LEMBAR KERJA PESERTA DIDIK

Mata Pelajaran	:	Kelas	:
Hari/Tanggal	:	Prog. Keahlian	:
Waktu	: **35 Menit**		

Nama Kelompok :

Anggota Kelompok :

:

:

:

:

Bagian 1: Identifikasi Kasus Kejahatan Siber

Instruksi: Bacalah 3 (tiga) studi kasus di bawah ini. Tentukan jenis kejahatan siber dari masing-masing kasus, berikan alasan analisis kalian, dan jelaskan langkah pencegahan yang tepat!

Kasus 1:

Seluruh komputer di sebuah rumah sakit tiba-tiba terkunci dan tidak bisa mengakses data rekam medis pasien. Di layar komputer muncul pesan yang meminta pihak rumah sakit mengirimkan sejumlah uang dalam bentuk Bitcoin (kripto) untuk mendapatkan kunci pembuka data tersebut.

Jenis Kejahatan:

....

.....

Alasan:

.....

.....

LIVEWORKSHEETS

Cara Pencegahan:

.....

.....

.....

.....

Kasus 2:

Budi menerima sebuah email yang mengatasnamakan bank resminya. Email tersebut mengarahkan Budi ke sebuah situs web yang tampilannya sangat mirip dengan situs web asli bank. Situs tersebut meminta Budi untuk memasukkan *username*, *password*, dan informasi kartu kreditnya.

Jenis Kejahatan:

.....

.....

Alasan:

.....

.....

Cara Pencegahan:

.....

.....

Kasus 3:

Pada hari pengumuman kelulusan, situs web sekolah tiba-tiba *down* dan sangat lambat. Setelah diperiksa, ternyata server sekolah kelebihan beban karena dibanjiri jutaan lalu lintas data palsu secara bersamaan dari berbagai perangkat yang tidak dikenal.

Jenis Kejahatan:

.....

.....

Alasan:

.....

LIVEWORKSHEETS

.....

Cara Pencegahan:

.....

.....

LIVEWORKSHEETS

Bagian 2: Drag and Drop Jenis Kejahatan Siber

Instruksi: Jodohkan (*Drag and Drop* / Tarik dan Letakkan) jenis kejahatan siber yang ada di dalam kotak ke 6 contoh kasus yang tepat di bawahnya!

BRUTE FORCE	SPAM	PHISHING	DDoS	PHISHING
BRUTE FORCE	PHISHING	DDoS	RANSOMWARE	SCAM

1.	Sebuah skrip otomatis digunakan oleh peretas untuk menguji ribuan kombinasi *password* secara coba-coba hingga menemukan kata sandi yang benar.	
2.	Penipuan melalui pesan WhatsApp yang memanfaatkan empati dengan mengaku sebagai keluarga yang sedang kecelakaan dan meminta transfer uang segera.	
3.	Menerima email promosi atau pesan tidak penting yang dikirimkan secara terus-menerus dan berulang-ulang setiap 5 menit.	
4.	Menginfeksi sistem komputer perusahaan dan mengenkripsi file berharga, lalu meminta tebusan uang agar file bisa dibuka kembali.	
5.	Seseorang membuat halaman *login* Instagram palsu untuk memancing korban agar memasukkan kata sandi mereka.	
6.	Server sebuah *game online* tiba-tiba lumpuh total karena membludaknya *traffic* palsu dari perangkat botnet secara bersamaan.	
7.	Peretas mencoba membuka pola kunci HP android korban dengan menggeser semua kemungkinan pola satu per satu secara sistematis.	
8.	Mendapatkan SMS penipuan yang menyatakan Anda memenangkan undian Rp 150 Juta dan meminta Anda mengklik tautan blogspot yang mencurigakan.	
9.	Lalu lintas jaringan sebuah layanan publik dibanjiri data sampah, menyebabkan pengguna sah tidak bisa mengakses layanan tersebut.	
10.	Seseorang menghubungi korban melalui telepon, menyamar sebagai petugas resmi untuk memanipulasi korban agar memberikan data sensitif.	

LIVEWORKSHEETS

Bagian 3: Esai — Mengaktifkan Autentikasi Dua Faktor (2FA)

Instruksi: Tuliskan langkah-langkah cara mengaktifkan fitur 2FA (Two-Factor Authenticaton) pada platofrm digital dibawah ini

1. **Email**

2. **Instagram**

3. **TikTok**

LIVEWORKSHEETS