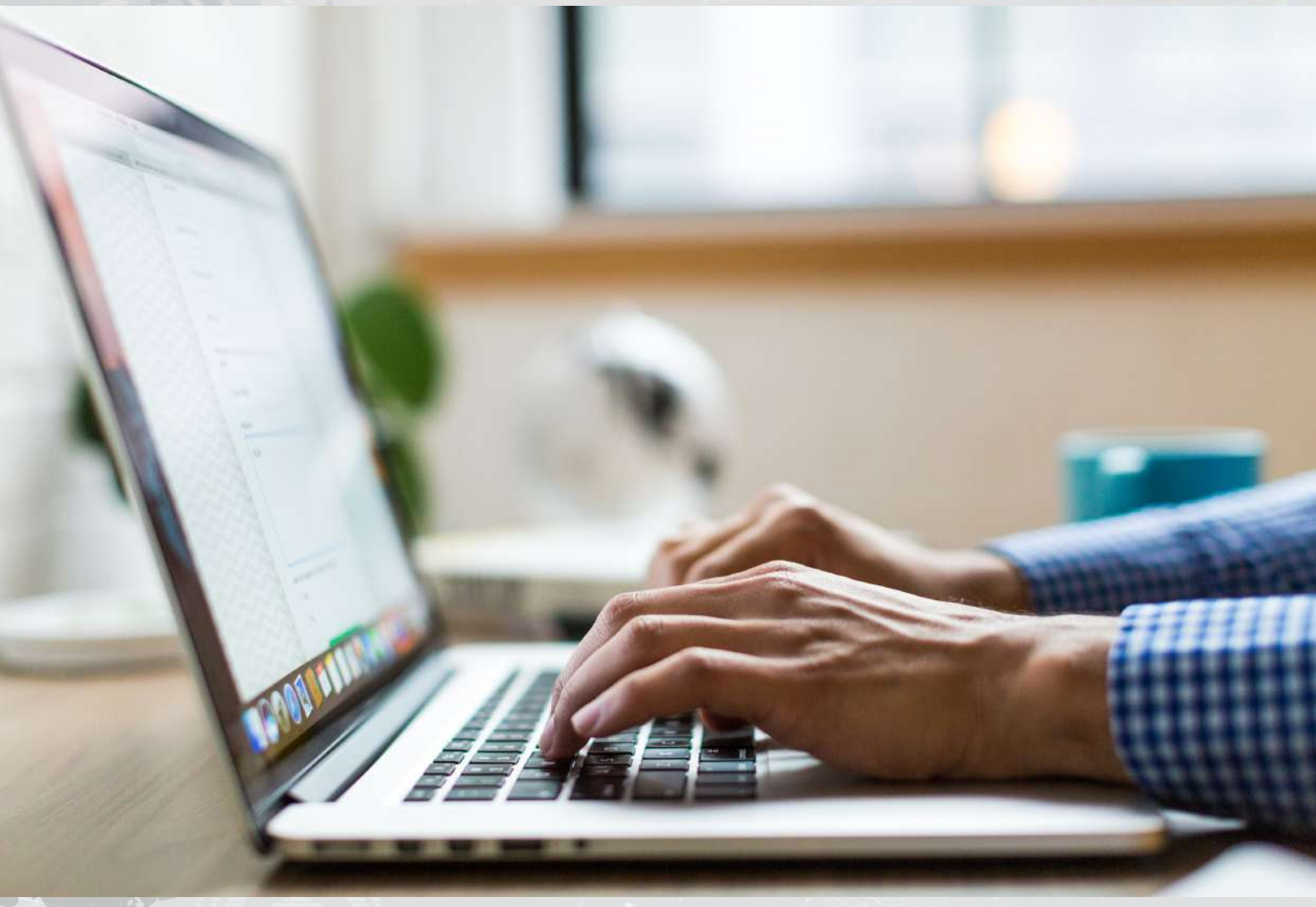
PANDUAN KEAMANAN YOUTUBE



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

TLP: WHITE

MEMPERBAIKI AKUN YOUTUBE YANG DIRETAS

Jika Anda menemukan salah satu hal berikut, Akun Google Anda mungkin telah diretas, dibajak, atau disusupi:

- **Perubahan yang tidak Anda buat** : Terdapat perbedaan pada gambar profil, deskripsi, setelan email, asosiasi AdSense, atau pesan yang dikirim.
- **Video yang diupload yang bukan milik Anda** : Seseorang telah memposting video yang seolah-olah berasal dari Akun Google Anda. Anda mungkin juga menerima notifikasi email tentang video ini terkait hukuman atau teguran akibat konten yang buruk.

Anda Masih Dapat Login ke Akun Google

Ikuti langkah-langkah berikut untuk mengamankan Akun Google Anda:

Melindungi Akun Anda Dengan Verifikasi 2 Langkah

Dengan verifikasi 2 langkah (juga dikenal sebagai autentikasi 2 langkah), Anda menambahkan lapisan keamanan ekstra ke akun Anda jika sandi dicuri. Setelah menyiapkan verifikasi 2 kangkah, Anda akan login ke akun Anda dalam dua langkah menggunakan:

- Sesuatu yang Anda ketahui, seperti sandi Anda
- Sesuatu yang Anda miliki, seperti ponsel Anda

Mengaktifkan Verifikasi 2 Langkah

1. Buka Akun Google Anda.
2. Di panel navigasi, pilih Keamanan.
3. Di bagian “Login ke Google”, pilih Verifikasi 2 Langkah Mulai.
4. Ikuti langkah-langkah di layar.

Akun Anda, namapengguna@gmail.com, terkait dengan kantor atau sekolah Anda. Jika Anda tidak dapat menyiapkan verifikasi 2 langkah, hubungi administrator Anda.

Memverifikasi Identitas Anda pada Langkah Kedua

Setelah mengaktifkan Verifikasi 2 Langkah, Anda harus menyelesaikan langkah kedua untuk memverifikasi identitas Anda saat login. Untuk membantu melindungi akun Anda, Google akan meminta Anda menyelesaikan langkah kedua yang spesifik.

Menggunakan perintah Google

Sebaiknya Anda login dengan perintah Google. Lebih mudah untuk mengetuk perintah daripada memasukkan kode verifikasi. Perintah juga dapat membantu melindungi dari pertukaran SIM dan peretasan berbasis nomor telepon lainnya.

Perintah Google adalah notifikasi push yang akan Anda terima di:

- Ponsel Android yang digunakan untuk login ke Akun Google Anda
- iPhone dengan aplikasi Smart Lock , aplikasi Gmail , atau aplikasi Google yang telah login ke Akun Google Anda

Berdasarkan info perangkat dan lokasi pada notifikasi, Anda dapat:

- Mengizinkan proses login jika Anda memintanya dengan mengetuk Ya
- Memblokir proses login jika Anda tidak memintanya dengan mengetuk Tidak

Untuk keamanan tambahan, Google mungkin meminta PIN atau konfirmasi lainnya kepada Anda.

Menggunakan metode verifikasi lain

Anda dapat menyiapkan metode verifikasi lainnya jika Anda:

- Menginginkan perlindungan yang lebih optimal terhadap phishing
- Tidak bisa mendapatkan perintah Google
- Kehilangan ponsel Anda

4 METODE VERIFIKASI LAINNYA

Menggunakan kunci keamanan untuk meningkatkan perlindungan phishing

Kunci keamanan fisik adalah perangkat kecil yang bisa Anda beli untuk membantu membuktikan bahwa Andalah yang login. Anda cukup menghubungkan kunci keamanan ke ponsel, tablet, atau komputer. Kunci keamanan membantu melindungi Akun Google Anda dari serangan phishing, saat peretas mencoba mengelabui Anda agar memberikan sandi atau informasi pribadi Anda yang lainnya kepada mereka.

