PANDUAN KEAMANAN SIBER UNTUK BISNIS KECIL ANDA

DIREKTORAT OPERASI KEAMANAN SIBER
BSSN - 2021

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

TLP: WHITE

Transformasi digital terus berkembang pesat terutama sejak hadirnya pandemi Covid-19. Seluruh aspek kehidupan bermasyarakat kini tidak lepas dari pemanfaatan Teknologi Informasi dan Komunikasi (TIK) khususnya internet. Salah satu sektor yang paling cepat beradaptasi dan berinovasi adalah sektor bisnis dan ekonomi.

Pemanfaatan teknologi justru membuat masyarakat semakin kreatif dalam menciptakan bisnis-bisnis kecil yang terus tumbuh. Kemudahan penggunaan teknologi internet menjadi *booster* untuk membesarkan usahanya.

Namun, teknologi internet juga memiliki sisi ancaman keamanan yang tidak boleh diabaikan. Pelaku-pelaku bisnis kecil kerap menjadi target ancaman keamanan siber, karena biasanya tidak memiliki sumber daya (*resources*) yang mumpuni dalam hal keamanan.

Untuk itulah, para pelaku bisnis kecil perlu mengetahui, meahami, dan melaksanakan standar-standar keamanan dasar yang penting untuk melindungi keberlangsungan bisnisnya.

CADANGKAN DATA SECARA RUTIN

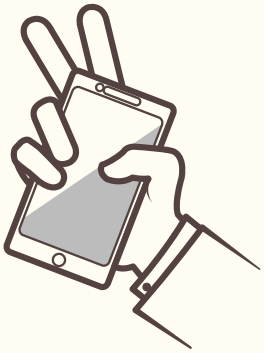
Serangan ataupun insiden siber dapat terjadi tanpa bisa diprediksi. Beberapa serangan dan insiden dapat menyebabkan data hilang, rusak, atau tidak dapat diakses. Hal ini dapat terjadi akibat terinfeksi virus, malware, ataupun terjadi kerusakan secara fisik pada perangkat. Untuk itulah, pencadangan perlu dilakukan secara rutin setiap bulan, minggu, bahkan setiap hari.

Cari tahu terlebih dahulu, data-data apa yang penting bagi bisnis anda, atau diperlukan dalam jangka waktu yang panjang. Mulailah untuk membuat urutan prioritas kepentingan data-data tersebut!

Pertimbangkanlah untuk menyimpan data cadangan di penyimpanan *cloud* (*online*). Hal ini mempermudah anda untuk mengakses data dari mana saja anda berada.

Data yang disimpan di *cloud* juga perlu komitmen keamanan yang ketat, seperti: tidak membagi kredensial (*username & password*) pada siapapun dan selalu *log-out* akun setelah digunakan.

Jika *cloud storage* bukan opsi pilihan anda, maka penyimpanan pada perangkat eksternal seperti *flash disk, CD,* ataupun hard drive external dapat menjadi opsi lain. Namun pastikan bahwa semua perangkat tersebut tidak secara permanen tersambung ke perangkat yang menyimpan file asli, baik secara fisik maupun dalam jaringan.



PASTIKAN KEAMANAN *SMARTPHONE / TABLET*

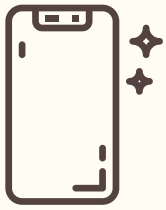
Teknologi selalu berkembang pesat untuk itulah selalu ada *update* pada perangkat anda, baik menambah fitur, maupun memperbaiki kerentanan, *bugs,* atau kecacatan pada sistem. Perbaharuilah (*update*) sistem operasi, perangkat lunak, dan aplikasi yang ada di perangkat anda, serta selalu unduh dan *install* aplikasi yang resmi.

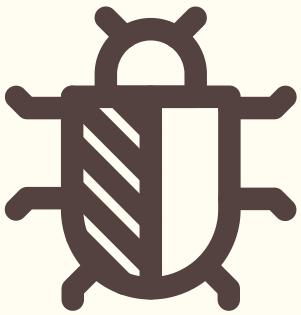
Aktifkan kunci layar (*screen lock*) baik menggunakan kode pin, *password,* atau biometrik seperti: *fingerprint,* pengenalan wajah (*face recognition*), dan iris mata.

Ketika mengirim data-data sensitif dan atau penting, hindari menggunakan WiFi publik, gunakanlah jaringan data seluler 3G, 4G, atau 5G.

