripsi aset-aset digital kita.

  * **Menyembunyikan jejak digital** ketika melakukan aktivitas daring. Strategi ini antara lain dilakukan melalui penggunaan jaringan virtual pribadi atau *virtual private network* (VPN) sehingga alamat protokol internet *(IP Address)* kita tidak dapat dilacak dengan mudah, serta penggunaan akun anonim untuk aktivitas berisiko tinggi.

* **Menggunakan alternatif platform atau layanan digital** yang lebih menjamin privasi dan atau keamanan penggunanya. Di luar layanan-layanan yang sudah kadung populer, seperti Google, sebenarnya banyak juga aplikasi lain yang tidak mengeksploitasi data pengguna, seperti Protonmail untuk Surel, Mega.nz untuk komputasi awan, dan lain-lain.

- **Pelatih menekankan tiga aspek yang saling berkaitan dalam hal keamanan digital, yaitu manusia, teknologi, dan kebijakan. Manusia adalah faktor penting sebagai pengguna teknologi, sementara teknologi ditentukan oleh seberapa baru teknologi yang digunakan. Terakhir adalah soal kebijakan, baik itu kebijakan personal maupun kebijakan lembaga. Ketiga faktor ini saling terkait satu sama lain.**
- **Pelatih memberikan penjelasan tentang prinsip dasar keamanan digital sebagai berikut.**

* **Menyesuaikan situasi personal dan konteks**. Setiap orang memiliki pemahaman dan kebutuhan keamanan digital berbeda-beda. Tingkat keamanan digital satu orang berbeda dengan orang lain; satu lembaga berbeda dengan lembaga lain. Organisasi yang intensif menggunakan media digital tentu berbeda tingkat keamanan dan prioritasnya dibandingkan dengan organisasi yang bekerja di akar rumput. Begitu pula dengan konteksnya. Apa yang berlaku pada situasi saat ini, belum tentu tepat diterapkan pada situasi selanjutnya. Selain karena situasinya berbeda, teknologinya juga mungkin akan berbeda. Oleh karena itu, penting untuk selalu melakukan penilaian risiko dan ancaman agar dapat menyesuaikan dengan situasi dan konteksnya.

* **Memengaruhi dan saling terkait.** Keamanan digital merupakan satu kesatuan tindakan yang akan saling memengaruhi dan terkait. Untuk dapat berkomunikasi menggunakan platform terenkripsi, misalnya, harus dilakukan oleh kedua belah pihak yang berkomunikasi. Jika pihak penerima tidak memiliki kunci enkripsi, maka dia tidak akan dapat membaca pesan terenkripsi tersebut. Secara personal, tindakan kita untuk mengamankan aset digital juga menuntut tindakan lain yang mendukung. Pemisahan identitas antara bekerja dan belanja secara daring, misalnya, akan lebih aman jika diikuti dengan pembuatan surel dan kata sandi berbeda pula. Untuk dapat mengelola kata sandi berbeda-beda, kita memerlukan aplikasi pengelola kata sandi (password manager). Contoh lain adalah dalam satu lembaga, tidak dapat kalau hanya satu orang yang punya standar tinggi tentang keamanan digital, sementara anggota lainnya dengan mudah mengekspos data atau aset lembaga. Hal ini secara umum juga membuat lembaga tersebut menjadi sangat berisiko.

* **Mencegah sebelum terjadi.** Banyak orang berpikir bahwa dirinya bukan siapa-siapa sehingga tidak perlu melakukan mitigasi karena merasa risiko dan ancamannya rendah. Padahal, sering kali serangan digital justru menyasar titik paling lemah dalam sebuah jaringan ataupun organisasi. Dia baru sadar ketika sudah mengalami serangan. Karena itu, akan lebih baik jika kita mencegah agar serangan tidak terjadi. Kalau pun terjadi, serangan itu tidak berhasil atau kalau serangan itu berhasil, dampaknya tidak akan terlalu besar karena sudah ada upaya mitigasi. Sebab, begitu serangan sudah terjadi dengan dampak buruk, akan lebih susah untuk memulihkannya. Hal ini sama seperti kesehatan, mencegah selalu lebih baik daripada mengobati.

* **Melawan kenyamanan.** Untuk dapat mencegah terjadinya serangan digital, kita harus mulai meninggalkan kenyamanan. Dalam banyak kasus, kenyamanan perilaku digital kita berbanding lurus dengan risiko yang kita hadapi. Misalnya, penggunaan satu kata sandi untuk semua akun *(one-for-all password)* memang sangat nyaman karena cukup mengingat satu kata sandi untuk akun berbeda-beda. Keamanan digital memerlukan tahapan yang lebih rumit dibandingkan perilaku sehari-hari. Bagi sebagian orang, tindakan ini akan membuat tidak nyaman, yaitu menggunakan kata sandi yang lebih panjang dan berbeda-beda tiap akun dan menambahkan pengamanan ganda untuk setiap akun.

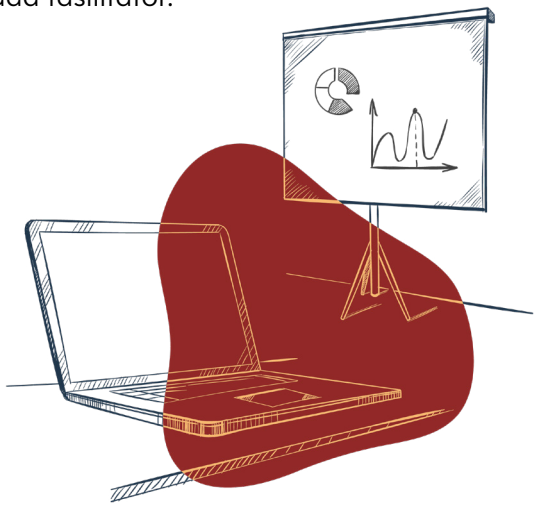
* **Mengubah persepsi dan perilaku.** Pada akhirnya, keamanan digital adalah soal perilaku. Pengetahuan dan kesadaran tentang keamanan digital saja tidak cukup. Pengetahuan itu harus diterapkan dalam bentuk perubahan perilaku. Dari semula menganggap data pribadi sebagai hal tidak berharga, menjadi menganggap sebagai hal yang penting untuk dijaga. Dari semula tidak sadar tentang potensi eksploitasi data pribadi untuk menyerang kita, menjadi sadar dan lebih waspada. Kesadaran itu kemudian diterapkan dalam bentuk perilaku sehari-hari, yaitu mengubah kebiasaan dan kenyamanan yang berbahaya, menjadi lebih waspada dengan terus-menerus menerapkan upaya mitigasi dalam perilaku sehari-hari. Hal ini tentu memerlukan konsistensi.

30 Menit Diskusi Kelompok

- **Pelatih membagi peserta menjadi tiga kelompok dengan cara berhitung 1, 2, 3 secara berurutan.**
- **Setiap kelompok diberi satu contoh perilaku berisiko atau contoh serangan digital. Misalnya phising lewat pesan singkat atau orang yang mengunggah foto KTP di media sosial.**
- **Setiap kelompok diminta untuk berdiskusi tentang risiko dari perilaku atau ancaman tersebut, serta apa mitigasinya.**
- **Hasil diskusi dicatat di atas kertas *flipchart*.**

20 Menit Presentasi Kelompok

Perwakilan peserta mempresentasikan hasil diskusinya dan tanya-jawab dengan pelatih dan peserta lain selama 20 menit. Pelatih memberi kesimpulan sesi, menutup sesi, dan mengembalikan kepada fasilitator.



Kebersihan Perangkat

Pengantar

Dalam sesi ini, peserta akan mempelajari pentingnya kebersihan digital dan menerapkannya pada ponsel dan laptop untuk meningkatkan keamanannya. Pelatih akan menjelaskan tahapan kebersihan perangkat, yaitu mengenali, melindungi, membersihkan, dan memperkuat perangkat.

Tujuan

Pada akhir sesi, peserta diharapkan mampu:

- Mengenali spesifikasi perangkatnya,
- Mengatur keamanan dan privasi perangkatnya,
- Membersihkan jejak digital perangkatnya, dan
- Menggunakan aplikasi untuk meningkatkan keamanan perangkatnya.

Pokok Bahasan

Materi sesi ini terdiri atas empat bagian utama, yaitu:

- Mengenali perangkat,
- Melindungi perangkat,
- Membersihkan perangkat, dan
- Memperkuat perangkat.

1. Mengenali Perangkat

Agar dapat menggunakan dan menguatkan perangkat, peserta terlebih dulu akan mengenali dan memahami perangkat yang digunakan berupa:

- Informasi perangkat dan
- Sistem operasi
- Pengaturan keamanan dan
- Pengaturan privasi

2. Melindungi Perangkat

Setelah mengenali perangkat, peserta akan melindungi perangkatnya termasuk:

- Pelindung luar,
- Penutup kamera, dan
- *Password* (kata sandi).

3. Membersihkan Perangkat

Peserta akan diajak untuk membersihkan perangkat mereka, dengan cara:

- Membersihkan tampilan,
- Menggunakan aplikasi pembersih, dan
- Membersihkan jejak wi-fi.

4. Melindungi Perangkat

Peserta diajak untuk memperkuat perangkat mereka dengan beberapa cara, seperti: perangkatnya termasuk:

- Memasang antivirus,
- Melakukan pencadangan data, dan
- Memperbarui aplikasi dan sistem operasi.

Bahan dan Peralatan

Bahan dan peralatan dalam sesi ini adalah:

- *Slide* (salindia) presentasi
- Layar,
- Proyektor,
- Laptop, dan
- Ponsel.

Waktu

- 135 menit.
  Sesi ini terbagi antara dua sesi, yaitu kebersihan perangkat laptop (75 menit) dan kebersihan *handphone* (ponsel) (90 menit).

