MODUL PELATIHAN

KEAMANAN DIGITAL BAGI PEMBELA HAM

****

ELSAM

LEMBAGA STUDI & ADVOKASI MASYARAKAT

MODUL PELATIHAN KEAMANAN DIGITAL

BAGI PEMBELA HAM

Modul Keamanan Digital bagi Pembela HAM

Penulis:

Atikah Nuraini
Yurino Juwanda

Editor:
Sueb Zakaria

Layout:

Dodi Sanjaya

Semua penerbitan ELSAM didedikasikan kepada para korban pelanggaran hak asasi manusia selain sebagai bagian dari upaya pemajuan dan perlindungan hak asasi manusia di Indonesia.

Pertama kali dipublikasikan dalam bahasa Indonesia oleh:

Lembaga Studi dan Advokasi Masyarakat (ELSAM) 2022

DAFTAR ISI

TITIK BERANGKAT

I. TITIK BERANGKAT

A. Latar Belakang

Serangan digital telah menjadi salah satu ancaman terbesar para pembela hak asasi manusia (HAM) saat ini. Berbagai bentuk serangan digital seperti peretasan dan penyebarluasan informasi pribadi di internet semakin sering terjadi seiring meningkatnya penggunaan sarana digital untuk melakukan pembelaan.

Para pembela HAM—aktivis, jurnalis, pembela lingkungan dan kelompok rentan, dan semua yang aktif melakukan pembelaan terhadap hak-hak warga, tidak dapat sepenuhnya terbebas dari serangan digital. Aktivitas yang mereka lakukan bersinggungan langsung dengan kelompok yang berkuasa, baik yang berafiliasi dengan pemerintah maupun swasta, atau keduanya. Dengan aktivitas tersebut, risiko pembela HAM mendapat serangan, termasuk serangan digital dengan sendirinya lebih besar daripada masyarakat umum.

Pembela HAM tidak dapat dilepaskan dari risiko serangan digital. Tapi ini tidak berarti pembela HAM tidak dapat melakukan apa pun untuk mengantisipasi dan mengurangi risiko-risikonya.

Pemahaman dasar mengenai bagaimana teknologi internet bekerja dan sejumlah teknik dasar menjaga keamanan digital telah banyak beredar dan dapat dipelajari. Sayangnya memang, sumber-sumber pengetahuan tersebut masih belum sistematis dan hanya sedikit orang yang memiliki waktu, ketekunan, dan kemampuan untuk mempelajarinya secara mandiri. Karennya, pelatihan keamanan digital, dengan kurikulum, metode, dan pemateri yang berpengalaman di bidangnya, tetap diperlukan.

Penulisan modul ini diharapkan dapat menjadi salah satu sarana untuk meningkatkan kapasitas para pembela HAM terkait keamanan digital. Sebagai acuan pelatihan, modul ini berisi ringkasan materi terkait keamanan digital metode, dan langkah-langkah dalam pelaksanaan pelatihan yang akan dilakukan.

B. Sumber Adaptasi

Materi dasar dari modul ini diadaptasi dari manual yang dirancang oleh EngageMedia yang dikembangkan untuk dapat digunakan di Negara-negara yang tergabung dalam *Greater Internet Freedom* (GIF) project.

C. Tujuan

Modul ini diharapkan dapat menjadi pegangan dalam pelatihan keamanan digital oleh organisasi masyarakat sipil. Adapun pelaksanaan pelatihan yang dirancang dalam modul ini memiliki beberapa tujuan:

1. Meningkatkan pemahaman dan keterampilan tentang keamanan digital
2. Meningkatkan pemahaman tentang risiko-risiko pemanfaatan teknologi internet
3. Menjadi sarana berbagi pengalaman antar-aktivis dalam memitigasi risiko serangan digital di organisasi masing-masing

D. Kelompok Sasaran

Pelatihan yang dirancang dalam modul ini ditujukan bagi para pembela HAM dan para pemimpin komunitas yang berisiko tinggi (*high-risk community leaders).* Mereka adalah para aktivis, jurnalis, pemimpin masyarakat adat, pembela kelompok marjinal, dan orang-orang yang dalam aktivitas pembelaan mereka rentan mengalami serangan digital.

E. Pokok Bahasan dan Isi Modul Pelatihan

Para peserta akan dapat meningkatkan pengetahuan dan keterampilan mereka dengan materi berikut ini:

1. Asesmen Risiko (*Risks Assessment*)
2. Kebersihan digital (*Digital Hygiene*)
3. Malware dan perlindungan (*Malware and Protection*)
4. Perangkat lunak bebas dan sumber terbuka (*Free and Open Source*
5. *Software - FOSS)*
6. Keamanan dan privasi peramban (*Browser security and privacy*)
7. Manajemen kata sandi (*Password management*)
8. Perlindungan file dan folder (*File and folder protections*)
9. Data Backup
10. Enkripsi data dan komunikasi (*Data and communication encryption*)
11. PGP dan enkripsi email (*PGP and email encryption*)
12. Cara kerja internet dan enkripsi jaringan dengan VPN dan Tor
13. Privasi dan keamanan di media sosial.
14. Risiko terkait ponsel dan penggunaan alat komunikasi yang aman
15. Perencanaan dan persiapan pelatihan bagi komunitas

F. Asesmen Pra-Pelatihan untuk Penilaian Kebutuhan dan Risiko

Sebelum pelatihan, penyelenggara disarankan untuk melalui analisis kebutuhan dan keterampilan atau literasi digital bagi para peserta. Setiap peserta berbeda dan mereka memiliki wilayah kerja yang berbeda yang berbeda pula risiko dan kebutuhannya. Dan ada baiknya mengetahui tingkat pengetahuan peserta yang ada untuk memilih topik dan metodologi pelatihan.

Disarankan untuk melakukan penilaian risiko sebelum pelatihan. Dan berdasarkan penilaian, buatlah persiapan dan antisipasi hal-hal yang tak

terduga. Penyelenggara dan fasilitator diharapkan selalu menyiapkan rencana cadangan. Saat merencanakan pelatihan, pertimbangkan hal-hal di bawah ini:

1. **Pelatihan apa yang perlu diberikan** – dan kepada siapa? – Perencanaan sesi perlu dilakukan berdasarkan data survei peserta yang ditargetkan. Pilihlah peserta dan topik yang relevan.

2. **Siapa yang melakukan pelatihan**? – Hasil pelatihan sebagian besar tergantung pada orang yang memfasilitasi pelatihan. Pelatih yang terampil dan berpengalaman, yang menguasai topik dengan baik harus dipertimbangkan untuk fasilitasi pelatihan.

3. **Siapa yang mengembangkan materi, penyelenggaraan dan proses pelatihan?** - Meskipun EngageMedia yang mengembangkan rancangan atau template kurikulum ini, namun setiap pelatihan hendaknya disesuaikan dengan lingkungan dan konteks lokalnya yang sesuai.

4. **Keanekaragaman latar belakang peserta**- Dalam pelatihan peserta akan berasal dari komunitas dan organisasi yang beragam. Mereka akan memiliki perbedaan usia, jenis kelamin, kepercayaan, wilayah kerja, dll. Mereka juga akan memiliki kebiasaan belajar yang berbeda. Pelatihan perlu dikelola dengan mempertimbangkan keragaman.

5. **Lingkungan atau konteks sosial dan politik** – Pelajari tentang lingkungan politik dan sosial lokal sebelum menyelenggarakan pelatihan.

G. Metodologi Pelatihan

Training ini menggunakan pendekatan **ADIDS** (*Activity, Discussion, Inputs, Deepening, and Synthesis*). ADIDS telah digunakan secara efektif dalam advokasi dan pelatihan keterampilan tentang isu-isu hak asasi manusia, dan ini berguna dalam membantu peserta, minimal untuk lebih memahami kompleksitas keamanan digital. Selain itu, metode ADIDS ini

untuk pelatih juga dapat memberikan kerangka kerja yang berguna saat membuat rencana pelajaran.

Rujukan lebih lanjut tentang ADIDS dapat di simak dari rujukan berikut ini: https://level-up.cc/before-an-event/preparing-sessions-using-adids/

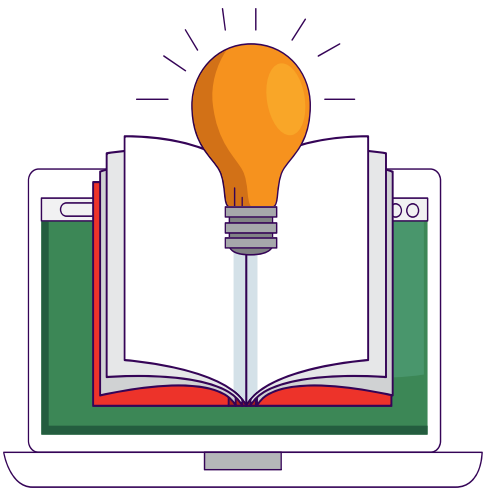
H. Monitoring, Pengujian dan Evaluasi

Sejalan dengan asesmen di awal pelatihan, maka penyelenggara dan fasilitator juga disarankan untuk menggunakan kerangka monitoring dan evaluasi untuk menilai keberhasilan dan perubahan yang diperoleh pasca pelatihan pelatihan. Hal-hal yang perlu dijabarkan dalam kerangka monitoring dan evaluasi ini meliputi:

1. **Pra-pelatihan** – Untuk mempelajari tentang pengetahuan peserta yang ada dan untuk merencanakan sesi yang tepat, disarankan untuk melakukan survei online. Ajukan beberapa pertanyaan terkait pekerjaan peserta dan agenda pelatihan.
2. **Selama Pelatihan** – Selama pelatihan, setelah setiap sesi evaluasi dari peserta mungkin dikumpulkan untuk memperbaiki sesi selanjutnya.
3. **Pasca pelatihan** - Di akhir pelatihan, asesmen atau model evaluasi lain direkomendasikan untuk mengevaluasi peningkatan peserta dari pelatihan.

