

"CyberSAFE™" KAH ANDA?



TIP & AMALAN TERBAIK KESELAMATAN SIBER

SENTIASA BIJAK, SENTIASA SELAMAT



MELINDUNGI
RUANG SIBER
ANDA

ARAHAN



CyberSAFE™



1. Buka aplikasi "Play Store" di peranti anda.
2. Taip "CyberSAFE" di dalam kotak carian aplikasi.
3. Klik butang "Muat Turun" ataupun "Pasang" untuk memulakan proses memuat turun aplikasi "CyberSAFE".
4. Selepas muat turun selesai, pengguna boleh mengakses aplikasi dengan mengklik butang "Buka" dan mula menggunakan aplikasi secara penuh.

1. *Open "Play Store" application on your device.*
2. *Search for "CyberSAFE" in the search bar.*
3. *Click and Install button to begin the download process of the "CyberSAFE" application.*
4. *After the download completes, users can access the app by clicking "Open" and begin to fully utilize the application.*



1. Buka aplikasi "Play Store" di peranti anda.
2. Taip "CyberSAFE" di dalam kotak carian aplikasi.
3. Klik butang "Install" ataupun "Pasang" untuk memulakan proses memuat turun aplikasi "CyberSAFE".
4. Selepas muat turun selesai, pengguna boleh mengakses aplikasi dengan mengklik butang "Buka" dan mula menggunakan aplikasi secara penuh.

1. *Open "Play Store" application on your device.*
2. *Search for "CyberSAFE" in the search bar.*
3. *Click and Install button to begin the download process of the "CyberSAFE" application.*
4. *After the download completes, users can access the app by clicking "Open" and begin to fully utilize the application.*

PRAKATA

Buku **"CyberSAFE™ KAH ANDA?"** merupakan koleksi Infografik yang dihasilkan oleh CyberSecurity Malaysia bertujuan untuk memberi maklumat berkaitan tip serta amalan terbaik mengenai isu dan permasalahan yang berlaku di alam siber. Ia juga menjadi rujukan atau peringatan awal bagi membendung dari menjadi mangsa ancaman dan serangan siber.

Buku ini merangkumi pelbagai jenis infografik berkaitan ancaman siber semasa yang boleh dijadikan rujukan oleh pengguna sewaktu menggunakan teknologi termasuk Internet dan media sosial.

Koleksi Infografik ini boleh dimuat turun secara percuma melalui laman sesawang CyberSecurity Malaysia (www.cybersecurity.my) manakala, setiap infografik yang dipaparkan juga boleh dimuat turun melalui pautan berikut: www.cybersecurity.my/infographic

Kami berharap agar buku ini dapat memberi manfaat dan digunakan oleh semua pengguna Internet sebagai sumber maklumat dalam usaha meningkatkan pengetahuan dan kefahaman mengenai keselamatan siber.

Panduan serta tip amalan terbaik yang dipaparkan akan dapat membantu pengguna Internet meningkatkan kesedaran, seterusnya menghindari dari menjadi mangsa jenayah siber.

Sentiasa Bijak Sentiasa Selamat, Bersama Ke Arah Kesejahteraan Siber.

CyberSecurity Malaysia

Diterbitkan oleh:
CyberSecurity Malaysia
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

Hak cipta terpelihara. Tidak dibenarkan mengeluarkan ulang mana-mana bahagian artikel, ilustrasi, dan isi kandungan buku ini dalam apa juga bentuk dan dengan cara apa juga sama ada secara elektronik, fotokopi, mekanik, rakaman, atau cara lain sebelum mendapat izin daripada penerbit.

1	Antivirus Di Gajet Anda.....	1
2	Berita Palsu	2
3	Ketirisan Data	3
4	Perlindungan Kata Laluan	4
5	Peraturan 20-20-20.....	5
6	Mengurus Permintaan Rakan Anak-Anak Dalam Talian.....	6
7	Mengelak Anak Anda Dari Menjadi Mangsa Antun Siber	7
8	Detoks Digital	8
9	Mengelak Dari Menjadi Mangsa Hendap Siber.....	9
10	Tip Keselamatan CyberSAFE™ Untuk Kanak-Kanak	10
11	Tip Keselamatan CyberSAFE™ Untuk Remaja.....	11
12	Tip Keselamatan CyberSAFE™ Untuk Ibu Bapa.....	12
13	Apa Yang Anda Perlu Tahu Mengenai Sexting.....	13
14	Hindar Buli Siber Di Media Sosial	14
15	Elak Diri Daripada Digodam.....	15
16	Bekerja Dari Rumah.....	16
17	Permainan Dalam Talian	17
18	Elak Ancaman & Serangan Siber (Peguna Individu).....	18
19	Elak Ancaman & Serangan Siber (Pentadbir Sistem)	19
20	Awas Penipuan Dalam Talian	20
21	Elak Dari Menjadi Mangsa Penipuan Pembelian Dalam Talian	21
22	Tip Kesejahteraan Siber.....	22
23	Tip Untuk Keselamatan Wi-Fi Di Rumah	23
24	Etika Siber: Jauhi Kandungan Yang Tidak Sesuai.....	24
25	Pengendalian Akaun Media Sosial (Individu).....	25
26	Transaksi Perbankan Dalam Talian.....	26
27	Keselamatan Penggunaan Aplikasi Persidangan Video Dalam Talian	27
28	Tip Penjagaan Media Storan Digital Akibat Banjir	28
29	Tip Keselamatan TikTok Untuk Ibu Bapa	29
30	Laporkan Insiden Buli Siber Ke Saluran Berikut	31
31	Membentuk Tingkah Laku Anak Dalam Talian.....	32
32	Pastikan Maklumat Itu Sahih Sebelum Kongsi	33
33	Buli Siber Salah Di Sisi Undang-Undang.....	34
34	Keibubapaan Siber	35
35	Berita Palsu: Jangan Sebar Berita Tidak Benar	36
36	Fikir Sebelum Menaip.....	37
37	Ingat Jejak Digital	38
38	Lindungi Privasi Digital Anda.....	39
39	Keibubapaan Siber	40
40	Buli Siber	41
41	Amalkan Etika Siber	42
42	Etika Siber.....	43
43	Guna Internet Secara Berhemah	44
44	Kecurian Data	45
45	Telegram Kene Godam	46
46	Ketirisan Maklumat di 'Dark Web'.....	47
47	Ketagihan Internet	48
48	Awas Serangan Siber	49

CyberSAFE™

ANTIVIRUS DI GAJET ANDA



ELAK JANGKITAN MALWARE PADA GAJET DIGITAL ANDA.