Metode

- Presentasi
- Praktik

Proses

- **Pelatih membuka sesi dengan menyapa peserta sebagai jembatan. Misalnya, dengan bertanya bagaimana tidurnya apakah enak atau tidak? Lanjutkan dengan pertanyaan, "Apakah ponselnya juga sudah mendapatkan istirahat yang sama?".**

- Pelatih membuka sesi dengan menyapa peserta sebagai jembatan. Misalnya, dengan bertanya bagaimana tidurnya apakah enak atau tidak? Lanjutkan dengan pertanyaan, “Apakah ponselnya juga sudah mendapatkan istirahat yang sama?”.
- Pelatih menanyakan kepada peserta, berapa lamakah waktu mereka bersama dengan ponsel mereka setiap hari? Pertanyaan ini untuk mengajak peserta menyadari betapa penting dan dekatnya ponsel dengan kehidupan mereka.
- Pelatih menjelaskan bahwa perangkat digital juga sama seperti tubuh manusia, perlu dikenali, dilindungi, dibersihkan, dan diperkuat agar lebih kuat menghadapi virus.
- Pelatih menerangkan bahwa kebersihan perangkat terdiri atas empat tahap utama, yaitu (1) mengenali, (2) melindungi, (3) membersihkan, dan (4) memperkuat.
- Pelatih bertanya kepada peserta mengenai apakah mereka mengenali perangkat masing-masing. Misalnya, pelatih bertanya ke salah satu peserta, “Apa nama perangkatnya?” atau “Berapa kapasitas memorinya?” Tujuan pertanyaan ini adalah untuk menggali sejauh mana peserta tahu tentang perangkatnya.
- Pelatih mengajak peserta untuk mengenali spesifikasi laptop dan ponsel masing-masing, termasuk nama, model, sistem operasi dan versinya, penyimpanan, dan lain-lain. Berikut adalah cara mengenali perangkat.

- WINDOWS: PENGATURAN – SISTEM – TENTANG – PENGELOLA PERANGKAT.
- MACOS : ABOUT THIS MAC – OVERVIEW – STORAGE.
- ANDROID : SETTING – ABOUT PHONE.
- IOS : SETTING – GENERAL – ABOUT.

- **Pelatih menjelaskan cara mengatur keamanan laptop dan ponselnya termasuk akses pada lokasi, mikrofon, kamera, gerakan, dan lain-lain. Tanyakan kepada diri sendiri, seberapa penting aplikasi tersebut memiliki akses pada perangkat kita berdasarkan kategori di atas. Bila dirasa tidak perlu, segera lepaskan atau atur "selalu bertanya."**

- **Pelatih menjelaskan tahapan melindungi laptop dan ponsel dengan terlebih dulu bertanya kepada peserta, "Kalau ponselnya rusak, akan diservis di mana?", "Apakah mereka kenal tukang servisnya?", "Bagaimana kalau tukang servisnya justru menyalahgunakan isi ponsel tersebut?"**

- **Pelatih lalu menjelaskan pentingnya melindungi perangkat baik dari sisi fisik maupun aplikasi.**

- **Pelatih menjelaskan perlindungan fisik pada perangkat digital termasuk melindungi dengan *soft case, hard case,* pelindung layar, dan pelindung kamera.**

- **Perlindungan fisik pada perangkat juga termasuk menggunakan secara wajar dan tidak berlebihan dari sisi waktu, misalnya, memakai ponsel sambil mengisi daya.**

- **Pelatih menerangkan bahwa tahapan perlindungan dari sisi aplikasi juga perlu dilakukan, termasuk dengan menggunakan kunci, PIN, kata sandi, pola, dan biometrik (sidik jari). Pelatih bertanya kepada peserta, apakah perangkat mereka (laptop dan ponsel) dikunci? Kalau tidak, apa alasannya? Kalau dikunci pakai jenis penguncian apa?**

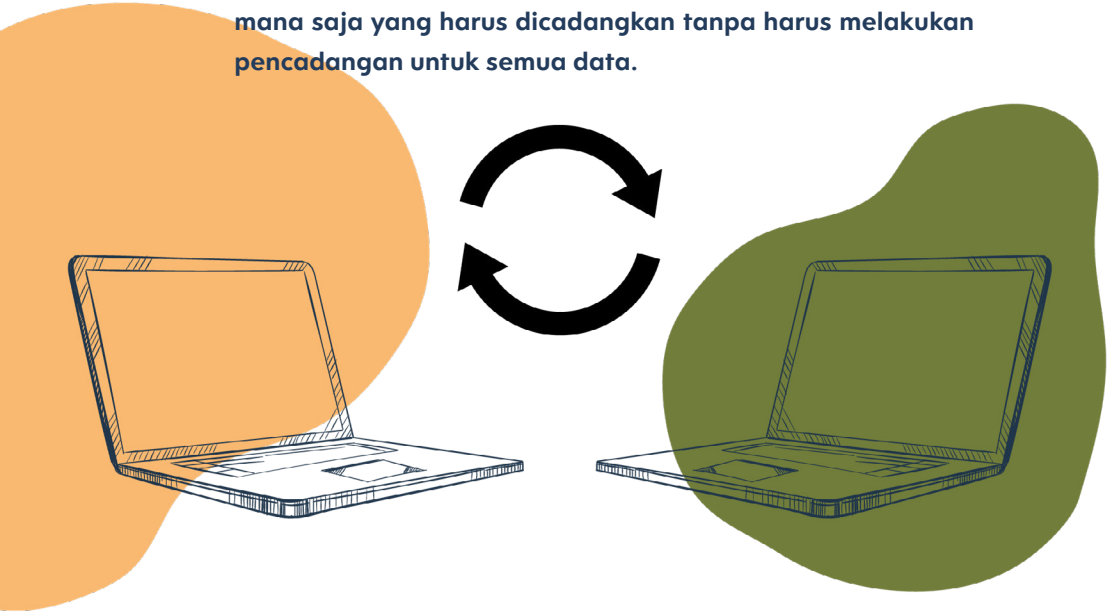
- **Pelatih menjelaskan apa saja kerentanan dan risiko yang mungkin terjadi dari tiap metode penguncian yang dilakukan. Di laptop kita bisa memilih antara menggunakan kata sandi atau PIN minimal enam angka. Di telepon pintar, pilihan yang disarankan adalah PIN dengan minimal enam angka atau menggunakan kata sandi. Menggunakan pengunci biometrik seperti sidik jari atau pengenalan wajah *(face id)* bukannya tidak aman, tetapi itu berarti kita memberikan data biometrik kita ke pihak ketiga yang mungkin saja akan bocor.**
- **Pelatih melanjutkan sesi dengan bertanya kepada peserta, "Siapa yang sudah membersihkan ponselnya dalam dua bulan terakhir?" Tujuan pertanyaan ini adalah untuk mengingatkan peserta tentang pentingnya membersihkan laptop dan ponsel sebagai bagian dari keamanan digital.**
- **Pelatih menjelaskan cara membersihkan perangkat, termasuk sampah di recycle bin dan jejak Wi-Fi. Jejak Wi-Fi yang tersimpan di perangkat punya risiko menjadikan pengguna sebagai target serangan digital. Penyerang dapat membuat Wi-Fi tiruan dengan nama Wi-Fi yang sebelumnya sudah disimpan oleh target. Lalu, ketika target terhubung ke Wi-Fi tersebut, mereka akan bisa melihat isi perangkat target. Selain itu, jejak-jejak Wi-Fi yang tersimpan itu ibaratnya sampah yang menempel di badan. Periksa semua Wi-Fi yang sudah tersimpan di perangkat, baik laptop maupun telepon pintar, hapus yang tidak lagi digunakan.**

- **Pelatih mengajak peserta untuk memasang aplikasi VirusTotal dan Files by Google di ponsel sebagai aplikasi untuk membersihkan sampah dan malware di ponsel.**

- **Pelatih memperlihatkan cara menggunakan VirusTotal dan Files di ponsel dan menerangkan apa fungsinya.**

- **Pelatih bertanya kepada peserta, "Kapan terakhir kali mereka mencadangkan data mereka?", "Apa yang mereka rasakan ketika perangkat mereka rusak dan mereka tidak dapat lagi mengakses data mereka?"**

- **Pelatih mengajak peserta untuk menggunakan aplikasi pencadangan seperti FreeFileSync yang dapat membantu memudahkan pencadangan. FreeFileSync dapat memilah data mana saja yang harus dicadangkan tanpa harus melakukan pencadangan untuk semua data.**



- **Pelatih menjelaskan pentingnya melakukan pencadangan secara berkala dengan beberapa tips berikut ini:**

    * **Lakukan pencadangan secara teratur.** Baik setiap awal bulan atau saat hendak turun ke lapangan atau keluar kota.

    * **Lakukan pencadangan setidaknya di dua tempat berbeda.** Bisa menggunakan diska keras eksternal (hard disk external) atau flash disk, serta menggunakan layanan cloud. Hal ini untuk menurunkan risiko hilangnya data. Ketika satu tempat pencadangan rusak atau tidak dapat diakses, masih ada tempat pencadangan lain.

    * **Jangan simpan data utama dan data yang dicadangkan di tempat yang sama.** Hal ini juga untuk mengurangi risiko kehilangan data. Bila data utama dan data cadangan disimpan di tempat yang sama dan misalnya terjadi musibah seperti kebakaran, tentu hasilnya sama saja. Data utama dan data cadangan hilang dan tidak terselamatkan.

- **Pelatih menjelaskan pentingnya pembaruan sistem operasi untuk mengurangi risiko serangan digital. Pembaruan aplikasi penting untuk memperbarui kelemahan atau kekurangan sebuah aplikasi yang rentan diekspos oleh penyerang.**

- **Pelatih menjelaskan cara-cara memeriksa pembaruan sistem operasi dan aplikasi, baik di perangkat laptop maupun di ponsel.**

- **Pelatih mempersilakan peserta untuk bertanya sebelum menutup sesi.**

Keamanan Akun dan Manajemen Identitas

Pengantar

Dalam sesi ini peserta akan belajar bagaimana mengelola identitas digital yang baik sehingga dapat mengurangi risiko mendapatkan serangan digital, termasuk mencari jejak digital dan mengamankan akun-akun media sosial.