I. Sumber-sumber Rujukan

Berikut ini adalah sumber-sumber rujukan yang disarankan:



Bahan Bacaan

- https://level-up.cc/
- https://ssd.eff.org/

- https://securityinabox.org/en/
- https://holistic-security.tacticaltech.org/
- https://digitalfirstaid.org/en/index.html
- https://gijn.org/digital-security/
- https://gcatoolkit.org/journalists/
- https://secfirst.org/
- https://www.frontlinedefenders.org/en/digital-security-resources

Perangkat Lunak, Aplikasi, Alat, dan Platform

- https://duckduckgo.com/ Google alternative search engine
- https://www.malwarebytes.com/ Malware removal tools
- https://www.avira.com/ Free antivirus
- https://www.avast.com/ Free antivirus
- https://virustotal.com/ Online malware scanner
- https://brave.com/ Open Source browser
- https://www.mozilla.org/en-US/firefox/new/ Opensource browser
- https://www.eff.org/https-everywhere HTTPS redirection extension for browser
- https://adblockplus.org/ Advertisement and tracker removal extension for browser
- https://keepassxc.org/ Opensource password manager
- https://authy.com/ 2FA app and guides
- https://youtu.be/F7pYHN9iC9I Video for social media awareness
- https://aesencryption.net/ Online text encryption platform
- https://aescrypt.com/ Small tools to encrypt files with password
- https://torproject.org/ Official site of Tor
- https://www.tunnelbear.com/ Paid VPN
- https://www.psiphon3.com/ Free VPN
- https://veracrypt.fr/ File folder encryption tool
- https://www.bleachbit.org/ Permanent file and folder removal tool.
- https://ccleaner.com/recuva Deleted file recovery tool
- http://exif.regex.info/ Meta data verification platform
- https://duplicati.com/ Encrypted backup creation tool
- https://www.openpgp.org/ Email encryption

- https://mailvelope.com/ Email encryption browser extension
- https://www.thunderbird.net/ Email Client
- https://signal.org/ Secure communication app
- https://wire.com/ Secure communication app
- https://briarproject.org/ Mobile app for offline secure communication

J. Format Pembelajaran

Pelatihan ini akan diselenggarakan secara daring (*online*) dalam format pembelajaran campuran (*blended learning*) yang memadukan metode sinkron dan asinkron. Prosesnya akan berlangsung intensif selama 16 kali pertemuan yang terdiri dari:

a. Registrasi dan Administrasi Pelatihan

b. Belajar mandiri yang terdiri dari:
   - Mengisi Asesmen pra dan pasca pelatihan
   - Menonton video yang ditugaskan
   - Menjawab pertanyaan atau memberi pendapat dalam brainstorming via perangkat pembelajaran daring
   - Membaca bahan bacaan, baik bacaan wajib maupun bacaan penunjang.
   - Menyelesaikan tugas-tugas individu atau kelompok.

C. Kelas Virtual 120-150 menit per pertemuan yang diselenggarakan 3 kali seminggu (pagi dan siang). Kelas Virtual terdiri dari:
   - Webinar /Ceramah di kelas,
   - Kelas Interaktif: Diskusi kelompok, Presentasi, Role Play dan Kerja Kolaboratif.

KURIKULUM DAN PANDUAN PELATIHAN

II. KURIKULUM DAN PANDUAN PELATIHAN

A. Alur Pelatihan

Training ini diselenggarakan oleh ELSAM dengan tujuan untuk meningkatkan kapasitas para pembela HAM, pendamping komunitas, dan siapapun yang bekerja untuk masyarakat agar memahami dan terampil dalam melakukan pengamanan digital. Fokus Pelatihan ini adalah meningkatnya kompetensi pengetahuan (*knowledge*) dan kompetensi keterampilan (*skills*) untuk para peserta. Materi-materi yang disusun dalam pelatihan ini merujuk pada berbagai informasi dan inovasi terkini terkait keamanan digital dari berbagai organisasi yang bekerja di bidang HAM dan teknologi informasi dan komunikasi.

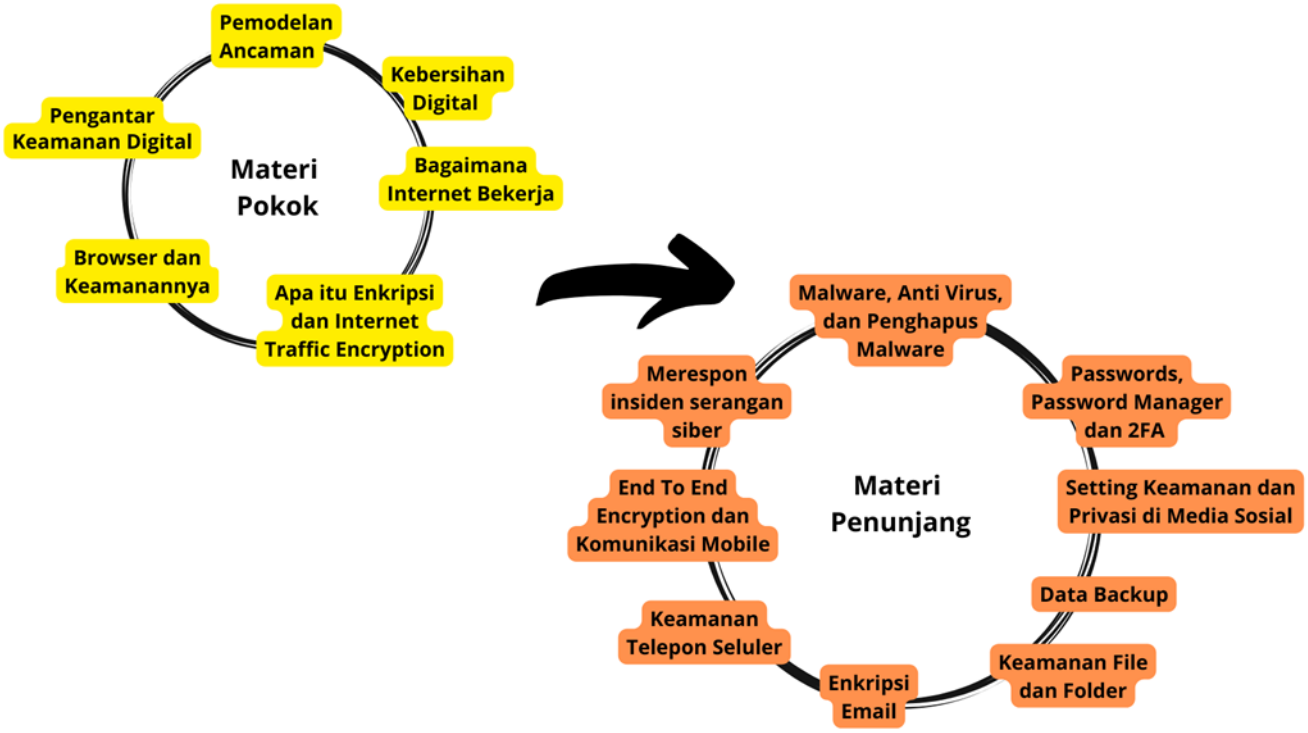
Materi Pokok

Topik-topik yang dianggap sebagai materi pokok dalam pelatihan ini meliputi 6 topik yaitu:

1. Pengenalan tentang Keamanan Digital.
2. Pemodelan Ancaman (*Threat Modeling*).
3. Kebersihan Digital (*Digital Hygiene*).
4. Bagaimana Internet Bekerja.
5. Browser dan Keamanannya.
6. Apa itu Enkripsi dan *Internet Traffic Encryption.*

Materi Penunjang keterampilan

1. Mengenali dan memahami *Malware,* Anti Virus, dan Perangkat Penghapus *Malware.*
2. Memahami pentingnya Passwords, Menggunakan dan mengelola *Password Manager* dan 2FA (*Two-Factors Authentication*).
3. Mengelola Setting Keamanan dan Privasi di Media Sosial.
4. Mengelola Keamanan *File* dan *Folder.*
5. Mengelola *Data Backup.*
6. Melakukan *Enkripsi Email.*
7. Memahami dan mengelola Keamanan Telepon Seluler.
8. Mengelola *End To End Encryption* dan Komunikasi Mobile.



Berikut ini adalah pengaturan sesi-sesi dan topik-topik pengembangan kompetensi pengetahuan dan keterampilan dalam pelatihan yang akan dilaksanakan:

Sesi 1 Pembukaan, Perkenalan, Orientasi Belajar (60 menit)Sesi 2 Pengenalan tentang Keamanan Digital (120 menit).

Sesi 3 Pemodelan Ancaman (*Threat Modeling*) (120 menit).

Sesi 4 Kebersihan Digital (*Digital Hygiene*) (120 menit).

Sesi 5 Bagaimana Internet Bekerja (120 menit).

Sesi 6 Browser dan Keamanannya (120 menit).

Sesi 7 Apa itu Enkripsi dan *Internet Traffic Encryption* (120 menit).

Sesi 8 Mengenali dan memahami *Malware*, Anti Virus, dan Perangkat Penghapus *Malware* (120 menit).

Sesi 9 Memahami pentingnya Passwords, Menggunakan dan mengelola *Password Manager* dan 2FA (*Two-Factors Authentication*), Latihan membuat *password* dan menggunakan *Password manager* (120 menit).

Sesi 10 Melakukan dan mengelola Enkripsi Email.

Sesi 11 Mengelola Keamanan *File* dan *Folder.*

Sesi 12 Melakukan dan mengelola *Data Backup.*

Sesi 13 Mengelola Setting Keamanan dan Privasi di Media Sosial.

Sesi 14 Keamanan Telepon Seluler.

Sesi 15 *End To End Encryption* dan Komunikasi *Mobile*.

Sesi 16 Merespon atau menanggapi insiden.

Sesi 17 Rencana Tindak Lanjut, Mempersiapkan Pelatihan Lanjutan,

Dengan 17 sesi tersebut maka secara ideal pelatihan daring dapat diselenggarakan selama 4-5 hari yang menggunakan pembelajaran campuran (*blended learning*) dan mengintegrasikan pembelajaran sinkron dan asinkron. Pengaturan sesi dapat disusun sebagai berikut:

Hari	**Sinkron Virtual**	**Siang/Sore**	**Asinkron**
	Pagi		**Pre-Assessment**
Hari 1	**Sesi 1** Pembukaan, Perkenalan, Orientasi Belajar. 60 menit **Sesi 2** Pengenalan tentang Keamanan Digital 120 menit	**Sesi 3** Pemodelan Ancaman (Threat Modeling). 180 menit	• Membaca bahan • Download dan pelajari aplikasi • Latihan praktik
Hari 2	**Sesi 4** Kebersihan Digital (*Digital Hygiene*). 180 menit	**Sesi 5** Bagaimana Internet Bekerja. 90 menit **Sesi 6** Browser dan Keamanan nya. 120 menit	• Membaca Bahan dan Praktik Individual • Download dan pelajari aplikasi • Latihan praktik

Hari	Sinkron Virtual	Siang/Sore	Asinkron
	Pagi		**Pre-Assessment**
Hari 3	**Sesi 7** Apa itu Enkripsi dan *Internet Traffic Encryption*.120 menit **Sesi 8** Mengenali dan memahami *Malware*, Anti Virus, dan Perangkat Penghapus *Malware*. 90 menit	**Sesi 9** Memahami pentingnya Passwords, *Password Manager* dan 2FA (*Two-Factors Authentication*), Latihan. 20 menit **Sesi 10** Melakukan dan mengelola Enkripsi Email. 90 menit	• Membaca Bahan dan Praktik Individual • Download dan pelajari aplikasi • Latihan praktik
Hari 4	**Sesi 11** Mengelola Keamanan File dan Folder. 90 menit **Sesi 12** Melakukan dan mengelola Data Backup. 90 menit	**Sesi 13** Mengelola Setting Keamanan dan Privasi di Media Sosial. 90 menit **Sesi 14** Keamanan Telepon Seluler. 90 menit	• Membaca Bahan dan Praktik Individual • Download dan pelajari aplikasi • Latihan praktik
Hari 5	**Sesi 15** *End To End Encryption* dan Komunikasi Mobile. 90 menit **Sesi 16** Merespon atau menanggapi insiden (90 menit)	**Sesi 17** Rencana Tindak Lanjut, Mempersiapkan Pelatihan Lanjutan, Evaluasi, dan Penutup	

B. Prinsip dan pendekatan Pelatihan

Pelatihan ini menerapkan sejumlah prinsip pembelajaran yang dituangkan dalam manual yaitu:

1. Manual ini menerapkan model pendidikan partisipatif di mana pusat pembelajaran ada pada peserta belajar. Pendekatan dan metode atau teknik fasilitasi yang digunakan adalah sebanyak mungkin bersifat partisipatoris dan mengedepankan interaksi dan komunikasi interpersonal.
2. Pelatihan ini merupakan proses belajar bersama antara peserta, peserta dan fasilitator dan narasumber.
3. Salah satu prinsip yang dikedepankan dalam Pelatihan ini adalah berlangsungnya pembelajaran kolektif (*collective learning*) yang lahir dari proses diskusi kelompok, diskusi kelas, pemberian umpan balik, dan praktik-praktik kerja bersama.
4. Peserta belajar menjadikan kelas dan pertemuan belajar sebagai forum yang setara dan saling bekerjasama/kolaborasi.
5. Belajar dari Pengalaman: Pelatihan ini bertumpu pada pengalaman peserta.
6. Beraksi dan Bertindak. Pelatihan ini diarahkan untuk memperkuat kemampuan bertindak dan beraksi.
7. Pelatihan ini bersifat praktis sesuai kebutuhan peserta, untuk terlibat dalam proses Pencegahan Penyiksaan di kantornya masing-masing.

