MEMBENTUK BUDAYA KEAMANAN SIBER DI TENGAH PANDEMIC COVID19

Webinar Nasional Universitas Muhammadiyah Semarang

Anton Setiyawan
Direktur Proteksi Ekonomi Digital, BSSN

Jakarta, 27 Juli 2020

GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT

(April 2020, INTERPOL)

a) Malicious domains
b) Online scams and phishing
c) Data-harvesting malware
d) Disruptive malware (ransomware and DDoS)
e) Vulnerability of working from home

What are cyber hygiene best practices?

- Loss of data.
- Misplaced data.
- Security breaches.
- Outdated software.
- Old security software.
- Poor or lack of vendor risk management.

There are ten controls in the **foundational** CIS controls, namely:

1) Email and web browser protections
2) Malware defenses
3) Limitation and control of network ports, protocols, and services
4) Data recovery capabilities
5) Secure configuration of network devices, such as firewalls, routers, and switches
6) Boundary defense
7) Data protection
8) Controlled access based on the need to know
9) Wireless access control
10) Account monitoring and control

CIS Controls V 7.1, April 2019


WORKING FROM HOME
SUDAH SIAP?
Patuhi jam kerja tetap seperti biasa
Siapkan bahan untuk laporan setiap hari
Pastikan koneksi Internet dan komunikasi tetap lancar
Persiapkan diri untuk rapat melalui aplikasi video confrence
Cari spot untuk kerja yang paling nyaman
Buat rencana dan target kerja harian


BADAN SIBER DAN SANDI NEGARA
JEJAK DIGITAL
MEMBENTUK CITRA ANDA DI MASA DEPAN
Jejak digital, yang tercipta atas segala perilaku digital penggunanya, akan lebih tepat jika disebut sebagai sebuah bom ranjau yang tertanam di dalam si pemilik jejak. Bom itu akan "meledak" terutama jika ada pihak-pihak tertentu yang mengincar si pemilik jejak digital sebagai target.
UNGGAH HAL POSITIF DI RUANG SIBER
Demi konten, jangan bangga posting tentang kenakalan atau nyinyir berujung ujaran kebencian dan SARA.
TIDAK MENGUMBAR DATA PRIBADI DI RUANG SIBER
Jangan membagi informasi lengkap tentang identitas diri seperti KTP maupun seluruh aktivitas pribadi sehari-hari.
PAHAMI CIRCLE KETIKA BERINTERAKSI DI RUANG SIBER
Kenali dengan siapa kita berkomunikasi. Batasi diri untuk tidak gegabah membagi informasi.
INFORMASI DI RUANG SIBER PERMANEN
Berpikir sebelum posting, apapun yang sudah berada di ruang siber mudah diduplikasi dan disebarluaskan oleh orang lain. Menghapusnya saja belum tentu bisa benar-benar melenyapkan jejak digitalmu.
INGAT #KAMIS INGAT #KEAMANANSIBER

PERLINDUNGAN SEDERHANA UNTUK GAWAIMU
SESEDERHANA H ♥ T I INI MENCINTAIMU

Hindari Tautan Berbahaya
dengan tidak mengklik
tautan yang tidak tepercaya.

Terus Mutakhirkan Software
untuk mengamankan
gawaimu.

Aktifkan Kunci Layar
untuk mencegah orang lain
menggunakan gawaimu
tanpa izin.

Instal Antivirus
dan mutakhirkan
secara berkala.

BADAN SIBER
DAN SANDI
NEGARA

Dapat Email Tapi Curiga Phishing ?
Yuk Hadapi Dengan BIJAK !

Biasakan mengecek dengan teliti siapa pengirim email, apakah benar dan tepercaya. Bisa jadi namanya hanya mirip dengan pengirim aslinya.

Ingat untuk tidak memberikan data pribadi seperti password kepada siapapun.

Jangan asal klik sembarang tautan yang terkirim melalui email.

Abaikan jika ada email yang meminta username, email address, password, tanggal lahir yang mengatas-namakan administrator.

Kenali ciri email phishing, segera hapus atau simpan di folder spam.

Email Phishing *adalah tindakan memperoleh informasi pribadi seperti User ID, Password dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah email.*

#KAMIS #KEAMANANSIBER

Chat-V?

