MODUL AJAR KURIKULUM MERDEKA

FASE D KELAS IX

BAB 8 DAMPAK SOSIAL INFORMATIKA

INFORMASI UMUM

I. IDENTITAS MODUL

Nama Penyusun	: Mukhamad Fathoni, M.Pd.I.
Satuan Pendidikan	: MTs Nurul Huda Sukaraja
Kelas / Kelas	: IX (Sembilan)/D
Mata Pelajaran	: Informatika
Prediksi Alokasi Waktu	: 8 JP (40’ x8)
Tahun Pelajaran	: 2024/2025

II. Tujuan Pembelajaran

Tujuan Pembelajaran untuk elemen Dampak Sosial Informatika kelas IX adalah, peserta didik mampu:

a. menjelaskan keamanan data dan informasi;
b. menjelaskan ancaman terhadap keamanan data yang dapat terjadi ketika menggunakan perangkat lunak;
c. menjaga keamanan data diri dari ancaman kejahatan digital.

III. Kata Kunci

Keamanan data dan informasi, peretasan, *information theft*, *fraud*, kerawanan di internet, otentikasi, enkripsi.

IV. Kaitan dengan Elemen Informatika dan Mata Pelajaran lain

Elemen Dampak Sosial Informasi (DSI) tentang keamanan data dan informasi sangat berkaitan dengan elemen Informatika lainnya, terutama Sistem Komputer. Pengembangan sistem komputer, perangkat lunak dan aplikasi yang dituntut cepat terkadang mengorbankan keamanan sehingga menimbulkan celah yang dapat dieksploitasi oleh para peretas. Pengetahuan tentang keamanan data dan informasi ini

juga penting untuk digunakan dalam pengembangan artefak komputasional yang dipelajari pada elemen pengetahuan Praktika Lintas Bidang. Pengembangan artefak komputasional harus dikembangkan dengan mengedepankan keamanan data dan informasi yang dikelolanya juga dengan etika dan praktik baik yang berkaitan dengan pengetahuan DSI.

V. Organisasi Pembelajaran

Tabel 8.1 Organisasi Pembelajaran Bab Dampak Sosial Informatika

Materi	Lama Waktu (JP)	Tujuan Pembelajaran	Aktivitas
Keamanan Data dan Informasi, Kejahatan di Dunia Digital, Kerawanan Dunia Digital	2	a. Peserta didik mampu menjelaskan keamanan data dan informasi. b. Peserta didik mampu menjelaskan ancaman terhadap keamanan data yang dapat terjadi ketika menggunakan perangkat lunak. c. Peserta didik mampu menganalisis dan mengevaluasi ancaman kejahatan di internet. d. Peserta didik mampu melindungi diri atas kejahatan internet.	DSI-K9-01-U: Keamanan Data dan Informasi di Internet DSI-K9-02-U: Studi Kasus Kejahatan di Internet

Perkakas untuk Melindungi Keamanan Data dan Informasi untuk Meningkatkan Keamanan Informasi	2	a. Peserta didik mampu menjelaskan perkakas untuk keamanan data dan informasi. b. Peserta didik mampu untuk merancang otentikasi untuk mengamankan data dan informasi.	DSI-K9-03-U: Situs yang Memanfaatkan Cookie dan Diinformasikan DSI-K9-04-U: Merancang Otentikasi Ruang Rahasia

VI. Pengalaman Belajar Bermakna, Proil Pelajar Pancasia, Berpikir Komputasional, dan Praktik Inti

Tabel 8.2 Pengalaman Belajar Bermakna, Proil Pelajar Pancasila, Berikir Komputasional, dan Praktik Inti Bab Dampak Sosial Informatika

Pengalaman Belajar Bermakna	Proil Pelajar Pancasila	Berpikir Komputasional	Praktik Inti
Peserta didik berdiskusi dan mengeksplorasi keamanan data dan informasi di internet.	Gotong Royong, Bernalar Kritis.	Abstraksi	Kolaborasi, Abstraksi
Peserta didik berdiskusi, menganalisis, menyimpulkan, dan memberikan usulan cara menghindari kejahatan di internet	Gotong Royong, Bernalar Kritis	Abstraksi, Algoritma	Kolaborasi, Abstraksi

Peserta didik mengeksplorasi itur keamanan data dan informasi pada perangkat lunak.	Mandiri, Bernalar Kritis, Kreatif	Abstraksi	Abstraksi
Peserta didik merancang cara mengamankan data dan informasi dengan menggunakan otentikasi.	Gotong Royong, Bernalar Kritis, Kreatif	Abstraksi, Algoritma, Pengenalan Pola	Kolaborasi, Abstraksi Pengembangan Artefak Komputasional

VII. Strategi Pembelajaran

Elemen pengetahuan Dampak Sosial Informatika pada kelas IX tentang keamanan data dan informasi diharapkan dapat menjadikan peserta didik memiliki pengetahuan tentang banyak hal mengenai keamanan data dan informasi di dunia digital dan internet. Selain berpengetahuan, peserta didik juga diharapkan mampu menjaga data dan informasi yang mereka miliki dari kejahatan di dunia maya serta mempunyai sikap hati-hati dalam memakai perangkat keras/perangkat lunak, serta saat sedang *online*.

Strategi pembelajaran pada elemen ini agak berbeda dengan elemen pengetahuan lain. DSI akan dipelajari dengan cara mendiskusikan materi yang selanjutnya peserta didik akan melakukan eksplorasi untuk pencarian informasi di internet atas problem yang diberikan dalam aktivitas. Proses berpikir komputasional juga dapat dikembangkan pada keamanan data dan informasi dengan memberikan aktivitas untuk merancang cara mengamankan data dan informasi pada kasus-kasus tertentu.

KOMPETENSI INTI

Materi DSI akan disampaikan dalam dua pertemuan.

Pertemuan 1: Keamanan Data dan Informasi (2 jp)

I. Tujuan Pembelajaran:

a. Peserta didik mampu menjelaskan keamanan data dan informasi.
b. Peserta didik mampu menjelaskan ancaman terhadap keamanan data yang dapat terjadi ketika menggunakan perangkat lunak.
c. Peserta didik mampu menganalisis dan mengevaluasi ancaman kejahatan di internet.

d. Peserta didik mampu melindungi diri atas kejahatan internet.

II. Apersepsi

Keamanan data dan informasi pada dunia digital merupakan hal yang tidak bisa dihindari saat ini. Penggunaan gawai yang telah banyak digunakan bahkan oleh peserta didik SMP mengharuskan peserta didik menyadari pentingnya data dan informasi yang dapat tercipta dan tersimpan dalam gawai atau peranti lainnya.

