MyGovUC MALAYSIA MADANI

KEBOCORAN DATA

Kebocoran Data adalah keadaan apabila data atau maklumat yang diklasifikasikan sebagai sensitif, dilindungi atau sulit diketahui oleh individu atau organisasi yang tidak berkenaan.

JENIS DATA

BUTIRAN LOG MASUK
Seperti *Username* atau alamat e-mel dan kata laluan.

HARTA INTELEK
Seperti kod sumber perisian, reka bentuk produk, formula rahsia dan data penyelidikan dan pembangunan.

MAKLUMAT ORGANISASI
Seperti rekod sumber manusia, alamat, rekod e-mel pegawai dan dokumen rahsia organisasi.

PANGKALAN DATA PELANGGAN
Seperti nama atau maklumat akaun serta maklumat dan rekod pembayaran.

MAKLUMAT PENGENALAN PERIBADI
Seperti nama penuh, alamat, nombor kad pengenalan, tarikh lahir dan lain-lain yang boleh digunakan untuk melaksanakan pencurian identiti.

MAKLUMAT KEWANGAN
Seperti nombor kad kredit atau debit, penyata bank, invois dan lain-lain.

SALURAN KEBOCORAN DATA

MEDIA SIMPANAN

FIZIKAL	ELEKTRONIK
DOKUMEN RAHSIA PERANTI MUDAH ALIH *HARD DRIVE* *PENDRIVE*	E-MEL *CLOUD STORAGE* PERANTI MUDAH ALIH

CARA - CARA KEBOCORAN DATA BERLAKU

MANUSIA	TEKNOLOGI
① Kehilangan media simpanan.	① E-mel atau maklumat sensitif tersalah hantar kepada orang yang tidak berkenaan.
② Orang tidak berkenaan mendapat akses kepada media simpanan.	② Tetapan perkongsian *Cloud Storage* tidak ditetapkan dengan betul.
③ Media simpanan dicuri oleh orang yang tidak berkenaan.	③ Peranti mudah alih diserang oleh perisian hasad *(Malware)*.

PERBEZAAN KEBOCORAN DATA DAN PENCEROBOHAN DATA

KEBOCORAN DATA

Punca :
Pihak dalaman seperti pegawai berkongsi maklumat sensitif sama ada secara tidak sengaja atau dengan niat jahat.

PENCEROBOHAN DATA

Punca :
Pihak luar seperti penceroboh mengambil kesempatan atas kelemahan perisian keselamatan atau kelalaian pegawai dengan niat untuk mencuri dan salah guna maklumat sensitif.

Hasil :
Maklumat sensitif diketahui oleh orang tidak berkenaan.

NOTA

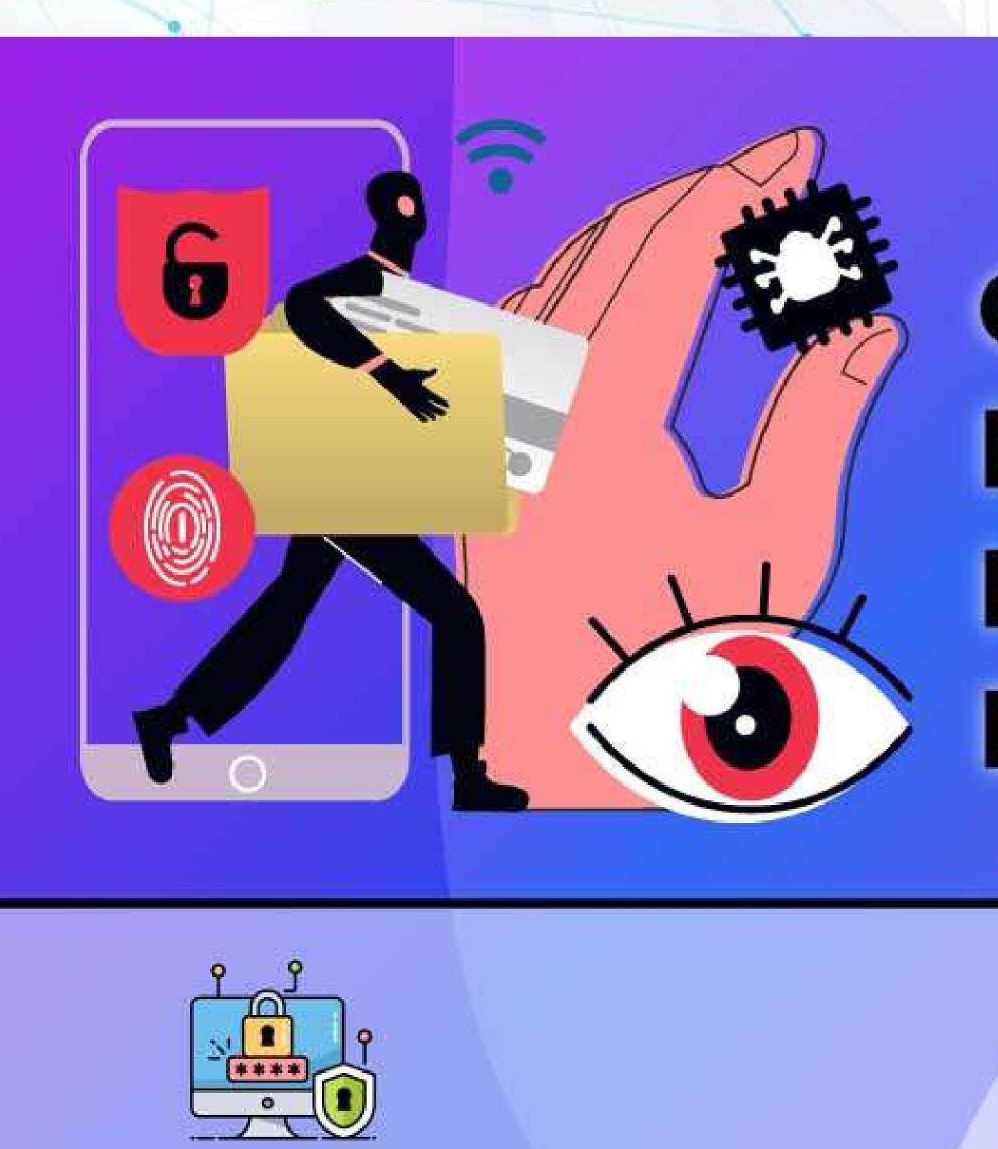
1. Sentiasa menjaga **keselamatan *Username*** atau alamat e-mel serta kata laluan anda kerana ia adalah kunci untuk mengakses sebarang maklumat.

