



Keamanan Digital bagi Organisasi Masyarakat Sipil



Aturan Kelas

- Privasi - Untuk menghormati privasi sesama fasilitator dan peserta, tidak diperbolehkan mengunggah foto atau video pelatihan ini.
- Audio -- Peserta diharapkan mematikan audio selama presentasi materi agar tidak mengganggu diskusi.
- Video -- Peserta diharapkan membuka video saat pengenalan dan diskusi. Selama presentasi materi, video peserta harap dimatikan untuk menghemat bandwidth dan agar tidak lebih fokus.
- Tanya Jawab -- Pertanyaan bisa langsung dilakukan melalui fasilitas chat di Zoom. Pada saat sesi tanya jawab, pertanyaan bisa diajukan secara lisan.
- Rekam -- Panitia akan merekam proses diskusi untuk keperluan dokumentasi serta bahan ajar jika diperlukan peserta.
- Foto Bersama -- Panitia akan melakukan foto bersama pada saat pembukaan dan penutupan. Peserta dipersilakan tidak membuka foto jika keberatan.

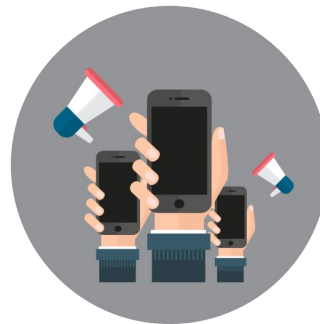
TEORI

Hak-Hak Digital

Hak untuk mengakses Internet

Hak untuk berekspresi

Hak atas rasa aman

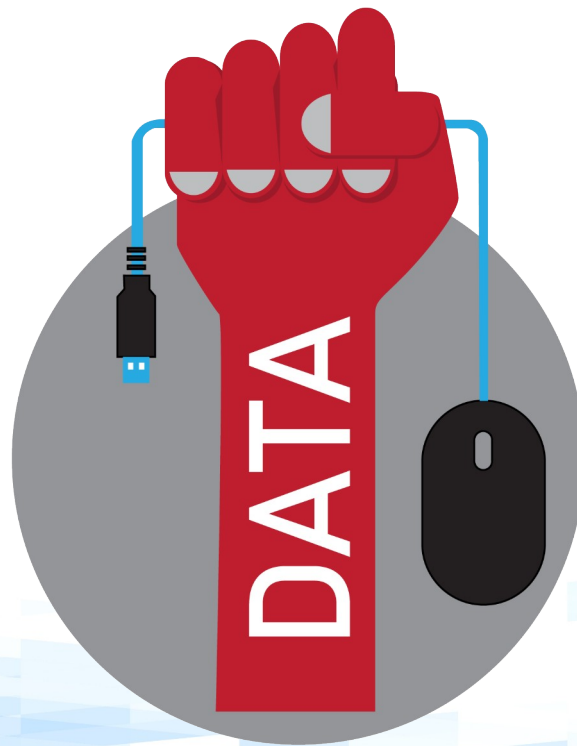


Politik Data

Data sebagai kekuatan

Data sebagai komoditas

Data sebagai senjata



Pertanyaan Pemantik

Apa itu rasa “AMAN” menurut Anda dan apa indikatornya?

Apa itu “PRIVASI” dan “KONSEN” di dunia digital?



Privasi

Kemampuan seseorang atau sekelompok grup untuk secara selektif mengekspresikan diri di publik



Data Pribadi

Berbagai informasi/
data/metadata, dalam
berbagai format, yang
dapat digunakan untuk
mengidentifikasi
seseorang



PII

Personally identifiable information atau berbagai yang dapat menunjukkan identitas seseorang

