



Lembar Kerja Peserta Didik

LKPD

Keamanan Data (Data Security Tools)



Nama Anggota Kelompok



A. Materi Pokok

Data Security Tools

B. Tujuan Pembelajaran

1. Peserta didik dapat menjelaskan cara menjaga platform digital dengan menggunakan data tools security dengan benar, melalui kegiatan diskusi kelompok.
2. Peserta didik dapat menerapkan data security tools untuk menjaga platform dengan baik, Melalui aktivitas kelompok di LKPD.
3. Peserta didik dapat menganalisis efektivitas penggunaan data security tools dengan membandingkan kelebihan dan kekurangan masing-masing dalam situasi yang berbeda dengan baik, melalui tugas analisis yang terdapat di LKPD.

C. Petunjuk Pengerjaan

1. Baca dan pahami kasus di LKPD dengan teliti, kemudian diskusikan dengan teman sekelompokmu
2. Praktikkan dan pilih salah satu data security tool yang dapat diterapkan untuk mengatasi kasus tersebut. (Langkah praktik tersedia di lampiran 1/2/3)
3. Kerjakan setiap soal-soal yang tersedia
4. Jika ada yang kurang jelas tanyakan pada guru.



Deskripsi Masalah

Baca dan cermati deskripsi masalah berikut ini bersama kelompokmu !

Di Sekolah Menengah Atas Harapan Bangsa, Andi adalah siswa yang aktif di media sosial. Suatu malam, ia menerima email yang tampaknya dari platform sosial media, meminta konfirmasi untuk mengubah kata sandinya. Tanpa memeriksa keaslian email tersebut, Andi mengklik tautan yang disediakan dan mengubah kata sandinya. Beberapa jam kemudian, Andi menyadari bahwa ia tidak bisa masuk ke akunnya. Akun sosial medianya dibajak, dan konten negatif mulai diposting. Kejadian ini bukan hanya merugikan Andi secara pribadi, tetapi juga menciptakan ketidaknyamanan di sekolah, di mana teman-teman dan orang tua mulai khawatir tentang privasi dan keamanan informasi pribadi.



Deskripsi Masalah

Baca dan cermati deskripsi masalah berikut ini bersama kelompokmu !

Lisa, seorang siswa kelas 12, aktif menggunakan berbagai platform digital untuk menunjang kegiatan sehari-harinya. Dia memiliki akun di banyak platform, mulai dari media sosial, layanan email, aplikasi pembelajaran, hingga platform belanja online. Dengan semakin banyaknya akun yang dimiliki, Lisa merasa kewalahan dalam mengingat semua kombinasi username dan kata sandi yang berbeda untuk setiap platform. Awalnya, ia mencoba menyederhanakan dengan menggunakan kata sandi yang sama untuk semua akun agar mudah diingat. Namun, semakin lama, Lisa menyadari bahwa pendekatan ini berisiko, karena jika satu akun terkena masalah keamanan, semua akunnya bisa terdampak.



Deskripsi Masalah

Baca dan cermati deskripsi masalah berikut ini bersama kelompokmu !

Rina, seorang siswi kelas 11, sering menggunakan ponselnya untuk mengakses aplikasi chatting dan media sosial. Suatu ketika, ia meminjamkan ponselnya kepada teman untuk menonton video. Teman Rina tanpa sengaja membuka aplikasi chatting yang berisi pesan pribadi dan foto-foto yang tidak ingin dibagikan. Rina merasa sangat terganggu dan malu ketika beberapa pesan tersebut dibaca dan dikomentari oleh temannya. Kejadian ini membuat Rina berpikir tentang perlunya melindungi aplikasi tertentu di ponselnya agar informasi pribadinya tetap aman.



1). Berdasarkan kasus tersebut pilih dan praktikkan salah satu data security tool yang cocok untuk mencegah kasus tersebut terjadi kembali bersama kelompok kalian (Kumpulkan screenshoot/photo bukti penerapannya di link berikut).

Klik Disini !

2). Jelaskan, mengapa kalian memilih data tools tersebut?



2). Bagaimana cara kerja data security tools yang kalian pilih tersebut?



3). Analisis seberapa efektif penerapan data tools security yang kalian pilih dalam mengatasi masalah tersebut?



Lampiran 1

Petunjuk: Otentikasi Dua Faktor

Pilih salah satu akun sosial media Anda (contoh: Instagram, Facebook, atau Gmail).

Langkah-langkah untuk mengaktifkan otentikasi dua factor di Instagram:

- Buka aplikasi Instagram dan masuk ke akun Anda.
- Ketuk ikon profil Anda di sudut kanan bawah.
- Ketuk "Menu" (tiga garis horizontal) di sudut kanan atas.
- Pilih "Pengaturan."
- Ketuk "Keamanan."
- Pilih "Otentikasi Dua Faktor."
- Pilih metode yang diinginkan (SMS atau aplikasi otentikasi) dan ikuti instruksi.
- Jika memilih aplikasi, unduh aplikasi seperti Google Authenticator atau Authy, dan pindai kode QR yang muncul.



Lampiran 2

Petunjuk: Manajemen Password

Langkah-langkah menerapkan aplikasi manajemen password :

1. Pilih Aplikasi Manajer Kata Sandi:

- Download aplikasi manajer kata sandi yang Anda sukai (misalnya, LastPass, 1Password, Bitwarden) melalui Google Play Store atau App Store.

2. Buat Akun dan Tambahkan Kata Sandi:

- Buat akun di aplikasi manajer kata sandi.
- Tambahkan minimal dua akun platform aplikasi yang akan disimpan.

3. Menguji Fungsi:

- Coba fitur autofill untuk mengisi kata sandi di aplikasi atau situs web yang Anda gunakan.



Lampiran 3

Petunjuk: Pengunci Aplikasi

Langkah-langkah menerapkan aplikasi pengunci aplikasi :

1. Persiapan

- Unduh dan instal aplikasi AppLock dari Google Play Store atau App Store.

2. Pengaturan Awal

- Buka aplikasi AppLock.
- Ikuti instruksi untuk membuat pola/ PIN/ kata sandi untuk mengunci aplikasi. Pastikan memilih pola/PIN/Kata sandi yang mudah diingat namun sulit ditebak oleh orang lain.

3. Mengunci Aplikasi

- Dari daftar aplikasi, pilih dan kunci aplikasi-aplikasi yang ingin diterapkan PIN/Pola/Kata sandi.

4. Pengujian Keamanan

- Setelah mengunci aplikasi, coba buka aplikasi yang sudah dikunci. Pastikan aplikasi meminta pola, PIN, atau kata sandi sebelum dapat diakses.