Modus serangan digital melalui SMS, dengan mengandalkan sebuah tautan yang dikirim melalui SMS dari nomor tidak dikenal. Teks berisi tautan tersebut tidak hanya mengganggu, tetapi juga mengancam privasi dan keamanan Anda. Pelaku penipuan mengirim sebuah tautan (link) untuk menginstal sejumlah aplikasi atau program berbahaya yang dapat mencuri data pengguna.

1. Jika menerima SMS berisi ajakan dan tautan dari nomor tidak dikenal, abaikan dan hapus SMS tersebut.
2. Pindai perangkat untuk mengetahui apakah ada program berbahaya yang ter-*install*.
3. Pastikan antivirus di perangkat anda aktif dan *update*, untuk meminimalkan risiko yang ditimbulkan program tersebut.
4. *Factory reset* bisa saja dilakukan, pastikan melakukan backup data secara rutin.
5. Tetap waspada ketika berselancar di dunia maya, berpikir sebelum klik.

BADAN SIBER DAN SANDI NEGARA

SIM SWAP?

SIM Swap adalah tindakan mengambil alih nomor ponsel sebagai sarana bagi pelaku kejahatan untuk mengakses akun perbankan.

1. Pelaku yang sudah mengumpulkan informasi perbankan personal milik korban
2. Dengan identitas palsu, pelaku menuju operator seluler dan meminta penggantian kartu SIM baru milik korban
3. Setelah melakukan verifikasi, kartu SIM pengganti (baru) akan diterbitkan
4. Kartu SIM asli yang masih berada di tangan pemilik sah dinonaktifkan
5. Pelaku melakukan transaksi, OTP akan dikirimkan ke kartu SIM baru

Pelaku dapat melakukan transaksi perbankan tanpa sepengetahuan korban.

LANGKAH PENCEGAHAN :

- Tingkatkan kesadaran dan keamanan dalam beraktivitas di ruang siber;
- Tidak memberikan informasi yang berkenaan dengan data-data pribadi di media sosial karena dapat disalahgunakan oleh pihak yang tidak bertanggung jawab;
- Tidak membagikan informasi sensitif kepada siapapun, misal *username, PIN, password, one-time password (OTP)* dan sebagainya;
- Berhati-hatilah terhadap pihak yang mengaku berasal dari otoritas berwenang, namun meminta data-data sensitif;
- Berhati-hati terhadap suatu *link* atau tautan yang mencurigakan atau tidak dikenal untuk menghindari diri dari serangan *phishing*.

#KAMIS #KeamananSiber

BADAN SIBER DAN SANDI NEGARA

KONTEMPLASI 2019

oleh Dr. Rudi Lumanto, M.Eng
Pusat Operasi Keamanan Siber Nasional

- Everything About Security is About Asset
- In Cyber, Everything Is Recorded
- Threat Follow Asset, Attack Follow Vulnerability.
- In Cyber, What you see is not always what you get.
- In Cyber, No 100% Protection.
- In Cyber, We Are Already in a War.
- In Cyber, The Key is People, Process, and Technology.

Prinsip-Prinsip Budaya Keamanan Siber (amanat PP 71/2019 ps.94 ayat 1)

1) Gunakan budaya bangsa Indonesia baik di dunia nyata maupun dunia maya;
2) Kenali dan pahami teknologi, selaraskan dengan kebutuhan;
3) Selalu waspada dan berhati-hati dalam interaksi di dunia maya;
4) Kembangkan kemampuan literasi digital;
5) Bangun tata kelola keamanan informasi yang baik.