C. Panduan Fasilitasi

Untuk membantu fasilitator memandu kelas, maka manual ini menyediakan panduan langkah demi langkah yang dapat digunakan oleh fasilitator, narasumber dan penyelenggara pelatihan dalam memandu proses pelatihan. Langkah-langkah fasilitasi ini dilengkapi dengan informasi mengenai tujuan sesi, durasi, metode, rujukan materi, serta bagaimana proses fasilitasinya.

Sesi 1: Pembukaan, Perkenalan, Orientasi Belajar

1. Peserta mengetahui informasi teknis mengenai kegiatan Pelatihan.
2. Peserta mengenal sesama peserta, fasilitator dan panitia pelatihan.
3. Peserta mengenali harapan mereka mengikuti pelatihan dan mencocokkannya dengan tujuan pelatihan.
4. Peserta memahami alur, agenda, dan prinsip pelatihan.

Pokok Bahasan

1. Pembukaan dan Penjelasan Tujuan Pelatihan.
2. Perkenalan Peserta, Fasilitator, dan seluruh Panitia Penyelenggara.
3. Mengisi Lembar Asesmen Pra-Training (dilakukan seminggu sebelum kegiatan).
4. Orientasi Pelatihan (identifikasi harapan, agenda, proses, metode, prinsip pembelajaran).
5. Pengenalan Perangkat Pembelajaran Daring.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis (ADIDS)

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. Perangkat Asesmen: Google Forms atau Survey Monkey (contoh form bisa dilihat di tautan berikut https://forms.gle/GbHPbdtgpXD9AX9w9
2. LMS: Google Classroom, Moodle, Canvas.
3. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
4. Presentasi: Google Slide, Jamboard.
5. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Waktu

60 Menit

Bahan Rujukan

- https://internews.org/
- https://engagemedia.org/

Langkah-langkah fasilitasi

1. Fasilitator menyambut peserta, mengucapkan selamat datang dan mempersilahkan ketua panitia untuk membuka pelatihan (5 menit).

2. Penyelenggara meminta Direktur ELSAM untuk memberikan sambutan (10 menit).
3. Fasilitator membuka kelas daring, menyambut peserta dan mengecek kelengkapan dan kesiapan peserta (5 menit).
4. Fasilitator mengajak peserta untuk berkenalan satu sama lain: Fasilitator meminta peserta menuliskan di kertas masing-masing (3 menit).

   Perkenalkan Nama peserta/panitia/fasilitator, buatlah satu gambar simbol yang menggambarkan kedekatanmu dengan dunia digital, tuliskan apa harapan mengikuti Pelatihan daring ini.

5. Fasilitator meminta peserta untuk memperkenalkan dirinya masing-masing dengan menyebutkan nama, simbol, dan harapan. Fasilitator menuliskan atau menempelkan kartu-kartu berisi nama, simbol, dan harapan tersebut di papan tulis daring
6. Fasilitator menganalisis daftar harapan dan simbol yang sudah dituliskan di papan (5 menit).
7. Fasilitator menjelaskan tujuan dan agenda Pelatihan daring (10 menit).
8. Fasilitator menggali kepada peserta apa prinsip pembelajaran dan aturan bersama untuk disepakati (10 menit).
9. Fasilitator merangkum catatan yang sudah disepakati, menutup sesi dan mengajak peserta untuk beristirahat sebentar sebelum masuk ke sesi berikutnya.

Sesi 2 Pengenalan tentang Keamanan Digital

Tujuan

1. Peserta memahami apa itu dunia digital dan pentingnya keamanan digital.
2. Peserta mengenal apa itu keamanan holistik.
3. Peserta merefleksikan keamanan digitalnya masing -masing.
4. Peserta mengenal apa itu *software* atau perangkat lunak yang terbuka dan tidak berbayar (*Free and Open Source Software* - FOSS).

Pokok Bahasan

1. Apa itu dunia digital dan pentingnya keamanan digital.
2. Apa itu Keamanan holistik (*holistic security*)
3. Pentingnya *self-care*.
4. Relevansi keamanan digital untuk kehidupan pribadi dan profesi kita.
5. mengenal FOSS (*free and open source software*).

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button
3. Presentasi: Google Slide, Jamboard
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet

Waktu

120 Menit

Bahan Rujukan

- https://holistic-security.tacticaltech.org/

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta menonton video tentang kasus-kasus terkait keamanan digital (20 menit).
3. Fasilitator mengundang komentar dan tanggapan

dari peserta tentang video tersebut. Fasilitator menggali dari peserta tentang pemahaman mereka terkait keamanan digital berdasarkan isi video (20 menit)

4. Fasilitator mengundang narasumber untuk memaparkan materi tentang keamanan digital dan keamanan holistik (45 menit). Kisi-kisi yang akan dibahas oleh narasumber adalah:
    a. Apa itu dunia digital dan pentingnya keamanan digital
    b. Apa itu Keamanan holistik (holistic security)
    c. Pentingnya self-care.
    d. Relevansi keamanan digital untuk kehidupan pribadi dan profesi kita
    e. Mengenal FOSS (free *and open source software*).
5. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya untuk merespon narasumber, narasumber menanggapi pertanyaan dan komentar peserta (45 menit).
6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

Keamanan digital adalah istilah kolektif yang menggambarkan sumber daya yang digunakan untuk melindungi identitas online, data, dan aset lainnya. Alat-alat ini termasuk layanan web, perangkat lunak antivirus, kartu SIM ponsel cerdas, biometrik, dan perangkat pribadi yang diamankan.

Singkatnya, keamanan digital berarti melindungi komputer, perangkat seluler, tablet, dan perangkat lain yang terhubung ke Internet dari penyusup, yang bisa berupa peretasan, phishing, dan banyak lagi. Keamanan digital juga dapat digunakan untuk melindungi data pribadi agar tidak digunakan dan dijual oleh perusahaan.

Keamanan siber (cybersecurity) penting karena melindungi semua kategori data dari pencurian dan kerusakan. Ini termasuk data sensitif, informasi pribadi yang dapat dikenali (PII - *personally identifiable information*), informasi kesehatan yang dilindungi (PHI - *protected health information*), informasi pribadi, kekayaan intelektual (*intellectual property*), data, dan sistem informasi pemerintah dan industri. Ketika setiap aspek keamanan digital Anda dilonggarkan, semua informasi pribadi - kartu kredit, rekening bank, akun email, seluruh identitas dapat mengalami risiko.

Keamanan holistik adalah pendekatan terpadu untuk keamanan digital, fisik, dan psiko-sosial bagi individu dan organisasi. Tujuan pendekatan holistik terhadap keamanan dan perlindungan aktivis dan pembela HAM meliputi:

- Memperkuat keberlanjutan aktivisme dalam konteks kekerasan (dipahami secara luas dan interseksional).
- Memperkuat kapasitas aktivis untuk berefleksi, belajar dan mengambil tindakan pencegahan untuk meningkatkan keamanan dan perlindungan mereka.
- Memperkuat ketahanan dan kemampuan aktivis untuk merespon secara kreatif selama masa 'krisis'.

FOSS (*Open Source Offers Flexibility, Collaboration and Enhanced Security*) atau Sumber Terbuka Menawarkan Fleksibilitas, Kolaborasi, dan Keamanan yang Ditingkatkan. Ini adalah perangkat lunak komputer yang dirilis di bawah lisensi di mana pemegang hak cipta memberikan hak kepada pengguna untuk menggunakan, mempelajari, mengubah, dan mendistribusikan perangkat lunak dan kode sumber (*source code*)-nya kepada siapa pun dan untuk tujuan apa pun. Perangkat lunak dengan Open Source dapat dikembangkan dengan cara publik yang kolaboratif.

Sesi 3 Pemodelan Ancaman (*Threat Modeling*)

Tujuan

1. Peserta memahami apa itu ancaman.
2. Peserta mengenali pemodelan ancaman.
3. Peserta menilai risiko pribadi dan pekerjaan dan contoh-contohnya.

Pokok Bahasan

1. Mengenal Pemodelan Ancaman (*threat modeling*).
2. Mengenal risiko (digital) pribadi dan pekerjaan.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis.

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

150 Menit

Bahan Rujukan

- https://ssd.eff.org/en/module/your-security-plan

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta mengenali resiko dan ancaman (digital) yang pernah mereka alami atau ketahui. Fasilitator menggali dari peserta tentang (20 menit).
3. Fasilitator mengundang narasumber untuk memaparkan diagram alur pemodelan ancaman dan mendiskusikan proses langkah demi langkahnya. Narasumber akan menyajikan risiko organisasi atau pribadi sebagai contoh (45 menit)
4. Narasumber meminta peserta untuk menilai risiko yang disebutkan dalam model. Narasumber akan

membahas tentang tanggapan yang dilakukan oleh peserta (45 menit).

5. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya untuk merespon narasumber, narasumber menanggapi pertanyaan dan komentar peserta (20 menit).
6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

Keamanan adalah sebuah proses, dan melalui perencanaan yang matang, kita dapat menyusun rencana yang tepat. Keamanan bukan hanya tentang alat yang digunakan atau perangkat lunak yang diunduh. Ini dimulai dengan memahami ancaman unik yang dihadapi dan bagaimana kita melawan ancaman tersebut. Pertanyaan Kunci

a. Apa yang ingin saya lindungi?
b. Dari siapa saya ingin melindunginya?
c. Seberapa buruk konsekuensinya jika saya gagal?
d. Seberapa besar kemungkinan saya perlu melindunginya?
e. Berapa banyak masalah yang ingin saya lalui untuk mencoba mencegah konsekuensi potensial?

Sesi 4 Kebersihan Digital (*Digital Hygiene*)

Tujuan

1. Peserta memahami apa kebersihan digital (digital *hygiene*).
2. Peserta merefleksikan sejauh mana mereka mempraktikkan kebersihan digital.
3. Peserta mempraktikkan bagaimana menyiapkan kebersihan digital.