2. Elakkan menulis maklumat tersebut di atas kertas dan memasukkan maklumat tersebut pada laman web yang mencurigakan atau tidak selamat.

JENIS ANCAMAN ORANG DALAM

	Kecuaian	Berniat Jahat	Impak
Punca	Tidak sengaja kerana kurang kesedaran terhadap klasifikasi maklumat dan cara pengendaliannya.	Kepentingan diri, balas dendam, pengintipan atau keuntungan kewangan.	Akaun pegawai yang terjejas akibat diceroboh masuk oleh penceroboh melalui *phishing, social engineering* atau perisian hasad.
Contoh	Pegawai tersalah kongsi maklumat sensitif kepada orang yang tidak berkenaan atau tertekan pautan yang mengandungi perisian hasad.	Pegawai atau bekas pegawai dengan sengaja berkongsi maklumat sensitif kepada pihak luar.	Penceroboh mendapat akses kepada akaun pegawai melalui serangan *phishing.* Kemudian mengakses dan menyalin maklumat sensitif kepada simpanan luar.

CARA MENCEGAH KEBOCORAN DATA



① **Lindungi Kata Laluan Anda**
a. Contoh - Kebocoran data berlaku apabila pegawai menggunakan butiran log yang sama seperti akaun rasmi di laman web yang terjejas. Ini menyebabkan boleh berlakunya akses tanpa kebenaran kepada akaun mereka.
b. Langkah Pencegahan - Tetapkan kata laluan unik bagi setiap akaun atau peranti mudah alih yang berbeza.

② **Berwaspada akan e-mel *phishing***
a. Contoh - E-mel *phishing* yang menyamar sebagai mesej daripada rakan sekerja atau pasukan IT yang ingin mendapatkan maklumat sensitif atau butiran log masuk akaun anda. Jika tidak disemak, akan berlakunya kebocoran data.
b. Langkah Pencegahan - Semak alamat e-mel penghantar dan pautan yang diberi terlebih dahulu.

③ **Lindungi Peranti Anda**
a. Contoh - Pegawai kehilangan peranti yang mempunyai maklumat sulit tanpa meletakkan kata laluan pada peranti. Sesiapa sahaja yang menjumpai peranti tersebut dapat membocorkan data yang disimpan.
b. Langkah Pencegahan - Tetapkan kata laluan pada peranti dan memastikan perisian keselamatan peranti sentiasa dikemas kini.

④ **Kongsi Maklumat Secara Selamat**
a. Contoh - Pegawai berkongsi data atau maklumat sensitif melalui platform yang tidak selamat seperti *Facebook* dan *Whatsapp* mengakibatkan keselamatan data atau maklumat tersebut terjejas.
b. Langkah Pencegahan - Sahkan penerima adalah betul sebelum berkongsi maklumat sensitif, dan gunakan platform yang selamat untuk pengkongsian tersebut.

⑤ **Aktifkan 2 - *Step Verification* (2SV)**
a. Contoh - Kata laluan pegawai terjejas akibat tersalah tekan pautan tetapi akaun pegawai tidak boleh diakses penceroboh kerana tidak mempunyai kod pengesahan yang kedua.
b. Langkah Pencegahan - Manfaatkan langkah keselamatan tambahan untuk melindungi akaun anda daripada dicerobohi dengan mudah.

⑥ **Fahami Klasifikasi Maklumat**
a. Contoh - Pegawai secara tidak sengaja berkongsi maklumat rahsia rasmi yang mengakibatkan kebocoran data kerana kurang kesedaran akan klasifikasi maklumat.
b. Langkah Pencegahan - Mengambil tahu akan klasifikasi maklumat serta protokol mengendalikannya.

Bahagian Pembangunan Perkhidmatan Gunasama Infrastruktur dan Keselamatan Digital
Jabatan Digital Negara
Kementerian Digital
☎ 03 - 8684 8484
mejabantuan@mygovuc.gov.my
Freshservice