Tujuan

Pada akhir sesi ini, peserta diharapkan mampu:

- Memahami konsep data pribadi,
- Mendata dan mengelola akun-akunnya,
- Mengetahui kekuatan kata sandinya,
- Memperkuat dan mengelola kata sandi,
- Mengamankan akun google, misalnya gmail, google drive, google file.

Pokok Bahasan

Materi sesi terdiri atas tiga bagian utama, yaitu:

- Teori dan konsep tentang jejak digital,
- Mendata dan mengelola akun-akun digital, dan
- Memperkuat keamanan akun google.

1. **Memahami konsep data pribadi identik termasuk:**

- Memahami konsep data pribadi,
- Mendata dan mengelola akun-akunnya,
- Mengetahui kekuatan kata sandinya,
- Memperkuat dan mengelola kata sandi,
- Mengamankan akun google, misalnya gmail, google drive, google file.

2. **Mendata dan mengelola aset digital termasuk:**

- Teori dan konsep tentang jejak digital,
- Mendata dan mengelola akun-akun digital, dan
- Memperkuat keamanan akun google.

3. **Mendata dan mengelola aset digital termasuk:**

- Teori dan konsep tentang jejak digital,
- Mendata dan mengelola akun-akun digital, dan
- Memperkuat keamanan akun google.

Bahan dan Peralatan

Bahan dan peralatan dalam sesi ini adalah:

- *Slide* presentasi,
- Layar,
- Proyektor,
- Laptop, dan
- Ponsel.

Metode

- Presentasi
- Praktik

Waktu

- 135 menit

Proses

- **Pelatih menyapa peserta untuk membangun jembatan sebelum masuk ke poin-poin materi. Contoh pertanyaan sebagai jembatan adalah "Berapa level energi peserta saat ini?" Setelah itu bisa dilanjutkan dengan pertanyaan, "Apa yang biasa dibagikan peserta di media sosial?"**

- **Pelatih menjelaskan apa saja topik yang akan disampaikan dan juga tujuan sesi.**

- **Pelatih meminta peserta untuk berpasangan lalu mengajak mereka melakukan pencarian informasi pribadi teman, termasuk nama lengkap, asal kampung, suku, nama marga (bila ada), akun media sosial, tempat tinggal, dan data pribadi lain. Waktu untuk mencari informasi adalah lima menit.**

- **Pelatih bertanya kepada dua peserta mengenai apa informasi pribadi yang dia temukan tentang pasangannya. Apakah ada informasi pribadi yang dapat berisiko jika disalahgunakan orang lain?**

- **Pelatih menjelaskan bagaimana data saat ini tidak hanya menjadi aset (harta), tetapi juga rentan disalahgunakan untuk menyerang pemiliknya (senjata).**

- **Pelatih menjelaskan bahwa serangan digital sering kali dilakukan dengan cara mengumpulkan jejak-jejak digital korban. Contohnya adalah *doxing* atau menyebarluaskan identitas korban.**

- **Pelatih menjelaskan konsep informasi personal identik (PII), seperti nama lengkap, nomor KTP, NPWP, dan nama ibu kandung.**

- **Pelatih mengajak peserta mencari jejak digitalnya sendiri di internet menggunakan Google. Tanyakan apakah ada informasi pribadi yang mungkin berisiko.**

- **Pelatih mengajak peserta membuat daftar akun-akunnya dalam sebuah tabel.**

- **Pelatih meminta peserta memeriksa kebocoran data di platform haveibeenpwned.com atau periksadata.com. Tanyakan kepada peserta, data apa saja yang bocor? Umumnya data yang paling sering bocor adalah kata sandi atau *password.***

- **Pelatih meminta peserta untuk memeriksa keamanan kata sandi di passwordmonster.com, dan melihat pengaturan kata sandinya**

- **Pelatih menjelaskan perbedaan antara *password* (kata sandi) dengan *passphrase* (kalimat sandi) dengan memeriksanya langsung di platform passwordmonster.com. Tekankan pentingnya membuat kata sandi yang kuat dengan menggabungkan huruf besar, huruf kecil, angka, simbol, dan bila memungkinkan, tambahkan spasi. Tekankan juga untuk mengganti kata sandi secara berkala, misalnya setahun sekali.**

- **Pelatih mengajak peserta menggunakan aplikasi pengingat kata sandi seperti KeepasXC yang bekerja secara offline atau Bitwarden yang bekerja secara *online.* Jelaskan cara kerja aplikasi tersebut sebagai aplikasi yang bekerja layaknya brankas yang menyimpan data penting kita. Kita hanya harus mengingat satu kata kunci, yaitu kata kunci untuk masuk ke aplikasi tersebut.**

- **Pelatih menanyakan siapa yang tidak menggunakan Google. Biasanya, tidak ada orang yang tidak memakai Google. Oleh karena itu, penting untuk mengamankan akun Google masing-masing.**

- **Pelatih menjelaskan bagaimana pengaturan keamanan dan privasi akun Google dan apa saja risiko keamanannya.**

- **Pelatih memperlihatkan satu per satu apakah ada peringatan keamanan dari Google, rekomendasi keamanan, kapan terakhir kali kata sandi diganti, apakah ada perangkat lain yang tersambung di akun tersebut, dan aplikasi apa saja yang mengakses akun Google. Berikut adalah langkah pengamanan privasi pada layanan Google.**

Periksa lagi apa saja aktivitas kita yang direkam platform Google, misalnya, di

https://policies.google.com/privacy dan
https://myactivity.google.com/myactivity.

Pengaturan privasi pada Google bisa dicek di
https://myaccount.google.com/intro/privacycheckup.

Temukan apa saja aktivitas kita yang direkam Facebook di
https://www.facebook.com/about/privacy.

Pengaturan privasi pada Facebook dapat dicek di
https://www.facebook.com/about/basics/manage-your-privacy.

Lakukan pemeriksaan serupa pada platform lain yang kita gunakan, seperti Twitter, Instagram, YouTube, dan lain-lain.

- **Pelatih menekankan pentingnya keamanan akun Google sebagai bagian penting dalam manajemen identitas.**

- **Pelatih mengajak peserta untuk memasang autentikasi dua langkah atau 2 *factor authentication* pada akun mereka, utamanya akun Google dan akun media sosial. Tekankan pentingnya 2FA ini sebagai kunci tambahan agar akun tidak bisa diakses orang lain meski mereka sudah punya kata sandinya. Jelaskan beberapa jenis autentikasi dua langkah yang kerap digunakan sebagai berikut:**

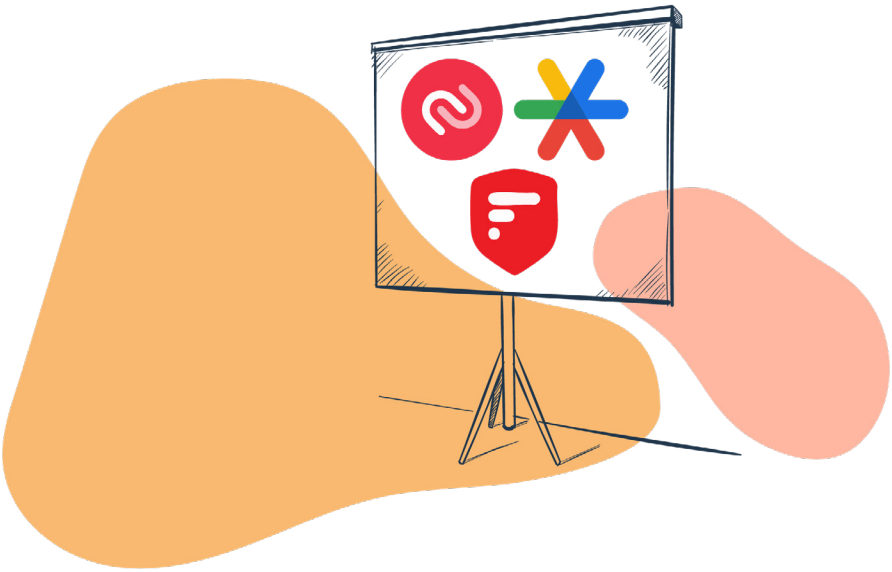
* **Menggunakan metode ketuk,** umumnya digunakan oleh Google. Ketika kita hendak mengakses akun di perangkat laptop, maka pemberitahuan akan muncul di ponsel tempat akun Google terpasang. Kita akan diminta mengetuk satu angka yang muncul di laptop.

* **Menggunakan SMS,** merupakan metode yang paling umum dilakukan. Aplikasi atau situs web akan mengirimkan angka tertentu lewat SMS yang harus dimasukkan sebelum dapat mengakses akun atau situs tersebut. Metode ini cukup berisiko karena bisa saja ada pihak ketiga yang melakukan pencegatan SMS di tengah jalan atau bisa membaca SMS yang kita terima.

* **Menggunakan *security key*,** yaitu benda dengan bentuk mirip dengan flash disk. Ketika akan masuk ke satu akun atau situs web, kita akan diminta memasukkan security key tersebut terlebih dahulu. Metode ini tidak disarankan untuk mereka yang teledor. Sebab, apabila alat ini tercecer, tentu repot untuk melakukan penggantian autentikasi dua langkah. Selain itu, harga security key juga tidak tergolong murah.