Pokok Bahasan

1. Pemahaman dasar tentang keamanan digital.
2. Kaitan Keamanan digital dengan kebersihan digital.
3. Bagaimana praktik kebersihan digital.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://coconet.social/digital-hygiene-safety-security/

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang tentang kebersihan digital (20 menit).
3. Fasilitator mengajak peserta untuk membahas poin-poin kebersihan digital dan kaitan Keamanan digital dengan kebersihan digital (45 menit).
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).
5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Jangan berbagi informasi keuangan Anda dengan siapa pun.
2. Saat Anda membuka email, pastikan untuk memeriksa detail pengirim.
3. Jangan mengklik tautan apapun sebelum mengkonfirmasi tujuan.
4. Lampiran bisa berbahaya, pindai dengan antivirus sebelum dibuka.
5. Selalu unduh perangkat lunak dari situs web asli (resmi).
6. Berikan prioritas pada perangkat lunak sumber terbuka.
7. Ubah kebiasaan *online* dan *offline*.
8. *Sign out*/keluar dari semua akun sebelum mematikan komputer.
9. Selalu hati-hati. Pahami di mana Anda mengklik, pikirkan sebelum mengklik.
10. Jangan membuka akun Anda di komputer atau ponsel orang lain.
11. Jangan pinjamkan perangkat Anda kepada orang lain. Jika Anda perlu meminjamkan perangkat Anda kepada orang lain, pastikan untuk mengawasinya.
12. Perbarui perangkat Anda secara teratur.
13. Jangan gunakan hotel, warnet, atau jaringan publik kecuali Anda mengambil tindakan yang diperlukan untuk mengamankan koneksi (seperti terhubung menggunakan VPN atau Tor). Jika Anda perlu menggunakan komputer orang lain, gunakan OS yang aman dan portabel seperti *Tails*.
14. Waspadai apa yang Anda publikasikan secara online.
15. Bawa hanya data / informasi pribadi yang diperlukan bersama Anda.
16. Pertahankan nama samaran dan privasi.
17. Gunakan enkripsi untuk bertukar informasi.
18. Keamanan digital bukan hanya masalah diri sendiri, bantu orang lain.

Sesi 5 Bagaimana Internet Bekerja

Tujuan

1. Peserta memahami bagaimana internet bekerja
2. Peserta memahami bagaimana transfer data dari satu titik ke titik lainnya
3. Peserta mengenali siapa saja aktor yang terlibat di dalamnya dan risiko-risikonya.

Pokok Bahasan

1. Bagaimana internet bekerja
2. Transfer data dari satu titik ke titik lainnya
3. Aktor-aktor yang terlibat
4. Risiko bekerja dengan internet
5. Keamanan dasar router (*basic router security*)

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://academind.com/tutorials/how-the-web-works/
- https://www.youtube.com/watch?v=7_LPdttKXPc
- https://vahid.blog/post/2020-12-15-how-the-internet-works-part-i-infrastructure/

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang bagaimana internet bekerja dan keamanan transfer data (20 menit).
3. Fasilitator meminta peserta untuk nonton video tentang tentang bagaimana internet bekerja.
4. Fasilitator mengundang narasumber untuk membahas:
    a. contoh pengiriman email atau browser situs web yang menjelaskan bagaimana data berpindah dari satu titik ke titik lainnya.

b. Aktor-aktor yang terlibat.

c. Risiko bekerja dengan internet.

d. Dasar-dasar setting untuk keamanan *router.*

5. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).

6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit)

Ringkasan Materi Sesi

1. Internet adalah jaringan yang lebih luas yang memungkinkan jaringan komputer di seluruh dunia yang dijalankan oleh perusahaan, pemerintah, universitas dan organisasi lain untuk berbicara satu sama lain.
2. Internet hanya memindahkan data dari satu tempat ke tempat lain, sehingga kita dapat mengobrol, menjelajah, dan berbagi.
3. Secara fisik, Internet adalah kumpulan komputer yang saling memindahkan bit melalui kabel, kabel, dan sinyal radio.
4. Perangkat <-> Router <-> ISP <-> DNS <-> Server
5. Keamanan *router* dasar-
6. Ubah kata sandi *default*.
7. Ubah nama WIFI *default*.
8. Gunakan kata sandi yang bagus untuk WIFI.
9. Gunakan enkripsi WPA2/3, hindari WEP.
10. Sembunyikan *ID* WIFI jika diperlukan.
11. Jangan berbagi jaringan Anda dengan orang lain, jika perlu buat jaringan tamu.

Sesi 6- Browser dan Keamanannya

Tujuan

1. Peserta memahami apa itu keamanan dan privasi dalam *web browser.*
2. Peserta mengenal jenis-jenis *web browser* dan bagaimana memilih web browser yang baik.

Pokok Bahasan

1. Belajarlah untuk memilih *browser* yang baik.
2. Pengaturan keamanan *browser* dan privasi pada browser menggunakan alat/ekstensi.
3. Pelajari perbedaan antara HTTP dan HTTPS.
4. Pelajari cara mengidentifikasi tautan phising dan Palsu.
5. Penggunaan *DuckDuckGo* atau *StartPage* atau Quant sebagai mesin pencari, bukan *Google*.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://brave.com/ Open Source browser
- https://www.mozilla.org/ Open Source browser
- https://www.eff.org/https-everywhere HTTPS redirection extension for browser
- https://duckduckgo.com/ Google alternative search engine
- https://adblockplus.org/ Advertisement and tracker removal extension for browser
- https://level-up.cc/curriculum/safer-browsing/

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang tentang *web browser* dan keamanannya (20 menit).
3. Fasilitator mengundang narasumber untuk membahas tentang (45 menit):
    - memilih browser yang baik dan penggunaan *web browser open source.*

- pengaturan keamanan browser dan privasi pada browser menggunakan alat/ekstensi,
- perbedaan antara HTTP dan HTTPS dan pentingnya HTTPS dan SSL
- cara mengidentifikasi tautan *phising* dan palsu
- penggunaan *DuckDuckGo* atau *StartPage* atau *Quant* sebagai mesin pencari, bukan *Google*

4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).
5. Fasilitator mengajak peserta peserta untuk praktik menggunakan *DuckDuckGo* atau *StartPage* atau *Quant* sebagai mesin pencari.
6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Sesi

1. Gunakan *browser web open source* seperti Brave, Firefox atau Chromium.
2. Jangan pernah menyimpan kata sandi Anda di *browser*.
3. Jangan menginstal add ons yang tidak dipercaya.
4. Matikan riwayat *browser* dan bersihkan *cache* dan *cookie browser* Anda secara teratur. Atau, Anda dapat menggunakan penjelajahan pribadi tetapi perlu diingat bahwa itu tidak akan memberi Anda anonimitas sebagai Tor.
5. Nonaktifkan Java dan *Flash* jika tidak diperlukan.
6. Gunakan *DuckDuckGo, StartPage* atau *Quant* untuk privasi pencarian.

7. Jangan masuk ke situs mana pun yang tidak memiliki HTTPS. Berhati-hatilah saat bertransaksi *online*.
8. Versi HTTPS dari URL web lebih aman dibandingkan dengan HTTP.
9. Halaman login palsu mungkin terlihat sama persis. Perhatikan bagian sebelum garis miring pertama (/).

Sesi 7—Apa itu Enkripsi dan *Internet Traffic Encryption*

Tujuan

1. Peserta memahami apa enkripsi dan pentingnya enkripsi dalam lalu lintas internet.
2. Peserta memahami bagaimana mengenkripsi lalu lintas internet.
3. Peserta melakukan praktik enkripsi lalu lintas internet.

Pokok Bahasan

1. Apa itu enkripsi.
2. Apa itu VPN dan bagaimana memilih VPN yang baik.
3. Apa itu TOR dan bagaimana TOR bekerjaPenggunaan *DuckDuckGo* Atau *StartPage* atau Quant sebagai mesin pencari, bukan Google.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan
2. Diskusi
3. Input dan Feedback
4. Penajaman dan Pendalaman
5. Sintesa

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://aesencryption.net/ Online text encryption platform
- https://aescrypt.com/ Small tools to encrypt files with password
- https://torproject.org/ Official site of TOR
- https://www.tunnelbear.com/ Paid VPN
- https://engagemedia.org/tunnelbear – free 1-year TunnelBear VPN subscription
- https://www.psiphon3.com/ Free VPN
- https://www.f-secure.com/en/home/articles/6-things-to-consider-when-choosing-a-vpn
- https://engagemedia.org/2021/indonesia-vpn/
- https://www.eff.org/pages/tor-and-https How HTTPS and Tor Work

---

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang apa itu enkripsi dan kegunaannya (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. *Internet block* dan *Circumventions.*
    b. Apa itu enkripsi dan mengapa kita perlu enkripsi untuk lalu lintas internet.
    c. Apa itu VPN dan bagaimana memilih VPN.
    d. Jaringan TOR.
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit). Peserta bisa berbagi apakah mereka pernah mengalami *website block* atau *circumvention* dan bagaimana mereka mengatasinya.
5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Enkripsi adalah proses mengambil teks biasa, seperti pesan teks atau email, dan mengacaknya ke dalam format yang tidak dapat dibaca — yang disebut “teks sandi.” Ini membantu melindungi kerahasiaan data digital baik yang disimpan di sistem komputer atau dikirim melalui jaringan seperti internet.
2. Jaringan pribadi virtual, lebih dikenal sebagai VPN, melindungi identitas dan aktivitas penjelajahan Anda dari peretas, bisnis, lembaga pemerintah, dan pengintai lainnya. Saat terhubung ke internet, data dan alamat IP Anda disembunyikan oleh sejenis terowongan virtual. Ini mencegah orang lain memata-matai aktivitas online Anda.
3. Saat memilih VPN-: periksa pengalaman keamanan penyedia VPN, Periksa kebijakan privasi VPN Anda, Jumlah lokasi server.
4. Tor adalah perangkat lunak sumber terbuka dan gratis untuk memungkinkan komunikasi anonim. Ini mengarahkan lalu lintas Internet melalui jaringan *overlay* sukarelawan gratis di seluruh dunia, yang terdiri dari lebih dari 7000 relai, untuk menyembunyikan lokasi dan penggunaan pengguna dari siapa pun yang melakukan pengawasan jaringan atau analisis lalu lintas.
5. Bagaimana itu bekerja:
    a. Membuat koneksi untuk Anda melalui 3 node tor acak.
    b. Setiap node tidak mengetahui asal dan tujuan koneksi apa pun.
    c. Semua lalu lintas dari Anda ke simpul terakhir dienkripsi.
6. Hasil: Enkripsi dan privasi.

Sesi— 8 *Malware*, Anti Virus, dan Perangkat Penghapus *Malware*

Tujuan

1. Peserta memahami apa itu virus dan *malware.*
2. Peserta mengetahui pentingnya anti virus dan penggunaan perangkat untuk menghapus atau membersihkan malware (*malware removal tools*).