Guru dapat menceritakan bahwa data dan informasi ada yang bersifat pribadi, privat, atau sering juga disebut data sensitif. Data sensitif yang tercuri dapat digunakan untuk tindak kejahatan yang dapat dilakukan di dunia maya atau dunia nyata.

Guru perlu menjelaskan kasus yang banyak terjadi di Indonesia, misalnya kasus penipuan yang meminta pin dengan dalih mendapatkan hadiah dari perusahaan ternama. Peserta didik diajak untuk mengetahui kejahatan ini dan tidak menginformasikan data sensitif seperti pin atau password miliknya atau orang tuanya kepada orang lain. Salah satu kejahatan internet bisa dibaca pada link berita berikut: https://regional.kompas.com/read/2021/02/09/12020281/pelaku-skimming-curi-data-atm-dengan-mudah-ini-cara-pencegahannya?page=all

III. Kebutuhan Sarana dan Prasarana

Tidak dibutuhkan sarana dan prasarana khusus pada pertemuan ini.

IV. Kegiatan Inti

Mengacu ke materi yang dijelaskan pada Buku Siswa, guru menjelaskan keamanan data dan informasi di dunia maya atau internet, kejahatan di dunia maya, sejarah *hacking* dari konotasi yang positif sampai konotasi negatif dan berubah menjadi area abu-abu, dan kerawanan di teknologi informasi yang memungkin adanya celah kejahatan. Setelah itu, guru memfasilitasi peserta didik untuk melaksanakan aktivitas Ayo, Kita Diskusikan DSI-K9-01-U pada Buku Siswa dengan membagi peserta didik dalam kelompok. Satu kelompok terdiri atas maksimum 4 peserta didik.

Setelah kelompok terbentuk, guru menjelaskan bagaimana pembagian peran dan tugas dari tiap anggota kelompok. Bagaimana menjelaskan diskusi dengan baik, yang dapat menggunakan *brainstorming placemat* (tatakan curah ide) yang ada pada Buku Siswa.

Setiap peserta didik akan berpendapat pada empat kotak dan hasil yang disetujui diletakkan pada lingkaran tengah. Hasil yang disepakati selanjutnya dibuatkan sebagai kesimpulan dan akan menjadi hasil diskusi yang akan dikumpulkan ke guru.

Topik 1 diskusi tentang pendapat antara dua orang yang berbeda. Pendapat pertama

tentang keamanan data dan informasi yang menjadi

tanggung-jawab pemilik agar tidak dibobol. Pendapat kedua yang menganjurkan pemberian stigma sosial bagi pembobol walaupun sistem tidak dikunci. Diskusi untuk topik pertama mungkin akan menimbulkan banyak perdebatan. Jawaban untuk diskusi ini bukan jawaban benar atau salah, tetapi yang lebih penting ialah argumentasi yang diajukan oleh peserta didik. Analogi keamanan sistem memang seperti keamanan di dunia nyata, di beberapa negara dengan tingkat kriminalitas yang rendah, rumah penduduk jarang yang diberi pagar seperti di Indonesia, tetapi aman-aman saja.

Aktivitas Kelompok

Aktivitas DSI-K9-02: Studi Kasus Kejahatan di Internet

Kasus:

Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) mencatat jumlah kasus peretasan di Indonesia selama tahun 2020 cukup besar. Hal itu disebabkan selama pandemi Covid-19, jumlah pengguna internet pun makin banyak. Dari laporan Pusopskamsinas yang dikutip Sabtu (6/3/2021) menjelaskan, kasus peretasan yang cukup banyak dilakukan melalui *phising*. "Pusopskamsinas pada tahun 2020 mendeteksi terjadinya email phishing sebanyak 2.549 kasus," tulis laporan tersebut.

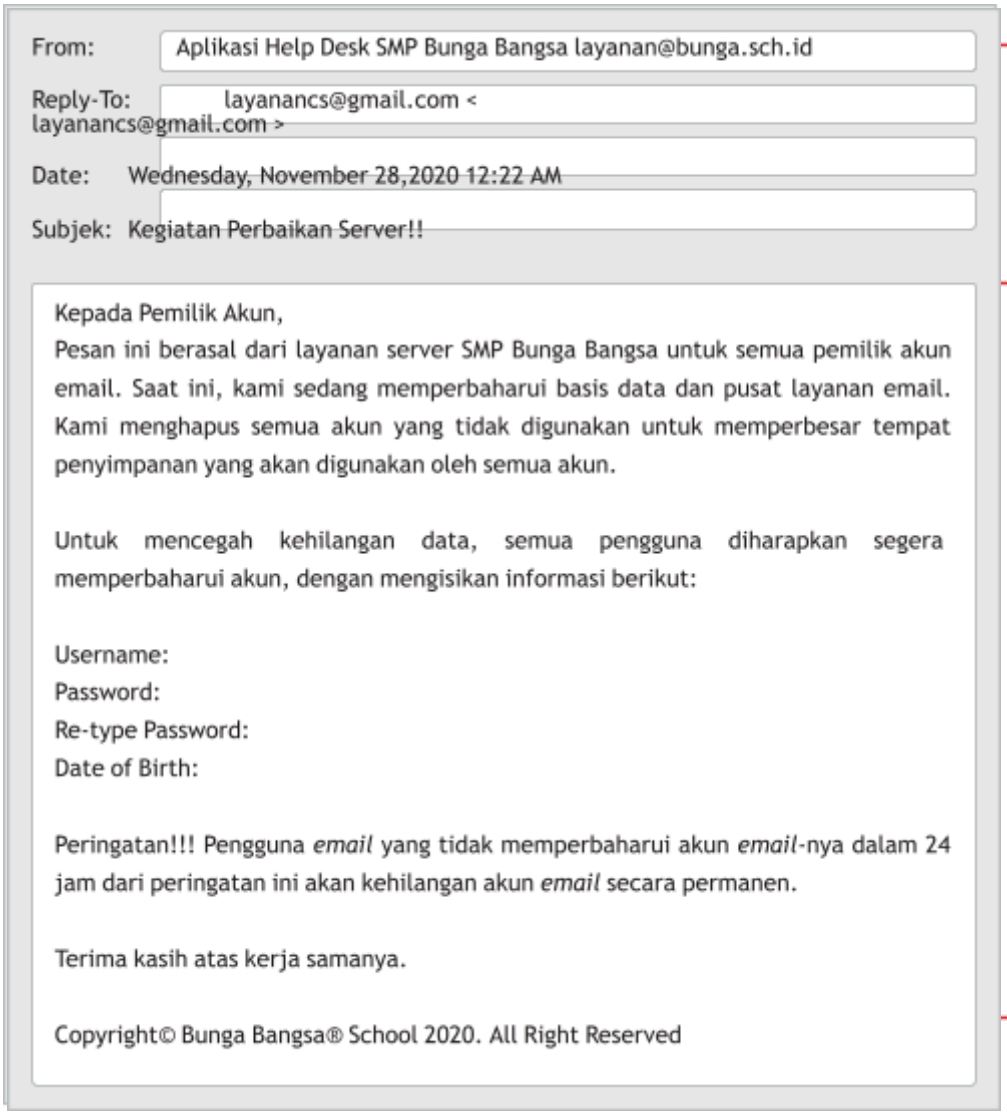
Diskusi topik ke 2 tentang kasus kejahatan internet yang sering terjadi di Indonesia, yaitu *phising email*. Peserta didik diharapkan menjawab beberapa pertanyaan yang merupakan pertanyaan HOTS dengan analisis dan evaluasi serta menyimpulkan rekomendasi yang akan harus dilakukan untuk menjaga keamanan data dan informasi diri.