Menggunakan Google Authenticator atau aplikasi kode verifikasi lainnya

Anda dapat menyiapkan aplikasi Google Authenticator atau aplikasi lain yang membuat kode verifikasi sekali pakai saat Anda tidak memiliki koneksi internet atau layanan seluler. Masukkan kode verifikasi di layar login untuk membantu memverifikasi identitas Anda.

Menggunakan kode verifikasi dari SMS atau panggilan telepon

Kode 6 digit dapat dikirimkan ke nomor yang telah Anda berikan sebelumnya. Kode dapat dikirim melalui pesan teks (SMS) atau melalui panggilan suara, tergantung setelan yang Anda pilih. Untuk memverifikasi identitas Anda, masukkan kode di layar login. **Tips:** Meskipun semua bentuk verifikasi 2 langkah meningkatkan keamanan akun, kode verifikasi yang dikirim melalui SMS atau panggilan dapat rentan terhadap peretasan berbasis nomor telepon.

Menggunakan kode cadangan

Anda dapat mencetak atau mendownload kumpulan kode cadangan 8 digit untuk disimpan di tempat yang aman. Kode cadangan sangat membantu jika Anda kehilangan ponsel.

Penting :
Jangan pernah memberikan kode verifikasi kepada siapa pun!

Anda Tidak Dapat Login ke Akun Google

Guna mendapatkan bantuan untuk login kembali ke Akun Google Anda:

1. Ikuti langkah-langkah untuk memulihkan Akun Google atau Gmail Anda.
   - Anda akan ditanyai beberapa pertanyaan untuk mengonfirmasi akun tersebut milik Anda. Jawab dengan sebaik-baiknya.
   - Jika Anda mengalami masalah, coba tips untuk menyelesaikan langkah-langkah pemulihan akun.
2. Setel ulang sandi Anda jika diminta. Pilih sandi kuat yang belum digunakan dengan akun ini.

Tips untuk menyelesaikan langkah-langkah pemulihan akun

Jika Anda tidak dapat login, ikuti langkah-langkah ini untuk memperbesar peluang Anda untuk login kembali ke Akun Google Anda:

1. Buka halaman Pemulihan akun.
2. Setelah menyelesaikan langkah-langkah tersebut, gunakan tips di bawah ini sebanyak mungkin:

a. Jawab pertanyaan sebanyak mungkin.

- Coba jawab semua pertanyaan. Jika Anda ragu menjawabnya, lebih baik berikan tebakan terbaik Anda daripada berpindah ke pertanyaan lain.

b. Gunakan perangkat dan lokasi yang biasa Anda gunakan.

Jika memungkinkan:

- Gunakan komputer, ponsel, atau tablet yang sering Anda gunakan untuk login
- Gunakan browser yang sama (seperti Chrome atau Safari) yang biasa Anda gunakan
- Akses di lokasi tempat Anda biasanya login, seperti di rumah atau kantor

c. Berikan sandi dan jawaban pertanyaan keamanan dengan tepat.

Info yang Anda berikan sangat penting, jadi hindari salah eja dan perhatikan huruf besar dan huruf kecil.

d. Kata Sandi.

Jika Anda dimintai sandi terakhir yang Anda ingat, masukkan sandi paling baru yang Anda ingat.

- Jika Anda tidak mengingat sandi terakhir Anda: Gunakan sandi sebelumnya yang Anda ingat. Semakin baru sandinya, akan semakin baik.
- Jika Anda ragu dan tidak dapat mengingat sandi sebelumnya: Berikan tebakan terbaik Anda.

e. Jawaban pertanyaan keamanan.

Jika ditanya pertanyaan keamanan dan Anda:

- Tidak ingat jawabannya: Berikan tebakan terbaik Anda.
- Mengetahui jawabannya namun tidak dapat memulihkan akun pada percobaan pertama: Coba gunakan variasi jawaban yang berbeda. Misalnya, coba "JKT" bukan "Jakarta" atau "Fit" bukan "Fitri".

f. Masukkan email yang terhubung ke akun Anda.

