1.1.1 Apa Itu Keamanan Siber?

Keamanan siber adalah upaya berkelanjutan untuk melindungi individu, organisasi, dan pemerintah dari serangan digital dengan melindungi sistem jaringan dan data dari pengguna yang tidak sah atau berbahaya.

|  |  |  |
| --- | --- | --- |
| Personal | Organisasi | Pemerintahan |
| Pada tingkat individu, kamu perlu menjaga keamanan identitas, data pribadi, dan perangkat komputer kamu. | Di tingkat organisasi, semua karyawan bertanggung jawab untuk melindungi reputasi, data, dan pelanggan | Dengan semakin banyaknya informasi digital yang dikumpulkan dan dibagikan, perlindungan terhadap informasi digital menjadi semakin penting di tingkat pemerintah, karena keamanan nasional, stabilitas ekonomi, serta keselamatan dan kesejahteraan warga negara menjadi taruhannya. |

Mari kita lihat lebih detail masing-masing dari ketiga tingkat ini

1.1.2 Melindungi Data Pribadi Kamu

Data pribadi adalah informasi apa pun yang dapat digunakan untuk mengidentifikasi kamu, dan informasi tersebut dapat berupa offline maupun online.

|  |  |
| --- | --- |
| Identitas Offline | Identitas Online |
| Identitas offline kamu adalah kepribadian di kehidupan nyata yang kamu tampilkan sehari-hari di rumah, di sekolah, atau di tempat kerja. Hasilnya, keluarga dan teman mengetahui detail kehidupan pribadi kamu, termasuk nama lengkap, usia, dan alamat.  Penting bagi kamu untuk tidak mengabaikan keamanan identitas offline. Pencuri identitas mungkin saja mencuri data kamu saat kamu tidak menyadarinya! | Identitas online kamu bukan sekadar nama. Itu tentang siapa kamu dan bagaimana kamu menampilkan diri kamu kepada orang lain secara online. Ini mencakup nama pengguna atau alias yang kamu gunakan untuk akun kamu, serta identitas sosial yang kamu bangun dan gambarkan di komunitas dan situs online.  kamu harus berhati-hati untuk membatasi jumlah  informasi pribadi yang kamu ungkapkan melalui identitas  online kamu. |

Banyak orang berpikir bahwa jika mereka tidak memiliki media sosial atau akun di internet, maka mereka tidak memiliki identitas online. Bukanlah seperti itu. Jika kamu menggunakan web, kamu memiliki identitas online.

1.1.3 Identitas Online Kamu

Ini hari pertama kamu bekerja, dan inilah saatnya memilih nama pengguna untuk identitas online kamu. Manakah dari opsi berikut yang akan kamu pilih?

Ini adalah kesempatan pertama kamu untuk mendapatkan beberapa poin keamanan yang berharga di perusahaan eLearning @Apollo, jadi luangkan waktu kamu dan pikirkan baik-baik sebelum menentukan pilihan.

Pilih dua jawaban yang benar, lalu Kirim.

j.doe12 jdoe

Benar, bagus sekali! kamu pasti tahu cara menjaga keamanan identitas online kamu.

Saat memilih nama pengguna, penting untuk tidak mengungkapkan informasi pribadi apa pun. Nama pengguna ini tidak boleh membuat orang asing berpikir kamu adalah sasaran empuk untuk kejahatan siber atau perhatian yang tidak diinginkan.

Beberapa tips berguna lainnya untuk membantu kamu membuat nama pengguna kamu:

1. Jangan gunakan nama lengkap atau sebagian alamat atau nomor telepon kamu.
2. Jangan gunakan nama di email kamu.
3. Jangan menggunakan kombinasi nama pengguna dan kata sandi yang sama, terutama pada akun keuangan.
4. Jangan memilih nama pengguna yang sangat aneh lalu menggunakannya kembali berulang kali — ini akan membuat kamu lebih mudah dilacak.
5. Jangan memilih nama pengguna yang memberikan petunjuk pada password kamu seperti rangkaian angka/huruf atau bagian pertama dari dua bagian frase, seperti knock-knock atau starlight, atau departemen tempat kamu bekerja, seperti IT.
6. Pilihlah nama pengguna yang sesuai dengan jenis akun, misalnya akun bisnis, sosial, atau personal.
7. Ingatlah untuk memeriksa poin kamu dengan mengklik ikon perisai di sudut kanan atas layar.

1.1.4 Data Kamu

Data pribadi menjelaskan informasi apa pun tentang kamu, termasuk nama kamu, nomor jaminan sosial, nomor surat izin mengemudi, tempat dan tanggal lahir, nama gadis ibu kamu, dan bahkan gambar atau pesan yang kamu kirimkan ke keluarga dan teman.