* **Menggunakan aplikasi,** metode ini paling direkomendasikan karena lebih sulit untuk diintip oleh pihak ketiga dan tidak perlu mengeluarkan biaya. Cara kerjanya adalah menghubungkan akun dengan aplikasi 2FA terlebih dahulu. Setelah tersambung, setiap kali mengakses akun tersebut, kita harus memasukkan enam angka yang muncul di aplikasi 2FA, selain tentu saja memasukkan sandi. Angka tersebut berubah setiap 30 detik atau 60 detik tergantung aplikasinya. Beberapa aplikasi autentikasi yang direkomendasikan adalah: 2FAS, ESSET, Authy, dan Google Authenticator.

- **Pelatih mengajak peserta mempraktikkan 2FA menggunakan aplikasi. Beberapa aplikasi yang dapat digunakan adalah 2FAS, Authy atau Google Authenticator. Hal yang paling penting adalah menjelaskan cara kerja aplikasi 2FA ini. Jangan lupa juga untuk menekankan pentingnya melakukan pencadangan isi aplikasi agar ketika perangkat hilang, kita tetap dapat membukanya di perangkat lain dan dapat mengakses akun kita.**
- **Pelatih mempersilakan jika ada pertanyaan dari peserta.**
- **Pelatih menutup sesi jika tidak ada pertanyaan.**



Komunikasi yang Aman

Pengantar

Komunikasi yang aman adalah salah satu faktor dalam menekan risiko serangan digital. Karena itu, penting untuk menjelaskan tentang apa itu komunikasi yang aman dan apa saja aplikasi alternatif yang bisa digunakan.

Tujuan

- Menerangkan bagaimana internet bekerja dalam konteks komunikasi.
- Menerapkan cara komunikasi yang lebih aman.
- Memilih aplikasi komunikasi (pesan singkat, surel, dan peramban/*browser*) yang lebih aman.
- Memilih platform media penyimpanan data yang lebih aman.
- Materi sesi terdiri atas tiga bagian utama, yaitu:
- Teori dan konsep tentang jejak digital,
- Mendata dan mengelola akun-akun digital, dan
- Memperkuat keamanan akun google.
- Memperkuat perangkat.

Pokok Bahasan

Beberapa materi yang dijelaskan dalam sesi ini antara lain:

- Prinsip dasar komunikasi di internet,
- Peramban/browser yang aman,
- Platform dan aplikasi yang lebih aman,
- Koneksi internet yang aman, dan
- Cara cek keamanan surel *(email)* dan tautan.

Bahan dan Alat

- Presentasi
- Laptop/ponsel

Waktu

- 120 menit

Metode

- Presentasi
- Diskusi dan tanya-jawab
- Praktik

Proses

- **Pelatih membuka sesi dengan menyapa peserta dan mengingatkan sedikit tentang materi di sesi sebelumnya agar ada keterkaitan materi.**
- **Pelatih menerangkan tentang tujuan dari sesi ini.**
- **Pelatih bertanya kepada peserta, "Apa itu internet?" dan "Tahukah mereka bagaimana internet bekerja?"**
- **Pelatih menjelaskan tentang cara kerja internet, utamanya dalam konteks komunikasi, salah satu video sederhana yang bisa menjelaskan bagaimana internet bekerja bisa dilihat di sini: *https://youtu.be/_fI7wWbV604?si=_UxmtCB89_FHW7FJ.* Video ini dapat ditayangkan untuk membantu peserta membayangkan bagaimana internet bekerja.**
- **Pelatih menerangkan tentang komponen komunikasi di internet sebagai berikut.**
  - **Perangkat pengguna,** baik laptop ataupun ponsel pintar yang dapat tersambung ke jaringan internet.
  - **Jaringan internet,** baik menggunakan kabel maupun nirkabel.
  - ***Router,*** atau alat yang menghubungkan dua atau lebih jaringan. Router membutuhkan jaringan kabel fiber *(fiber optic),*
  - ***Internet service provider* (ISP),** atau penyedia layanan internet. Sebuah perusahaan yang menyediakan layanan internet di suatu daerah,
  - ***Internet backbone,*** secara sederhana bisa disebut sebagai tulang punggung jaringan internet. Ini adalah jaringan terbesar dan tercepat yang menghubungkan kabel fiber optik (termasuk di bawah laut) dengan router.

- **Pelatih menekankan tiga komponen yang saling berkait dalam konteks keamanan komunikasi sebagai berikut.**
  - ***Confidentiality*** berarti kerahasiaan yang merujuk bahwa hanya orang yang berhak menerima informasi tersebut yang dapat mengakses data. Tidak ada pihak lain yang dapat mengakses apalagi membaca pesannya.
  - ***Integrity*** berarti integritas atau keutuhan data yang dikirim dari pengirim hingga penerima adalah data yang sama. Tidak ada data yang diubah atau hilang selama perjalanan dari ujung satu ke ujung lain.
  - ***Availability*** atau ketersediaan, berarti data yang dikirimkan dari satu pihak ke pihak lain tersedia untuk diakses. Dalam sebuah situs web atau akun media sosial, misalnya, data-data dari akun-akun tersebut harus selalu

- **Pelatih menerangkan ragam saluran komunikasi yang digunakan di internet, yaitu:**
  - **peramban,**
  - **surat elektronik (surel),**
  - **VPN,**
  - **pesan ringkas,**
  - **komputasi awan *(cloud)*, dan**
  - **dokumen kolaborasi.**

- **Pelatih bertanya kepada peserta mengenai siapa saja yang menggunakan Google Chrome. Jelaskan bagaimana Google Chrome merekam aktivitas kita lewat bantuan tayangan video ini *https://www.youtube.com/watch?v=18En4NBbw3c.***

- **Pelatih mengajak peserta menggunakan peramban yang lebih aman, seperti Brave. Pelatih dapat menunjukkan beberapa fitur dari Brave yang lebih menghargai privasi, termasuk penggunaan *New Private Window with Tor.***

- **Pelatih menjelaskan tentang keamanan protokol termasuk perbedaan antara http dan https.**
- **Pelatih mengajak peserta menggunakan surel alternatif, seperti Proton. Sampaikan mengenai fitur keamanan dari Proton, seperti end-to end encryption, serta fitur menentukan berapa lama surel dapat dibaca sebelum hancur dengan sendirinya.**
- **Pelatih menjelaskan tentang pentingnya VPN dan mengajak peserta untuk menggunakan Proton VPN.**
- **Pelatih memperkenalkan komputasi awan *(cloud)* alternatif seperti Mega atau ProtonDrive.**
- **Pelatih memperkenalkan aplikasi kerja kolaborasi seperti Cryptpad.fr yang berfungsi sama dengan Google Docs, dengan dukungan keamanan yang lebih kuat.**
- **Pelatih memperkenalkan situs web yang dapat memeriksa tautan atau berkas yang dianggap mencurigakan, yaitu virustotal.com.**
- **Pelatih menutup sesi dengan bertanya apakah ada hal yang belum dimengerti kepada peserta. Bila masih ada waktu, ulangi atau jelaskan kembali materi yang belum dimengerti oleh peserta.**

Komunikasi Aman di Lapangan

Pengantar

Dalam sesi ini, peserta akan belajar bagaimana berlaku dan berkomunikasi ketika di lapangan agar lebih aman secara digital dari persiapan sebelum berangkat hingga kembali setelah melakukan pekerjaan di lapangan.

Tujuan

Setelah mengikuti sesi ini, peserta diharapkan mampu:

- Memahami risiko dan ancaman serangan digital saat di lapangan;
- Menerapkan strategi keamanan digital saat di lapangan;
- Mengantisipasi situasi tanpa internet saat di lapangan; dan
- Membuat simulasi ketika melakukan pekerjaan berisiko di lapangan.
- Memperkuat perangkat.

Pokok Bahasan

- Risiko dan ancaman keamanan digital saat di lapangan
- Persiapan sebelum ke lapangan
- Antisipasi terhadap serangan digital saat di lapangan
- Menyembunyikan berkas sensitif
- Komunikasi tanpa internet

Bahan dan Alat

- Materi Presentasi
- Laptop

Waktu

- 90 menit

Metode

- Presentasi
- Diskusi
- Simulasi

Proses

- **Pelatih menyapa peserta lalu membuka dan menjelaskan tujuan sesi.**
- **Pelatih memulai dengan bertanya kepada peserta tentang pengalaman mereka di lapangan, seberapa sering mereka ke lapangan, apa yang dilakukan, dan pengalaman lainnya.**
- **Pelatih menjelaskan risiko dan ancaman keamanan digital saat di lapangan.**
- **Pelatih menjelaskan tentang pentingnya melakukan analisis risiko terhadap lokasi yang akan didatangi, misalnya dengan menjawab beberapa pertanyaan berikut.**

    * **Berapa jauh lokasi dari tempat tinggal?**
    * **Transportasi apa yang dapat digunakan ke lokasi?**
    * **Apakah di lokasi ada sinyal?**
    * **Bagaimana dengan penginapan?**
    * **Siapa yang akan menemani ke lokasi, atau siapa *buddy* yang akan menjadi tandem ketika turun ke lokasi; serta pertanyaan lainnya.**

- **Pelatih menyampaikan materi tentang kesadaran situasional yang mengingatkan peserta untuk terus waspada pada situasi di sekitar, termasuk perubahan situasi yang tidak normal. Pada sesi ini, pelatih dapat memberikan simulasi dengan menampilkan gambar selama dua menit, lalu menutupnya dan meminta peserta mengingat apa saja yang ada di gambar tersebut atau apa hal yang tidak umum di gambar tersebut.**
- **Pelatih menjelaskan tentang OODA *loop* sebagai berikut.**
    * ***Observe*,** atau observasi, yaitu kondisi saat kita harus melakukan observasi atau pengamatan pada lingkungan sekitar dan perubahan yang terjadi.
    * ***Orientation,*** atau orientasi. yaitu kondisi saat kita harus menentukan orientasi atau tujuan kita.
    * ***Decide,*** atau memutuskan, yaitu kondisi saat kita harus memutuskan langkah selanjutnya.
    * ***Action,*** atau aksi, yaitu kondisi saat kita melakukan aksi dalam merespons situasi sekitar atau situasi yang berubah.
- **Pelatih menjelaskan strategi dan mitigasi keamanan digital saat di lapangan, termasuk menyiapkan ponsel cadangan, mengurangi informasi sensitif, mematikan fungsi lokasi, dan seterusnya.**