TIPE DATA PRIBADI

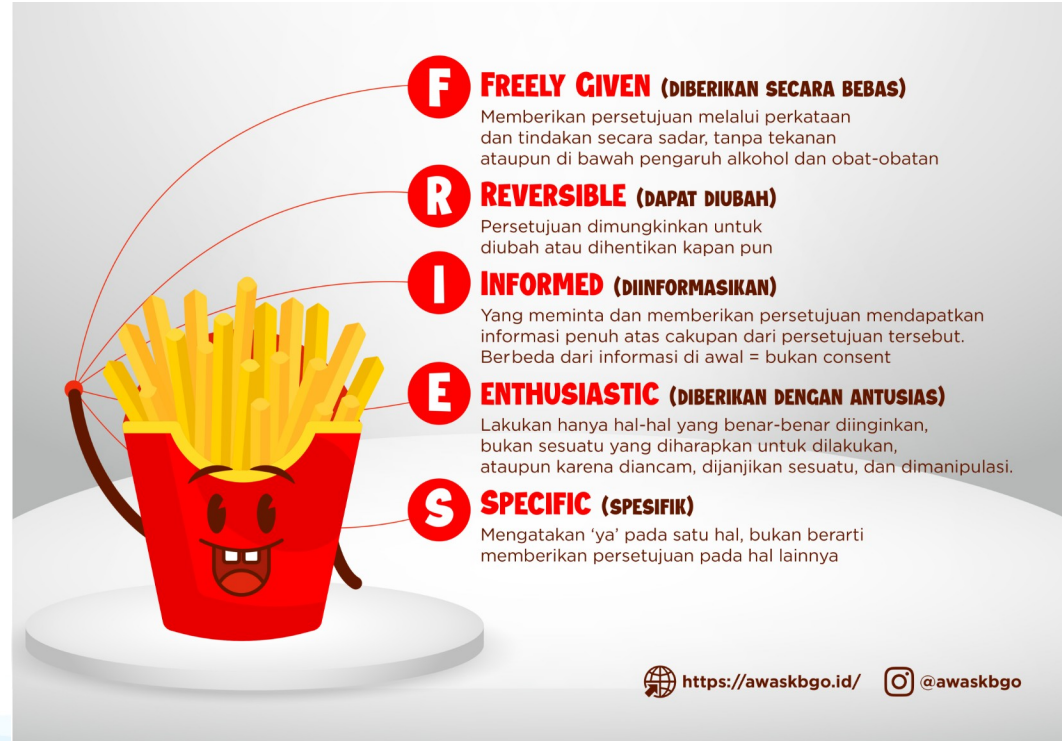
CONTOH

Nama	nama lengkap, nama semasa kecil, nama ibu, alias
Nomor identitas pribadi	NIK, NPWP, SIM, nomor paspor, plat nomor kendaraan, nomor kartu anggota rumah sakit, rekening bank, nomor kartu kredit
Alamat pribadi	alamat rumah, email
Nomor kontak personal	ponsel pribadi, telepon rumah
Karakteristik personal	gambar fotografik (utamanya atas wajah atau bagian lain yang menunjukkan karakteristik yang dapat dikaitkan pada seseorang), sidik jari, tulisan tangan
Data biometrik	scan retina, tanda suara (<i>voice signature</i>), sidik jari, geometri wajah
Informasi atas properti pribadi	nomor kendaraan, akta tanah dan bangunan
Informasi aset teknologi	alamat Internet Protocol (<i>IP address</i>) atau alamat <i>Media Access Control (MAC address)</i> yang secara konsisten terhubung pada satu individu tertentu
Lainnya	tanggal dan tempat lahir, nomor telepon bisnis, alamat email atau surat menyurat untuk keperluan bisnis, ras, agama, indikator geografis, dan informasi terkait pekerjaan, kesehatan, edukasi, atau finansial

Di dunia maya, data pribadi seperti ini sangat dianjurkan untuk tidak diumbar, terutama oleh diri sendiri saat menggunakan menggunakan media sosial (Facebook, Twitter, Instagram, dll) atau aplikasi percakapan (WhatsApp, Line, Telegram) dan lainnya.

Consent

- Persetujuan atau mengizinkan sesuatu untuk terjadi
- menghargai kehendak tiap individu yang terlibat dalam consent tersebut
- terutama terkait dengan ketubuhan, privasi, data pribadi
- prinsip FRIES harus terpenuhi



Prinsip Dasar Keamanan Digital

Personal dan kontekstual

Satu kesatuan dan saling terhubung

Perilaku adalah kunci (harus update dan up-to-date!)

Lebih baik mencegah, ingat jejak digital itu abadi!

Berbanding terbalik dengan kenyamanan



Gejala Terjadinya Serangan Digital

- Aktivitas tidak biasa
- Tidak bisa masuk akun
- Perangkat mendadak lambat
- Mengirim pesan ringkas atau email sendiri
- Baterai dan atau data cepat habis
- Ada aplikasi baru tanpa kita tahu