Jangan gunakan perisian crack/keygen setelah tempoh percubaan perisian antivirus tamat

Lengkap gajet digital anda dengan perisian antivirus terkini

Pilih perisian antivirus yang popular berbanding perisian antivirus yang kurang popular

Sentiasa periksa perisian antivirus supaya gajet dapat berfungsi dengan selamat setiap waktu

Dapatkan perisian antivirus daripada sumber yang sah sebelum dimuat turun

Pastikan fungsi kemaskini automatik diaktifkan agar perisian antivirus sentiasa dikemaskini kepada versi terkini

Muat turun perisian antivirus daripada laman sesawang rasmi perisian antivirus tersebut

Jangan memuat turun lebih daripada satu perisian antivirus ke dalam gajet digital anda



AR

BERITA PALSU

FAKE NEWS



**HINDAR DARI SEBAR BERITA PALSU,
PADAHNYA IALAH HUKUMAN
UNDANG-UNDANG.**

**JANGAN MUDAH
TERPEDAYA** dengan
e-mel, mesej and
maklumat yang diterima



PASTIKAN e-mel, maklumat
& mesej dari sumber yang
dipercayai (seperti pihak
berkuasa atau individu yang
ada kredibiliti)



SENTIASA PERIKSA
kesahihan e-mel, mesej
and maklumat tersebut



SIASAT latar belakang
pengirim e-mel, mesej &
maklumat atau
penyebarnya maklumat



INGAT, bukan semua
maklumat di Internet
dan laman media
sosial itu benar



Jika **TIDAK PASTI**,
JANGAN KONGSI! Semak
maklumat sahih di
<https://sebenarnya.my>



SEBENARNYA.MY
Tidak Pasti Jangan Kongsi



AR

CyberSAFE™

KETIRISAN DATA

Ketirisan data membawa pelbagai implikasi kepada organisasi seperti reputasi, risiko keselamatan, masalah kewangan, kepercayaan dan integriti, ancaman siber serta gangguan operasi.

AMBIL LANGKAH BERIKUT UNTUK ELAK DARI BERLAKUNYA KETIRISAN DATA

PATUHI peraturan perlindungan data

LAKUKAN penilaian kerentanan secara berkala

SENTIASA PEKA dengan perkembangan keselamatan siber

LAKUKAN konfigurasi pangkalan data dan repositori awan

KEMAS KINI perisian secara berkala

LENGKAPKAN DIRI dengan kemahiran melalui program latihan

PASANG tembok api (firewall), pengesan pencerobohan dan sistem antivirus



PERLINDUNGAN KATA LALUAN

TIP UNTUK MEMBINA DAN MELINDUNGI KATA LALUAN:

01

BINA kata laluan yang mempunyai sekurang-kurangnya **8 aksara dengan kombinasi nombor, simbol, huruf besar dan huruf kecil**



02

ELAK daripada menggunakan perkataan atau istilah yang berkaitan dengan diri anda (seperti tarikh lahir, tempat lahir, hobi, nama ibu / ayah / anak)



D.O.B

03

JANGAN bina kata laluan menggunakan perkataan yang terdapat di dalam kamus



04

JANGAN kongsi kata laluan dengan sesiapa



05

UBAH kata laluan anda sekurang-kurangnya **3 ke 6 bulan sekali**



06

BEZAKAN setiap kata laluan bagi setiap akaun yang anda akses (e-mel dan akaun sosial media)



CyberSAFE™

PERATURAN 20-20-20

Penggunaan gajet digital yang berlebihan boleh menyebabkan rabun jauh pada kanak-kanak serta 'Digital Eye Syndrome' (DES) seperti kabur penglihatan, ketegangan, keletihan mata, kekeringan dan mata menjadi merah serta sakit kepala.

Antara tip mengurangkan kesan penggunaan gajet digital pada penglihatan adalah:

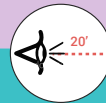
AMALKAN peraturan 20-20-20



Selepas penggunaan
gajet digital selama
20 minit



Rehat selama 20 saat



Lihat sejauh 20 kaki



KELIPKAN mata secara
kerap untuk elak mata
menjadi kering



PASTIKAN jarak
penglihatan dengan gajet
digital tidak kurang dari 18
inci (untuk kanak-kanak)



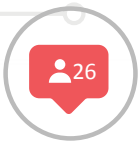
BUAT pemeriksaan mata
untuk elak daripada
menjadi rabun (untuk
kanak-kanak)

Sumber: Buku Cyberparenting – Ke Arah Kesejahteraan Siber 2019

Tip Keibubapaan:

Mengurus Permintaan Rakan Dalam Talian Bagi Anak-Anak

Anak-anak masa kini melihat satu keistimewaan apabila mempunyai ribuan pengikut dan rakan di media sosial



Berbincang berkaitan implikasi menerima permintaan menjadi rakan



Mengadakan garis panduan Internet di rumah



Memberi peringatan untuk menyekat dan melapor orang tidak dikenali



Memberitahu orang dewasa yang dipercayai jika mereka berhadapan situasi yang tidak selesa dalam talian



Sumber: <https://www.childnet.com/blog/how-to-help-children-and-young-people-manage-friend-requests-online->

TIP CyberSAFE™

MENGELAK ANAK ANDA DARI MENJADI MANGSA ANTUN SIBER

**1**

AMBIL TAHU

Sentiasa mengambil tahu dengan siapa anak-anak berkomunikasi di alam siber khususnya anak-anak di bawah umur.