Penjahat siber dapat menggunakan informasi sensitif ini untuk mengidentifikasi dan menyamar sebagai kamu, sehingga melanggar privasi kamu dan berpotensi menyebabkan kerusakan serius pada reputasi kamu.

|  |  |  |
| --- | --- | --- |
| Data Medis | Data Pendidikan | Data Pekerjaan dan Keuangan |
| Setiap kali kamu mengunjungi dokter, informasi pribadi mengenai kesehatan fisik dan mental serta kesejahteraan kamu ditambahkan ke catatan kesehatan elektronik / electronic health records (EHRs) kamu. Karena sebagian besar catatan ini disimpan secara online, kamu perlu menyadari informasi medis yang kamu bagikan.  Rekam medis kamu tidak hanya terbatas pada catatan yang disimpan di ruangan dokter. Misalnya, banyak alat pelacak kebugaran mengumpulkan data klinis, seperti detak jantung, tekanan darah, dan kadar gula darah. Data ini dikirim, disimpan, dan ditampilkan melalui cloud. Oleh karena itu, penting untuk mempertimbangkan data tersebut sebagai bagian dari rekam medis kamu. | Catatan pendidikan berisi informasi tentang kualifikasi dan prestasi akademik kamu. Namun, catatan ini juga dapat mencakup informasi kontak kamu, catatan kehadiran, laporan pelanggaran, catatan kesehatan dan imunisasi, serta catatan pendidikan khusus, termasuk program pendidikan individual / individualized education programs (IEP). | Data ketenagakerjaan dapat bermanfaat bagi peretas jika mereka dapat mengumpulkan informasi tentang pekerjaan kamu sebelumnya, atau bahkan ulasan kinerja kamu saat ini.  Data keuangan kamu dapat mencakup informasi tentang pendapatan dan pengeluaran. Catatan pajak kamu mungkin mencakup gaji, laporan kartu kredit, peringkat kredit kamu, dan rincian rekening bank kamu. Semua data ini, jika tidak dijaga dengan baik, dapat membahayakan privasi kamu dan memungkinkan penjahat siber menggunakan informasi kamu demi keuntungan mereka sendiri. |

1.1.5 Di Mana Data Kamu?

Ini membuat kamu berpikir. Baru kemarin, kamu membagikan beberapa foto hari pertama kamu bekerja dengan beberapa teman dekat kamu. Tapi itu seharusnya tidak masalah, bukan? Mari kita lihat…

|  |  |  |  |
| --- | --- | --- | --- |
| kamu mengambil beberapa foto di tempat kerja menggunakan ponsel kamu. Salinan foto-foto ini sekarang tersedia di perangkat seluler kamu. | kamu membagikan foto tersebut dengan lima teman dekat kamu, yang tinggal di berbagai lokasi di seluruh dunia. | Semua teman kamu mengunduh foto tersebut dan sekarang memiliki salinan foto kamu di perangkat mereka. | Salah satu teman kamu sangat bangga sehingga mereka memutuskan untuk memposting dan membagikan foto kamu secara online. Foto-foto tidak lagi hanya ada di perangkat kamu. Foto-foto tersebut sebenarnya ada di server yang berlokasi di berbagai belahan dunia dan orang-orang yang bahkan tidak kamu kenal kini memiliki akses ke foto kamu. |

1.1.6 Lebih Lanjut...

Ini hanyalah salah satu contoh yang mengingatkan kita bahwa setiap kali kita mengumpulkan atau membagikan data pribadi, kita harus mempertimbangkan keamanan kita. Terdapat berbagai undang-undang yang melindungi privasi dan data di negara kamu. Namun apakah kamu tahu ada di mana data kamu?

|  |  |
| --- | --- |
| Setelah kamu bertemu dengan dokter, dokter akan memperbarui rekam medismu. Untuk tujuan penagihan, informasi ini dapat diberikan ke perusahaan asuransi. Dalam kasus seperti tersebut, rekam medis kamu, atau sebagian dairnya, kini dapat diakses di perusahaan asurasnsi. | Kartu loyalitas toko dapat membuatmu menghemat uang saat berbelanja, tetapi juga dapat digunakan untuk membuat profil perilaku pembelian dan menargetkan kamu dengan penawaran khusus. |

1.1.7 Perangkat Cerdas

Pertimbangkan seberapa sering kamu menggunakan perangkat komputasi untuk mengakses data pribadi kamu. Kecuali kamu memilih untuk menerima laporan dalam bentuk kertas, kamu mungkin mengakses salinan digital laporan rekening bank melalui situs web bank kamu. Dan saat membayar tagihan, kemungkinan besar kamu telah mentransfer sejumlah dana yang diperlukan melalui aplikasi mobile banking.

Selain memungkinkan kamu mengakses informasi kamu, perangkat komputer juga dapat menghasilkan informasi tentang kamu.

Teknologi yang dapat dikenakan seperti jam tangan pintar dan pelacak aktivitas mengumpulkan data kamu untuk penelitian klinis, pemantauan kesehatan pasien, serta pelacakan kebugaran dan kesejahteraan. Seiring berkembangnya pasar pelacak kebugaran / fitness tracker secara global, risiko terhadap data pribadi kamu juga meningkat.

Kelihatannya informasi yang tersedia secara online itu gratis. Namun, apakah privasi adalah harga yang harus kita bayar untuk kenyamanan digital ini?

