Praktikum Keamanan Komputer
Teknik Informatika | Universitas Negeri Padang

JOBSHEET 11

Security on Social Network

Nama:	**Najwa Alawiyah Siregar**
NIM:	**22346040**
Dosen Pengampu:	**Melri Deswina, S.Pd., M.Pd.T**

Fakultas	Proram Studi	Kode MK
Teknik	Teknik Informatika	TIK1.61.2303

TUJUAN PRAKTIKUM

1. Mahasiswa mampu Memahami dan mengaplikasikan penggunaan berbagai fitur yang tersedia di situs jaringan sosial.
2. Mahasiswa mampu Mengidentifikasi risiko dan tantangan yang terkait dengan keamanan dan privasi dalam penggunaan situs jaringan sosial.
3. Mahasiswa mampu Mengevaluasi dampak penggunaan situs jaringan sosial terhadap hubungan sosial dan profesional.
4. Mahasiswa mampu Mengembangkan keterampilan dalam mengelola profil pengguna dan berbagi konten secara efektif di platform sosial.
5. Mahasiswa mampu Melakukan Langkah – Langkah untuk mengamankan akun di aplikasi jaringan social.

ALAT/BAHAN

1. Komputer atau laptop dengan akses internet
2. Jaringan Wi-Fi untuk koneksi

PETUNJUK

Awali setiap aktivitas dengan doa, semoga berkah dan mendapat kemudahan. Pahami tujuan, dasar teori, dan latihan-latihan praktikum dengan baik dan benar. Kerjakan tugas-tugas praktikum dengan baik, sabar, dan jujur. Tanyakan kepada asisten/dosen apabila ada hal-hal yang kurang jelas.

TEORI SINGKAT

❖ MATERI

Situs jaringan sosial adalah platform berbasis internet yang memungkinkan pengguna untuk berinteraksi, membangun hubungan, dan berbagi konten. Platform ini memungkinkan pengguna untuk membuat profil digital, berbagi informasi melalui teks, gambar, dan video, serta berkomunikasi dengan teman atau orang baru. Seiring berkembangnya teknologi, situs jaringan sosial kini berperan penting dalam hiburan, pendidikan, dan pemasaran, serta menjadi alat untuk membangun jejaring profesional dan memperluas bisnis.

Berikut ada beberapa risiko keamanan yang mungkin timbul dalam penggunaan situs jejaring sosial, seperti yang dijelaskan dalam berbagai artikel

Cyberbullying
Cyberbullying mencakup berbagai bentuk pelecehan dan intimidasi yang dilakukan melalui platform daring. Pengguna sering menjadi target karena perbedaan pendapat, penampilan fisik, atau latar belakang. Dampaknya bisa berupa stres, gangguan mental, hingga depresi, terutama pada remaja yang sering menggunakan media sosial sebagai bagian dari interaksi sosial mereka. Pelaku sering memanfaatkan anonimitas untuk menghindari tanggung jawab atas tindakan mereka.

Pencurian Data
Media sosial sering meminta pengguna untuk membagikan informasi pribadi seperti nama, lokasi, tanggal lahir, atau bahkan preferensi tertentu. Informasi ini dapat dieksploitasi oleh pihak tidak bertanggung jawab untuk pencurian identitas, penipuan finansial, atau penargetan dengan iklan manipulatif. Lebih parahnya, beberapa aplikasi pihak ketiga yang terhubung ke akun media sosial dapat mengakses data tanpa sepengetahuan pengguna.

Phishing
Serangan phishing melalui media sosial biasanya terjadi dalam bentuk pesan atau tautan yang tampak seperti berasal dari sumber tepercaya. Pengguna yang terjebak dapat memberikan informasi seperti kata sandi atau detail kartu kredit mereka. Taktik ini sering menggunakan manipulasi psikologis, seperti menciptakan rasa urgensi atau ketakutan untuk membuat korban bereaksi cepat tanpa berpikir panjang.

Malware
Perangkat lunak berbahaya dapat disebarkan melalui tautan atau file yang diunggah di media sosial. Malware seperti spyware dapat mencuri data pengguna, sementara ransomware dapat mengunci file penting dan meminta tebusan untuk akses kembali. Serangan ini sering kali disamarkan sebagai konten menarik untuk mengelabui korban.

Doxxing dan Risiko Aktivisme
Aktivis sosial yang menggunakan media sosial untuk menyuarakan pendapat mereka sering menjadi target serangan balik. Informasi pribadi mereka dapat dibocorkan secara publik (doxxing), yang berpotensi membahayakan keamanan mereka secara fisik maupun digital. Serangan ini sering ditujukan untuk mengintimidasi atau membungkam mereka.

Strategi Perlindungan

Untuk mengurangi risiko ini, berikut beberapa langkah yang bisa diambil:

- Gunakan autentikasi dua faktor untuk meningkatkan keamanan akun.
- Batasi informasi pribadi yang dibagikan di media sosial.
- Hindari mengklik tautan dari sumber yang tidak jelas.
- Edukasi diri dan orang sekitar tentang tanda-tanda phishing dan malware.
- Selalu perbarui perangkat lunak keamanan untuk melindungi dari ancaman terbaru.

Kesadaran terhadap risiko ini dan penerapan langkah-langkah pencegahan dapat membantu menciptakan pengalaman yang lebih aman di dunia digital

Tanggapan
Risiko-risiko ini menunjukkan pentingnya meningkatkan literasi digital dan kesadaran keamanan siber. Langkah-langkah perlindungan seperti menggunakan autentikasi dua faktor, membatasi informasi yang dibagikan, dan berhati-hati terhadap tautan yang mencurigakan sangat diperlukan. Pengguna juga sebaiknya mengedukasi diri tentang cara mengenali tanda-tanda serangan phishing dan menjaga privasi secara aktif di media sosial.

Keamanan sosial media bukan hanya tanggung jawab pengguna, tetapi juga penyedia platform untuk memastikan ekosistem yang lebih aman.

1. DAFTAR PUSTAKA

Get Save Online. (n.d.). Situs Jejaring Sosial. Retrieved from Get Save Online: https://www.getsafeonline.id/personal/artikel/situs-jejaring-sosial/

Merdeka.com. (2020). 10 Macam media Sosial yang paling sering digunakan oleh orang indonesia. Retrieved from Merdeka.com: https://www.merdeka.com/jatim/10-macam-media-sosial-yang-paling-sering-digunakan-oleh-orang-indonesia-kln.html?page=11

S.Negara, E. (2022, September 13). Berbicara Tentang Apa Itu Situs Jaringan. Retrieved from Lingkaran.id: https://lingkaran.id/sains-teknologi/berbicara-tentang-apa-itu-situs-jejaring-sosial

Universitas STEKOM. (n.d.). Ensiklopedia Dunia. Retrieved from P2K.Stekom: https://p2k.stekom.ac.id/ensiklopedia/Layanan_jejaring_sosial