- **Pelatih menunjukkan metode menyembunyikan berkas menggunakan enkripsi atau aplikasi bawaan pada perangkat.**

- **Pelatih menunjukkan beberapa metode berkomunikasi tanpa menggunakan internet, seperti Bluetooth.**

- **Pelatih membuat 2–3 simulasi (sesuai jumlah peserta), yaitu seorang aktivis akan melakukan investigasi ke lapangan. Setiap kelompok akan membahas satu simulasi dengan fokus pada mitigasi keamanan digital yang perlu dilakukan saat ke lapangan. Waktu diskusi 15 menit.**

- **Setiap kelompok akan mempresentasikan hasil diskusinya masing-masing selama 10 menit, termasuk tanya-jawab.**

- **Fasilitator membantu dengan mendampingi setiap peserta agar dapat mengikuti tahapan yang ditunjukkan pemateri.**

- **Baik pelatih maupun fasilitator, harus memastikan bahwa semua peserta dapat mengikuti sesi dan menerapkannya**

- **Pelatih mempersilakan peserta untuk bertanya jika masih ada yang bingung sebelum menutup sesi.**

Pertolongan Pertama Pada Serangan Digital

Pengantar

Dalam sesi ini, peserta diberikan informasi tentang apa saja yang dapat dilakukan ketika menjadi korban serangan digital. Tindakan yang dilakukan tentu saja adalah tindakan pertolongan pertama sebelum meminta bantuan lebih jauh dari orang yang lebih paham teknis.

Tujuan

Setelah sesi ini, peserta diharapkan mampu:

- Memahami langkah pertama yang dilakukan saat menjadi korban serangan digital;
- Membantu korban serangan digital untuk melakukan langkah pengamanan awal saat menjadi korban serangan digital.

Pokok Bahasan

Pertolongan pertama atau langkah pertama yang dapat dilakukan saat menjadi korban beberapa serangan digital.

Bahan dan Alat

- Materi presentasi
- Laptop

Waktu

- 60 Menit

Metode

- Presentasi
- Diskusi

Proses

- **Pelatih membuka sesi dengan menanyakan kabar peserta dan mengingatkan secara cepat materi-materi yang telah dibahas sebelumnya.**

- **Pelatih bertanya, apakah ada peserta yang pernah menjadi korban serangan digital? Bila ada, maukah berbagi cerita?**

- **Pelatih memberikan materi tentang apa tindakan pertama yang dilakukan ketika menjadi korban phising sebagai berikut.**

  * Nonaktifkan jaringan internet. Beberapa aplikasi phishing membutuhkan internet untuk melakukan aksinya.

  * Periksa perangkat Anda, baik secara manual ataupun menggunakan aplikasi antivirus. Bila ada aplikasi yang mencurigakan, segera lepas atau *uninstall.*

  * Ganti kata sandi di aplikasi yang sering menjadi sasaran phishing seperti *mobile banking* atau akun belanja

- **Pelatih memberikan materi tentang apa tindakan pertama yang dilakukan ketika menjadi korban *doxing* sebagai berikut**

- Laporkan akun dan postingan yang memuat *doxing* tersebut kepada platform. Minta bantuan sebanyak-banyaknya kepada teman yang dapat dipercaya. Semakin banyak yang melaporkan postingan tersebut, kemungkinan postingan tersebut diturunkan akan semakin besar,
- Kunci akun media sosial untuk sementara.
- Matikan sementara nomor telepon utama yang sudah terekspos. Gunakan nomor lain yang hanya diberikan kepada orang yang dipercaya. Aktifkan fitur membisukan penelepon yang tidak dikenal di WhatsApp dengan cara:

  Pengaturan > Privasi > Telepon > Bisukan penelepon tidak dikenal.
- Bila memungkinkan, cari tempat yang aman dengan asumsi alamat Anda sudah terekspos. Pastikan hanya orang terdekat yang tahu.
- Amankan akun yang berhubungan dengan perbankan, ganti kata sandi.
- Pastikan punya *support system* atau teman-teman dan keluarga yang dapat membantu dan melindungi,
- Pantau terus perkembangan *doxing* tersebut, apakah sudah mereda atau tidak.

- **Pelatih memberikan materi tentang apa yang harus dilakukan ketika menjadi korban *trolling* atau komentar buruk sebagai berikut**
  - Abaikan. Pelaku *trolling* atau komentar buruk menginginkan kemarahan dari targetnya. Semakin targetnya marah, semakin mereka senang. Karena itu, abaikan komentar mereka, tetap bersikap tenang, dan tidak usah membalas.

- abaikan komentar mereka, tetap bersikap tenang, dan tidak usah membalas.
- Blokir. Beberapa akun mungkin sudah berlebihan dan menyerang Anda dengan sangat personal. Gunakan fungsi blokir pada media sosial agar Anda tidak lagi melihat komentar mereka.
- Laporkan. Gunakan juga fitur laporkan apabila komentar mereka memang sudah melanggar aturan dari media sosial tersebut seperti bernuansa SARA, bermuatan pelecehan seksual, menjatuhkan martabat, atau pengumbaran data pribadi.
- Atur privasi. Setiap media sosial punya fitur mengatur privasi, gunakan fitur tersebut. Bila memang mengharuskan, kunci akun Anda.

- **Pelatih memberikan materi tentang apa yang harus dilakukan ketika menjadi korban peretasan atau pengambilalihan akun sebagai berikut.**
  - Manfaatkan fitur pelaporan pada setiap platform untuk bisa mengambil kembali akun Anda.
  - Waktu pemulihan akun tergantung platform bersangkutan.
- **Pelatih memberikan materi tentang apa yang harus dilakukan ketika menjadi korban KBGO sebagai berikut.**
  - Dokumentasikan semuanya. Mulai dari tangkapan layar, sampai tautan postingan tersebut. Catat dalam bentuk kronologi kejadian. Agar tidak menimbulkan trauma, simpan di tempat yang aman, namun mudah untuk diakses. Hal ini penting karena akan digunakan saat melakukan pelaporan.

- Putuskan hubungan dengan pelaku. Putus semua akun komunikasi, atau bila pelakunya menggunakan media sosial, blokir akunnya. Bila perlu tutup akun untuk sementara waktu, atau mengganti permanen akun media sosial atau akun pesan ringkas.

- Lakukan pemetaan risiko. Buat pertanyaan seperti ini, “Apa risiko yang mungkin terjadi dari ancaman ini?”, “Data atau informasi apa yang dimiliki pelaku?”, “Apabila ada konten intim yang dimiliki pelaku, apakah konten itu menunjukkan wajah saya?” Jawab pertanyaan itu untuk tahu kira-kira seberapa besar risikonya bagi korban.

- Laporkan ke platform. Media sosial besar pada umumnya punya fitur untuk melindungi penggunanya, apalagi korban kekerasan seksual. Manfaatkan fitur ini dan segera laporkan akun pelaku.

- Laporkan juga ke pihak yang dapat membantu. Anda dapat memanfaatkan layanan aduan dan pendampingan bagi korban kekerasan seksual, termasuk kepada pihak penegak hukum.

- **Selama pemaparan, pelatih harus memberikan kesempatan kepada peserta untuk berdiskusi atau memberikan pendapat.**

- **Pelatih menutup sesi.**

Menjaga Dinamika Pelatihan

Penyegaran

Salah satu faktor penting dalam sebuah pelatihan adalah penyegaran. Aktivitas ini sangat berperan untuk menaikkan energi peserta setelah rehat singkat maupun makan siang. Penyegaran yang bagus sebaiknya memenuhi tiga hal, yaitu ada gerakan fisik, kompetitif, dan menghibur.

TEBAK KATA

- Peserta dibagi dalam dua kelompok yang sama jumlahnya dan berbaris ke belakang.
- Panitia menyiapkan 20 kata yang terkait dengan pelatihan baik logistik, tempat, ataupun konten.
- Perwakilan tiap peserta akan maju satu per satu menggunakan gerakan untuk menunjukkan kata yang ditulis panitia.
- Semua anggota tiap kelompok bebas untuk menjawab.
- Peserta yang menebak dengan benar terlebih dulu akan mendapatkan nilai satu poin.
- Peserta yang sudah selesai bertugas menunjukkan dengan gerakan harus mundur dan digantikan peserta lain.
- Kelompok yang paling banyak menebak dengan benar akan keluar sebagai juara.

DOR!

Permainan Kelipatan atau Angka

- Peserta membentuk lingkaran
- Prinsip permainan ini adalah meneruskan hitungan angka secara berurutan. Setiap angka dari kelipatan dan angka tersebut mendapatkan giliran, peserta harus membentuk pistol seperti menembak.
- Pemimpin permainan menentukan kelipatan berapa yang ingin digunakan. Jika setiap angka dari kelipatan tersebut, maka harus melakukan DOR!
- Misalnya pemimpin permainan menentukan kelipatan 3 dan juga angka yang mengandung angka 3 harus melakukan DOR!
- Artinya setiap angka 3,6,9,12,13,15,18,21,23, dst.., peserta harus melakukan **DOR!**
- Urutan pertama untuk memulai permainan adalah yang ditunjuk oleh pemimpin permainan.
- Orang pertama menyebut angka 1, orang kedua menyebut angka 2, orang ketiga menyebut angka 3, dst.
- Jika ada yang terlalu lambat atau salah menyebut DOR!, peserta tersebut harus keluar dari lingkaran dan nantinya akan melakukan kotak pandora.
- Lakukan terus secara berulang-ulang dengan angka dan jumlah kelipatan yang berbeda.
- Demikian seterusnya sampai nanti dirasa sudah menaikkan energi.