Pokok Bahasan

1. Bahaya-bahaya di dunia internet dan perangkat kita sehari-hari.
2. Jenis-jenis *malware.*
3. Pentingnya *antivirus.*
4. Perbedaan antara *antivirus* berbayar dan gratis
5. Metode dan Perangkat untuk menghapus *malware.*

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button
3. Presentasi: Google Slide, Jamboard
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet

Durasi

120 Menit

Bahan Rujukan

1. https://www.malwarebytes.com/ Malware removal tools
2. https://www.avira.com/ Free/paid antivirus
3. https://www.avast.com/ Free/paid antivirus
4. https://virustotal.com/ Online malware scanner
5. https://level-up.cc/ curriculum/malware-protection

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang tentang virus dan *malware* (20 menit).
3. Fasilitator mengundang narasumber untuk membahas tentang ancaman umum pada perangkat online dan sehari-hari, jenis-jenis *malware*, tindakan yang harus diambil, serta persamaan inti dari antivirus gratis dan berbayar (45 menit).
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).

5. Narasumber memperkenalkan peserta untuk alat penghapus *malware* dan mereka akan diminta untuk melakukan pemindaian malware selama sesi untuk memberikan pengalaman langsung.
6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Perhatikan bagian terakhir dari nama file (ekstensi).
2. Jangan membuat keputusan hanya dengan melihat ikon file.
3. Jika ekstensi file disembunyikan, hidupkan.
4. Dalam kebanyakan kasus, komputer Anda terinfeksi dengan menghubungkan perangkat eksternal.
5. Tetap perbarui sistem operasi komputer Anda.
6. Nonaktifkan opsi autorun di komputer Anda.
7. Gunakan antivirus dan pindai dengan benar sebelum membuka perangkat eksternal.
8. Jangan gunakan perangkat lunak yang diperoleh melalui sumber (tidak terpercaya). Mungkin membawa *malware* itu sendiri.
9. Beli antivirus jika memungkinkan atau gunakan versi gratis. Lihat daftar yang direkomendasikan di halaman xx.
10. Perbarui basis data antivirus secara berkala.
11. Alat penghapus malware dapat memperbaiki file / sistem yang sudah terinfeksi. Ini sama sekali bukan alternatif antivirus.
12. Sebagian besar perusahaan antivirus menawarkan berbagai alat penghapus *malware* gratis.
13. Agar aman dari *malware* atau tautan phishing, file, tautan, atau halaman *login* apa pun harus dipindai sebelum dibuka.

Sesi 9— Passwords, *Password Manager* dan 2FA

Tujuan

1. Peserta memahami apa itu *password* dan pentingnya membuat *password* yang solid atau kuat.
2. Peserta memahami bagaimana mengelola *password* dengan *password manager* dan mempraktikkannya.
3. Peserta mengenal bagaimana menggunakan 2FA.

Pokok Bahasan

1. Pentingnya kata sandi atau *password* yang kuat dan unik
2. Cara membuat kata sandi yang baik.
3. Keamanan kata sandi.
4. Pengantar pengelola kata sandi (*password manager*)
5. Pengantar otentikasi dua faktor (2FA).

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://keepassxc.org/ Opensource password manager
- https://authy.com/ 2FA app and guides
- https://ssd.eff.org/en/module/creating-strong-passwords

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang tentang penggunaan *password* atau kata sandi (20 menit).
3. Fasilitator mengundang narasumber untuk membahas (45 menit):
    a. membahas tentang pentingnya *password* yang kuat
    b. cara membuat *password* yang baik,
    c. langkah-langkah keamanan apa yang harus diambil selama penggunaan kata sandi.

d. Keepass (pengelola kata sandi *open source*) dan panduan langkah demi langkah akan disajikan.

e. Apa itu 2FA, mengapa itu penting dan bagaimana mengintegrasikannya.

4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).

5. Narasumber mengajak peserta peserta untuk mempraktikkan penggunaan *password manager* (30 menit).

6. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Kata sandi adalah kunci untuk semua informasi Anda dan bagian penting dari keamanan digital.
2. Panjang - Gunakan kata sandi minimal 14 karakter.
3. Kombinasi - Gunakan angka, simbol, huruf besar dan kecil serta spasi jika memungkinkan, dalam kata sandi Anda.
4. Acak – Jangan gunakan struktur yang sama dalam semua kasus dan hindari kata-kata yang ada di kamus.
5. Hubungan- Hindari informasi pribadi.
6. Ingat - Gunakan kata sandi yang dapat Anda ingat.
7. Privasi - Rahasiakan, jangan bagikan dengan siapa pun.
8. Simpan - Jangan menulis di atas kertas atau file teks.
9. Unik - Jangan gunakan kata sandi yang sama di tempat lain.

10. Jika memungkinkan, tambahkan layar keamanan ke perangkat Anda. Yang mencegah orang-orang di lingkungan melihat layar perangkat Anda.
11. Saat memasukkan kata sandi, pastikan tidak ada orang di sekitar Anda yang duduk atau memperhatikan.
12. Buat penutup saat memasukkan PIN di loket ATM.
13. Pastikan tidak ada kamera atau cermin di dekatnya.

Sesi 10— Melakukan dan mengelola Enkripsi Email

Tujuan

1. Peserta memahami apa itu enkripsi dan pentingnya enkripsi email.
2. Peserta memahami bagaimana melakukan enkripsi komunikasi email.
3. Peserta mempraktikkan bagaimana melakukan enkripsi email.

Pokok Bahasan

1. Bagaimana email dikirim, diarahkan, dan diterima, termasuk di mana dan bagaimana konten email dapat dibaca.
2. Cara untuk meminimalkan paparan email ke pengawasan yang tidak diinginkan.
3. Apa itu GPG/PGP dan apa yang dilakukan dan tidak dilakukan, termasuk berbagai masalah yang terkait dengan penggunaannya (misalnya, berpotensi "menarik perhatian" untuk penggunaan Anda, keterbatasan untuk dapat menggunakannya pada perangkat seluler, dll .).
4. Membuat pasangan kunci pribadi/publik, mengunggah kunci publik ke gantungan kunci,

menemukan dan mengunduh kunci publik orang lain, dan mengautentikasi identitas dan kunci orang lain.

5. Mengirim dan menerima email yang ditandatangani atau dienkripsi menggunakan GPG/PGP.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button
3. Presentasi: Google Slide, Jamboard
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet

Durasi

150 Menit

Bahan Rujukan

- https://www.openpgp.org/ Email encryption
- https://mailvelope.com/ Email encryption browser extension
- https://www.thunderbird.net/ Opensource mail client with PGP support

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang bagaimana berkomunikasi via email secara aman (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. Komunikasi via email.
    b. Perpindahan data dan komunikasi via email dari pengirim ke penerima.
    c. Risiko keamanan dalam komunikasi email dan bagaimana mitigasinya.
6. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).
7. Selanjutnya Narasumber menjelaskan dan mengajak peserta berpraktik:
    a. Panduan langkah-langkah ekstensi *browser* keamanan email open source *Mailvelope*
    b. Panduan langkah-langkah klien email open source dengan dukungan *openPGP Thunderbird.*
4. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Lebih dari 90% serangan terhadap organisasi dimulai dari email berbahaya. Email, percakapan obrolan, dan pesan instan selalu melalui seseorang yang tidak kita kenal karena cara kerja Internet. Beberapa orang memiliki akses ini dengan desain untuk mengelolanya, seperti ISP atau penyedia layanan seluler kita.
2. Orang lain mungkin memilikinya karena akses tingkat tinggi, yang dapat melalui cara legal atau "kurang legal", seperti panggilan pengadilan yang diperintahkan secara publik, atau badan intelijen. Orang lain dapat mengaksesnya karena kelemahan pada sistem yang digunakan, seperti peretas.
3. *Pretty Good Privacy* (PGP) adalah sistem enkripsi yang digunakan untuk mengirim email terenkripsi dan mengenkripsi file sensitif. Ini digunakan untuk Mengirim dan menerima email terenkripsi. Memverifikasi identitas orang yang mengirimi Anda pesan ini. Mengenkripsi file yang disimpan di perangkat Anda atau di *cloud*. *Mailvelope* adalah ekstensi *browser* yang memungkinkan komunikasi email aman berdasarkan standar OpenPGP. Ini dapat digunakan dengan email Anda saat ini untuk mengenkripsi dan menandatangani pesan elektronik, termasuk file terlampir, tanpa menggunakan klien email asli yang terpisah. Thunderbird 78 memiliki dukungan bawaan untuk dua standar enkripsi, OpenPGP dan S/MIME. OpenPGP telah diaktifkan secara default sejak versi 78.2
4. Jangan pernah membagikan kunci pribadi Anda kepada orang lain.

Sesi 11— Mengelola Keamanan *File* dan *Folder*

Tujuan

1. Peserta memahami pentingnya keamanan dokumen dan folder dokumen.
2. Peserta memahami bagaimana memastikan.

keamanan dokumen dan folder dokumen.

3. Peserta mengenali perangkat enkripsi *file* dan *folder*.
4. Peserta mempraktikkan bagaimana mengenkripsi dokumen dan *folder* dokumen.

Pokok Bahasan

1. Pentingnya keamanan data.
2. Apa itu metadata dan mengapa itu penting.
3. Bagaimana mengenkripsi file dan folder dengan perangkat enkripsi.
4. Bagaimana menghapus file atau folder secara permanen.
5. Bagaimana memulihkan file yang terhapus.
6. Langkah-langkah *Veracrypt*.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://veracrypt.fr/ File folder encryption tool
- https://cryptomator.org/
- https://www.bleachbit.org/ Permanent file and folder removal tool
- https://ccleaner.com/recuva Deleted file recovery tool
- http://exif.regex.info/ Meta data verification platform
- https://ssd.eff.org/en/module/why-metadata-matters

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang keamanan *file* dan *folder* (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. Praktik pengamanan file dan folder.
    b. keamanan informasi yang disimpan secara lokal.

c. Meta data dan pentingnya meta data.

d. Cara memulihkan file yang dihapus secara tradisional dan cara menghapusnya secara permanen dari komputer.

e. Panduan langkah demi langkah alat enkripsi file/folder opensource Veracrypt.

4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).

5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi

1. Mengurangi risiko pelanggaran dan serangan data sangat penting. Menerapkan kontrol keamanan untuk mencegah akses tidak sah ke informasi sensitif.
2. Prinsip dasar keamanan informasi adalah kerahasiaan, integritas, dan ketersediaan.
3. Saat Anda menghapus file secara tradisional, itu tidak benar-benar menghapusnya. Hal ini dimungkinkan untuk pulih. Menghapus file secara permanen pada hard disk magnetik (HDD) normal memerlukan penggantian sesuatu di lokasi yang sama.
4. Waspadalah terhadap file seperti *Temporary* / *History* / *Cache* / *Log* dll. Ini membawa informasi penting lainnya termasuk riwayat *browser* Anda, *log* obrolan.
5. *Metadata* adalah informasi tentang komunikasi digital yang Anda kirim dan terima. Metadata membawa banyak informasi penting. Yang dapat menimbulkan ancaman bagi keamanan Anda. Pastikan untuk mencoba

menghapus atau meminimalkan metadata. Beberapa contoh *metadata* meliputi:

a. baris subjek email anda.
b. panjang percakapan Anda.
c. kerangka waktu di mana percakapan terjadi.
d. lokasi Anda saat berkomunikasi (serta dengan siapa).

