KESELAMATAN DALAM TALIAN
UNTUK KANAK-KANAK
PANDUAN BAGI IBU BAPA

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Brunei Computer Emergency Response Team (BruCERT) ditubuhkan pada tahun 2004 dan menjadi agensi rujukan sehenti pertama negara yang diberi kepercayaan untuk mengurus insiden sekuriti yang berkaitan dengan komputer dan internet di Brunei Darussalam.

BruCERT merupakan hab utama yang membuat koordinasi dengan CERT antarabangsa, pembekal perkhidmatan jejaring, vendor sekuriti, agensi-agensi kerajaan serta organisasi lain yang berkaitan untuk memudahkan pengesanan, analisis dan pencegahan insiden sekuriti dalam internet.

BruCERT memperoleh maklumat berharga mengenai ancaman sekuriti IT dan berkongsi dapatan mengenai risiko sekuriti yang dikesan dalam infrastruktur IT negara melalui hubungan global dengan CERT yang lain. Dapatan tersebut boleh diakses oleh orang awam dengan objektif untuk meningkatkan kesedaran Sekuriti IT.

T +673 245 8001

F +673 245 6211

E cert@brucert.org.bn

www.brucert.org.bn

@BruneiCERT

facebook.com/BruneiCERT

instagram.com/BruneiCERT

SECURE
VERIFY
CONNECT

SecureVerifyConnect merupakan inisiatif BruCERT bertujuan meningkatkan kesedaran tentang keselamatan Internet dan keselamatan maklumat di kalangan masyarakat Brunei. Kita semua mempunyai tanggungjawab untuk mendidik diri sendiri tentang ancaman siber dan risiko kepada privasi dan keselamatan kami. Kanak-kanak mudah terpengaruh dan memerlukan bimbingan supaya mereka boleh menikmati menggunakan Internet dengan selamat.

www.secureverifyconnect.info

Terbitan pertama 2009
Edisi kedua 2011
Edisi Ketiga 2015

Ibu bapa yang dihormati,

Bagi kebanyakan kita, penggunaan internet telah menjadi sebahagian keperluan rutin harian. Dengan banyaknya kebaikan yang boleh diperoleh dari internet, para pengguna internet harus mendidik diri masing-masing mengenai potensi bahaya yang datang bersamanya. Kanak-kanak lebih terdedah dan memerlukan bimbingan agar mereka boleh menggunakan internet dengan selamat.

Buku panduan ini direka bentuk untuk membantu para ibu bapa mendidik dan melindungi anak-anak mereka daripada bahaya yang mungkin mereka hadapi semasa dalam talian.

ISI KANDUNGAN

ANCAMAN DALAM INTERNET

PERISIAN MALICIOUS (PERISIAN HASAD)

Perisian hasad atau Malware ialah perisian yang direka bentuk untuk mengganggu operasi komputer, menggumpul maklumat sensitif, atau mendapatkan akses tanpa kebenaran dari sistem komputer. Malware termasuklah virus, worms (cecacing), Trojan horses (kuda Trojan), spyware (perisian intip), adware (perisian iklan), kebanyakan rootkit dan program hasad lain.

CECACING KOMPUTER (COMPUTER WORM)

Cecacing komputer program yang membuat salinan sendiri untuk merebak ke komputer lain; sering menggunakan jejaring komputer untuk menular. Cecaing (Cecacing) boleh mengambil kesempatan melalui kelemahan sekuriti untuk menular ke komputer lain secara automatik melalui jejaring.

VIRUS KOMPUTER

Virus komputer merupakan kod program yang menyerang sistem komputer dan sistem jejaring melalui fail data yang 'tercemar' (terjangkiti), yang disalurkan ke dalam sistem melalui disk atau internet. Apabila terjangkit, ia akan melekat pada sistem operasi komputer yang disasarkan atau program lain, dan mereplika dirinya sendiri untuk merebak ke komputer atau jejaring lain.

ROOTKIT

Rootkit ialah perisian yang dipasang oleh penggodam bagi membolehkan mereka mengakses sistem pada bila-bila masa walaupun kata laluan ditukar. Ia boleh dipasang pada komputer dan telefon pintar, dan selalunya tidak dapat dikesan oleh pengguna biasa.

SPYWARE (PERISIAN INTIP)

Spyware merupakan program yang selalunya dipasang secara rahsia pada komputer untuk mengumpul maklumat tentang pengguna tanpa pengetahuan mereka.

TROJAN HORSE (KUDA TROJAN)

Trojan horse ialah fail atau program yang tidak mencuba untuk memasukkan dirinya ke dalam fail lain, berlainan daripada virus komputer. Biasanya, Trojan horse kelihatan seperti fail atau program yang sah. Trojan horse boleh membuat salinan mengenai dirinya, mencuri maklumat atau merosakkan sistem komputer.