ALUR ADUAN
INSIDEN SIBER

Segera laporkan !!!

apabila anda menemukan insiden siber

Terjadi
insiden siber

Aduan segera
kami tangani

BADAN SIBER DAN SANDI NEGARA
BSSN

Kumpulkan bukti insiden berupa
foto / screenshot insiden / log file
yang ditemukan

Hubungi (021) 78833610
Laporkan & Kirimkan bukti ke
bantuan70@bssn.go.id atau
pusopskamsinas@bssn.go.id

PUSAT KONTAK SIBER

Pusat Operasi Keamanan Siber Nasional BSSN

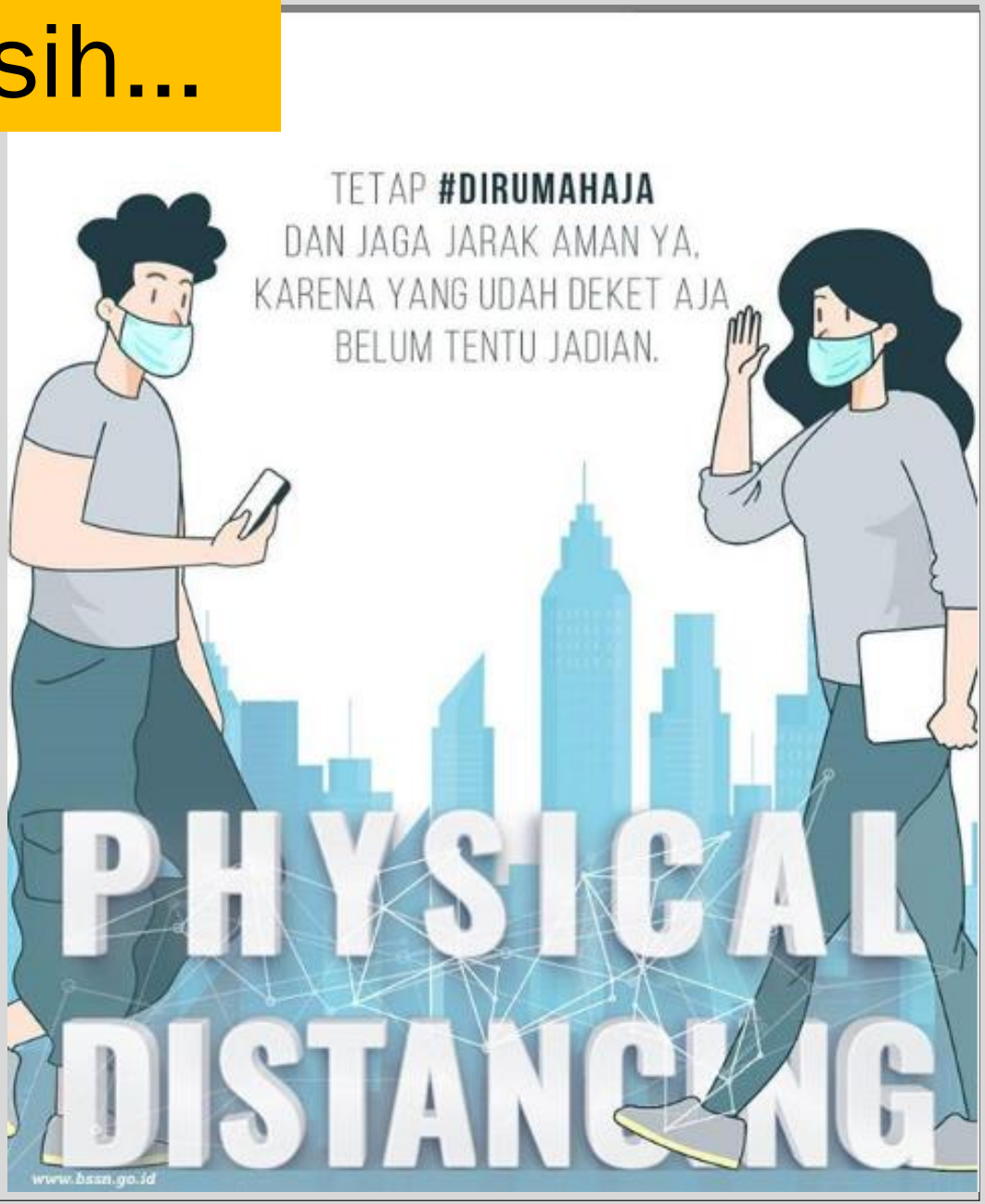
BADAN SIBER DAN SANDI NEGARA

https://bssn.go.id/tips-singkat-dan-praktis-di-dunia-siber/

TIPS SINGKAT & PRAKTIS DI DUNIA SIBER

DARI BSSN UNTUK MASYARAKAT

Terima Kasih...



anton.setiyawan@bssn.go.id