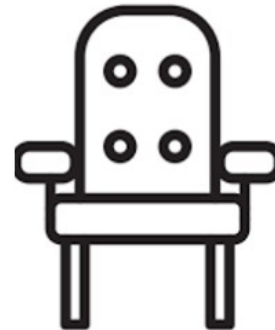


Motif-motif Serangan Digital

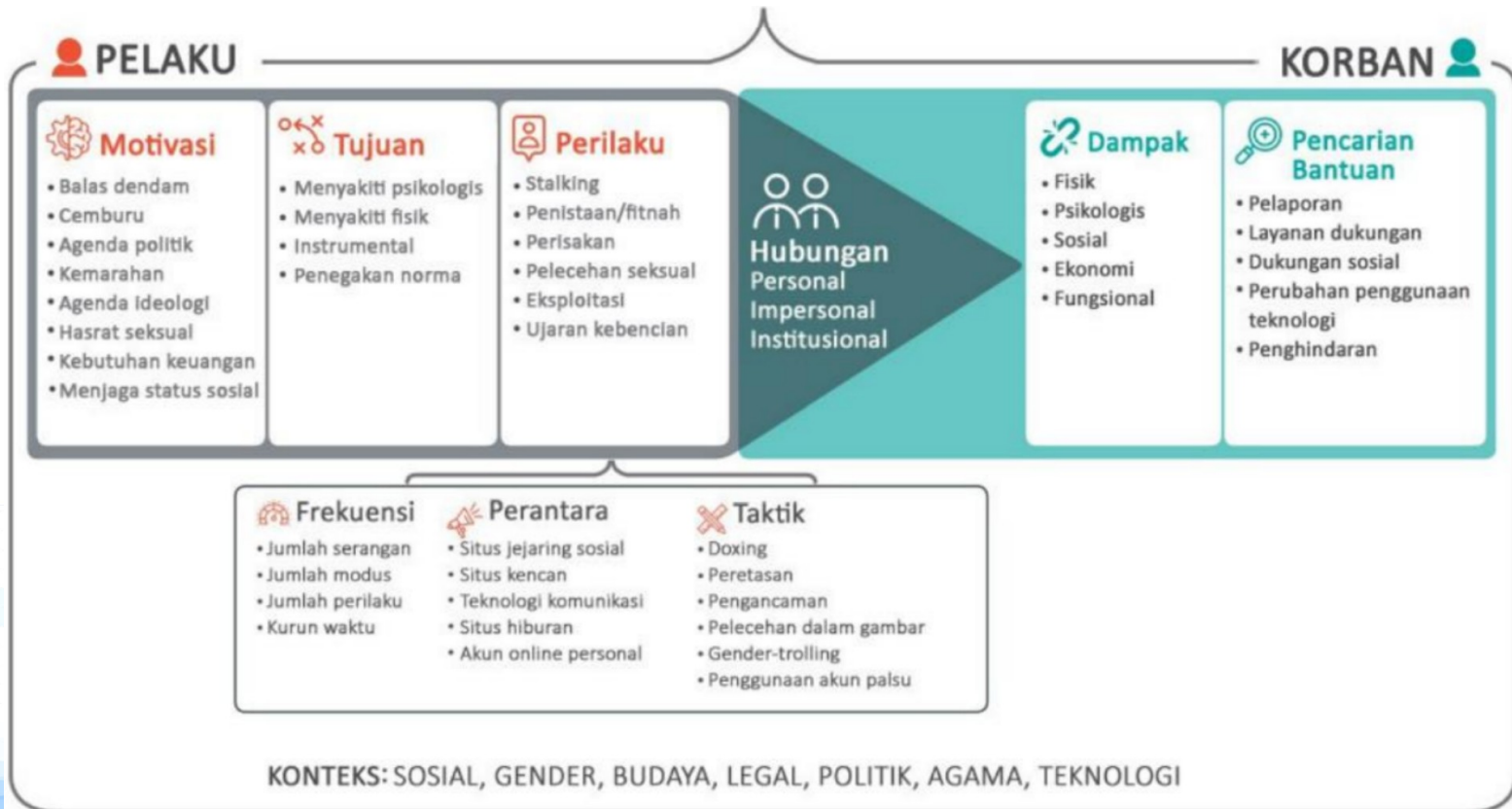
Personal

Ekonomi

Politik



Kekerasan Berbasis Gender Online



Aduan KBGO

Sumber:
Laporan Situasi
Hak-hak Digital 2020

Jenis-jenis KBGO selama 2020



NCII
208
Kasus



NCII dengan
motif hubungan
149
Kasus



NCII dengan
pemerasan
111
Kasus



Perusakan
reputasi
51
Kasus



Pelecehan
secara online
46
Kasus



Pelanggaran
privasi
38
Kasus



Pengancaman
6
Kasus



Penipuan dan
permintaan foto tubuh
3
Kasus

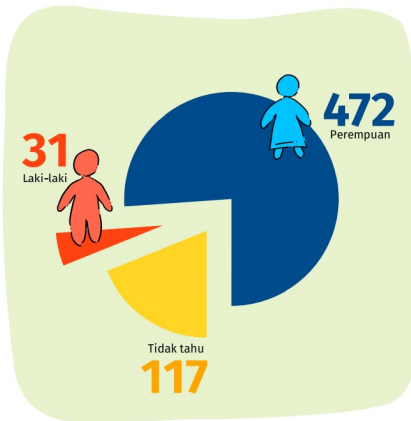


Tanpa penjelasan
4
Kasus



Lain-lain
4
Kasus

TOTAL
620



Contoh Kasus:
**Penyebaran
Konten Intim
Non-Konsensual
dan Aplikasi
Deteksi Telepon
Spam**



Contoh Kasus: **Pinjol, Pelanggaran Privasi dan KBGO**

Sumber: Tribunnews, 11/08/2021, “Perempuan di Jakarta Diteror Pinjol Gara-gara Telat Bayar Utang 5 Hari”

Perusahaan pinjol tersebut meneror PDY dengan cara menyebar foto dirinya yang disandingkan dengan gambar wanita telanjang.