Jika diminta untuk memasukkan alamat email yang dapat diperiksa saat ini juga, masukkan satu alamat email yang telah Anda tambahkan ke akun. Berikut beberapa contohnya:

- Alamat email pemulihan membantu Anda untuk kembali login dan menjadi email tujuan pengiriman pemberitahuan keamanan.
- Alamat email alternatif adalah alamat email yang dapat digunakan untuk login.
- Alamat email kontak adalah tempat Anda mendapatkan informasi tentang sebagian besar layanan Google yang Anda gunakan.

g. Tambahkan info yang dapat membantu.

Jika ditanya mengapa Anda tidak dapat mengakses akun, berikan info yang membantu. Sebagai contoh:

- Anda sedang bepergian.
- Anda mendapatkan pesan error tertentu.
- Anda merasa akun telah disusupi karena malware atau alasan lainnya.
- Anda mengubah sandinya minggu lalu dan tidak dapat mengingatnya.

Jika penjelasan Anda sesuai dengan informasi yang Google miliki, persamaan ini dapat membantu Anda.

h. Memeriksa apakah ada pesan di folder spam Anda

Penting: Google tidak pernah meminta sandi Anda melalui email, panggilan telepon, atau pesan. Masukkan sandi Anda hanya di ***accounts.google.com***.

Jika sepertinya Anda menerima email dari Google tetapi tidak dapat menemukannya, periksa folder spam atau sampah Anda dan temukan email dengan judul, "Pertanyaan dukungan Google Anda". Masih belum bisa login? Pertimbangkan untuk membuat Akun Google pengganti.

"Jika sudah mencoba memulihkan akun dan mendapat pesan "Google tidak dapat memverifikasi bahwa akun ini milik Anda", Anda dapat mencoba lagi."

MENGAMANKAN AKUN YouTube

Mengamankan akun YouTube Anda dapat membantu agar akun Anda tidak diretas, dibajak, atau disusupi.

1 Buat **sandi yang kuat** dan **amankan** sandi

Sandi yang kuat membantu Anda menjaga keamanan informasi pribadi dan mencegah orang lain mengakses akun Anda.
Buat kata sandi yang **kuat dan kompleks**: Gunakan 8 karakter atau lebih. Dapat berupa kombinasi huruf, angka, dan simbol.
Buat sandi yang **unik**: Jangan gunakan sandi akun YouTube Anda di situs lain. Jika situs lain diretas, sandi tersebut dapat digunakan untuk masuk ke akun YouTube Anda.
Hindari penggunaan informasi pribadi dan kata-kata umum: Jangan gunakan informasi pribadi seperti tanggal lahir Anda, kata-kata umum seperti “sandi”, atau pola umum seperti “1234”.

Lindungi sandi Anda dari peretas
Dapatkan notifikasi saat Anda memasukkan sandi di situs non-Google dengan mengaktifkan Notifikasi Sandi untuk Chrome. Misalnya, Anda akan mendapatkan notifikasi jika memasukkan sandi di situs yang meniru Google, lalu Anda dapat mengubah sandi akun YouTube Anda.

Kelola sandi Anda
Pengelola sandi dapat membantu Anda membuat dan mengelola sandi yang kuat dan unik. Coba gunakan pengelola sandi dari Chrome atau penyedia pengelola sandi tepercaya lainnya.
Tips: Untuk mencari tahu apakah sandi yang tersimpan di Akun Google Anda mungkin terekspos, lemah, atau digunakan ulang untuk beberapa akun, gunakan Pemeriksaan Sandi.

Jangan pernah bagikan info login Anda
Jangan berikan sandi Anda. YouTube tidak akan pernah meminta sandi dalam email, pesan, atau panggilan telepon. YouTube tidak akan pernah mengirim formulir yang meminta informasi pribadi seperti nomor identitas, data keuangan, atau sandi.