7. Aktifkan enkripsi jika operasi kami mendukungnya. Atau gunakan perangkat lunak bebas dan sumber terbuka seperti *Veracrypte*, yang menyediakan *enkripsi on-the-fly*. Itu dapat membuat disk terenkripsi virtual di dalam file atau mengenkripsi partisi atau seluruh perangkat penyimpanan dengan otentikasi pra-boot.
8. Atau, Anda juga dapat menggunakan *Cryptomator* untuk menyimpan data Anda terenkripsi. Jika Anda menggunakan *Cryptomator*, Anda dapat membuat brankas yang dihosting di *drive virtual*. Data yang disimpan di brankas kemudian dienkripsi. Pengguna dapat menentukan lokasi brankas, misalnya penyedia *cloud*.

Sesi 12— Mengelola *Data Backup*

Tujuan

1. Peserta memahami pentingnya *Backup* data.
2. Peserta memahami bagaimana menciptakan dan menyimpan data secara aman.

Pokok Bahasan

1. Peserta memahami pentingnya *backup data*.
2. Peserta memahami bagaimana menciptakan dan menyimpan data secara aman.
3. Panduan *backup data* dengan duplicati.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://duplicati.com/ Encrypted backup creation tool
- https://www.duplicati.com/articles/Getting-Started/
- https://support.microsoft.com/en-us/windows/backup-and-restore-in-windows-10-352091d2-bb9d-3ea3-ed18-52ef2b88cbef

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang *backup* data dan pentingnya backup data (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. Apa dan mengapa Backup data.
    b. Bagaimana praktik-praktik *backup* data.
    c. Panduan langkah-langkah perangkat *open source encrypted* data backup dengan Duplicati.
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).
5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi

1. Membuat *Backup* sangat penting dalam manajemen data. Backup melindungi dari kesalahan manusia, kegagalan perangkat keras, serangan virus, kegagalan daya, dan bencana alam. Backup dapat membantu menghemat waktu dan uang jika kegagalan ini terjadi.

2. Perangkat Anda mungkin rusak, dicuri, atau hilang. Atau *file* penting mungkin hilang.
3. Simpan backup reguler. Disarankan lebih dari satu.
4. Jangan simpan data asli dan data backup di tempat yang sama.
5. Pastikan backup dienkripsi.
6. Gunakan alat yang bagus dan andal untuk cadangan.
7. Jenis backup: backup penuh, backup tambahan, backup diferensial
8. Pada sistem operasi windows Anda dapat menggunakan fitur built-in backup. Tetapi jangan backup file ke harddisk yang sama dengan tempat Windows diinstal. Misalnya, jangan backup file ke partisi pemulihan. Selalu simpan media yang digunakan untuk backup (hard disk eksternal, DVD, atau CD) di tempat yang aman untuk mencegah orang yang tidak berwenang mengakses file Anda; lokasi tahan api yang terpisah dari komputer Anda dianjurkan. Anda mungkin juga mempertimbangkan untuk mengenkripsi data pada backup Anda.
9. Duplicati adalah klien *backup opensource* gratis yang dengan aman menyimpan backup terenkripsi, inkremental, terkompresi pada layanan penyimpanan cloud dan server file jarak jauh.

Sesi 13— Mengelola *Setting* Keamanan dan Privasi di Media Sosial

Tujuan

1. Peserta memahami pentingnya keamanan dan privasi di media sosial.
2. Peserta mengetahui bagaimana mengelola keamanan dan privasi di media sosial.
3. Peserta mempraktikkan bagaimana menyesuaikan **setting** keamanan dan privasi di media sosial.

Pokok Bahasan

1. Risiko dan kehati-hatian dalam jaringan media sosial.
2. Apa itu rekayasa sosial.
3. Setting keamanan dan privasi di Jaringan dan Situs-situs media sosial.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://youtu.be/F7pYHN9iC9I Video for social media awareness
- https://level-up.cc/curriculum/social-media-safety/
- https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
- https://www.csoonline.com/article/2124681/what-is-social-engineering.html
- https://ssd.eff.org/en/module/protecting-yourself-social-networks

---

Langkah langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang keamanan dan privasi di media sosial (20 menit).
3. Fasilitator meminta peserta untuk nonton video tentang tentang kesadaran media sosial.
4. Fasilitator mengundang narasumber untuk membahas:
    a. risiko di media sosial dan cara mencegahnya.
    b. Detail tentang rekayasa sosial
    c. Pengaturan keamanan dan privasi di platform media sosial populer.

5. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit). Peserta bisa berbagi pengalaman pribadi atau organisasi mereka tentang penggunaan media sosial dan insiden sebelumnya.
6. Narasumber mengajak peserta peserta untuk mempraktikkan setting keamanan dan privasi di media sosial (30 menit).
7. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. Risiko yang perlu Anda waspadai adalah:
    2. *cyberbullying* (intimidasi menggunakan teknologi digital)
    3. pencurian informasi dan pencurian identitas.
    4. pelanggaran privasi.
    5. anak Anda melihat gambar dan pesan yang menyinggung.
    6. kehadiran orang asing yang mungkin ada untuk 'merawat' anggota lain.
2. Serangan rekayasa sosial datang dalam berbagai bentuk dan dapat dilakukan di mana saja di mana interaksi manusia terlibat. Insinyur sosial memanipulasi perasaan manusia, seperti rasa ingin tahu atau takut, untuk melakukan skema dan menarik korban ke dalam perangkap mereka. Oleh karena itu, berhati-hatilah setiap kali Anda merasa khawatir dengan email, tertarik pada penawaran yang ditampilkan di situs web, atau ketika Anda menemukan media digital yang berbohong.

3. Jangan buka email dan lampiran dari sumber yang mencurigakan.
4. Gunakan otentikasi multifaktor.
5. Berhati-hatilah dengan tawaran yang menggiurkan.
6. Perbarui perangkat lunak antivirus/*antimalware* Anda.
7. Jejaring sosial penuh dengan bahaya, yang dapat memiliki konsekuensi besar pada Anda atau bisnis Anda. Anda dapat menghindari banyak jebakan ini hanya dengan menggunakan jaringan ini dengan hati-hati. Selain itu, langkah-langkah berikut sering membantu:
    a. Atur pengaturan privasi sehingga hanya teman yang memiliki akses ke postingan Anda.
    b. Hindari memposting informasi pribadi, rencana liburan, dll.
    c. Jangan menerima permintaan atau pesan dari orang yang tidak Anda kenal.
    d. Hindari mengklik URL yang dipersingkat Laporkan akun yang dicurigai atau menghina/mengancam.
    e. Pisahkan akun pribadi dan kerja.
    f. Menyelenggarakan pelatihan media sosial bagi karyawan, khususnya tentang keamanan data.

Sesi 14— Mengelola Keamanan Telepon Seluler

Tujuan

1. Peserta memahami pentingnya keamanan dan privasi dalam penggunaan telefon seluler.
2. Peserta memahami risiko-risiko peretasan telefon seluler.

Pokok Bahasan

1. Risiko-risiko yang dibawa dan yang berkaitan dengan penggunaan telepon seluler.
2. Bagaimana meminimalisir risiko.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi .
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

150 Menit

Bahan Rujukan

- https://level-up.cc/curriculum/mobile-safety/
- https://ssd.eff.org/en/playlist/privacy-breakdown-mobile-phones
- https://securityinabox.org/en/guide/basic-security/android/
- https://securityinabox.org/en/guide/basic-security/ios/

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang risiko-risiko terkait telefon seluler (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. Risiko-risiko penggunaan telefon seluler
    b. Setting privasi dan keamanan telefon seluler
    c. Praktik memasang setting privasi dan keamanan di telefon seluler
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit).
5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi

Ancaman keamanan seluler adalah sarana serangan siber yang menargetkan perangkat seluler seperti ponsel cerdas dan tablet. Mirip dengan serangan peretasan pada PC atau server perusahaan, ancaman keamanan seluler mengeksploitasi kerentanan dalam perangkat lunak, perangkat keras, dan koneksi jaringan seluler untuk mengaktifkan aktivitas berbahaya dan tidak sah pada perangkat target.

Ada kemungkinan bagi peretas untuk mendapatkan akses ke ponsel Anda dan melakukan apa pun yang mereka inginkan. Misalnya: dengarkan suara Anda melalui mikrofon, rekam panggilan Anda, ambil foto, atau rekam video. Mereka juga dapat menelepon atau mengirim sms dari perangkat Anda.

1. Tetap Perbarui OS Perangkat Anda
2. Selalu gunakan kata sandi di ponsel Anda.
3. Jangan biarkan orang lain menggunakannya.
4. Saat memasang aplikasi, pertimbangkan izin yang Anda izinkan.
5. Aktifkan Enkripsi Disk Penuh.
6. Matikan GPS.
7. Jangan Jailbreak atau Rooting Ponsel Anda
8. Waspadalah terhadap pesan atau media yang tidak dikenal.
9. Jangan gunakan pada WIFI publik.
10. Optimalkan keamanan layar kunci Anda
11. Jangan dibawa ke mana-mana. Jika Anda ingin menghadiri rapat atau protes yang aman dan Anda tidak ingin mengungkapkan lokasi Anda, tinggalkan ponsel Anda di rumah.

Sesi 15— *End To End Encryption* dan Komunikasi Mobile

Tujuan

1. Peserta memahami apa itu enkripsi dan pentingnya *end-to-end encryption.*
2. Peserta menyadari bagaimana berkomunikasi yang aman dengan menggunakan perangkat E2EE.

Pokok Bahasan

1. Memahami metode *end-to-end encryption.*
2. Memilih aplikasi yang terenkripsi untuk komunikasi mobile .

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback.*
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://protonmail.com/blog/what-is-end-to-end-encryption/
- https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work key exchange system. (advance)
- https://signal.org/ Secure communication app
- https://wire.com/ Secure communication app
- https://briarproject.org/ Mobile app for offline secure communication.

Langkah-langkah fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas tentang apa itu enkripsi dan kegunaannya (20 menit).
3. Fasilitator mengundang narasumber untuk membahas:
    a. Apa itu Enkripsi dan *end-to-end encryption*, bagaimana itu bekerja dan mengapa penting untuk keamanan dan privasi.

b. Perangkat untuk E2EE yang bisa digunakan untuk mobile apps.

c. Praktik mendownload aplikasi *Signal/Wire* untuk komunikasi ke depan.

4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas (20 menit). Peserta bisa berbagi apakah mereka pernah menggunakan E2EE.

5. Fasilitator membuat ringkasan dan catatan penting hasil diskusi akhir, menjelaskan tentang tugas dan menutup sesi (5 menit).