Jenis-jenis *phising email* adalah sebagai berikut.

1. *Phising email* yang menginginkan balasan email. Balasan email yang diharapkan oleh pembuat *phising email* ialah menyertakan informasi privat yang dapat merugikan pemiliknya jika dicuri.

   (Sumber: https://security.arizona.edu/content/phishing-and-fraudulent-email-illustrated)

Contoh *phising email* yang menginginkan balasan:



From: Aplikasi Help Desk SMP Bunga Bangsa layanan@bunga.sch.id

Reply-To: layanancs@gmail.com < layanancs@gmail.com >

Date: Wednesday, November 28,2020 12:22 AM

Subjek: Kegiatan Perbaikan Server!!

Kepada Pemilik Akun,
Pesan ini berasal dari layanan server SMP Bunga Bangsa untuk semua pemilik akun email. Saat ini, kami sedang memperbaharui basis data dan pusat layanan email. Kami menghapus semua akun yang tidak digunakan untuk memperbesar tempat penyimpanan yang akan digunakan oleh semua akun.

Untuk mencegah kehilangan data, semua pengguna diharapkan segera memperbaharui akun, dengan mengisikan informasi berikut:

Username:
Password:
Re-type Password:
Date of Birth:

Peringatan!!! Pengguna *email* yang tidak memperbaharui akun *email*-nya dalam 24 jam dari peringatan ini akan kehilangan akun *email* secara permanen.

Terima kasih atas kerja samanya.

Copyright© Bunga Bangsa® School 2020. All Right Reserved

Jika dicermati secara lebih rinci, *email* berisi hal-hal:

From: Aplikasi Help I layanan@bunga.sch.id angsa

Reply-To: layanancs@gmail.com < layanancs@gmail.com >

Date: Wednesday, November 28,2020 12:22 AM

Subjek: Kegiatan Perbaikan Server!!

Kepada Pemilik Akun,

Pesan ini berasal dari layanan server SMP Bunga Bangsa untuk semua pemilik akun email. Saat ini, kami sedang memperbaharui basis data dan

pusat layanan email. Kami menghapus semua akun yang tidak digunakan untuk memperbesar tempat penyimpanan yang akan digunakan oleh semua akun.

Untuk mencegah kehilangan data, semua pengguna diharapkan segera memperbaharui akun, dengan mengisikan informasi berikut:

Username:
Password:
Re-type Password:
Date of Birth:

Peringatan!!! Pengguna *email* yang tidak memperbaharui akun *email*-nya dalam 24 jam dari peringatan ini akan kehilangan akun *email* secara permanen.

Terima kasih atas kerja samanya.

Balasan *email* terkirim ke akun gmail, bukan akun sekolah

Akun seolah-olah layanan resmi dari sekolah, tetapi balasan terkirim ke akun gmail

From: Aplikasi Help Desk SMP Bunga Bangsa layanan@bunga.sch.id

Reply-To: layanancs@gmail.com < layanancs@gmail.com >

Date: Wednesday, November 28,2020 12:22 AM

Subjek: Kegiatan Perbaikan Server!!

Kepada Pemilik Akun,
Pesan ini berasal dari layanan server SMP Bunga Bangsa untuk semua pemilik akun email. Saat ini, kami sedang memperbaharui basis data dan pusat layanan email. Kami menghapus semua akun yang tidak digunakan untuk memperbesar tempat penyimpanan yang akan digunakan oleh semua akun.

Untuk mencegah kehilangan data, semua pengguna diharapkan segera memperbaharui akun, dengan mengisikan informasi berikut:

Username:
Password:
Re-type Password:
Date of Birth:

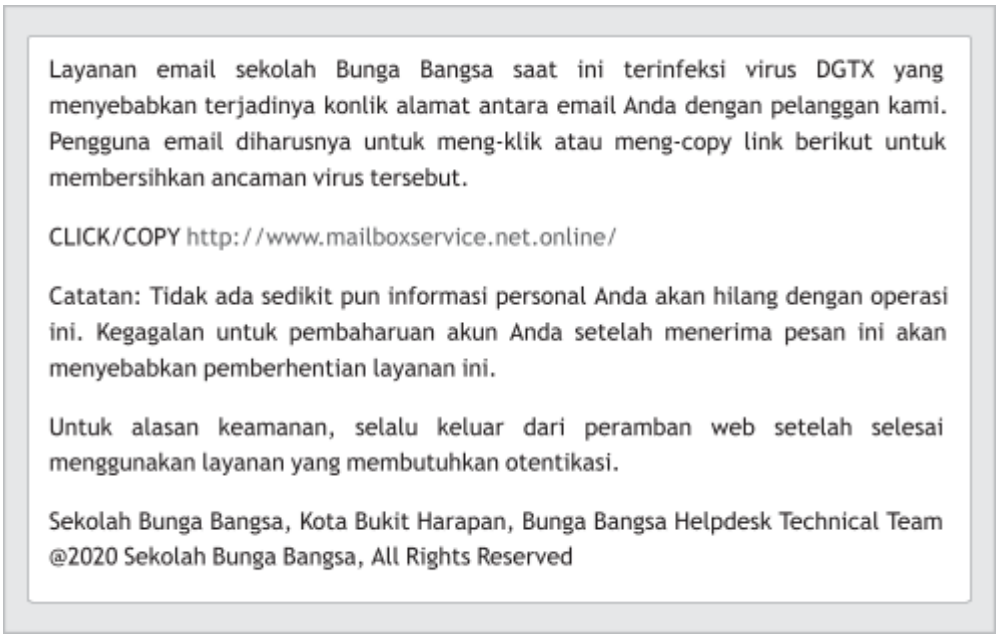
Membuat email seolah-olah *urgent* dan harus segera dibalas untuk memancing kepanikan

Peringatan!!! Pengguna *email* yang tidak memperbaharui akun *email*-nya dalam 24 jam dari peringatan ini akan kehilangan akun *email* secara permanen.