Aliran Listrik

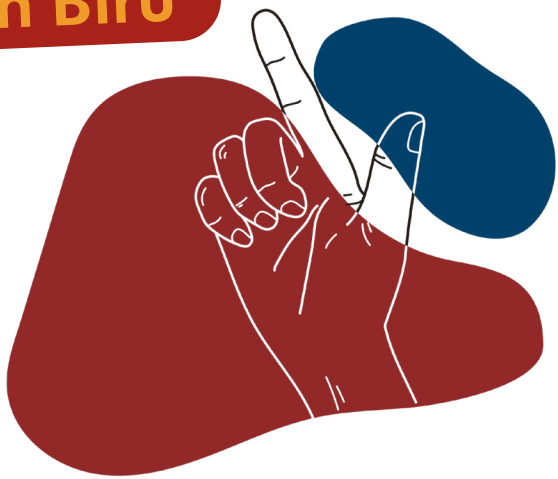
- Peserta dibagi menjadi dua barisan dan saling berhadapan. Setiap barisan harus memiliki jumlah yang sama agar adil. Masing-masing anggota dalam barisan saling bergandengan tangan
- Di tengah-tengah dan di setiap ujung barisan terdapat dua orang (biasanya panitia atau pemandu game) yang bertugas sebagai penghitung dan sebagai pemegang tisu keberhasilan. Perhatikan jarak antara orang tengah dan juga jarak antara barisan, harus dengan jarak yang sama.
- Di setiap barisan, ada dua orang yang bertugas, yaitu yang bertugas melihat hitungan dan yang bertugas mengambil tisu keberhasilan.
- Semua orang dalam setiap barisan harus menutup mata, kecuali orang pertama di paling ujung yang bertugas untuk melihat hitungan dari orang tengah.
- Ketika hitungan ketiga, orang pertama dari barisan tersebut harus mengeratkan genggaman kepada orang kedua, orang kedua mengeratkan genggaman kepada orang ketiga, dan seterusnya.
- Ketika orang terakhir merasakan genggaman, secepat mungkin langsung mengambil tisu keberhasilan dari orang tengah.
- Siapa yang paling cepat mengambil tisu keberhasilan, dialah pemenangnya.
- Teruskan permainan dengan mengganti posisi orang pertama dan orang terakhir secara berurutan agar permainan menjadi lebih seru.

Menjadi Gajah

- Konsepnya hampir sama seperti permainan DOR!, tetapi tidak melibatkan perhitungan.
- Peserta membentuk lingkaran.
- Prinsip permainan ini adalah ada yang menjadi telinga dan belalai gajah.
- Pemimpin dalam permainan akan menunjuk orang yang akan menjadi belalai. Cara membentuk belalai adalah dengan membentangkan tangan yang dikepal ke depan dan ke arah bawah.
- Orang yang ada di sebelah kiri dan kanan dari yang membentuk belalai, harus membentuk telinga. Cara membentuk telinga adalah dengan menggunakan telapak tangan yang terbuka.
- Pemimpin akan menentukan terus siapa orang yang akan menjadi belalai. Kecepatan permainan akan ditentukan oleh pemimpin permainan.
- Apabila ternyata ada orang yang salah dan/atau telat menjadi belalai maupun telinga, maka keluar dari lingkaran dan harus menerima kotak pandora.
- Demikian seterusnya sampai nanti dirasa sudah menaikkan energi.

- Prinsipnya adalah kata pertama bagian tubuh dan kata kedua warna
- Pemimpin permainan akan menentukan bagian tubuh yang dipilih dan warna benda yang akan disentuh oleh bagian tersebut.
- Misalnya, telunjuk jari kanan - merah.
- Artinya, setiap peserta harus menggunakan telunjuk di jari kanan untuk menyentuh benda apapun yang berwarna merah.
- Permainan ini bisa dilakukan berulang-ulang. Bebas menggunakan bagian tubuh manapun.
- Setiap peserta bisa menjadi pemimpin permainan agar dinamika permainan menjadi lebih menyenangkan.
- Demikian seterusnya sampai nanti dirasa sudah menaikkan energi.

Tangan Biru



- Peserta dibagi menjadi beberapa kelompok dengan jumlah yang sama
- Pemimpin permainan menentukan satu kata yang akan diperagakan.
- Contoh kata yang diperagakan RAMBUTAN.
- Setiap peserta harus menggerakan tubuh sesuai dengan kalimat yang disampaikan
- Setiap orang menggerakan tubuh untuk setiap huruf R-A-M-B-U-T-A-N, bergantian secara terus-menerus hingga huruf terakhir.
- Setiap kelompok memiliki kata-kata yang berbeda.
- Demikian seterusnya sampai nanti dirasa sudah menaikkan energi.

Senam dengan Youtube

- Pemimpin kelas menentukan senam yang akan diikuti, kemudian tampilkan pada layar.
- Setiap peserta bisa mengikuti gerakan yang ada pada layar proyektor
- Contoh senam-senam yang bisa diikuti

- **Senam ponsel**

https://www.youtube.com/watch?v=e9JisYFJluU&pp=ygUMc2VuY-W0gcG9uc2Vs

- **Senam penguin**

https://www.youtube.com/watch?v=aYx7SBMlZis&pp=ygUNc2VuY-W0gcGluZ3Vpbg%3D%3D

- **Senam Gemu Fa Mi Re**

https://www.youtube.com/watch?v=8-Mzdh4RY5Q&pp=y-gUNc2VuYW0gcGluZ3Vpbg%3D%3D

- **Senam Iya iyalah**

https://www.youtube.com/watch?v=IQwbAeIgtiI&pp=ygUSc2VuY-W0gaWNlIGJyZWFraW5n

- **Senam ayam**

https://www.youtube.com/watch?v=l5sIspLfmXM&pp=ygUNY-2hpY2tlbiBkYW5jZQ%3D%3D

- **Senam kewer-kewer**

https://www.youtube.com/watch?v=jo4FXUKgeF0&pp=ygURc2VuY-W0ga2V3ZXIga2V3ZXI%3D

CATATAN TAMBAHAN

Jika memiliki ide lainnya di luar daftar permainan penyegaran, bisa dicoba dan yang paling penting adalah mengembalikan fokus peserta sebelum memulai kembali sesi. Biasanya setelah makan siang, sebagian besar peserta masih merasa ngantuk.

Penilaian Sebelum Pelatihan (pre test)
Penilaian Selama Pelaksanaan
Penilaian Setelah Pelaksanaan

Bagian 5: Penilaian

Penilaian bertujuan untuk melihat sejauh mana keberhasilan atau kegagalan dalam pelatihan keamanan digital. Penilaian ini dapat menilai peningkatan pengetahuan peserta, hingga menilai kenyamanan peserta dalam mengikuti pelatihan.

- Penilaian dilakukan di seluruh rangkaian kegiatan pelatihan:
- Tahap persiapan atau sebelum pelatihan (pre-test),
- Tahap pelaksanaan (refleksi harian dan observasi),
- Setelah pelaksanaan pelatihan (evaluasi dan post-test).

Penilaian Sebelum Pelatihan (pre test)

Di bagian ini, panitia yang bekerja sama dengan pelatih akan memberikan pertanyaan seputar tema pelatihan. Pertanyaan ini bertujuan untuk mengukur kemampuan maupun kesiapan peserta. Beberapa contoh pertanyaan yang bisa dimasukkan adalah sebagai berikut.

- Apakah peserta pernah mengikuti pelatihan keamanan digital sebelumnya?
- Apa perangkat lunak yang digunakan peserta di laptop dan ponsel masing-masing?
- Khusus untuk laptop, versi berapa perangkat lunak yang mereka gunakan?
- Dalam skala 1–5, berapa tingkat pengetahuan mereka terkait keamanan digital?
- Apakah pernah mengalami serangan digital?
- Dan pertanyaan lain terkait hal teknis perangkat.

Pertanyaan ini diberikan sebelum peserta memulai pelatihan. Bila memungkinkan, saat pelaksanaan pelatihan (bisa di sesi pertama), peserta diajak untuk mengisi PAKEM DIRI. PAKEM DIRI adalah singkatan dari Penilaian Keamanan Mandiri, sebuah sistem yang dibangun oleh SAFEnet untuk mengukur tingkat risiko keamanan digital individu secara mandiri.

PAKEM DIRI dapat diakses di tautan **pakemdiri.safenet.or.id**.

Penilaian Selama Pelaksanaan

Selama pelaksanaan pelatihan, penting juga untuk melakukan penilaian agar panitia dan pelatih dapat mengukur dinamika pelatihan, baik tingkat pengetahuan peserta, maupun hal teknis dan nonteknis terkait pelatihan.

Berikut metode yang bisa digunakan.

- **Review**. Biasanya dilakukan di pagi hari sebelum dimulainya kegiatan dan dimulai di hari kedua pelatihan. Tujuan dari proses ini adalah mengetahui sejauh mana peserta memahami materi yang sudah dipelajari di hari sebelumnya. Review bisa dilakukan dengan beberapa cara supaya tidak membosankan seperti di bawah ini:
  - **Tanya-jawab** dengan cara bertanya kepada setiap peserta secara acak atau berurutan terkait dengan apa yang dipelajari di hari sebelumnya.
  - **Mengoper benda** dengan cara memindahkan sebuah benda, misalnya spidol, kepada peserta secara acak kemudian yang mendapat benda tersebut harus menjawab pertanyaan yang diberikan oleh pelatih atau fasilitator
  - **Arisan pertanyaan** dilakukan dengan cara menyiapkan kertas kecil yang sudah digulung. Kertas kecil tersebut berisi beberapa pertanyaan dan beberapa lainnya dibiarkan kosong. Peserta akan mengambil kertas tersebut dan setiap orang akan mendapatkan satu kertas. Ketika dibuka bersama-sama, peserta yang mendapat kertas berisi pertanyaan akan mengajukan pertanyaan tersebut kepada peserta yang mendapat kertas kosong.
  -

- **Tebak istilah atau tebak kata** bisa dilakukan dengan cara pelatih atau fasilitator menampilkan gambar atau kata yang berkaitan dengan hak-hak digital dalam slide presentasi. Peserta akan menebak arti kata tersebut dan menjelaskan makna dari gambar atau kata tersebut.