PEMANGSA DALAM TALIAN

Pemangsa dalam talian ialah pengguna internet yang mengeksploitasi individu rentan, biasanya untuk tujuan seks atau penyalahgunaan lain. Ruang sembang, pemesejan segera, forum internet dan laman jejaring sosial merupakan tempat-tempat yang biasa dikunjungi pemangsa. Di Negara Brunei Darussalam, telah berlaku beberapa kes yang berkaitan dengan rogol dan gangguan seksual yang melibatkan kanak-kanak bawah umur yang menjumpai pelaku mereka dari dalam talian.

KANDUNGAN YANG TIDAK SESUAI

Beberapa kandungan yang terdapat dalam internet berkemungkinan kurang sesuai atau membahayakan kanak-kanak. Contohnya bahan ganas atau seks, imej penderaan kanak-kanak, dan video yang menunjukkan tingkah laku berisiko atau menyalahi undang-undang.

PEMBULIAN SIBER (CYBERBULLYING)

Pembulian siber berlaku apabila internet atau telefon bimbit digunakan untuk membahayakan kanak-kanak secara sengaja, berulang dan ganas seperti membuat ancaman atau menyebabkan malu. Jika seorang dewasa dibuli, ia dipanggil sebagai gangguan siber atau hendapan siber.

HENDAPAN SIBER (CYBER THREATS)

Hendapan siber berlaku apabila seseorang menggunakan internet atau peralatan elektronik lain untuk menghendap atau mengganggu individu atau sekumpulan individu. Penghendap siber berkemungkinan tidak dikenali, dan dia mungkin mendapatkan bantuan orang lain yang dalam talian yang tidak mengenali mangsa.

PENIPUAN DALAM TALIAN (ONLINE SCAMS)

Penipuan dalam talian merujuk kepada penggunaan internet untuk membuat tuntutan palsu kepada mangsa yang berpotensi untuk membuat transaksi palsu atau untuk menghantar pendapatan palsu itu kepada institusi yang tidak baik/haram atau kepada yang lain berkaitan dengan skim tersebut. Penipuan dalam talian boleh berlaku dalam ruang sembang (chat room), melalui e-mel, SMS atau dalam laman web.

KEJURUTERAAN SOSIAL (SOCIAL ENGINEERING)

Kejuruteraan soslal merupakan seni memanipulasikan orang untuk mendedahkan maklumat sulit atau peribadi. Ia biasanya melibatkan tipu muslihat bagi tujuan mengumpulkan maklumat, penipuan atau akses ke sistem komputer.

PHISHING

Phishing ialah teknik penipuan untuk mendapatkan maklumat peribadi. Biasanya, phisher menghantar e-mel atau SMS yang seolah-olah datang seperti dari sebuah perniagaan yang sah – contohnya, sebuah bank, atau syarikat kad kredit yang meminta "pengesahan" maklumat, dan memberi ancaman jika maklumat tidak diberikan. E-mel tersebut selalunya mengandungi pautan ke laman web palsu yang kelihatan seperti sah dengan logo syarikat dan kandungannya, serta mempunyai borang yang meminta maklumat peribadi awda.

PENGGAYAAN KANAK-KANAK (CHILD GROOMING)

Penggayaan kanak-kanak ialah perbuatan seorang dewasa yang berkawan dengan kanak-kanak untuk mendapatkan kepercayaan kanak-kanak sebagai persediaan untuk aktiviti seksual atau eksploitasi. Teknik ini mungkin digunakan untuk menarik perhatian golongan bawah umur agar terlibat dalam aktiviti jenayah seperti pelacuran kanak-kanak atau pornografi kanak-kanak.

PORNOGRAFI KANAK-KANAK

Pornografi kanak-kanak merujuk pada gambar-gambar atau filem (juga dikenali sebagai gambar/imej salah guna kanak-kanak) yang menggambarkan aktiviti lucah yang melibatkan kanak-kanak. Di Negara Brunei Darussalam, adalah menjadi satu jenayah untuk menghasilkan, mengedar, menerima atau memiliki pornografi kanak-kanak.

TIP KESELAMATAN INTERNET

Sebagai ibu bapa, penting bagi awda untuk mendidik diri sendiri tentang perkembangan terkini mengenai ancaman dalam Internet, mewujudkan peraturan dan membincangkan amalan keselamatan untuk mendidik anak-anak mengenai penggunaan internet yang selamat. Remaja lebih berisiko kerana mereka selalunya berada dalam talian tanpa pengawasan, dan berkemungkinan lebih terdedah kepada aktiviti dalam talian berbanding daripada kanak-kanak yang lebih muda.

Berikut adalah beberapa tip untuk membantu awda melindungi anak-anak awda apabila mereka melayari internet:

1 MENETAPKAN PERATURAN UMUM

Tetapkan peraturan dan garis panduan bagi penggunaan komputer yang munasabah untuk anak awda, bincangkan peraturan tersebut dan tampalkan berhampiran komputer untuk mengingatkan mereka.