Terima kasih atas kerja samanya.

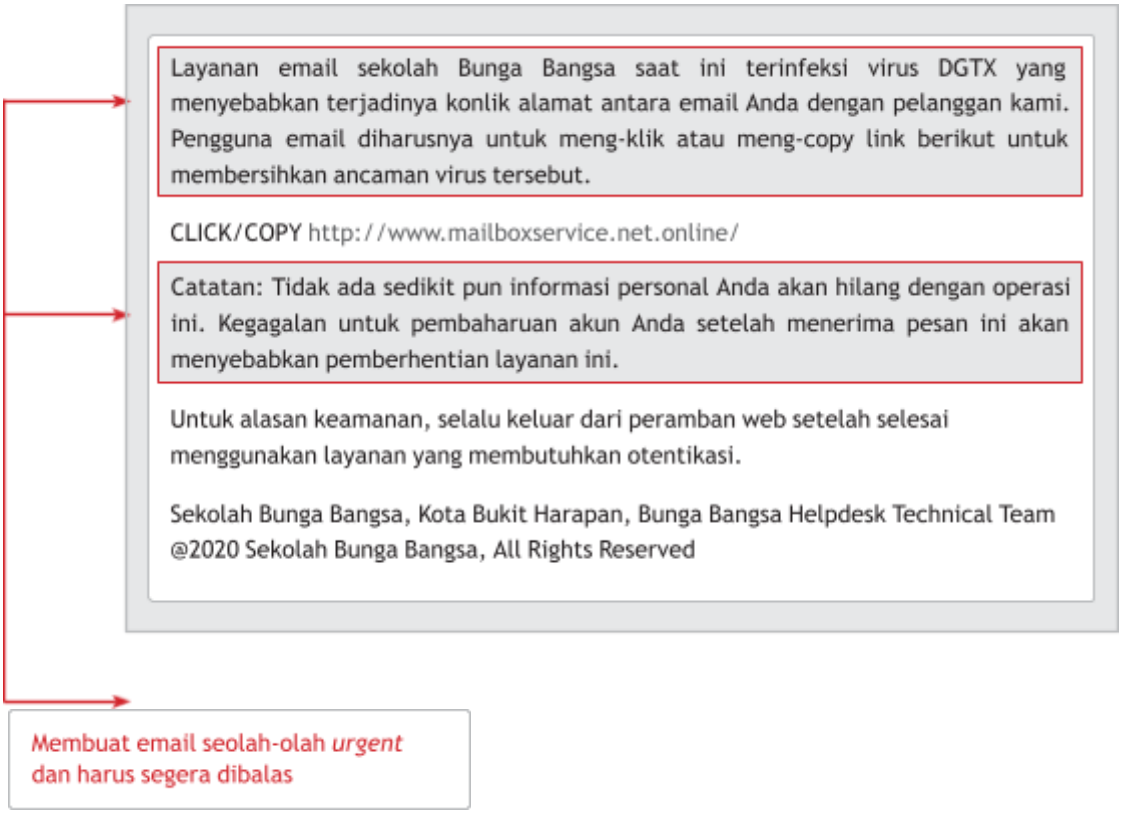
Username:
Password:
Re-type Password:
Date of Birth:

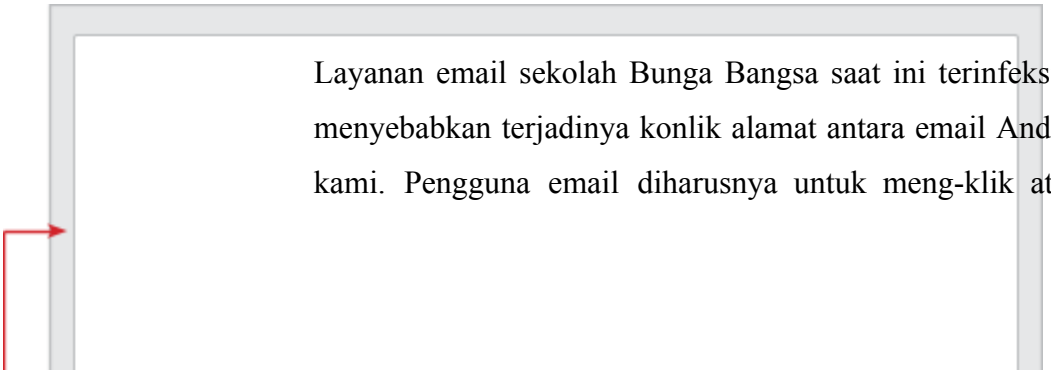
Informasi ini adalah informasi privat, pemilik akun harus sangat berhati-hati jika diminta informasi seperti ini.

2. 

Phising Email dengan *link*. Contoh *phising email* dengan *link:*

Jika dicermati secara rinci, *email* tersebut menunjukkan *phising email* dan bukan *email* yang resmi dari institusi sekolah atau lembaga.

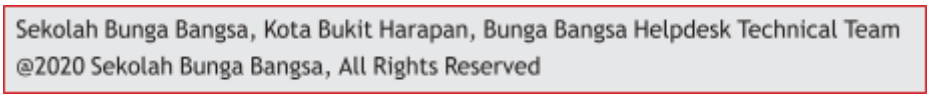




berikut untuk membersihkan ancaman virus tersebut.

Catatan: Tidak ada sedikit pun informasi personal Anda akan hilang dengan operasi ini. Kegagalan untuk pembaharuan akun Anda setelah menerima pesan ini akan menyebabkan pemberhentian layanan ini.