- **Gacha penalty,** bisa dilakukan dengan menunjuk peserta secara acak, bisa dilakukan langsung oleh pelatih, fasilitator, atau dengan bantuan aplikasi spinner nama. Peserta yang terpilih harus menjawab pertanyaan yang sudah disediakan. Apabila menjawab dengan benar, peserta itu lolos dari hukuman, apabila tidak bisa menjawab dengan benar, dia akan menerima hukuman. Hukumannya tidak boleh memuat unsur kekerasan, pemerasan, atau pelecehan. Tujuannya untuk bersenang-senang sambil mengingat materi.

- **Permainan X/O,** aturan permainannya adalah "X" adalah pihak yang kalah sehingga maju ke depan, sementara "O" adalah pihak yang menang dan berhak tetap duduk di tempat. "X" menjawab pertanyaan sebagai konsekuensi dari kekalahan. Pertanyaan berisi materi yang sudah dipelajari selama sesi berlangsung dan berasal dari undian yang diambil secara acak. Permainan ini dapat berfungsi untuk meninjau ulang materi yang sudah dipelajari peserta.

- **Tebak gambar.** Siapkan gambar sejumlah peserta, misalnya 12–15 gambar. Gambar itu berhubungan dengan materi hari kemarin. Peserta berbaris, dan bergiliran menebak gambar yang disajikan di layar. Jika salah atau tidak bisa menebak, peserta pindah ke barisan paling belakang dan memberi kesempatan peserta selanjutnya untuk menebak.

- **Benar atau salah.** Fasilitator menampilkan satu pernyataan atau isyarat. Peserta harus mengangkat tangan kiri jika salah dan tangan kanan jika benar. Lakukan secara bergiliran dengan peserta lainnya.

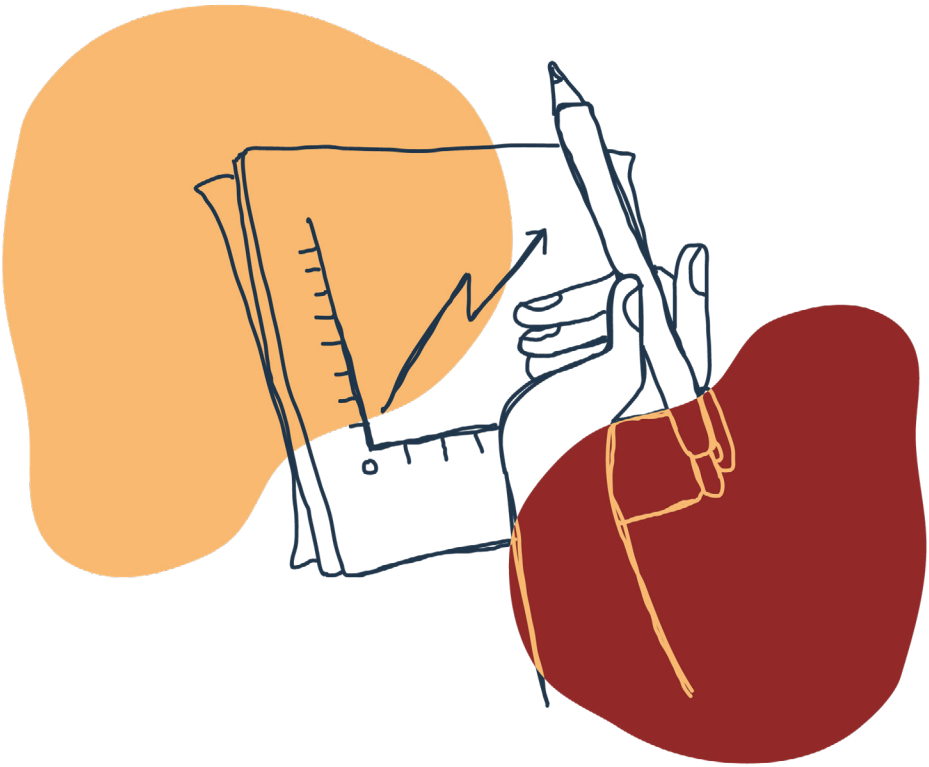
- **Joget keliling.** Peserta diatur dalam bentuk lingkaran, di lantai dibuat satu kotak menggunakan lakban. Fasilitator kemudian memutar lagu dan meminta peserta untuk bergerak keliling sambil berjoget sesuai lagu tersebut. Fasilitator akan mematikan lagu secara acak, saat lagu berhenti dan ada peserta yang berdiri tepat di atas kotak maka dia harus menjawab pertanyaan yang diberikan fasilitator.

- **Alpha & Delta.** fasilitator menyediakan flipchart yang dibagi menjadi dua bagian dan ditandai dengan bagian alpha dan bagian delta. Peserta akan diminta menuliskan pengalaman dan hal baik yang dapat dipertahankan atau ditingkatkan selama sesi pelatihan di bagian alpha dan hal yang bisa diperbaiki selama pelatihan di sisi delta. Metode ini biasa dilakukan setiap hari setelah seluruh sesi berakhir.

- **Kuis:** dapat dilakukan secara daring, misalnya dengan bantuan Kahoot, berisi pertanyaan seputar materi pelatihan. Metode ini sebaiknya dilakukan saat penutupan kegiatan dan bisa ditambahkan dengan hadiah untuk pemenang

- **Surat cinta:** dilakukan dengan menempelkan amplop kosong di dinding ruangan yang sudah dinamai dengan seluruh nama yang hadir dalam kegiatan. Setiap orang menuliskan pesan secara anonim atau terbuka dan meletakkan pesannya sesuai dengan nama orang yang dituju. Amplop akan dibagikan sesuai dengan nama pemiliknya setelah seluruh kegiatan selesai. Metode ini cocok untuk pelatihan yang berlangsung lebih dari dua hari karena kedekatan antarpeserta sudah terasa.
- **Monitoring keaktifan dan observasi interaksi:** dapat dilakukan oleh panitia, fasilitator dan pelatih untuk melihat perkembangan pengetahuan dan percaya diri peserta dalam mengikuti pelatihan keamanan digital. Metode ini dapat digunakan untuk mengukur seberapa besar antusiasme peserta dan menentukan metode pelatihan

- **Brief dan Debrief** dilakukan secara internal untuk panitia, fasilitator dan pelatih. Briefing bisa dilakukan sehari sebelum pelatihan dimulai atau setiap pagi sebelum kegiatan dimulai untuk memastikan persiapan sudah sesuai. Debrief bisa dilakukan setiap sore hari untuk menilai apa yang harus ditingkatkan di hari berikutnya dan membahas komentar peserta yang ada di alpha dan delta.



Penilaian Setelah Pelaksanaan

Setelah pelatihan selesai bukan berarti seluruh rangkaian pelatihan juga selesai. Setidaknya panitia, fasilitator, dan pelatih perlu mengetahui perkembangan pengetahuan ataupun pandangan peserta terhadap pelatihan itu sendiri.

Beberapa metode penilaian setelah pelatihan yang bisa dilakukan adalah sebagai berikut:

- **Testimoni,** fasilitator meminta kepada semua peserta untuk memberikan testimoni terhadap pelatihan. Testimoni dituliskan di sebuah kertas kecil dan dikumpulkan. Peserta boleh untuk anonim atau tidak perlu menyebut nama.

- **Skala**, fasilitator meminta kepada peserta untuk memberikan angka dalam skala 1–100 terhadap pelatihan ini. Peserta cukup memberikan angka tanpa memberikan alasan.

- **Post-test,** panitia dan fasilitator menyiapkan beberapa pertanyaan post-test untuk mengukur peningkatan pengetahuan peserta. Pertanyaan post-test bisa sama dengan pertanyaan pre-test untuk melihat perkembangan pengetahuan peserta secara kuantitatif, bisa juga pertanyaan lain untuk melihat perkembangan pengetahuan secara kualitatif. Sebaiknya adalah gabungan dari dua jenis penilaian tersebut. Jangan lupa juga sisipkan bagian saran atau masukan dari peserta terkait pelatihan.