Selain itu, dalam pesan singkat yang disebar ke orang-orang terdekat PDY, pelaku juga memberi keterangan 'OPEN BO + YUK JAPRI'.

← [Redacted] Pinjaman Uan..

Versi 1.0.8 dapat meminta akses ke

-  **Kalender**
 - Baca acara kalender dan detailnya
-  **Kamera**
 - ambil gambar dan video
-  **Kontak**
 - baca kontak Anda
 - cari akun pada perangkat
-  **Lokasi**
 - akses lokasi pasti hanya saat di latar depan
 - akses perkiraan lokasi (berbasis jaringan) hanya di latar depan
-  **Ponsel**
 - baca identitas dan status ponsel
-  **Penyimpanan**
 - memodifikasi atau menghapus konten penyimpanan bersama Anda
 - membaca konten penyimpanan bersama Anda

Metode Serangan

Berbasis website

Melalui aplikasi

Menggunakan jaringan





Jenis-jenis Serangan Digital

- Memancing (phishing)
- Meniru (impersonate)
- Mengumbar informasi pribadi tanpa izin (doxing)
- Menggeruduk (persekusi)
- Meretas (hacking)
- Menerobos (compromise)
- Menyadap (intercept)

Jenis-Jenis Serangan Digital



Impersonate

Meniru orang lain di internet, khususnya di media sosial dengan maksud mengambil keuntungan dari individu yang asli atau merusak reputasi individu yang asli.



Doxing

adalah sebuah praktik berbasis internet untuk meneliti dan menyebarkan informasi pribadi secara publik (termasuk data pribadi) terhadap seseorang individu atau organisasi. Metode ini digunakan untuk memperoleh informasi termasuk mencari basis data yang tersedia untuk umum dan situs sosial media (seperti Facebook), meretas, dan rekayasa sosial.



Persekusi

adalah perlakuan buruk atau penganiyaan secara sistematis oleh individu atau kelompok terhadap individu atau kelompok lain, khususnya karena suku, agama, atau pandangan politik. Berdasarkan Kamus Besar Bahasa Indonesia, persekusi merupakan pemburuan sewenang-wenang terhadap seorang atau sejumlah warga yang kemudian disakiti, dipersusah, atau ditumpas. Persekusi biasanya diawali dengan doxing.

Targeted Digital Attacks



Pada 19 Oktober 2020 beredar konten berupa foto, video, lokasi, nomer induk mahasiswa, nomer telepon disertai narasi memframe “tokoh penggerak demo berakhir rusuh di Yogyakarta” pada Azhar Jusardi Putra, Ernawati, Ardy Syihab di WhatsApp dan diunggah akun Instagram @sewordofficial dan @NCI4NKRI serta akun Twitter @demoanarki dan @NCI4NKRI

<https://twitter.com/demoanarki/status/1320529472936943616?s=21>

Akun Whatsapp Jusardi diambilalih.

Pada 20 Oktober 2020, ibu dari Jusardi menerima ancaman pembunuhan dari nomer telpon yang dibagikan oleh akun @demoanarki

Sumber:
<https://koran.tempo.co/read/nasional/459216/penolak-omnibus-law-jadi-korban-serangan-doxing>

Doxing Sebagai Pintu Masuk Kejahatan

Termasuk
dalam
**Advanced
Persistent
Threat (APT)**

*A Study of Doxing, its Security
Implications and Mitigation
Strategies for Organizations*
Roney Simon Matthews,
Concordia University
College of Alberta, Canada

Proses mengumpulkan PII seseorang atau sekelompok orang, **dengan tujuan** untuk mempermalukan, menakut-nakuti, memeras, memfitnah, menggertak, atau membahayakan target.

Motif:

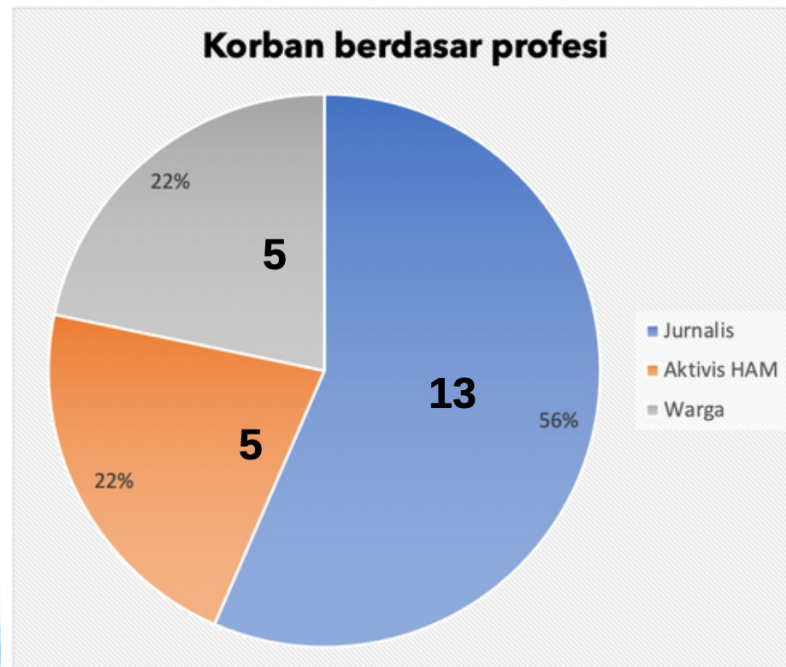
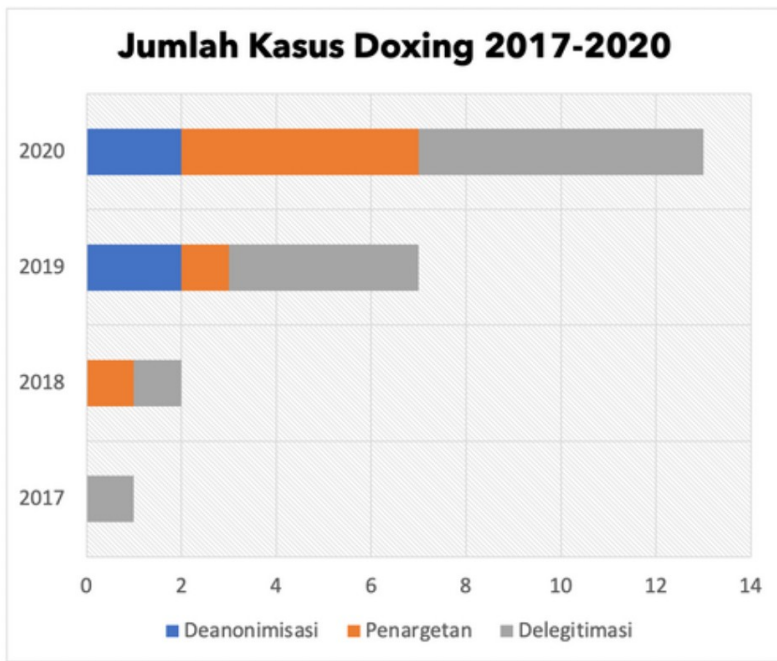
- Rasa ingin tahu tentang seseorang atau perusahaan
- Balas dendam, pemerasan, atau membuat malu target.

Potensi bahaya:

- Membahayakan individu yang ditargetkan
- Menyeret keluarga dan teman dari target, termasuk anak-anak.

Doxing bisa jadi pintu masuk kejahatan dunia maya lebih lanjut termasuk pencurian identitas, uang, phishing, peretasan.

Doxing di Indonesia



phishing

Phishing adalah serangan siber yang berupaya mengelabui orang agar memberikan informasi seperti sandi, atau nomor rekening bank dan kartu kredit melalui email yang dibuat sedemikian rupa supaya seolah terlihat berasal dari sumber yang "terpercaya".

APA YANG DIINCAR PELAKU PHISHING?



Kata Sandi



Data Keuangan



Data Pribadi



Uang

MEDIA YANG DIGUNAKAN PELAKU PHISHING



Email



Pesan WhatsApp



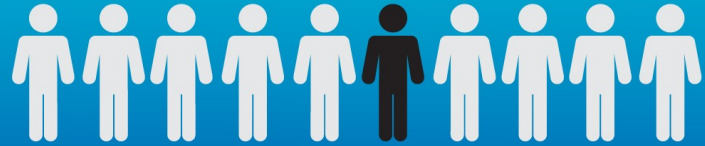
Facebook



Video Conference



SMS



1 DARI 10 PERCOBAAN PHISHING BISA BERHASIL*

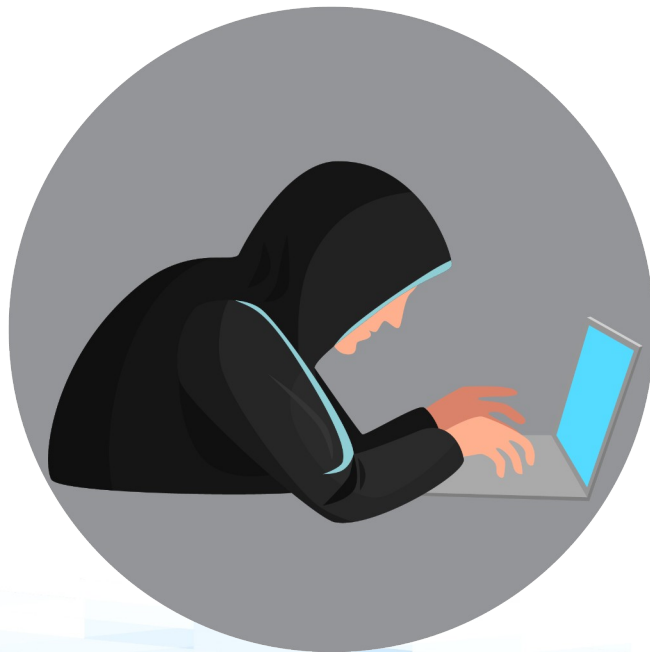
WASPADAI!