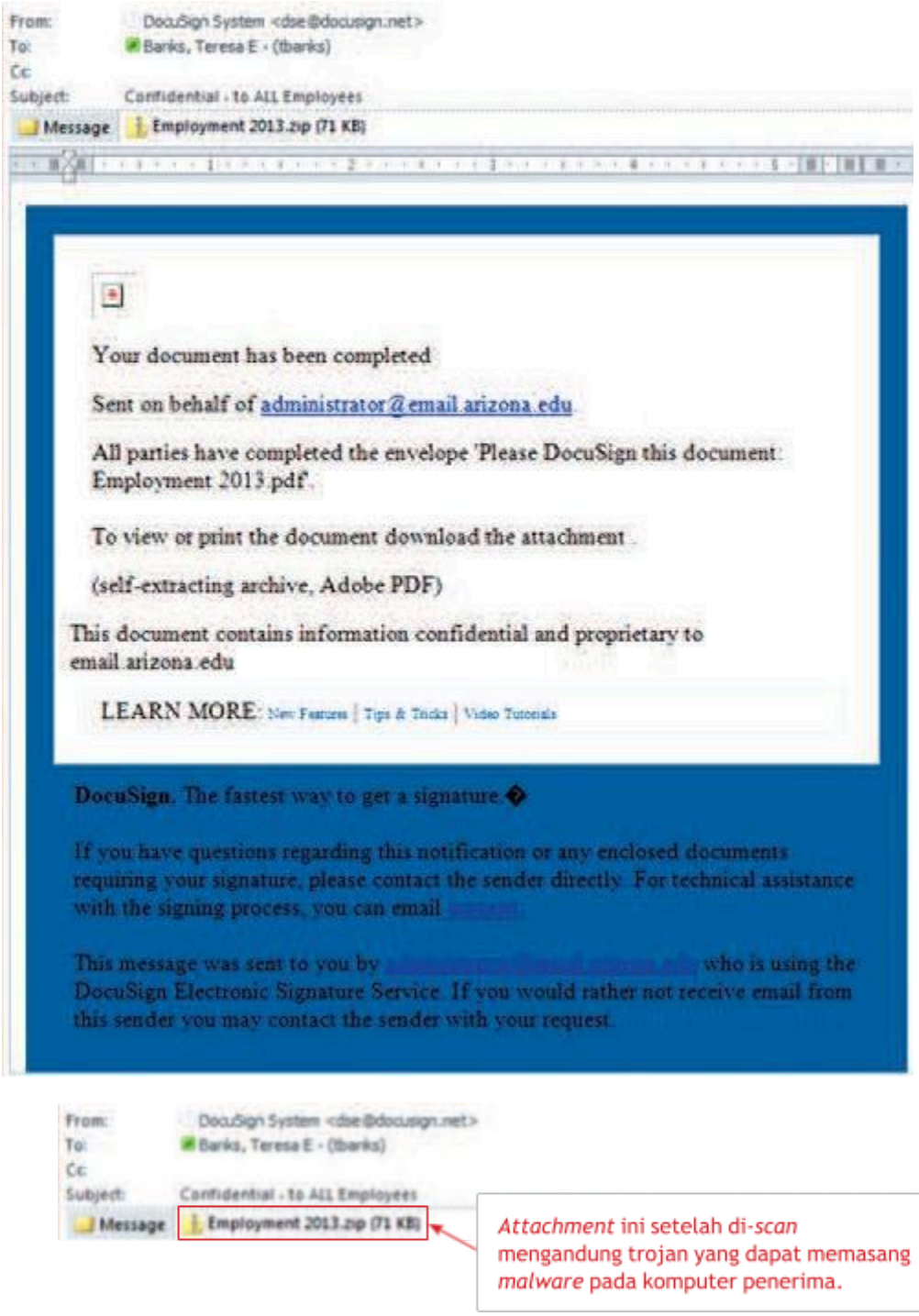
Untuk alasan keamanan, selalu keluar dari peramban web setelah selesai menggunakan layanan yang membutuhkan otentikasi.



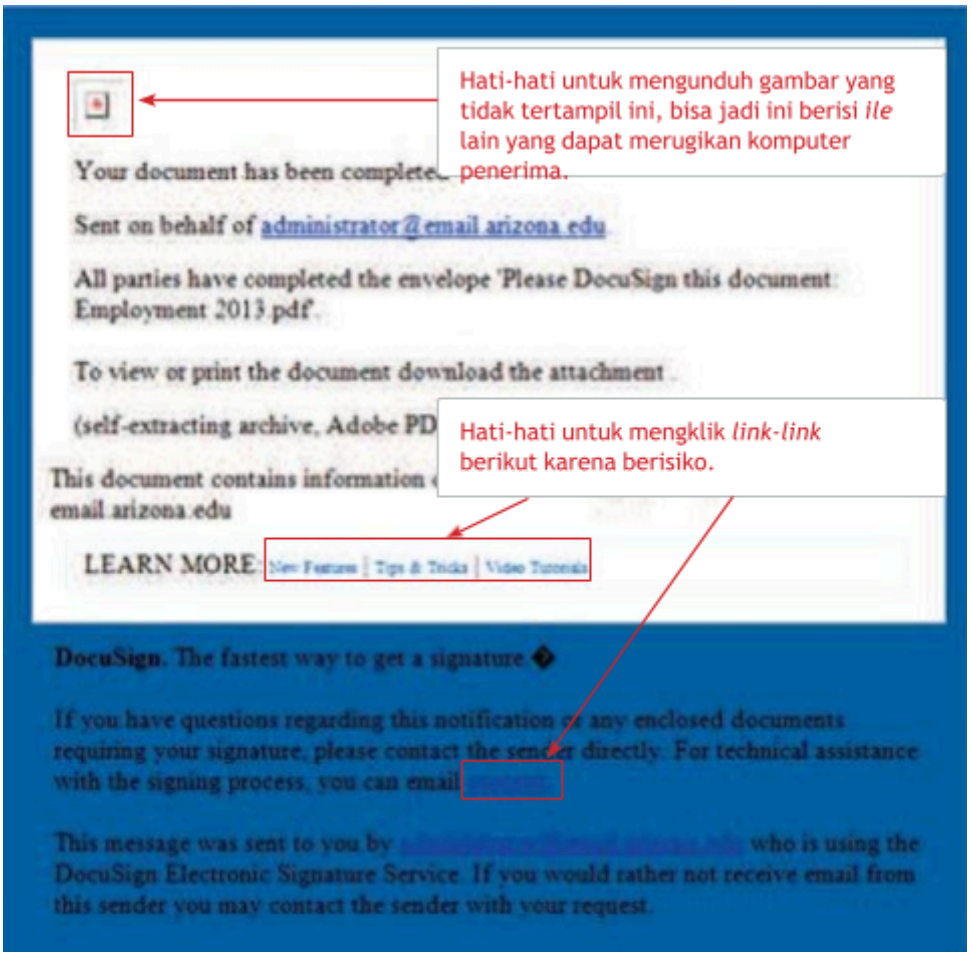
Link ini tidak berasal dari domain universitas (edu) walaupun *email* di klaim berasal dr univ. Arizona

3. *Phising Email* dengan *attachment*

   Contoh *phising email* dengan *attachment* tampak pada Gambar XX. *Email* yang dikirim seolah-olah dari administrator *email* dari arizona. edu, tetapi sebenarnya *email* tersebut adalah *phising email*.