2

BERITAHU

Sentiasa beritahu anak-anak adanya penjenayah siber di dalam talian yang menyamar sebagai orang yang baik.

3

BERWASPADA

Sentiasa lihat dan semak platform media sosial yang anak-anak gunakan.

4

PESANAN

Sentiasa pesan kepada anak-anak untuk memaklumkan kepada anda jika mereka berasa diganggu oleh orang dewasa.

5

PERHATIKAN

Sentiasa perhatikan kelakuan dan perubahan drastik yang berlaku pada anak-anak anda.

Sentiasa Bijak, Sentiasa Selamat
CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my



Sentiasa Bijak, Sentiasa Selamat
CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my

TIP CyberSAFE™

DETOKS DIGITAL



1 SENTIASA FOKUS

TUTUP fungsi paparan notifikasi di telefon anda untuk kekal fokus dan tidak terganggu melihat skrin telefon

2 MASA BERKUALITI

SIMPAN telefon sewaktu makan dan luangkan masa yang berkualiti bersama keluarga.

3 URUS MASA

JADUALKAN masa bebas gajet sewaktu menonton televisyen dan menghadiri acara keluarga untuk menghormati privasi dan tingkatkan kesejahteraan.

4 REHAT YANG CUKUP

KENALI kawasan tanpa teknologi contohnya di bilik tidur untuk rehat yang cukup demi kesihatan anda.

5 BACA BUKU

AMALKAN tabiat membaca buku kerana ia dapat menghadkan masa skrin.

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my

TIP CyberSAFE™

MENGELAK DARI MENJADI MANGSA HENDAP SIBER

RAHSIA

Bagi mereka yang bekerja dan mempunyai perniagaan, rahsiakan alamat rumah.

Sebaiknya, gunakan alamat tempat kerja ataupun alamat Peti Surat.

KATA LALUAN

Sentiasa amalkan penggunaan kata laluan yang kukuh dan sukar untuk diteka di semua akaun sosial media dan akaun transaksi dalam talian.

CARIAN

Jika anda was-was dengan kenalan baharu, lakukan carian di Google profil dan imej untuk mengetahui kesahihan kenalan tersebut.

MENGIMBAS KOMPUTER

Jika anda berasa mengalami hendap siber, lakukan imbasan komputer anda. Mungkin komputer anda telah di tanam dengan spyware.

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE

Cyber Security Awareness For Everyone

www.cybersafe.my

TIP KESELAMATAN CyberSAFE™ UNTUK KANAK-KANAK

1/ **TIDAK KENAL**

Tidak bersembang dengan orang tidak dikenali semasa dalam talian.

2/ **JANGAN KONGSI**

Tidak memberikan nama, alamat rumah atau nombor telefon kepada orang yang tidak dikenali dalam talian.

3/ **KATA LALUAN**

Hanya berkongsi kata laluan dengan ibu bapa.

4/ **BERSIKAP POSITIF**

Menghormati orang lain dan berkongsi kandungan yang baik.

5/ **LAPOR**

Memberitahu ibu bapa atau guru jika berasa kurang selesa dengan rakan dalam talian.



TIP KESELAMATAN CyberSAFE™ UNTUK REMAJA



1/ **AWAS**

Waspada dengan taktik penipuan dalam talian.

2/ **FIKIR**

Berfikir dahulu sebelum berkongsi maklumat dengan orang lain.

3/ **SEIMBANG**

Imbangi masa belajar dan berhibur.

4/ **LAPOR**

Membuat laporan terhadap kandungan berunsur gangguan di platform media sosial.

5/ **KAWAL KENDIRI**

Elak dari membuat kecaman atau komen berunsur perkauman, keagamaan atau institusi di raja.



AR

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE

Cyber Security Awareness For Everyone

www.cybersafe.my

TIP KESELAMATAN CyberSAFE™ UNTUK IBU BAPA

1/ PANTAU

Sentiasa pantau aktiviti anak-anak dalam talian.

2/ BINCANG

Sentiasa berbincang dengan anak-anak tentang ancaman alam siber.

3/ MUAT TURUN

Menggunakan aplikasi kawalan ibu bapa sebagai langkah membantu pengawasan.

4/ TELADAN

Menunjukkan contoh keseimbangan digital yang baik dengan melakukan aktiviti bersama anak-anak.

5/ KAWAL

Hanya membenarkan masa skrin yang sepatutnya untuk anak-anak.



TIP CyberSAFE™

APA YANG ANDA PERLU TAHU MENGENAI SEXTING



CyberSAFE

Sexting boleh mengakibatkan penderaan seksual kanak-kanak 🙄

Sexting boleh membawa kepada pembulian seksual 😞

Sexting membuka pintu kepada penjenayah seksual 😞

Sexting boleh mengancam remaja dengan ugutan seksual 😞

Sexting tidak akan pernah terpadam di dalam talian 😞

Sexting mampu merosakkan reputasi seseorang 🙄

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my**AR**

TIP CyberSAFE™

HINDAR BULI SIBER DI MEDIA SOSIAL



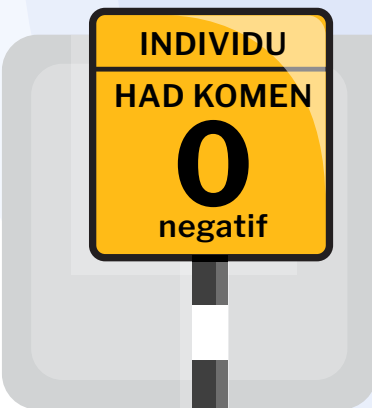
TUNJUKKAN SIKAP SOPAN DAN EMPATI

Contoh yang baik bermula dengan anda, muat naik hanya komen positif dan optimis.



TUTUP RUANGAN KOMEN

Bersikap terbuka semasa membaca komen, negatif atau positif.