- 
1. Ejaan atau tulisan dari pesan yang diterima
 2. Nama pengirim
 3. Isi email yang terlalu bombastis
 4. Lampiran yang mencurigakan
 5. Url atau tautan yang tidak biasa

Pindai URL Mencurigakan

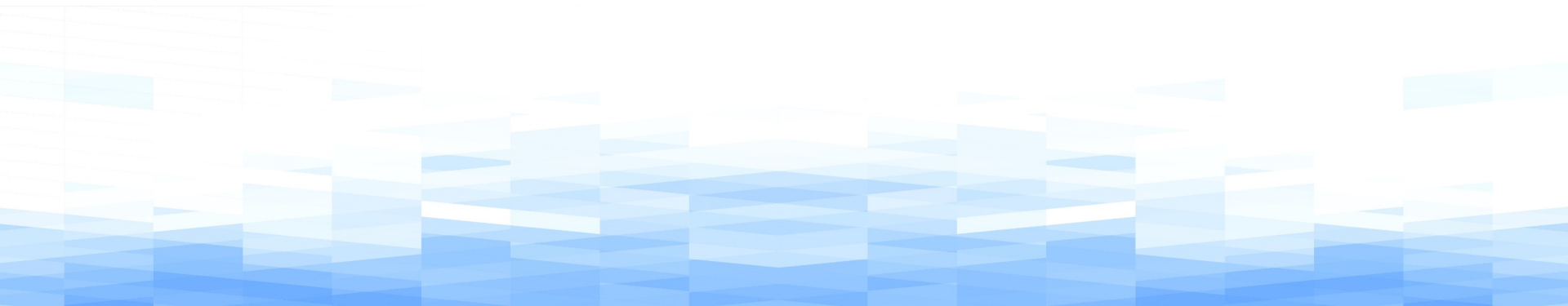
<https://virustotal.com/>

<https://urlscan.io/>





Sesi Tanya Jawab





<https://phishingquiz.withgoogle.com/>

Praktik

Strategi

Kurangi

Kendalikan

Lindungi

Bersembunyi

Gunakan Alternatif





Tingkat Pengamanan

Perangkat keras (device)

Apakah sudah dikunci?

1. PIN
2. Password
3. Pola
4. Sidik jari (finger print)
5. Pengenalan wajah (face recognition)

Perangkat lunak (aplikasi)

- Apakah selalu mengecek izin/permission tiap aplikasi yang dipasang?
- Apakah menggunakan aplikasi/software yang resmi?
- Apakah aplikasi yang digunakan selalu update?



Kurangi

Pikirkan sebelum unggah

Pertimbangkan sebelum membagi

Telusuri jejak digital

Cek <https://myactivity.google.com>





Kendalikan

Pengaturan Privasi: <http://myaccount.google.com/privacycheckup>

Pengaktifan Lokasi

Perekaman Riwayat

Monitor aktivitas Gawai

Kendalikan Gawai sendiri dengan perkecil kemungkinan orang lain bisa menggunakan, walaupun dia orang terdekat