2 Lakukan **pemeriksaan** keamanan **rutin**

Tambahkan atau perbarui opsi pemulihan akun

Nomor telepon dan alamat email pemulihan Anda dapat digunakan untuk:

- Memblokir seseorang agar tidak dapat menggunakan akun Anda tanpa izin
- Memberi tahu Anda jika ada aktivitas mencurigakan di akun Anda
- Memulihkan akun Anda jika akun terkunci

Hapus orang yang mencurigakan dari akun Anda

Jika Anda tidak mengenali orang yang mengelola akun Anda, akun Anda mungkin telah diretas, dan seseorang telah memverifikasi kepemilikan akun Anda untuk mendapatkan sesuatu. Anda dapat mengubah atau menghapus orang, bergantung pada jenis akun Anda.

- Mengubah atau menghapus akses dari Akun YouTube Anda
- Mengubah atau menghapus akses dari Akun Bisnis Anda

Hapus situs dan aplikasi yang tidak Anda perlukan

Untuk melindungi akun YouTube Anda, jangan instal aplikasi tidak dikenal atau aplikasi dari sumber tidak dikenal. Kelola dan hapus aplikasi yang tidak diperlukan dari akun terhubung Anda.

Update software Anda dan cadangkan akun Anda

Jika browser, sistem operasi, atau aplikasi Anda sudah lama tidak diupdate, software mungkin tidak aman dari peretas. Selalu update software Anda dan cadangkan akun Anda secara rutin.

3 **Lindungi diri** dari **pesan dan konten** yang **mencurigakan**

Phishing adalah ketika peretas menyamar sebagai seseorang yang dapat dipercaya untuk mengambil informasi pribadi, seperti data keuangan, nomor KTP/nomor jaminan sosial, atau nomor kartu kredit.

Peretas dapat berpura-pura menjadi institusi, anggota keluarga, atau rekan kerja dengan menggunakan email, SMS, halaman web, dan sebagainya.

YouTube **tidak pernah** meminta sandi, alamat email, atau informasi akun lainnya dari Anda. **Jangan terkecoh** jika seseorang menghubungi Anda dengan berpura-pura seolah-olah dari YouTube.

Hindari permintaan yang mencurigakan

- Jangan jawab email, SMS, pesan instan, halaman web, atau panggilan telepon mencurigakan yang meminta informasi pribadi atau keuangan Anda.
- Jangan klik link di email, pesan, halaman web, atau jendela pop-up dari situs atau pengirim yang tidak dapat dipercaya.
- Email YouTube hanya berasal dari alamat @youtube.com atau @google.com.

Hindari halaman web yang mencurigakan

Google Chrome dan Penelusuran didesain untuk memperingatkan Anda tentang konten yang mencurigakan dan software yang tidak diinginkan.

Laporkan spam atau phishing

Untuk melindungi diri Anda dari phishing, jangan pernah masukkan sandi Anda di halaman apa pun kecuali myaccounts.google.com. Jika Anda menemukan video di YouTube yang Anda pikir mungkin spam atau phishing, harap laporkan video itu agar ditinjau oleh tim YouTube. Untuk informasi lebih lanjut tentang spam dan phishing, buka National Cyber Security Alliance.

4 Atur dan periksa perizinan di channel Anda

Jika Anda adalah kreator, Anda dapat mengundang orang lain untuk mengelola channel YouTube Anda tanpa memberikan akses ke Akun Google Anda. Undang seseorang untuk mengakses channel mereka sebagai:

- Pengelola: Dapat menambahkan atau menghapus orang lain dan mengedit detail channel.
- Editor: Dapat mengedit semua detail channel.
- Penonton: Dapat melihat (tetapi tidak dapat mengedit) semua detail channel.
- Penonton (terbatas): Dapat melihat (tetapi tidak dapat mengedit) semua detail channel kecuali informasi pendapatan.

Catatan: Jika memiliki akun Bisnis, Anda dapat mengundang seseorang untuk mengelola Akun Google dan channel YouTube Anda.