HADKAN KOMEN

Hadkan hanya individu tertentu untuk memberi dan membaca komen untuk membentuk aura positif.



SINGKIRKAN INDIVIDU YANG MEMBUAT KOMEN NEGATIF

Wujudkan suasana positif di media sosial dengan menyingkirkan individu yang membuat komen negatif.

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE
Cyber Security Awareness For Everyone

www.cybersafe.my

TIP CyberSAFE™

ELAK DIRI DARIPADA DIGODAM



ELAK daripada menggunakan Wi-Fi awam

KEMAS KINI perisian operasi dan aplikasi di dalam gajet anda

JANGAN simpan segala data peribadi di dalam gajet anda

GUNAKAN kata laluan yang kukuh

AKTIFKAN penggunaan dua langkah pengesahan

MEMUAT TURUN DAN PASANG aplikasi dari sumber yang sah

ABAIKAN segala bentuk Spam



AR

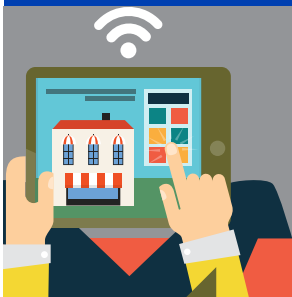
Sentiasa Bijak, Sentiasa Selamat
CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my

TIP CyberSAFE™ BEKERJA DARI RUMAH

Sentiasa Selamat, Sentiasa Sihat, CyberSAFE™ diri anda dengan :



WASPADA
Berhati-hati dengan ancaman siber.



Wi-Fi

Jangan guna Wi-Fi awam. Guna sambungan internet di rumah atau rangkaian mudah alih atau Virtual Private Network (VPN).

DOKUMEN

Jangan sekali-kali menggunakan aplikasi percuma untuk menghantar dokumen rasmi.



PENDUA

Sentiasa buat data pendua (Back up) terutama apabila bekerja dari rumah.



JADUAL

Sentiasa susun jadual kerja anda.



LAPOR

Jika berlaku pencerobohan, hubungi Jabatan IT pejabat anda dan buat laporan atau hubungi talian cyber999.

MASA

Pilih masa yang paling produktif untuk bekerja.



KATA LALUAN

Pastikan semua kata laluan pada sistem dikemas kini, disahkan dan selamat.



Sentiasa Bijak, Sentiasa Selamat

CyberSAFE
Cyber Security Awareness For Everyone
www.cybersafe.my

IMBAS

Guna perisian anti-virus untuk mengimbas fail yang anda muat turun ke dalam komputer atau peranti anda.

SEMAK

Sebelum anda mula bermain, semak dahulu aplikasi permainan sekiranya terdapat virus atau *malware* yang boleh mengganggu sistem peranti anda.

HATI-HATI

Permainan dalam talian membolehkan anda berinteraksi antara satu sama lain, namun berhati-hati dengan pembuli siber yang membuatkan anda rasa tidak selesa.

REHAT

Setiap 20 minit, rehatkan mata anda daripada melihat skrin komputer, telefon atau televisyen. Lihat objek lain sejauh 20 kaki selama 20 saat.

IDENTITI

Jangan dedahkan identiti sebenar anda apabila bermain permainan dalam talian. Anda boleh menggunakan nama samaran yang tidak mudah dikenali.



TIP **CyberSAFE™** PERMAINAN DALAM TALIAN

Sentiasa Bijak, Sentiasa Selamat

CyberSAFE

Cyber Security Awareness For Everyone

www.cybersafe.my

AMALAN TERBAIK

UNTUK ELAK ANCAMAN & SERANGAN SIBER

PENGUNA INDIVIDU



Jangan klik pada pautan atau lampiran (imej dan video) di dalam e-mel serta laman media sosial



Pasang perisian anti-virus di dalam peranti dan kemaskini secara berkala



Putuskan sambungan kepada Wi-Fi awam setelah selesai digunakan



Perkukuh dan perbaharui kata laluan setiap 3 atau 6 bulan sekali



Guna rangkaian yang selamat apabila melakukan transaksi dalam talian (perbankan atau pembelian Internet)



Log keluar daripada e-mel, media sosial dan lain-lain; bukan sekadar menutup pelayar web



Putuskan sambungan Bluetooth jika tidak digunakan

AMALAN TERBAIK

UNTUK ELAK ANCAMAN & SERANGAN SIBER

PENTADBIR SISTEM



Kemaskini dan naik taraf sistem pengoperasian dan aplikasi anda



Lakukan pemeriksaan dan pengukuhan terhadap sistem pelayan



Buat salinan pendua bagi semua maklumat penting secara berkala



Sentiasa aktifkan sistem log server



Laksanakan strategi keselamatan untuk melindungi sistem aplikasi dan rangkaian

AWAS PENIPUAN DALAM TALIAN

AMBIL LANGKAH BERIKUT BAGI MENANGANINYA:



- 1** Semak kesahihan maklumat yang diterima melalui e-mel & mesej teks (Whatsapp, Telegram) mengenai COVID-19.



- 2** Jangan kongsi maklumat peribadi/data kewangan melalui e-mel & mesej teks.



- 3** Jangan beri maklumbalas terhadap permintaan maklumat sulit/peribadi melalui e-mel & mesej teks dari pengguna tidak dikenali.



- 4** Jangan muat turun pautan dari e-mel & mesej teks dari pengguna tidak dikenali.



- 5** Rujuk hanya kepada sumber yang dipercayai, iaitu laman web atau saluran yang diperakui oleh Kerajaan untuk sahkan maklumat terkini mengenai COVID-19.



- 6** Pastikan gajet ICT dipasang dan dikemaskini dengan perisian antivirus kepada tetapan pangkalan data antivirus terkini.