Misalnya, perusahaan media sosial menghasilkan sebagian besar pendapatannya dengan menjual iklan khusus berdasarkan data pelanggan yang telah dikumpulkan menggunakan algoritma atau formula. Tentu saja perusahaan-perusahaan tersebut akan berargumen bahwa mereka tidak 'menjual' data pelanggan, melainkan 'berbagi' data pelanggan dengan mitra pemasarannya. kamu dapat mengambil keputusan sendiri!

Apa yang Diinginkan Peretas?

Jadi, dengan semua informasi tentang kamu tersedia secara online, apa yang diinginkan peretas? Tentu mereka menginginkan uang kamu.

Bisakah kamu memikirkan sebuah contoh kejadian dari pengalaman kamu sendiri atau orang lain yang pernah kamu dengar atau baca tentang pelaku kejahatan siber yang mengakses atau mencoba mengakses informasi keuangan secara online?

Apakah kamu dapat memikirkan setidaknya satu contoh?

Penjahat siber dapat mengambil keuntungan dari hubungan kamu, mengakses akun online kamu dan memanfaatkan sifat baik kamu untuk mencoba menipu kamu agar mengirimkan uang ke teman atau keluarga kamu pada saat dibutuhkan. Misalnya, ada banyak kasus yang dilaporkan mengenai peretas yang menyamar sebagai anggota keluarga dan mengirimkan pesan yang menyatakan bahwa mereka memerlukan transfer uang untuk pulang dari luar negeri setelah kehilangan dompet mereka.

Meskipun kamu mungkin berpikir bahwa frequent flyer air miles kamu tidak berharga bagi penjahat siber, pikirkan lagi. Pada tahun 2015, penjahat siber meretas sekitar 10.000 akun American Airlines dan United, membuatnya memesan tiket secara gratis dan meningkatkan layanan dengan menggunakan kredensial yang telah dicuri. Meskipun frequent flyer miles telah dikembalikan oleh maskapai penerbangan kepada para pelanggan, contoh ini menunjukkan nilai dari kredensial akun kamu.

Penjahat siber tentu saja sangat kreatif dalam mencari cara untuk mengakses uang kamu Namun bukan hanya itu yang mereka incar — mereka juga dapat mencuri identitas kamu dan menghancurkan hidup kamu.

Mari cari tahu lebih lanjut.

1.1.9 Pencurian Identitas

Tidak puas dengan mencuri uang kamu demi keuntungan finansial jangka pendek, penjahat dunia maya berinvestasi untuk keuntungan jangka panjang berupa pencurian identitas.

|  |  |
| --- | --- |
| Pencurian Medis | Perbankan |
| Meningkatnya biaya pengobatan telah menyebabkan peningkatan pencurian identitas medis, dimana penjahat siber mencuri asuransi kesehatan untuk memanfaatkannya bagi diri mereka sendiri. Jika hal ini terjadi, prosedur medis apa pun yang dilakukan atas nama kamu akan disimpan dalam rekam medis kamu. | Mencuri data pribadi dapat membantu penjahat siber mengakses rekening bank, kartu kredit, profil sosial, dan akun digital lainnya. Dengan informasi ini, seorang pencuri identitas dapat mengajukan pengembalian pajak palsu dan mengambil uangnya. Mereka bahkan bisa mengajukan pinjaman dengan menggunakan identitas kamu dan merusak riwayat kredit kamu (serta kehidupan kamu). |

1.1.10 Siapa Lagi yang Menginginkan Data Saya?

Bukan hanya penjahat yang mencari data pribadi kamu.

Klik judul di bawah untuk mengetahui entitas lain yang tertarik dengan identitas online kamu dan alasannya.

|  |  |  |  |
| --- | --- | --- | --- |
| Penyedia Layanan Internet (ISP) | Pengiklan | Mesin pencari dan platform media sosial | Situs web yang kamu kunjungi |
| ISP kamu melacak aktivitas online kamu dan, di beberapa negara, mereka dapat menjual data ini kepada pengiklan untuk mendapatkan keuntungan.  Dalam keadaan tertentu, mereka mungkin diwajibkan secara hukum untuk membagikan informasi online kamu kepada lembaga atau otoritas pengawasan milik pemerintah. | Iklan khusus adalah bagian dari pengalaman menggunakan Internet. Pengiklan memantau dan melacak aktivitas online kamu seperti kebiasaan berbelanja dan preferensi pribadi serta mengirimkan iklan khusus sesuai keinginan kamu. | Platform ini mengumpulkan informasi tentang jenis kelamin, geolokasi, nomor telepon, serta ideologi politik dan agama kamu berdasarkan riwayat pencarian dan identitas online kamu. Informasi ini kemudian dijual kepada pengiklan untuk mendapatkan keuntungan. | Situs web menggunakan cookie untuk melacak aktivitas kamu guna memberikan pengalaman yang lebih personal. Namun hal ini meninggalkan jejak data yang terkait dengan identitas online kamu yang sering kali berakhir di tangan pengiklan! |

Selanjutnya...

Jelas bahwa para pelaku kejahatan siber semakin canggih dalam upaya mereka untuk mencari data pribadi yang berharga. Namun, mereka juga merupakan ancaman besar bagi data organisasi.