Akun YouTube Anda berkaitan erat dengan akun Google. Berikut adalah cara-cara untuk mengamankan Akun Google.

Tinjau Aktivitas

Tinjau aktivitas akun Anda

1. Buka Akun Google Anda.
2. Di panel navigasi kiri, klik Keamanan.
3. Di panel Peristiwa keamanan baru-baru ini, pilih Tinjau peristiwa keamanan.
4. Periksa aktivitas yang mencurigakan:
    - Jika Anda menemukan aktivitas yang tidak Anda lakukan, pilih Tidak, bukan saya. Lalu, ikuti langkah-langkah di layar untuk membantu mengamankan akun Anda.
    - Jika Anda yang melakukan aktivitas tersebut, pilih Ya. Jika Anda tetap yakin bahwa orang lain menggunakan akun Anda, cari tahu apakah akun Anda telah diretas.

Tinjau perangkat mana yang menggunakan akun Anda

1. Buka Akun Google Anda.
2. Di panel navigasi kiri, klik Keamanan.
3. Di panel Perangkat Anda, pilih Kelola perangkat.
4. Periksa apakah ada perangkat yang tidak Anda kenali.
    - Jika menemukan perangkat yang tidak dikenali, pilih Tidak mengenali perangkat? Lalu, ikuti langkah-langkah di layar untuk membantu mengamankan akun Anda.
    - Jika Anda mengenali semua perangkat, tetapi tetap yakin orang lain menggunakan akun Anda, cari tahu apakah akun Anda telah diretas.

Lakukan langkah-langkah keamanan lainnya

Bantu amankan aplikasi dan perangkat Anda

- Jika akses untuk aplikasi yang kurang aman diaktifkan, sebaiknya nonaktifkan setelan tersebut karena dapat membuat akun Anda kurang aman.
- Gunakan opsi kunci layar perangkat jika ada.

Hubungi bank Anda atau otoritas setempat

Pastikan orang lain tidak memberikan petunjuk kepada bank atau pemerintah, misalnya untuk membuka rekening atau mentransfer uang. Ini penting jika Anda:

- Menyimpan info perbankan di akun Anda, seperti kartu kredit yang tersimpan di Google Pay atau Chrome.
- Menyimpan info pribadi seperti info pajak atau paspor di akun Anda. Misalnya, Anda mungkin menyimpan info pribadi di Google Foto, Google Drive, atau Gmail.
- Merasa seseorang menggunakan atau meniru identitas Anda.

Hapus software berbahaya

Jika menurut Anda ada aktivitas yang mencurigakan di akun Anda, Anda mungkin perlu menghapus software berbahaya. Untuk meningkatkan keamanan akun Anda, instal dan jalankan software antivirus tepercaya.

Anda juga dapat mereset komputer Anda ke setelan pabriknya dan menginstal ulang sistem operasi.

Bantu amankan produk Google lainnya yang Anda gunakan

- Gmail: Tinjau tips keamanan ini, dan hapus label, filter, atau aturan penerusan yang tidak Anda siapkan.
- Chrome: Uninstal ekstensi yang tidak Anda kenali dan update Chrome ke versi terbaru.
- Google Drive: Tinjau aktivitas dan versi file yang tidak wajar.
- Google Foto: Jika Anda melihat tindakan berbagi album yang tidak Anda kenali, hentikan berbagi album tersebut.
- Lokasi: Nonaktifkan Berbagi Lokasi yang tampak tidak wajar.

Bantu cegah pencurian sandi dengan Notifikasi Sandi

Jika Anda memasukkan sandi Anda di situs non-Google, Notifikasi Sandi di Google Chrome akan memberi Anda notifikasi. Dengan demikian, Anda akan tahu jika suatu situs berpura-pura menjadi Google untuk mencuri sandi Anda.

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

Source:
https://support.google.com/youtube/topic/3024171?hl=id&ref_topic=9257498