- 7** Lapor insiden/ancaman siber ke Pusat Rujukan Insiden Siber Cyber999 di saluran berikut:



Telefon:
1-300-88-2999 (waktu pejabat)



E-mel:
cyber999@cybersecurity.my



Mobile:
+60 19 - 266 5850
(24x7 panggilan laporan insiden kritikal sahaja)



Aplikasi Cyber999:
Muat turun aplikasi di Appstore & Google Play



AR

ELAK DARI MENJADI MANGSA PENIPUAN



PEMBELIAN DALAM TALIAN



Semak *profile* penjual - pastikan ada maklumat dipaparkan pada laman penjual



Buat perbandingan harga terlebih dahulu, jangan terpedaya dengan tawaran harga yang menarik



Baca dengan teliti, **fahami terma dan syarat** pembelian serta semak jaminan atau polisi '*return/refund*'



Semak pengesahan pesanan sebelum klik setuju dengan pembelian



Semak tanda atau simbol pengesahan keselamatan urusan pada laman penjual *online*



Baca komen serta testimoni pembeli pada laman penjual *online* (jika ada)



Jangan lakukan pembelian melalui komputer awam (kafe siber)



Beli dari penjual *online* **yang dipercayai** dan mempunyai reputasi yang baik



Simpan maklumat pembelian untuk rujukan di masa akan datang



1 Hormati diri anda dan orang lain di dalam talian

Kongsi hanya perkara yang baik dan sentiasa waspada semasa membuat hantaran maklumat di dalam talian

TIP

KESEJAHTERAAN SIBER

2 Sentiasa selamat di dalam talian

Kenal pasti rakan siber anda kerana kadangkala mereka mungkin akan mengancam diri anda

4 Bersuara dan lapor

Sekiranya anda berhadapan dengan aktiviti dalam talian yang mencurigakan, maklumkan kepada orang yang anda percaya atau lapor kepada pihak berkuasa

3 Kekal berhubung dengan dunia sebenar

Luangkan masa dengan melakukan aktiviti fizikal dan bergembira bersama keluarga serta rakan taulan

5 Tetapkan matlamat penggunaan Internet

Berehat sekurang-kurangnya 5 minit setiap jam untuk melakukan aktiviti fizikal. Belajar untuk menghargai dunia sebenar

**AR**

TIP UNTUK KESELAMATAN WI-FI DI RUMAH



Tukar nama pengguna dan kata laluan yang diberi oleh penyedia WiFi kepada nama dan kata laluan anda



Padamkan rangkaian Wi-Fi jika anda tiada di rumah



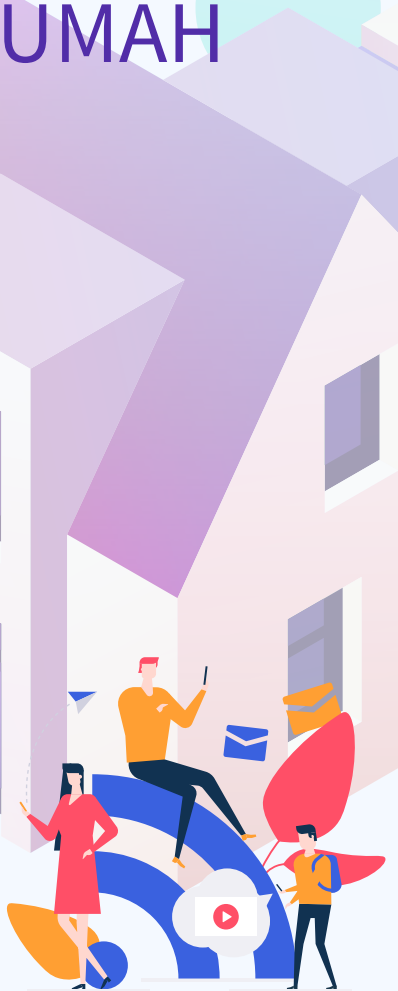
Aktifkan penyulitan rangkaian tanpa wayar untuk melindungi data rangkaian anda



Guna perisian tembok api bagi melindungi peranti digital di rumah



Pastikan perisian 'router' anda dikemaskini untuk keselamatan rangkaian internet di rumah anda



CyberSAFE™ ETIKA SIBER

JAUHI KANDUNGAN YANG TIDAK SESUAI

ELAK

dari melayari kandungan berunsur lucah, ganas, cacian, makian, rasis, hasutan

JANGAN

- Memuat turun kandungan yang tidak berfaedah
- Simpan kandungan yang tidak sesuai di dalam gajet digital anda
- Kongsi isi kandungan yang tidak sesuai dengan rakan-rakan
- Komen atau kecam status dan kandungan yang tidak sesuai

LAPORKAN

kepada pihak berkuasa jika anda terima kandungan yang tidak sesuai termasuk yang menyentuh isu sensitif seperti agama, perkauman, bahan lucah dan lain-lain



AMALAN TERBAIK PENGENDALIAN AKAUN MEDIA SOSIAL (INDIVIDU)



Bina kata laluan yang kukuh bagi memastikan ia sukar digodam



Jangan benarkan individu lain guna identiti dan kata laluan akaun anda



Keluar (*logout*) dari akaun media sosial setelah selesai digunakan



Elak berkongsi maklumat peribadi secara berlebihan di media sosial



Elak dari memuat turun aplikasi yang tidak diketahui tahap keselamatan



Tetapkan keselamatan profile yang bersesuaian



Pasang perisian keselamatan seperti AV dan tetapkan keselamatan terkini pada telefon mudah alih



Aktifkan '*Multi-Factor-Auntentication*' untuk keselamatan yang lebih kuat

PATUHI AMALAN TERBAIK DAN GARIS PANDUAN KESELAMATAN APABILA MELAKUKAN

TRANSAKSI PERBANKAN DALAM TALIAN



- 1 GUNAKAN perisian *Video Teleconference* (VTC) terkini yang mempunyai reputasi
- 2 MUAT TURUN perisian VTC dari laman sesawang rasmi dan sumber yang sahih sahaja
- 3 JANGAN gunakan perisian cetak rompak
- 4 PANTAU sesi *teleconferencing* dan pastikan peserta yang dibenarkan sahaja

An illustration showing various devices used for video conferencing: a laptop, a tablet, and a smartphone. Each device displays a person in a video call. There are also speech bubbles and a heart icon. The background features a faint world map and a network of connected nodes.