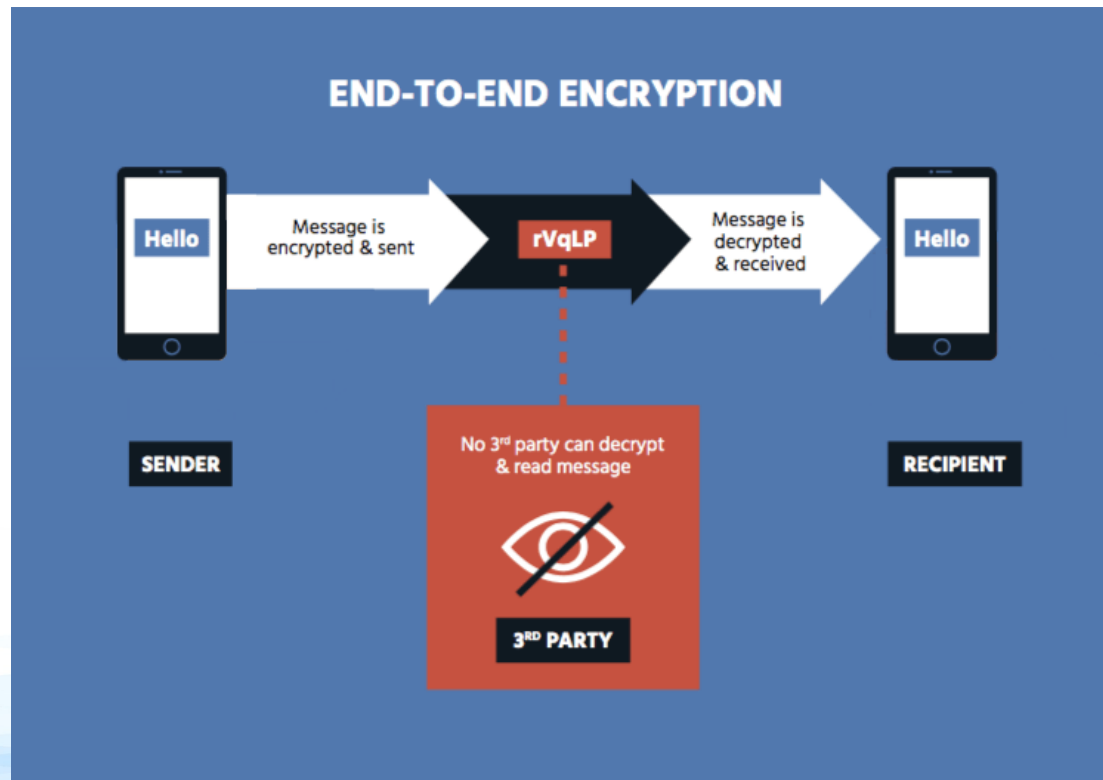
Lindungi

- Lakukan inventarisasi aset digital
- Kata kunci/Password
- Pilih atau aktifkan enkripsi
- Manajemen password
- Instal anti virus: gunakan yang legal/original dan rajin update, hindari versi bajakan
- Aktifkan 2FA
- Aktifkan Firewall

Inventarisasi Aset Digital

IDENTITAS	PENGAMANAN	ASET	LOKASI
Email	Password bagus + 2FA	Foto	Laptop
Akun Belanja	Password kurang, OTP	Alamat, No Rek	Mobile App dan Browser

Enkripsi



Enkripsi

- BitLocker pada Windows
- Filevault pada OSX

```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.18362
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [Windows]
[OS Volume]

Size: 39.44 GB
BitLocker Version: 2.0
Conversion Status: Used Space Only Encrypted
Percentage Encrypted: 100.0%
Encryption Method: XTS-AES 256
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: Unknown
Key Protectors:
    Password
    Numerical Password
```



Backup



Simpan tiga salinan file penting

satu file utama (di komputer, laptop, atau ponsel) dan dua cadangan di media penyimpanan yang lain



Gunakan dua jenis media yang berbeda

misalnya, satu komputer dan satu *hard drive*, atau satu *hard drive* dan satu penyimpanan berbasis *cloud*



Menyimpan satu backup di luar kantor

memiliki *backup* file di lokasi yang berbeda di luar kantor adalah hal penting dan itu menyediakan: redundansi dan kemudahan pemulihan paska bencana. Memiliki *backup* di luar kantor memberikan tingkat redundansi jika *backup* di lokasi pertama gagal.

Kata Kunci (Password)

- Mudah diingat
- Kuat
- kombinasi huruf besar, kecil, angka, karakter, spasi
- Ganti secara berkala
- Jangan disimpan sembarangan
- Jangan diinformasikan pada orang lain
- Berbeda untuk tiap aset digital
- Gunakan password manager
- Periksa kekuatan password: <https://lastpass.com/howsecure.php>





Periksa Kebocoran Email

Periksa apakah email dan/atau password kita pernah bocor di Internet sebelumnya.

- monitor.firefox.com
- haveibeenpwned.com
- periksadata.com

Jika ada indikasi pernah bocor, segera ganti password

Password Manager

Mengapa disarankan menggunakan password manager?

1. Lebih aman
2. Manusia cepat lupa
3. Berisiko jika dicatat di notes karena tanpa kunci
4. Password sebaiknya berbeda untuk tiap akun





Password Manager

Online

Contoh: Bitwarden, RememBear

- Perlu daftar
- Lebih mudah sinkronisasi untuk multi perangkat
- Ada fitur berbayar

Offline

Contoh: KeePass

- Tidak perlu daftar
- Sinkronisasi manual antar perangkat
- Selalu gratis

Two Factor Authentication (2FA)

- Aplikasi Authenticator
- Contoh: Google Authenticator, Authy, FreeOTP
- SMS
- 2FA dengan Push
- Kunci keamanan (security key)