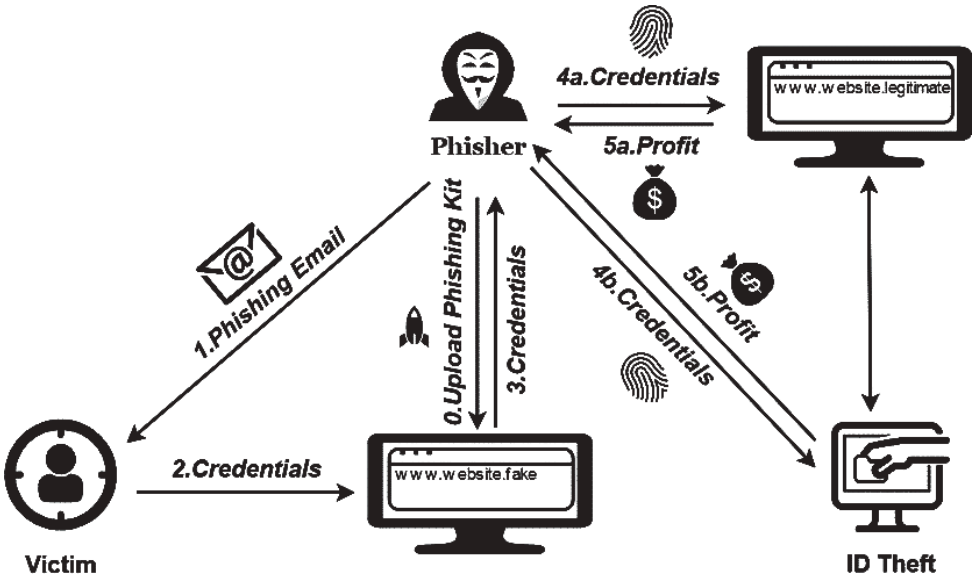


Jika dicermati, secara rinci, *email* tersebut memiliki keanehan yang menunjukkan *phising email*. Keanehan tersebut di antaranya adalah:



Jawaban untuk diskusi pada topik 2.

1. Diagram bagaimana *phising email* bekerja



Gambar 8.1. Diagram *Phising Email*

Phising email bekerja dengan urutan sebagai berikut (dengan link:

0. *Phiser* mempersiapkan situs web palsu dengan kelengkapan perkakas untuk *phising*, seperti kode yang dapat menyimpan data yang dimasukkan oleh korban.
1. *Phiser* mengirimkan banyak *email* ke pengguna secara *bulk* dan acak.
2. Ketika *email* diterima korban, isi *email* memancing korban agar dapat terkecoh dan tergiring untuk mengklik *link/attachment.*
3. Korban dapat terkecoh dengan mengirimkan kredensial mereka. Misalnya: *username* dan *password.*

4.a. Kredensial tersebut dapat digunakan untuk mengakses situs asli.

5.a. *Phiser* mengambil keuntungan seperti mengambil uang dari rekening bank korban.

Atau

4.b. Kredensial dapat digunakan untuk mengakses rekening melalui ATM atau media transaksi *online* lainnya.

5.b. *Phiser* mendapat keuntungan dengan mencuri uang dari rekening korban.

2. Kategori kerawanan dari *phising email* adalah kerawanan pada sifat manusia yang kurang hati-hati dan tergesa-gesa bereaksi, atau biasa disebut *social engineering*.
3. Akibat dari *phising email*:
   a. kerugian material/inansial dari korban,
   b. kerugian immaterial jika yang dicuri adalah data-data pribadi yang kemudian di ekspos ke publik.
4. Agar tidak menjadi korban *phising email,* pengguna *email* harus berhati-hati jika menerima *email* yang tidak dikenal. Dari ketiga jenis *phising email* di atas, pengguna *email* harus berhati-hati jika diminta:
   (a) mengisikan informasi pribadi/privat yang sensitif,
   (b) mengklik *link* dengan domain yang tidak jelas.
   (c) mengunduh *attachment*, gambar, dan *link* menu yang ada pada *email. Attachment* dapat dipindai terlebih dahulu sebelum di eksekusi.

Pertemuan 2: Perkakas untuk Melindungi dan Meningkatkan Keamanan Data dan Informasi (2 jp)

I. Tujuan Pembelajaran:

a. Peserta didik mampu menjelaskan perkakas untuk keamanan data dan informasi.
b. Peserta didik mampu untuk merancang otentikasi untuk mengamankan data dan informasi.

II. Alat dan Bahan

Komputer yang telah terpasang peramban dan memiliki koneksi internet.

III. Apersepsi

Pada pertemuan sebelumnya, telah dipelajari banyaknya ancaman kejahatan di dunia maya. Pada pertemuan ini, guru dapat membahas perkakas yang dapat melindungi data dan informasi kita di internet sehingga lebih aman. Guru dapat menunjukkan alat-alat tambahan yang dapat digunakan untuk menambah keamanan data dan informasi, seperti *key* Bank A, token Bank M, token Bank N, token Bank H, dll. *Key* dan Token dari bank ini sangat penting untuk menjaga transaksi perbankan tetap aman, karena pihak bank akan mengirim pin/*password* khusus ke nasabah bank yang hanya berlaku untuk satu transaksi. Beberapa gambar dari *key* dan token sebagai berikut.

Gambar 8.2. *Token generator* salah satu bank swasta.
Sumber: https://id.wikipedia.org/wiki/Berkas:Digipass_270_HSBC.JPG

Gambar 8.3. *Key generator* salah satu bank swasta.
Sumber: https://www.febriyanlukito.com/tips-membuka-blokir-key-bca/

IV. Kegiatan Inti

Guru memberikan pengantar tentang perkakas untuk keamanan data dan informasi di internet. Guru menjelaskan dan mendemokan beberapa teknik keamanan data dan informasi seperti: enkripsi, antivirus dan penggunaan *trusted application*, otentikasi web, otentikasi *user*, dll.

Aktivitas Individu

Aktivitas DSI-K9-03-U: Situs yang Memanfaatkan *Cookie* dan Diinformasikan

Aktivitas kalian melakukan penjelajahan di internet dengan menggunakan *browser* dicatat pada *ile* yang disebut *cookie*. Segala sesuatu yang kalian lakukan di peramban akan dicatat di dalamnya, yang mungkin dapat dimanfaatkan oleh aplikasi lain atau *malware* untuk mencuri identitas pribadi kalian. Untuk itulah, kalian harus memahami cara melakukan pengaturan agar kalian dapat berinternet dengan aman.

Apa yang Kalian Perlukan?

Komputer yang telah terpasang peramban dan memiliki koneksi internet.

Aktivitas 1: Setelah memberikan penjelasan materi, guru memfasilitasi peserta didik untuk melaksanakan aktivitas Ayo, Kita Eksplorasi DSI-K9- 03-U pada Buku Siswa secara individu. Peserta didik mengerjakannya pada lembar kerja peserta didik.