GARIS PANDUAN KESELAMATAN PENGGUNAAN APLIKASI PERSIDANGAN VIDEO DALAM TALIAN

- 5 LINDUNGI sesi *teleconferencing* dengan kata laluan yang kukuh
- 6 ELAKKAN daripada berbincang perkara-perkara sulit dan sensitif
- 7 ELAKKAN perkongsian dokumen sulit dan sensitif
- 8 JANGAN kongsi pautan atau ID VTC dengan orang lain



AR

TIP PENJAGAAN MEDIA STORAN DIGITAL

LANGKAH-LANGKAH YANG PERLU
DILAKUKAN SEWAKTU MENGENDALIKAN MEDIA STORAN
DIGITAL YANG ROSAK AKIBAT BANJIR.



1. BERTINDAK SEGERA

Untuk mengelakkan karat, bertindak segera bagi mendapat peluang pemulihan data yang lebih tinggi.



2. UTAMAKAN KESELAMATAN

Pastikan peranti digital dicabut dari palam sumber kuasa apabila mengeluarkan cakera keras daripada komputer.



3. JANGAN HIDUPKAN PERANTI

Jangan cuba menghidupkan peranti digital dan media storan anda kerana akan memburukkan lagi kerosakan.



4. PASTIKAN MEDIA STORAN DIGITAL SEPERTI SEDIA KALA

Jangan keringkan, bersihkan atau basuh media storan digital yang terjejas oleh banjir kerana sangat sensitif dan terdedah kepada calar yang boleh memusnahkan data yang disimpan.



5. JANGAN DIY (BUAT SENDIRI)

Media storan digital yang rosak akibat banjir memerlukan penyelesaian dan prosedur pembersihan khusus termasuk persekitaran bilik yang bersih untuk memulihkan data.



6. KEDAPKAN ALAT MEDIA STORAN

Adalah dinasihatkan untuk masukkan media storan digital di dalam beg plastik kedap udara.



7. DAPATKAN BANTUAN PROFESIONAL

Dapatkan bantuan profesional untuk memulihkan media storan digital yang rosak akibat banjir.

TIP KESELAMATAN TIKTOK UNTUK IBU BAPA



Ibu bapa perlu memastikan anak-anak mereka menggunakan TikTok dengan selamat. Ikuti panduan ibu bapa ini untuk menguruskan akses anak-anak di TikTok.



1 LAKUKAN TETAPAN PRIVASI TERHADAP AKAUN ANAK ANDA

LANGKAH 1

Pergi ke halaman profil

LANGKAH 2

Tekan pada 3 titik yang berada di atas kanan skrin

LANGKAH 3

Pilih "Tetapan dan Privasi"

LANGKAH 4

Pilih "Privasi" dan hidupkan pilihan "Akaun Peribadi"

2 AKTIFKAN TETAPAN PENGURUSAN MASA SKRIN DAN MOD TERBATAS BAGI KESEJAHTERAAN DIGITAL

LANGKAH 1

Pilih "Privasi" di "Tetapan dan Privasi"

LANGKAH 2

Tekan pada "Komen" di bawah pilihan "Keselamatan"

LANGKAH 3

Pilih "Rakan" atau "Tiada Siapa" di bawah "Siapa Boleh Komen Video Anda" untuk menghadkan komen kepada orang yang dikenali anak anda dalam aplikasi

LANGKAH 4

Anda juga boleh menutup sebarang komen di video tertentu dengan mematikan pilihan "Benarkan komen" di butang menu

3 BENARKAN HANYA PENGIKUT AKAUN ANDA UNTUK MEMBUAT KOMEN ATAU TUTUP RUANG KOMEN SEPENUHNYA

LANGKAH 1

Pilih "Privasi" di "Tetapan dan Privasi"

LANGKAH 2

Tekan pada "Mesej Langsung" di bawah pilihan "Keselamatan"

LANGKAH 3

Pilih "Rakan" atau "Tiada Siapa" di bawah "Siapa Boleh Hantar Mesej Langsung"

TIP KESELAMATAN **TIKTOK** UNTUK IBU BAPA

4

HADKAN PASANGAN DUET ANAK-ANAK HANYA KEPADA PENGIKUT ANDA YANG MELIPUTI SEMUA VIDEO

LANGKAH 1

Pilih "Kesejahteraan Digital" di "Tetapan dan Privasi"

LANGKAH 2

Hidupkan pilihan "Pengurusan Masa Skrin" dan "Mod Terbatas"

LANGKAH 3

Masukkan kod laluan untuk kedua-dua pilihan tersebut

5

HADKAN ATAU MATIKAN PENGHANTARAN MESEJ KE AKAUN TIKTOK ANAK-ANAK ANDA DALAM TETAPAN PRIVASI DAN KESELAMATAN

LANGKAH 1

Pilih "Privasi" di "Tetapan dan Privasi"

LANGKAH 2

Tekan pada "Duet" di bawah pilihan "Keselamatan"

LANGKAH 3

Pilih "Rakan" atau "Hanya Saya" di bawah "Siapa Boleh Duet dengan Video Anda"

6

LAPORKAN DAN SEKAT AKAUN PENGGUNA DENGAN SEGERA KEPADA PENTADBIR PLATFORM ATAU AGENSI PENGUATKUASAAN UNDANG-UNDANG SEKIRANYA MEREKA MELANGGAR KESELAMATAN ANAK-ANAK ANDA

LAPOR PENGGUNA

LANGKAH 1

Tekan pada 3 titik di bahagian atas skrin profail pengguna tersebut

LANGKAH 2

Pilih sekat atau laporkan

LANGKAH 3

Pilih sebab laporan dibuat

LAPOR KOMEN

LANGKAH 1

Tekan seketika pada komen tersebut

LANGKAH 2

Pilih "Laporkan" dan ikuti arahan selanjutnya

LAPOR VIDEO

LANGKAH 1

Pergi ke video

LANGKAH 2

Tekan ikon kongsi

LANGKAH 3

Tekan "Laporkan" dan ikuti arahan selanjutnya

LAPORKAN

INSIDEN BULI SIBER

KE SALURAN BERIKUT:



1

**Polis Diraja Malaysia (PDRM)**

Pengadu boleh hadir ke balai polis berhampiran bagi pembukaan kes dengan laporan secara bertulis

2

**Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM)**

Pengadu boleh email kepada aduanskmm@mcmc.gov.my

Talian bebas tol 1-800-188-030

3

**TALIAN Kasih
15999****Talian Kasih Kementerian Pembangunan Wanita, Keluarga dan Masyarakat (KPWKM)**

Pengadu boleh menelefon talian 15999 yang dibuka 24 jam

Menggunakan aplikasi WhatsApp 019 - 261 5999

4

**Talian Sokongan Psikososial**

03 - 2935 9935

014 - 322 3392

011 - 639 96482

011 - 639 94236

5

BeFriends
Kuala Lumpur**Talian BeFriends**

Panggilan percuma ke talian 24 jam
03 - 762 72929

www.befriends.org.my

6

**Platform Media Sosial
(FaceBook, Twitter, Instagram)**

www.facebook.com/help/report

How to report abusive behavior on Twitter | Twitter Help

Report Tweet

Penyalahgunaan dan Spam | Pusat Bantuan Instagram

7

Cyber999**Laporkan juga insiden keselamatan siber berkaitan isu-isu teknikal juga boleh terus disalurkan kepada Pusat Rujukan Insiden Siber Cyber999**

Telefon:
1-300-88-2999
(Waktu Pejabat)

E-mel:
cyber999@cybersecurity.my

Mobile:
+60 19 - 266 5850
(24x7 panggilan laporan insiden kritikal sahaja)

Aplikasi Cyber999:
Muat turun aplikasi di Appstore & Google Play



TIP BAGI MEMBENTUK TINGKAH LAKU DALAM TALIAN YANG BAIK UNTUK ANAK ANDA

Cara terbaik bagi ibu bapa untuk melindungi anak-anak daripada kebencian dalam talian dan hasut maya adalah dengan menunjukkan minat terhadap aktiviti sosial mereka dalam dan luar talian.



Pastikan mereka tahu bagaimana memperlakukan orang lain sebagaimana mereka mahu diperlakukan

Menasihati mereka agar tidak menyebarkan kandungan yang berbau kebencian atau ancaman dalam talian

Beritahu mereka untuk tidak mengatakan sesuatu dalam talian yang tidak akan mereka katakan secara bersemuka

Pastikan mereka tahu tentang panduan komuniti pada setiap platform yang digunakan seperti Instagram dan Facebook

Memastikan mereka dapat mengenalpasti kandungan dalam talian yang berbau kebencian ketika kejadian itu berlaku

Galakkan anak-anak supaya mempunyai bersikap terbuka dan rasa ingin tahu yang jujur terhadap orang lain

Pastikan anak-anak sentiasa mengamalkan penggunaan bahasa yang sopan dalam perbualan

Sumber: www.internetmatters.org



PASTIKAN MAKLUMAT ITU SAHIH DAN DARI SUMBER YANG DIPERCAYAI SEBELUM KONGSI

- Jangan klik pautan dari sumber yang meragukan
- Sentiasa periksa kesahihan e-mel, mesej dan maklumat
- Siasat latar belakang pengirim atau penyebar maklumat

Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

BULI SIBER

SALAH DI SISI
UNDANG-UNDANG



SEBARKAN
POSITIVITI
UNTUK
PERSEKITARAN SIBER YANG
HARMONI



Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber



Sebagai ibu bapa, anda adalah contoh utama bagi anak-anak anda.

Amalkan Etika Digital untuk kesejahteraan dan keharmonian keluarga.

KEIBUBAPAAAN SIBER

Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

JANGAN SEBAR BERITA TIDAK BENAR

kerana ia mampu menimbulkan suasana panik dan menggugat kesejahteraan dan keselamatan negara.

BERITA PALSU



Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

JARI MUNGKIN LEBIH
TAJAM DARI LIDAH

**FIKIR SEBELUM
MENAIP**

**SENTIASA BIJAK,
SENTIASA SELAMAT**
BERSAMA KE ARAH
KESEJAHTERAAN SIBER



INGAT JEJAK DIGITAL

Berhati hati dalam berkongsi
maklumat di media sosial

Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

LINDUNGI PRIVASI DIGITAL ANDA

Jadilah seorang pengguna Internet yang bijak.

Amalkan langkah terbaik bagi memperkukuhkan privasi dalam talian bagi menjamin keselamatan diri anda dan keluarga.



Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

KEIBUBAAPAAN SIBER

Amalan yang baik bermula dari rumah.
Tunjukkan budaya positif kepada anak
anda semasa berada di alam siber.



Sentiasa Bijak, Sentiasa Selamat
Bersama Ke Arah Kesejahteraan Siber

BULI SIBER

Ibu bapa perlu menerapkan nilai-nilai murni semasa melayari internet dan media sosial.

Elakkan menjadi mangsa dan juga pemangsa salah laku siber



AMALKAN ETIKA SIBER

Jadi pengguna siber yang berhemah. Sentiasa berwaspada dan segera laporkan sekiranya terdapat kandungan yang tidak berfaedah.



ETIKA SIBER

Amalkan Etika Siber sebagai satu budaya sewaktu anda berada di dalam talian. Kekal positif, berhemah dan saling hormat menghormati.