Konfigurasikan perangkat anda dengan pengaturan khusus agar ketika perangkat anda hilang atau dicuri, dapat ditelusuri keberadaanya, atau dapat secara *remote* dikunci maupun dihapus datanya.

Apabila spesifikasi perangkat anda sudah tidak mumpuni dengan fitur-fitur aplikasi yang baru (yang biasanya memuatsistem keamanan yang lebih baik), segeralah ganti dengan perangkat yang lebih baru.





MENCEGAH DAMPAK AKIBAT TERINFEKSI MALWARE

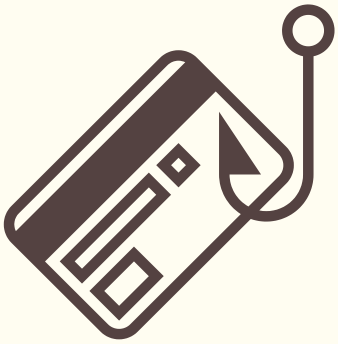
Gunakan ***antivirus*** pada komputer dan laptop anda dan pilihlah software antivirus yang resmi.

Edukasi pegawai anda untuk tidak mengunduh dan memasang aplikasi yang resmi, bukan dari pihak ke-3.

Lakukan perbaikan (*patch*) yang dirilis oleh pengembang aplikasi untuk menghindari eksploitasi kerentanan pada sistem. Agar tidak mudah lupa, aktifkan pembaruan otomatis (*automatically update)*.

Minimalisir akses terhadap media penyimpanan sementara seperti *hard drisk* eksternal atau flashdisk. Edukasilah pegawai anda untuk mengirim *file* dengan menggunakan email.

Aktifkan *firewall* pada perangkat, khususnya komputer. Hal ini dapat memberikan perlindungan dasar ketika perangkat terhubung ke internet.



MENGHINDARI SERANGAN PHISHING

Phishing merupakan teknik *social engineering* atau pengelabuan terhadap manusia. Teknik ini dilakukan untuk mendapatkan kredensial hak akses milik korban, atau untuk membuat korban mengunduh malware yang akan menginfeksi perangkatnya.

Edukasi terhadap pegawai mengenai ancaman phishing sangatlah penting dilakukan secara rutin.

CIRI-CIRI PHISHING :

- Menawarkan hadiah;
- Ditulis dengan tata bahasa yang tidak benar;
- Menggunakan alamat kirim (email, nomor hp, dll) yang mencurigakan;
- Meminta username, password, OTP, dll. ;
- Meminta korban untuk meng-klik tautan;
- Tautan yang diberikan, meminta untuk melakukan reset password;
- dll.

Hindari menggunakan perangkat dengan akses khusus (Admin), untuk keperluan lain, seperti: *browsing* dan mengecek email.

Dengan antivirus, *scan* secara berkala untuk mendeteksi adanya malware.

Segera ganti *password* jika terdapat percobaan phishing yang berhasil (anda telah dikelabui).

Jangan menghukum pegawai yang terkena *phishing,* karena hal ini akan membuat mereka enggan melapor ketika ada kejadian serupa di masa depan.

MENGELOLA PASSWORD

1. **Ganti *default password*** dari semua perangkat anda.

2. Buatlah *password* yang **unik**, **panjang**, **mudah diingat**, tapi **sulit ditebak**.

3. Sediakanlah tempat **penyimpanan yang aman,** agar pegawai dapat menuliskan *password*. Jangan tulis dan simpan *password* di perangkat.

4. Pertimbangkanlah untuk menggunakan aplikasi ***password manager***, namun gunakan hanya untuk akun akun yang tidak terlalu penting, atau tidak menimbulkan dampak permanen.

4. Selalu aktifkan **2-FACTOR** atau **MULTI-FACTOR AUTHENTICATION** dan hubungkan ke nomor handphone yang dipercaya.

Informasi ini dibuat pada September 2021. Dokumen ini merupakan adaptasi dari publikasi National Cyber Security Centre (NCSC) United Kingdom: Small Business Guide: Cyber Security
Seluruh gambar dan foto pada dokumen ini merupakan produk dan atas izin pihak ketiga.

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

DIREKTORAT OPERASI KEAMANAN SIBER
BADAN SIBER DAN SANDI NEGARA
Jalan Harsono RM No.70
Ragunan, Jakarta Selatan, Indonesia
(021) 7805814 Email: humas@bssn.go.id
Pusat Kontak Siber: bantuan70@bssn.go.id
https://idsirtii.or.id https://bssn.go.id