Contoh situs yang memanfaatkan *cookie* dan diinformasikan adalah sebagai berikut.

Tabel 8.3 Contoh Situs yang Memanfaatkan Cookie

No	Nama situs	Manfaat cookie (*)	Cookie mudah diatur (ya/tidak) (**)
1	Permatabank.com (Bank Permata)	Membuat interaksi di situs lebih mudah dan lancar	tidak
2	Booking.com (Pemesanan tiket Booking.com)	Menganalisis lalu lintas, atau untuk tujuan pengiklanan.	tidak
3	Jenius.com (Bank BTPN)	Mengumpulkan informasi statistik pengunjung untuk meningkatkan layanan	tidak

		dari situs Jenius.	
4	Ef.co.id (Lembaga Pendidikan English First)	Lebih menyesuaikan situs dan produk EF untuk kepentingan dan kebutuhan pengguna	tidak
5	Mini.co.id (Situs web mobil mini cooper)	Membuat interaksi di situs lebih mudah dan lancar	ya

*): manfaat *cookie* dijelaskan pada situs web ybs

**): mudah berarti situs memberikan itur khusus untuk menggunakan *cookie* atau tidak.

Aktivitas Kelompok

Aktivitas DSI-K9-04-U: Merancang Otentikasi Ruang Rahasia

Kalian sebagai pengembang perangkat lunak, mendapat proyek untuk merancang otentikasi sebuah ruang yang menyimpan teknologi rahasia dan *blueprint* alat. Untuk amannya, ruang ini harus dilengkapi dengan otentikasi yang multifaktor, dan ruang ini hanya boleh diakses oleh pemilik dan keluarganya yang berjumlah 4 orang yang telah dewasa.

Tantangan

Rancanglah model otentikasi pada proyek ini. Jelaskan alasan menggunakan model tersebut.

Setelah peserta didik selesai mengerjakan tugasnya, guru dapat mendiskusikan hasil eksplorasi peserta didik dan memberikan umpan balik atas hasil temuan peserta didik.

Aktivitas 2: Aktivitas berikutnya adalah aktivitas perancangan mekanisme pengamanan data dengan kasus otentikasi ruang rahasia. Aktivitas DSI-K9-04-U ini dilakukan secara berkelompok dengan peserta didik maksimum sebanyak 4 anggota. Guru memfasilitasi peserta didik untuk beraktivitas merancang mekanisme pengamanan data dalam ruang rahasia.

Rancangan otentikasi multifaktor mensyaratkan minimal memiliki dua *item* dari kategori yang berbeda. Kategori tersebut seperti berikut.

1. Sesuatu yang diketahui oleh pengguna, misalnya kata sandi, PIN, atau frasa kunci rahasia.
2. Sesuatu tentang diri pengguna, seperti: suara, sidik jari, atau pemindaian

retina.

3. Sesuatu yang dimiliki pengguna, misalnya kartu debit, kartu kredit, ponsel cerdas, pin generator (seperti *key* pada bank B), atau *fob*.

Jawaban:

Untuk perancangan otentikasi ruang rahasia, yang tidak bergerak, otentikasi bisa menggunakan kombinasi dari ketiga cara tersebut.

Beberapa contoh rancangan otentikasi multifaktor yang bisa digunakan

Tabel 8.4 Contoh Rancangan Otentikais Multifaktor

No	Otentikasi	Alasan
1	Menggunakan kata sandi dan biometrik sidik jari.	Otentikasi ini cukup murah karena tidak perlu menambah alat khusus.
2	Menggunakan kata sandi dan kartu masuk ruang (bisa kartu magnetik).	Walaupun menambah alat khusus, otentikasi ini cukup murah karena kartu magnetik telah banyak tersedia di pasar.
3	Menggunakan kartu magnetik dan biometrik retina mata.	Otentikasi ini menambah alat khusus, yaitu kartu magnetik dan menggunakan biometrik retina. Sensor untuk retina lebih mahal dari sensor sidik jari.

Masih banyak rancangan yang dapat dijadikan jawaban, peserta didik-peserta didik diharapkan mengeksplorasi kemungkinan alat lain, yang pernah dialaminya.

Aktivitas selanjutnya ditutup dengan releksi tentang aktivitas dan materi hari ini.

Metode Pembelajaran Alternatif

Pembelajaran pada bab ini menggunakan model aktivitas *unplugged.* Model ini dapat dikatakan cara pembelajaran tradisional yang dapat dilakukan oleh sekolah. Pada saat eksplorasi pada tugas, memang idealnya peserta didik diharapkan untuk mencari informasi menggunakan internet, namun jika proses pembelajaran terkendala oleh sarana dan prasarana maka informasi untuk bahan diskusi dapat dicetak oleh guru atau ditayangkan di kelas, dan kolaborasi bisa

dilaksanakan dengan menggunakan tatakan curah ide yang dicetak di atas kertas.

Pengayaan

Guru memberikan pengayaan kepada peserta didik yang kecepatan belajarnya tinggi dengan memberi saran dan tugas tambahan. Tugas tambahan bisa didapatkan dari situs-situs yang memiliki reputasi bagus, seperti berikut.

1. Keamanan online, https://www.unicef.org/indonesia/id/press-releases/laporan-unicef-tentang-keamanan-online-menyoroti-risiko-dan-peluang-bagi-anak-anak
2. Keamanan internet: https://edu.gcfglobal.org/en/tr_id-internet- safety/
3. Windows Security: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963#:~:text=Windows%20Security%20is%20your%20home,Windows%2010%20in%20S%20mode.)
4. Sara Baase and Timothy M. Henry, A Gift of Fire, Social, Legal, and Ethical Issues for Computing Technology, Fifth Edition, Pearson, 2018.

Remedial

Aktivitas pembelajaran pada kelompok rendah (remedial) bisa dikembangkan dengan melakukan pendampingan kepada peserta didik untuk topik ini. Guru dapat juga memberikan trik-trik khusus untuk memudahkan pemahaman materi. Tutorial sebaya juga dapat dilakukan dengan mengajak berdiskusi peserta didik yang telah memahami materi. Penjelasan dalam bentuk video tutorial yang dapat diakses oleh generasi Z juga sangat membantu, sehingga peserta didik dapat mempelajari materi pembelajaran menggunakan gawai mereka di saat yang tepat.

Asesmen dan Rubrik Penilaian

Asesmen dilakukan dengan penilaian formatif melalui diskusi dan menjawab pertanyaan pada aktivitas DSI-K9-01-U, DSI-K9-02-U, DSI- K9-03U, dan DSI-K7-04-U. Kasus pada aktivitas ini dapat juga digantikan dengan kasus sejenis yang terjadi di dunia maya.