Daftar Istilah (Glosarium)

Berikut adalah istilah terkait hak digital dan keamanan digital

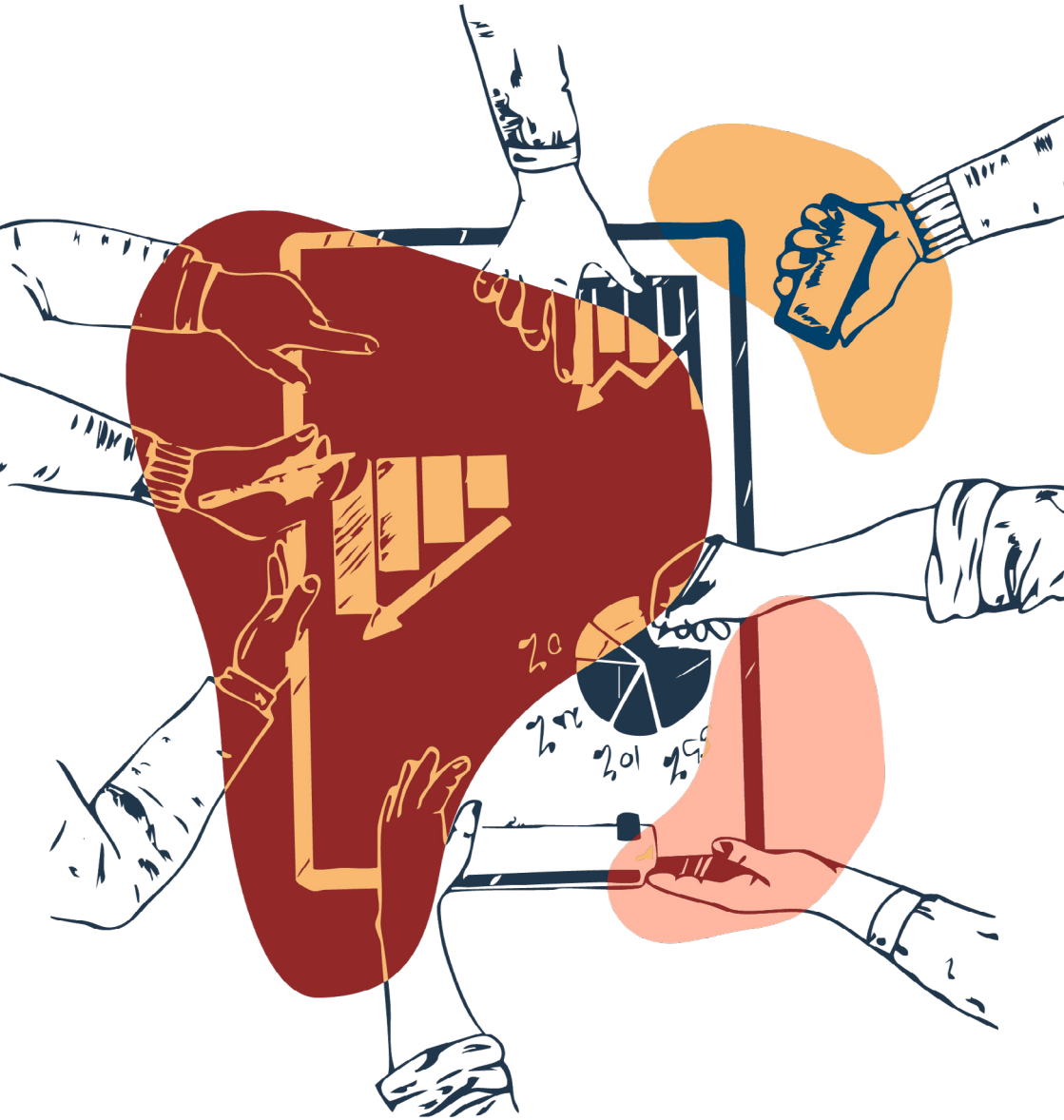
ISTILAH	ARTI
ANTIVIRUS	Perangkat lunak untuk mendeteksi dan menghapus aplikasi berbahaya.
AUTENTIFIKASI	Proses membuktikan identitas seseorang. Autentifikasi digunakan untuk mencegah akses ilegal ke sistem atau data. Autentifikasi biasanya menggunakan SMS, aplikasi autentikator, atau kode cadangan.
BIOMETRIK	Metode identifikasi dan verifikasi identitas seseorang berdasarkan karakteristik fisik atau perilaku unik yang mereka miliki. Ciri-ciri ini, seperti sidik jari, wajah, iris mata, suara, atau bahkan pola perilaku seperti cara berjalan, dapat digunakan untuk memastikan bahwa seseorang adalah orang yang sebenarnya dan memiliki akses ke sistem atau data tertentu.
BLUETOOTH	Teknologi nirkabel jarak pendek yang memungkinkan perangkat elektronik untuk terhubung dan berkomunikasi satu sama lain tanpa kabel. Ia beroperasi pada pita frekuensi 2.4 GHz dan sering digunakan untuk menghubungkan perangkat seperti headphone, speaker, keyboard, dan mouse ke ponsel, tablet, atau komputer.

BUDDY	Secara umum bisa diartikan sebagai tandem atau pasangan.
DATA PRIBADI	Data pribadi adalah data atau informasi tentang seseorang yang bisa diidentifikasi secara langsung atau tidak langsung melalui sistem elektronik atau non-elektronik.
DOXING	Penyebaran data pribadi ke media sosial tanpa izin. Dalam konteks KBGO, penyebaran dilakukan dengan menggunakan data pribadi korban untuk disalahgunakan sebagai konten tidak beradab. Contoh: penyebaran riwayat aktivitas seksual.
ENKRIPSI	Proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci khusus.
HAK DIGITAL	Hak asasi manusia yang berkaitan dengan akses, penggunaan, pembuatan, dan penyebaran media digital, serta akses dan penggunaan komputer dan perangkat elektronik lainnya. Secara umum SAFEnet membagi hak digital menjadi empat bagian, yaitu: hak atas akses, hak atas kebebasan berekspresi, hak atas rasa aman termasuk aman dari kekerasan berbasis gender online.

PROVIDER	Kerap juga disebut ISP atau Internet Service Provider. Layanan yang dikeluarkan oleh perusaaan tertentu untuk memberikan suplai Internet kepada masyarakat dengan cara berlangganan
KBGO	Kekerasan Berbasis Gender Online. Kekerasan berbasis gender yang difasilitasi teknologi dan/atau internet. Misalnya pelecehan seksual di kolom komentar media sosial.
KEBEBASAN BEREKSPRESI	Proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci khusus.
GANGGUAN INTERNET	Gangguan terhadap jaringan dan akses internet, sering diartikan juga dengan istilah internet shutdown (pemadaman internet), internet outage dan istilah sejenis.
KONTEN	Informasi yang tersedia melalui media atau produk elektronik. Informasi tersebut terdiri atas beberapa jenis, seperti foto, video, keterangan (caption), tagar (hastag) atau label metadata media sosial, postingan, geotag atau lokasi, postingan dalam postingan (repost atau retweet), siaran langsung (live streaming) dan lainnya.

KONTEN INTIM	Sebuah konten yang bermuatan kesusilaan, pornografi dan/atau bernuansa seksual berupa gambar, sketsa, ilustrasi, foto, tulisan, suara, bunyi, gambar bergerak, animasi, kartun, percakapan, gerak tubuh, atau bentuk pesan lainnya melalui berbagai bentuk media komunikasi dan/atau pertunjukan di muka umum, yang memuat kecabulan atau eksploitasi seksual yang melanggar norma kesusilaan dalam masyarakat.
KORBAN KRIMINALISASI	Orang yang dilaporkan disebabkan oleh ekspresi yang sah dan aktivitasnya di Internet dengan menggunakan pasal dan aturan tertentu.
KRIMINALISASI	Penentuan suatu perilaku yang sebelumnya tidak dipandang sebagai suatu kejahatan menjadi suatu perbuatan yang dapat dipidana.
OFFLINE (DARING)	Luar jaringan atau disingkat luring dalam Bahasa Indonesia. Interaksi yang terputus melalui jaringan internet, tetapi terjadi di dunia nyata.
ONLINE (LURING)	Dalam jaringan atau disingkat daring dalam Bahasa Indonesia. Interaksi yang terhubung melalui jaringan internet
PELAPOR	Orang yang memberikan laporan, informasi, atau keterangan kepada penegak hukum mengenai tindak pidana yang akan, sedang, atau telah terjadi.

PHISHING	Upaya untuk menipu seseorang untuk memberikan informasi pribadi atau data keuangan.
PLATFORM	Ruang digital yang menyediakan fasilitas bagi pengguna untuk berkolaborasi, berinteraksi, atau bertransaksi digital.
PRE-TEST	Test yang diberikan sebelum pelaksanaan pelatihan, tujuannya untuk mengetahui kapasitas peserta sebelum memulai pelatihan
POST-TEST)	Test yang diberikan setelah pelaksanaan pelatihan, tujuannya untuk tahu perkembangan pengetahuan atau kapasitas peserta setelah menjalani pelatihan.
TROLLING	Tindakan sengaja memposting pesan atau komentar yang provokatif, ofensif, atau tidak relevan di internet dengan tujuan untuk memicu reaksi emosional dari orang lain. Dalam bahasa Indonesia bisa disebut sebagai komentar buruk.
WARGANET (NETIZEN)	Orang yang aktif menggunakan internet.



Penutup

Selamat! Kamu telah menyelesaikan modul Pelatihan Keamanan Digital. Kami harap kamu sudah belajar tentang:

- pengantar hak digital
- dasar-dasar keamanan digital
- kebersihan laptop dan ponsel
- pengelolaan identitas,
- komunikasi yang aman,
- komunikasi yang aman di lapangan, dan
- pertolongan pertama pada serangan digital dan KBGO.

Semoga setelah belajar, kamu mendapatkan pemahaman yang lebih kuat tentang hak digital kamu dan lebih percaya diri dalam menjelajahi dunia maya. Tentu kamu juga harus terus mengingat bahwa belajar keamanan digital adalah sesuatu yang tidak akan pernah berakhir. Teknologi terus berkembang dengan pesat, dan dengan perkembangannya akan muncul pula tantangan serta ancaman baru.

Apa yang kita pelajari hari ini mungkin perlu sedikit penyesuaian besok. Oleh karena itu, komitmen untuk terus belajar dan berad-aptasi adalah kunci utama untuk tetap aman dan berdaya di ranah digital.

Modul ini telah membekali kamu dengan alat dan pengetahuan esensial, tetapi ini hanyalah permulaan. Kami mendorong kamu untuk terus:

- mencari informasi terbaru
- mempraktikkan kebiasaan digital yang aman, dan
- berbagi pengetahuan ini dengan komunitas dan jejaring kamu.

Setiap langkah kecil yang kamu ambil untuk melindungi diri sendiri dan orang lain berkontribusi pada lingkungan digital yang lebih aman bagi semua, termasuk teman-teman masyarakat adat dan pendamping masyarakat adat.

Terima kasih atas partisipasi aktif dan semangat belajar kamu.

Dunia digital menanti kamu untuk dijelajahi dengan lebih aman dan penuh percaya diri.

Mari terus berdaya bersama di era digital yang dinamis ini!