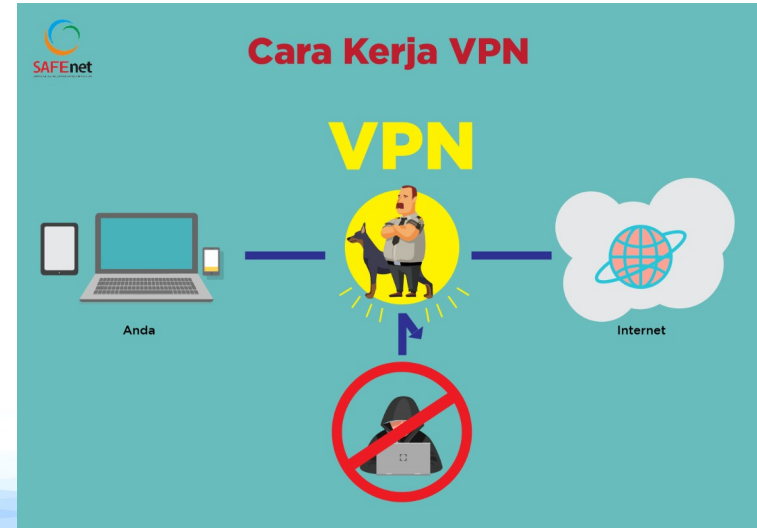


Setting 2FA

- Cek di <https://ictwatch.id/2fa> / <https://twofactorauth.org>
- WhatsApp: settings → account → two step verification
- Facebook: settings & privacy → security and login → Two Factor Authentication
- Instagram: settings → security → Two Factor Authentication
- Twitter: settings and privacy → account → security → Two Factor Authentication
- Google: <https://myaccount.google.com> login → security → 2-Step verification

Bersembunyi

- Manajemen identitas, disarankan untuk jika akan posting sesuatu yang sensitif tidak menggunakan akun yang ada identitas jelas.
- VPN (Virtual Private Network)
- Private Window/Incognito



Gunakan Alternatif

- Email selain Gmail/Yahoo: [Protonmail](#), [Posteo](#), [Riseup](#), [Espiv](#)
- Aplikasi Percakapan selain WA/FB Messenger: [Telegram](#), [Signal](#), [Wire](#), [Chatsecure](#)
- Browser selain Chrome: [Firefox](#), [TOR browser](#), [Brave](#)
- Mesin pencari selain Google: [Duckduckgo](#), [SearX](#), [Startpage](#)
- Dokumen kolaboratif selain Google Drive: [Etherpad](#), [Riseup Pad](#), [Cryptpad](#)
- Video conference selain Google Hangout/Meet, Zoom: [Jitsi](#), [Big Blue Button](#)
- Peta online selain Google Maps: [OpenStreetMap](#)



Prinsip Pendampingan Korban

Prinsip Pendampingan Korban



Mengutamakan Kerahasiaan Identitas

Ingat Privasi!

Semua Tindakan Harus dengan Konsen dari Korban

Ingat Prinsip FRIES!

Keamanan Korban dan Pendamping adalah Prioritas

Ingat Prinsip Satu Kesatuan!



Publikasi terkait Kekerasan Berbasis Gender Online



<https://awaskbgo.id/publikasi/>



Kelas Perempuan Aman Internetan

Materi: Privasi, Konsen, Keamanan Digital Dasar, Pengantar KBG (total 20 materi)

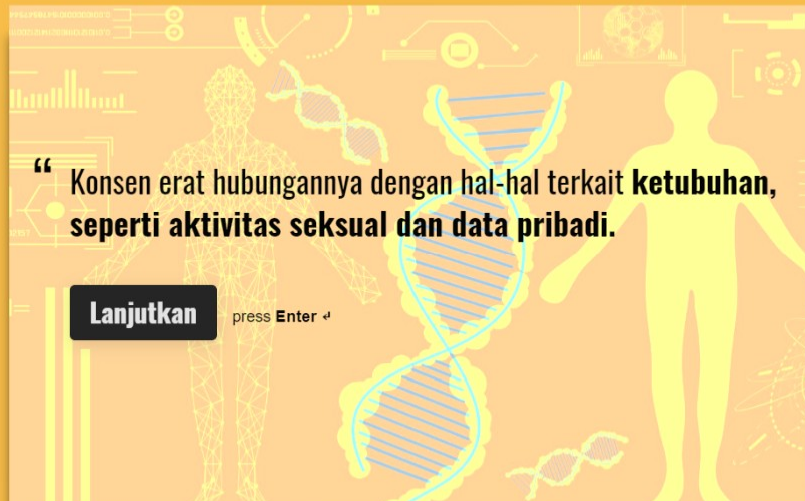
Durasi: ± 2-3 Jam; Status: GRATIS dan tersedia E-Sertifikat



Data pribadi itu apa, sih?

Mulai

press Enter ↵



<https://kelas.awaskbgo.id/>



Lapor Serangan Digital / KBGO

Lapor Serangan Digital: <https://s.id/laporserangan>

Lapor KBGO: <https://awaskbgo.id/layanan>

Daftar Kasus UU ITE: <https://semuabisakena.jaring.id>

Email: aduan@safenet.or.id

Hotline: **08119223375**