Asesmen juga dilakukan secara sumatif dengan menggunakan contoh-contoh soal pada uji kompetensi. Guru diharapkan membuat soal yang setara dengan contoh soal tersebut.

Rubrik Penilaian

Rubrik untuk Pembuatan Diagram dalam Bentuk Poster/Slides (Penilaian Grup)

Tabel 8.5 Rubrik Penilaian Pemvbuatan Diagram dalam Bentuk Poster/ Slides

Komponen Penilaian	A = Baik Sekali	B = Baik	C = Cukup	D = Kurang
Tampilan Poster	Rapi dan bagus	Rapi	Kurang rapi dan bagus	Kurang rapi dan kurang bagus
Konten diagram	Tepat menggambarkan cara kerja *phising email* sebanyak lebih dari dan sama dengan 80%.	Tepat menggam-barkan cara kerja *phi- sing email* sebanyak 60 – 79 %.	Tepat meng-gambarkan cara kerja *phising email* sebanyak 40 - 59%.	Tepat menggam-barkan cara kerja *phi-sing email* sebanyak kurang dari 40%.
Tepat waktu	Tepat waktu	Terlambat	Terlambat	Tidak me-ngumpul-kan

Penilaian Keaktifan Individu dalam Kelompok

Tabel 8.6 Rubrik Penilaian Keaktifan Individu dalam Kelompok

Komponen Penilaian	A = Baik Sekali	B = Baik	C = Cukup	D = Kurang
Keaktifan sebagai partisipan	Peserta didik sangat aktif ketika bekerja dalam tim.	Peserta didik aktif ketika bekerja dalam tim.	Peserta didik cukup aktif ketika bekerja dalam tim.	Peserta didik kurang aktif ketika bekerja dalam tim.

Penilaian Diskusi

Tabel 8.7 Rubrik Penilaian Diskusi

Komponen Penilaian	A = Baik Sekali	B = Baik	C = Cukup	D = Kurang
Ketepatan jawaban diskusi	≥ 80% betul	60%--79% betul	40%--59% betul	< 40% betul

Jawaban Uji Kompetensi

Mencocokkan

Cookie	1-e	Data kecil pencatat aktivitas di peramban
Phising	2-f	Iris Mata
Biometrik	3-h	Otentikasi
Botnet	4-j	Perangkat lunak tambalan karena bug
Otentik	5-g	Request Flooding
Patch	6-b	Robot and Network
Denial of Service	7-a	Signature
HTTPS	8-d	Situs palsu
AntiVirus	9-c	Trusted Application
Developer Certiicate	10-i	TSL

Soal Uraian

1. Kalau dilihat dari sejarahnya mengapa banyak kerawanan yang ada di internet?

   Jawaban:

   Kerawanan yang akan menjadi celah keamanan di internet terjadi karena:

   a. kompleksitas yang melekat pada sistem komputer, seperti sistem operasi yang dikembangkan pada awalnya tidak terlalu memprioritaskan keamanan data dan informasi;
   b. sejarah perkembangan Internet dan Web itu sendiri, internet awalnya tidak dikembangkan secara aman, karena memprioritaskan

fungsionalitas;

c. perangkat lunak dan sistem komunikasi dibalik penggunaan telepon, web, sistem industri, dan peranti lainnya. Pengembangan perangkat lunak dan sistem komunikasi pada awalnya memang belum memprioritaskan keamanan penggunaan teknologi;
d. sifat manusia yang dapat direkayasa, dengan rekayasa sosial manusia dapat digerakkan untuk melakukan sesuatu yang merugikan dirinya.

2. Mengapa sistem operasi memiliki banyak celah keamanan? Sebutkan paling tidak tiga alasan.

   Jawaban:

   a. Kompleksitas sistem operasi yang tinggi karena mengatur banyak hal, sehingga berpotensi menjadi celah keamanan.
   b. Pengembangan sistem operasi yang melibatkan banyak orang, sehingga pengendalian pengembang terkadang berpotensi menjadi celah keamanan.
   c. Sistem operasi yang berhubungan dengan piranti lain, seperti camera, sensor biometrik, dll yang juga berpotensi menjadi celah keamanan.

3. Mengapa cookie sangat bermanfaat bagi situs web? Sebutkan minimal tiga kegunaannya.

   Jawaban:

   a. Membuat interaksi di situs lebih mudah dan lancar.
   b. Menganalisis lalu lintas, atau untuk tujuan pengiklanan.
   c. Mengumpulkan informasi statistik pengunjung untuk meningkatkan layanan situs.
   d. Lebih menyesuaikan situs dengan kepentingan dan kebutuhan pengguna

4. Ketika kalian menggunakan situs e-banking yang harus melakukan *login* dengan sidik jari dan menggunakan pin yang dikirimkan ke sms. Apakah cara *e-banking* tersebut telah masuk dengan kriteria otentikasi multifaktor? Jelaskan jawaban kalian.

   Jawaban:

   Telah menggunakan kriteria otentikasi multifaktor, karena telah menggunakan dua kategori otentikasi yang berbeda, yaitu (1) sesuatu

tentang diri pengguna, yaitu sidik jari, dan (2) sesuatu yang dimiliki pengguna (sms yang dikirimkan ke ponsel milik pengguna)

Interaksi Guru dan Orang Tua/Wali

Peran orang tua/wali untuk mempelajari Dampak Sosial Informatika terutama yang berkaitan dengan keamanan data dan informasi sangatlah penting bagi peserta didik. Orang tua dapat memberikan informasi dan pemahaman kepada peserta didik ketika bertransaksi elektronis yang mungkin masih belum dilakukan oleh peserta didik.

Refleksi Guru

Setelah mengajarkan materi DSI, guru diharapkan merefleksi proses pembelajaran yang telah dilakukannya. Elemen DSI memiliki materi yang sedikit berbeda dengan yang lain karena DSI kental dengan aspek sosial, guru dapat bereleksi dengan menjawab pertanyaan relektif berikut.

a. Materi mana yang membuat peserta didik bosan?
b. Apa usaha Anda untuk menghilangkan kendala bosan pada peserta didik tersebut?
c. Apakah ada sesuatu yang menarik pada pembelajaran materi ini?
d. Materi mana yang ingin Anda dalami untuk kepentingan pembelajaran berikutnya?

Mengetahui, Kepala madrasah,	Sukaraja, 2 Januari 2025 Guru mata pelajaran,
Nur Khamid, S.Pd. NIP. –	**Mukhamad Fathoni, M.Pd.I.** NIP. 198002162005011003