Ringkasan Materi Sesi

1. *End-to-end encryption* (E2EE) adalah metode komunikasi aman yang mencegah pihak ketiga mengakses data saat ditransfer dari satu sistem atau perangkat ujung ke perangkat lainnya. Di E2EE, data dienkripsi pada sistem atau perangkat pengirim dan hanya penerima yang dapat mendekripsinya.
2. *End-to-end encryption* saat ini merupakan cara paling aman untuk mentransfer data rahasia, dan itulah sebabnya semakin banyak layanan komunikasi beralih ke sana.
3. Hindari panggilan seluler biasa jika Anda ingin menjaga kerahasiaan informasi.
4. Selalu gunakan aplikasi yang didukung open source dan enkripsi ujung ke ujung untuk komunikasi seluler.
5. Signal adalah aplikasi perpesanan dan obrolan suara gratis yang berfokus pada privasi yang dapat Anda gunakan di smartphone Apple dan Android dan melalui desktop. Yang Anda butuhkan hanyalah nomor telepon untuk bergabung. Komunikasi di Signal dienkripsi ujung-ke-ujung, yang berarti hanya orang-orang dalam pesan yang dapat melihat konten pesan tersebut — bahkan perusahaan itu sendiri.

6. *Wire* mirip dengan Signal tetapi Anda dapat membuat akun di *Wire* tanpa nomor ponsel. Anda dapat memilih antara email dan nomor telepon yang akan digunakan untuk pembuatan akun.
7. *Briar* adalah aplikasi perpesanan yang dirancang untuk para aktivis, jurnalis, dan siapa saja yang membutuhkan cara berkomunikasi yang aman, mudah, dan kuat. Tidak seperti aplikasi perpesanan tradisional, Briar tidak bergantung pada server pusat - pesan disinkronkan langsung antara perangkat pengguna. Jika internet mati, *Briar* dapat menyinkronkan melalui *Bluetooth* atau Wi-Fi, menjaga informasi tetap mengalir dalam krisis. Jika internet aktif, Briar dapat menyinkronkan melalui jaringan Tor, melindungi pengguna dan hubungan mereka dari pengawasan.

Sesi 16 Merespon insiden gangguan keamanan digital

Tujuan

1. Peserta memiliki pemahaman tentang jenis-jenis serangan siber.
2. Peserta mengetahui bagaimana mendeteksi dan menangani insiden, meminimalisir dampak dan kerusakan, mitigasi kerentanan yang telah dieksploitasi, dan mengembalikan kembali layanan IT yang telah berjalan.
3. Peserta mengenali contoh prosedur penanganan insiden.

Pokok Bahasan

1. Jenis-jenis serangan siber.
2. Deteksi dan penanganan insiden, meminimalisir dampak dan kerusakan, mitigasi kerentanan yang telah dieksploitasi, dan mengembalikan kembali layanan IT yang telah berjalan.
3. Contoh prosedur penanganan insiden.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

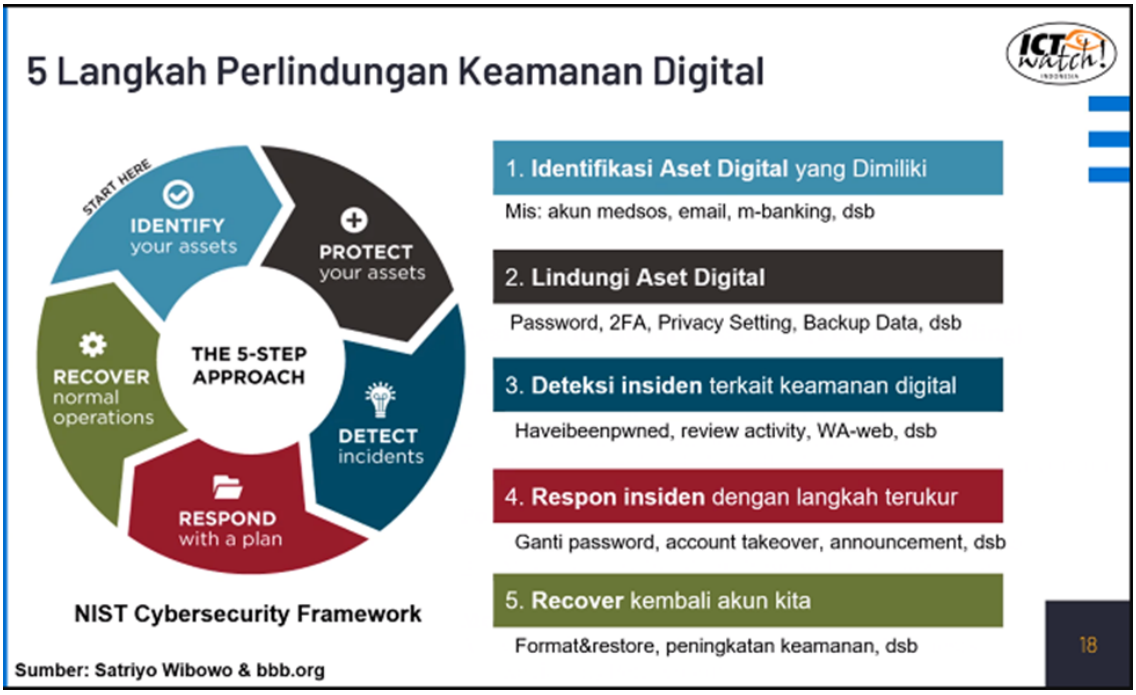
1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Langkah-langkah Fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit).
2. Selanjutnya Fasilitator mengajak peserta membahas mengenai jenis-jenis serangan siber dan mengundang bila ada peserta yang pernah mengalaminya. Fasilitator meminta peserta memperhatikan diagram berikut ini dan mengundang respons apa yang harus dilakukan untuk mencegah serangan siber.



3. Fasilitator mengundang narasumber untuk menjelaskan (45 menit):
    a. Jenis-jenis serangan siber.
    b. Deteksi dan penanganan insiden, meminimalisir dampak dan kerusakan, mitigasi kerentanan yang telah dieksploitasi, dan mengembalikan kembali layanan IT yang telah berjalan.
    c. Contoh prosedur penanganan insiden
4. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan pengalamannya terkait poin-poin yang sudah dibahas narasumber (30 menit)
5. Fasilitator mencatat poin-poin pembelajaran dari sesi yang sudah berlangsung. Fasilitator menunjukkan diagram berikut ini meminta peserta mencermati hal-hal yang penting untuk menangani insiden.

Ringkasan Sesi

Prinsip Penanganan Insiden

Pada dasarnya apa yang harus dilakukan sebuah organisasi jika terjadi insiden terkait dengan keamanan informasi? Secara prinsip, tujuan dari manajemen penanganan insiden adalah:

1. Sedapat mungkin berusaha untuk mengurangi dampak kerusakan yang terjadi akibat insiden keamanan dimaksud;
2. Mencegah menjalarnya insiden ke lokasi lain yang dapat menimbulkan dampak negatif yang jauh lebih besar;
3. Menciptakan lingkungan penanganan insiden yang kondusif, dimana seluruh pihak yang "terlibat" dan berkepentingan dapat bekerjasama melakukan koordinasi yang terorganisir;
4. Agar proses resolusi atau penyelesaian insiden dapat berjalan efektif dan dalam tempo sesingkat mungkin;
5. Mencegah terjadinya kesimpangsiuran tindakan yang dapat mengarah pada dampak negatif yang lebih besar lagi; dan
6. Memperkaya referensi jenis insiden serta prosedur penanganannya sehingga dapat dipergunakan di lain kesempatan pada peristiwa insiden yang sama oleh berbagai kalangan terkait.

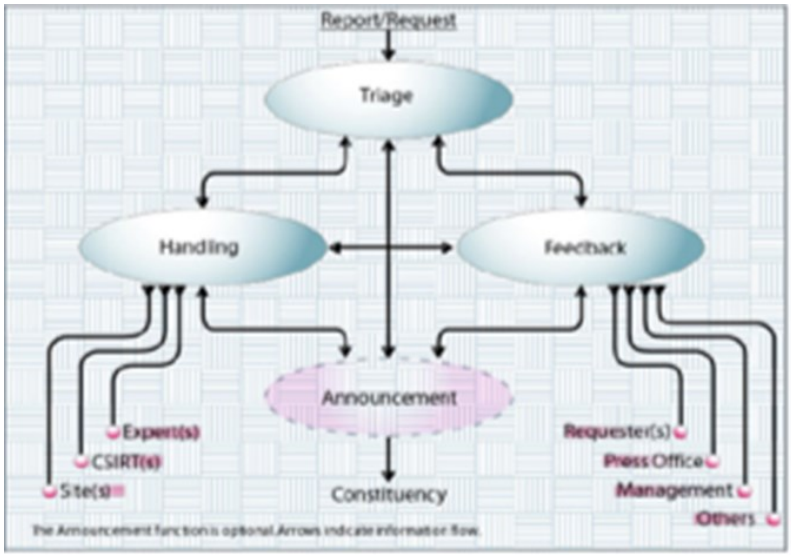
Dalam prakteknya, mendefinisikan dan menjalankan mekanisme "incident handling" merupakan tantangan bagi organisasi yang peduli akan pentingnya mengurangi dampak resiko dari peristiwa yang tidak diinginkan ini.

Kerangka Dasar Fungsi Penanganan Insiden.

CERT/CC melalui publikasinya "Handbook for CSIRTs" menggambarkan kerangka fungsi penanganan insiden yang terdiri dari sejumlah entitas atau komponen seperti yang diperlihatkan dalam gambar berikut.

Triage Function

"*Triage*" merupakan fungsi yang bertugas menjadi "*a single point of contact*" atau sebuah entitas/unit yang menjadi pintu gerbang komunikasi antara organisasi dengan pihak luar atau eksternal. Seluruh informasi yang berasal dari luar menuju dalam maupun dari dalam menuju luar harus melalui unit "pintu gerbang" ini – karena di sinilah pihak yang akan menerima, menyusun, mengorganisasikan, memprioritaskan, dan menyebarluaskan data atau informasi apa pun kepada pihak yang berkepentingan. Fungsi "*triage*" ini sangat penting agar koordinasi dalam situasi kritis karena insiden berjalan secara lancar dan efektif (baca: satu pintu). Dengan kata lain, laporan adanya insiden baik yang diterima secara lisan maupun melalui sensor teknologi, pertama kali akan masuk melalui fungsi "*triage*" ini.



Handling Function

"Handling" merupakan fungsi pendukung yang bertugas untuk mendalami serta mengkaji berbagai insiden, ancaman, atau serangan terhadap keamanan informasi yang terjadi. Fungsi ini memiliki tanggung jawab

utama dalam meneliti mengenai laporan insiden yang diterima, mengumpulkan bukti-bukti terkait dengan insiden yang ada, menganalisa penyebab dan dampak yang ditimbulkan, mencari tahu siapa saja pemangku kepentingan yang perlu dihubungi, melakukan komunikasi dengan pihak-pihak yang terkait dengan penanganan insiden, dan memastikan terjadinya usaha untuk mengatasi insiden.

Announcement Function

"*Announcement*" merupakan fungsi yang bertugas mempersiapkan beragam informasi yang akan disampaikan ke seluruh tipe konstituen atau pemangku kepentingan yang terkait langsung maupun tidak langsung dengan insiden yang terjadi. Tujuan disebarkannya informasi kepada masing-masing pihak adalah agar seluruh pemangku kepentingan segera mengambil langkah-langkah yang penting untuk mengatasi insiden dan mengurangi dampak negatif yang ditimbulkannya. Aktivitas pemberitahuan ini merupakan hal yang sangat penting untuk dilakukan agar seluruh pihak yang berkepentingan dapat saling berpartisipasi dan berkoordinasi secara efektif sesuai dengan porsi tugas dan tanggung jawabnya masing-masing.