GUNA INTERNET SECARA BERHEMAH. ELAK DARI MENJADI MANGSA SALAH LAKU INTERNET



Jika anda menghadapi ancaman dan insiden keselamatan siber, laporkan ke Pusat Rujukan Insiden Siber Cyber999 melalui saluran berikut:

 **Cyber999**



Telefon:
1-300-88-2999 (waktu pejabat)



E-mel:
cyber999@cybersecurity.my



Mobile:
+60 19 - 266 5850
(24x7 panggilan laporan insiden kritikal sahaja)



Aplikasi Cyber999:
Muat turun aplikasi di Appstore & Google Play





KECURIAN DATA

MAKLUMAT YANG BOLEH DICURI

1. Nama penuh
2. No IC
3. No kad bank bersama CVV
4. Alamat rumah
5. No telefon
6. Kata laluan aplikasi/laman sesawang
7. Maklumat dalaman organisasi



CARA MENDAPATKAN DATA SECARA HARAM

1. Penggodaman data.
2. Pembelian data secara haram.
3. Pengumpulan maklumat dari media sosial.

KESAN-KESAN KECURIAN DATA

*Dengan data peribadi
berkenaan, penjenayah boleh*

1. Melakukan urusan jual beli menggunakan maklumat yang dicuri.
2. Melakukan urusan peminjaman bank yang boleh menjejaskan mata kredit.
3. Mengambil alih akaun peribadi sosial media dan menghalang dari diakses.
4. Melakukan penipuan atas talian.

CARA MENGATASI

1. Baca dan teliti terma dan syarat berkaitan dengan perkongsian dan penyimpanan data
2. Elakkan menekan pautan URL yang tidak dikenali
3. Elakkan terlalu mendedahkan maklumat di media sosial
4. Menetapkan kata laluan yang baik dan tukar kata laluan setiap enam bulan sekali
5. Log keluar (log out) laman sesawang selepas melakukan urusan atas talian



Laporkan jenayah kecurian data ke **Pusat Rujukan Siber**  **Cyber999**
Layari laman sesawang www.mycert.org.my untuk maklumat lanjut.

ALAMAK TELEGRAM KENA GODAM!



Kenalpasti jika akaun telegram anda melakukan suatu aktiviti yang mencurigakan.

TANDA - TANDA TELEGRAM DIGODAM

1. Akaun telegram tidak dapat diakses
2. Video, mesej dan gambar dihantar ke kontak lain tanpa pengetahuan anda
3. Telegram meminta 'detail' anda setiap kali anda login akaun
4. Mendapat SMS ataupun 'notification' yang akaun Telegram diakses dari gajet lain yang bukan kepunyaan anda

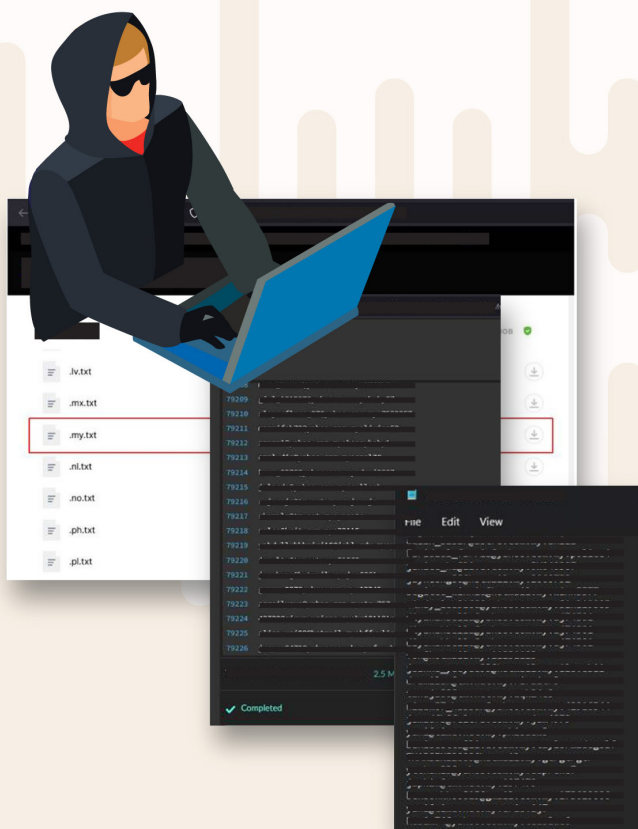


LAKUKAN PERKARA BERIKUT

1. Tetapkan 'Two-Step Verification' pada akaun telegram
2. Log keluar akaun telegram jika membukanya dengan gajet awam
3. Jangan dedahkan kod OTP telegram
4. 'Reset' atau nyahaktif akaun telegram anda jika anda kenalpasti akaun melakukan aktiviti yang mencurigakan
5. Laporkan kepada pihak polis jika penggodaman telegram melibatkan wang dan nyawa

PERINGATAN!

Awas ketirisan maklumat yang melibatkan data warga Malaysia di **'Dark Web'.**



Orang ramai digesa untuk **mengambil langkah proaktif** dengan **menukar kata laluan emel** bagi melindungi maklumat dari digodam dan disalahgunakan oleh pihak yang tidak bertanggungjawab.

KETAGIHAN INTERNET

Pengurusan masa skrin bukanlah satu-satunya penyelesaian. Kita juga harus menggalakkan anak-anak kita untuk membentuk tabiat positif dalam kehidupan seharian mereka dan belajar menggunakan masa dengan bijak.





AWAS SERANGAN SIBER

- Pasang program antivirus pada peranti anda dan pastikan ia sentiasa dikemaskini.
- Muat turun perisian antivirus hanya dari sumber yang dipercayai.
- Elakkan memasang beberapa program antivirus pada peranti anda.

CyberSecurity Malaysia

Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia

Tel: +603 8800 7999

Fax: +603 8008 7000

Email: info@cybersecurity.my

Customer Service Hotline: 1 300 88 2999

www.cybersecurity.my

 @cybersecuritymy

 CyberSecurityMalaysia

 cybersecurity_malaysia

 CyberSecurityMy

© CyberSecurity Malaysia 2023 – All Rights Reserved



KEMENTERIAN
KOMUNIKASI DAN DIGITAL

ISBN 978-967-0118-12-3



9 789670 118123