Feedback Function

"*Feedback*" merupakan fungsi tambahan yang tidak secara langsung berhubungan dengan insiden yang terjadi. Fungsi ini bertanggung jawab terhadap berbagai aktivitas rutin yang menjembatani organisasi dengan pihak eksternal seperti media, lembaga swadaya masyarakat, institusi publik, dan organisasi lainnya dalam hal diseminasi informasi terkait dengan keamanan informasi. Termasuk di dalamnya jika ada permintaan khusus untuk wawancara atau dengar pendapat atau permohonan rekomendasi terkait dengan berbagai fenomena keamanan informasi yang terjadi di dalam masyarakat.

[Dikutip dari: Richardus Eko Indrajit, *Pengantar Konsep Keamanan Informasi di Dunia Siber*, APTIKOM, 2011, halaman 111-112].

Sesi 17— Rencana Tindak Lanjut, Mempersiapkan Pelatihan Lanjutan, Evaluasi, dan Penutup.

Tujuan

1. Peserta bagaimana mempersiapkan diri untuk memberikan pelatihan lanjutan.
2. Peserta membuat perencanaan untuk pelatihan lanjutan.
3. Peserta melakukan refleksi terhadap hasil-hasil pelatihan.

Pokok Bahasan

1. Bagaimana memfasilitasi pelatihan.
2. Bagaimana membuat presentasi yang baik.
3. Apa yang harus disiapkan dan dipertimbangkan sebelum, saat dan pasca pelatihan Bagaimana merencanakan sesi pelatihan.
4. Bagaimana merespon pertanyaan-pertanyaan dalam pelatihan.

Metode

Activity-Discussion-Inputs-Deepening-Synthesis

1. Kegiatan/Penugasan.
2. Diskusi.
3. Input dan *Feedback*.
4. Penajaman dan Pendalaman.
5. Sintesa.

Perangkat

1. LMS: Google Classroom, Moodle, Canvas.
2. Virtual Meeting: Zoom, Google Meet, Big Blue Button.
3. Presentasi: Google Slide, Jamboard.
4. Penugasan dan Kolaborasi: Jamboard, Miro, Padlet.

Durasi

120 Menit

Bahan Rujukan

- https://level-up.cc/before-an-event/preparing-sessions-using-adids/
- https://level-up.cc/you-the-trainer/golden-rules-of-effective-training/

Langkah-langkah Fasilitasi

1. Fasilitator membuka sesi, mengulas sesi sebelumnya dan menjelaskan kepada peserta tujuan dan proses yang akan dilakukan dalam sesi ini (5 menit)
2. Selanjutnya Fasilitator mengajak peserta membahas bagaimana memfasilitasi pelatihan lanjutan.
3. Fasilitator memberi kesempatan peserta untuk bertanya, berdiskusi dan menyampaikan

pengalamannya terkait poin-poin yang sudah dibahas (20 menit)

4. Fasilitator mengajak peserta untuk melakukan refleksi terhadap hasil-hasil pelatihan. Undang peserta untuk menuliskan apa pendapat mereka tentang:
    a. Perubahan yang mereka peroleh setelah mengikuti pelatihan terkait pengetahuan, keterampilan, dan pengalaman.
    b. Apa saran mereka untuk perbaikan pelatihan ke depan.
5. Narasumber mengundang peserta untuk menyampaikannya secara lisan (30 menit). Fasilitator membagikan tautan untuk *post test* (asesmen pasca pelatihan dan lembar evaluasi) untuk diisi peserta.
6. Fasilitator mengundang Panitia untuk menutup acara (5 menit).

Ringkasan Materi

Manajemen waktu:

1. Berhati-hatilah dengan waktu.
2. Dorong peserta untuk mengikuti waktu yang tepat.
3. Jadwal sesuai dengan isinya.
4. Luangkan waktu untuk bertanya.
5. Jeda sesuai kebutuhan.

Peserta:

1. Tunjukkan rasa hormat kepada peserta.
2. Pastikan mereka memahami topik.
3. Ajukan pertanyaan dan dorong mereka untuk bertanya.
4. Perhatikan jika mereka merasa kesal.
5. Memahami situasi
6. Tidak semuanya bisa selalu berjalan mulus.
7. Bersiaplah untuk mengubah rencana.
8. Jadilah kreatif dan fleksibel tergantung pada situasi.
9. Ubah konten sesuai dengan permintaan atau situasi.
10. Rencanakan topik sebagai arus yang relevan.
11. Pertahankan pengereman es dan waktu yang menyenangkan agar peserta tetap aktif.

Peralatan dan pengaturan yang diperlukan:

1. Lakukan tindakan pencegahan.
2. Pastikan perangkat yang Anda butuhkan berfungsi.
3. Pastikan alat yang diperlukan ada seperti yang dipersyaratkan untuk semua peserta.

Pembuatan Presentasi:

1. Tetap sederhana dan bersih.
2. Gunakan *font* yang mirip. Hindari penggunaan warna ekstra.
3. Jangan menambahkan terlalu banyak teks, cukup tambahkan beberapa gambar.
4. Menjaga kesinambungan topik. Diskusikan masalahnya terlebih dahulu dan kemudian solusinya.
5. Tetap *uptodate*.

6. Berikan contoh terkait dengan peserta.
7. Tidak mencantumkan hal-hal yang menyinggung perasaan peserta.
8. Beri ringkasan di akhir.

D. Kuis untuk Penilaian Keterampilan Keamanan Digital

Jawablah pertanyaan berikut untuk menentukan keterampilan dan kebutuhan Anda. Hasil dari penilaian ini akan membantu kami untuk merancang pelatihan yang lebih baik untuk Anda. Juga, harap diingat bahwa beberapa pertanyaan mungkin memiliki beberapa atau sangat dekat beberapa jawaban yang benar, pilih yang menurut Anda terbaik.

1. Apa prinsip terpenting dalam keamanan digital?

a. Perbarui program *antivirus*

b. Memperbarui sistem operasi

c. Tidak percaya siapapun

d. Jangan buka lampiran email

2. Berapa banyak karakter kata sandi Anda setidaknya?

a. Panjang 8 karakter

b. Panjang 10 karakter

c. Panjang 20 karakter

d. Panjang 25 karakter

3. Mengapa kompleksitas kata sandi itu penting?

a. Itu membuat kata sandi jauh lebih sulit untuk dipecahkan dengan menggunakan perangkat lunak seperti *brute force*?

b. Itu membuat enkripsi kata sandi lebih lama?

c. Itu membuat kata sandi lebih sulit ditebak

d. Itu membuat kata sandi lebih sulit dipahami

4. Bagaimana cara melindungi komputer Anda dari gangguan fisik?

a. Format hard disk Anda

b. Enkripsi seluruh harddisk Anda

c. Enkripsi dokumen Anda

d. Kunci komputer Anda

5. Di mana Anda menyimpan file cadangan?

a. Pada drive terpisah di komputer yang sama.

b. Pada folder tersembunyi di komputer yang sama

c. Saya tidak menyimpan cadangan apa pun

d. Pada perangkat dan lokasi terpisah.

6. Bagaimana cara memeriksa kebenaran https di situs *web*?

a. Saya memeriksa https di *header*

b. Saya melihat kunci kunci di URL

c. Saya memeriksa sertifikat digital

d. Saya memeriksa nama di URL

7. Apa cara aman untuk mengirim dan menerima *email*?

a. Surat aman

b. SMTP

c. FTP

d. PGP

8. Untuk mengirimi Anda email terenkripsi, apa yang saya butuhkan?

a. Kunci pribadi Anda

b. Kunci publik Anda

c. Kedua kunci Anda

d. Tidak ada

9. Apa yang Anda lakukan dengan akun terbuka Anda (Email, Twitter, Facebook, dsb.) sebelum Anda mematikan komputer?

a. Tutup saja penutup laptop

b. Tutup *browser* kemudian matikan komputer.

c. Log out dari akun tutup browser kemudian matikan komputer.

d. Tekan tombol daya hingga komputer mati.

10. Haruskah Anda menyimpan kata sandi di *browser* Anda untuk dapat mengakses akun Anda dengan mudah?

a. Ya

b. Tidak

11. Haruskah Anda menyimpan kata sandi di browser Anda untuk dapat mengakses akun Anda dengan mudah?

a. Iya

b. Tidak

12. Haruskah Anda menggunakan kata sandi yang berbeda untuk setiap akun? Atau satu kata sandi untuk semua akun saya sehingga Anda tidak lupa dan kehilangan akun Anda? *

a. Satu untuk semua.

b. kata sandi yang berbeda untuk setiap akun.

12. Bagaimana Anda bisa tahu sistem operasi mana yang Anda miliki di komputer Anda?

a. Dengan menghubungi perusahaan manufaktur.

b. Itu tertulis di bagian belakang komputer

c. Klik kanan pada komputer saya dan klik pada properti.

d. Saya membawanya ke bengkel dan mereka akan memberitahu saya.

13. Menggunakan lebih dari satu program *Anti-Virus* memberikan perlindungan lebih.

a. Iya

b. Tidak

14. Apa yang dilakukan *root kit*?

a. Sembunyikan deteksi bentuk virus dan *Trojan*

b. Sembunyikan file

c. Hentikan program antivirus

d. Instal perangkat lunak perusak

15. Apakah format yang cukup baik untuk menghapus data saya.

a. Iya

b. Tidak

16. Untuk melindungi dari USB dan virus cd?

a. Saya tidak boleh menggunakan USB apa pun

b. Saya harus menonaktifkan autorun di *window*

c. Saya harus memindai komputer saya

d. Saya seharusnya tidak melakukan apa-apa

17. Jika Anda menerima tautan atau lampiran dalam email dari teman Anda yang tidak Anda harapkan, apa yang Anda lakukan?

a. Anda Memeriksanya dan memutuskan untuk membukanya atau tidak.

b. Anda Buka karena Anda memiliki antivirus yang baik yang melindungi komputer Anda.

c. Hubungi pengirim dan periksa apakah dia mengirimnya lalu periksa dan buka.

d. Buka karena firewall diaktifkan tidak ada yang dapat membahayakan komputer Anda.

18. Sebelum Anda menginstal aplikasi di ponsel Anda, apa yang harus Anda periksa?

a. Izin apa yang dibutuhkan

b. Siapa yang mengembangkannya

c. Jika itu mengungkapkan lokasi saya

d. Jika menghabiskan banyak *bandwidth*

19. Jika Anda memiliki pertemuan penting dan Anda tidak ingin perusahaan seluler mengetahui lokasi Anda?

a. Anda mematikan GPS di ponsel

b. Mereka tidak dapat mengetahui lokasi saya ponsel saya sudah tua dan tidak memiliki GPS

c. Sebelum rapat dimulai, matikan telepon dan keluarkan kartu sim

d. Matikan ponsel, lepaskan baterai sebelum Anda meninggalkan rumah

20. Untuk melindungi ponsel Anda dari siapa pun untuk mengaksesnya:

a. Gunakan kode sandi

b. Gunakan enkripsi perangkat lengkap

c. Gunakan kode sandi untuk kartu sim

d. Gunakan pola untuk membuka telepon