- Galakkan anak-anak awda untuk berkongsi pengalaman mereka menggunakan internet.
- Jika mereka melayari chat room (ruang sembang), menggunakan pemesejan segera, bermain permainan dalam talian atau aktiviti lain yang memerlukan membuat log masuk nama untuk mengenal pasti mereka, maka bantulah mereka untuk memilih nama yang tidak mendedahkan maklumat peribadi mereka.
- Beritahu anak awda untuk tidak memberikan maklumat yang senang dikenal pasti seperti nama sebenar, alamat rumah, nombor telefon, nama sekolah atau maklumat terperinci mengenai keberadaan mereka.
- Beritahu anak-anak awda bahawa bukan semua paparan dalam talian yang mereka baca dan lihat adalah perkara yang betul. Galakkan mereka untuk bertanya jika kurang pasti.
- Pastikan anak-anak awda tahu bahawa mereka jangan sesekali berjumpa dengan sesiapa yang diketahui melalui dalam talian tanpa membincangkannya terlebih dahulu dengan awda.
- Ajarlah anak-anak awda mengenai etika baik, dan untuk selalu bersopan santun ketika melayari internet.

2 KAWAL LAMAN WEB YANG BOLEH DILAYARI DAN TIDAK BOLEH DILAYARI OLEH ANAK AWDA

- Buat akaun komputer yang berbeza untuk anak awda dan ciptakan kata laluan untuk melindunginya.
- Kawal aktiviti dalam talian anak awda menggunakan perisian kawalan ibu bapa untuk menapis kandungan yang tidak sesuai, memantau laman web yang mereka layari, dan ambil tahu apa yang mereka buat.
- Hadkan 'masa skrin' mereka melayari internet. Contohnya, Sistem operasi Windows 7 terdapat kawalan ibu bapa yang berupaya untuk menyekat penggunaan komputer anak awda.

3 TINGKATKAN KESELAMATAN DAN PRIVASI AWDA

- Didik diri awda mengenai ancaman terkini untuk kanak-kanak yang terdapat dalam talian seperti pembulian siber, sexting, pornografi kanak-kanak, penipuan dalam talian, dll.
- Kurangkan pendedahan anak awda kepada internet dengan mengajarkan mereka tentang pemangsa dan penyamar dalam talian.
- Sekat kandungan yang tidak sesuai menggunakan perisian kawalan ibu bapa sebelum anak awda terlihat mengenainya tanpa sengaja.
- Gunakan program Anti-Virus dan Anti-Spyware untuk mengesan virus berbahaya, cecacing, kuda Trojan dan perisian lain yang tidak berguna.
- Selaraskan seting pelayar internet awda untuk mengawal sekuriti dan privasi awda.

4 LIBATKAN DIRI DENGAN AKTIVITI DALAM TALIAN ANAK AWDA

- Pantau aktiviti-aktiviti dalam internet anak awda; sentiasa periksa siapa dengan mereka berbual, apa jenis mainan yang mereka main, dll.
- Pelajari tabiat internet mereka dan pantau apa yang mereka suka buat dalam talian.
- Luangkan masa sekali-sekala dengan anak awda ketika mereka melayari internet, dan bantu mereka jika diperlukan.

5 AJARKAN TENTANG KESELAMATAN JEJARING SOSIAL KEPADA ANAK AWDA

Pada masa ini, kanak-kanak semakin aktif menggunakan jejaring sosial untuk berhubung dengan kawan-kawan sekolah, keluarga atau sesiapa saja di seluruh dunia. Mereka boleh menggunakan laman jejaring sosial yang direka untuk orang dewasa seperti Window Messenger, YouTube, MySpace, Flickr, Twitter, Facebook dan yang lain-lain. Ibu bapa perlu menolong anak-anak memahami bahawa laman jejaring sosial boleh dilihat oleh sesiapa sahaja yang mempunyai akses internet. Oleh itu, sebarang maklumat yang mereka paparkan boleh mendedahkan mereka kepada penipuan, phishing, pembulian siber dan pemangsa internet.

Berikut adalah beberapa tip yang boleh digunakan oleh ibu bapa untuk diajarkan kepada anak-anak tentang penggunaan jejaring sosial dengan selamat:

- Beritahu anak awda, jangan paparkan gambar tanpa izin awda. Jangan dedahkan terlalu banyak maklumat pada gambar.
- Beritahu anak awda, jangan berjumpa dengan kawan yang mereka kenali dalam talian. Jelaskan kepada mereka bahawa kawan dalam talian itu mungkin tidak seperti yang diperkatakan oleh kawan berkenaan.
- Berkomunikasi dengan anak awda tentang pengalaman mereka. Nasihati mereka untuk memberitahu awda jika mereka terlihat dalam internet perkara yang membuatkan mereka berasa tidak selesa, cemas atau terancam.
- Beri amaran kepada anak awda tentang meluahkan perasaan kepada orang asing. Beritahu anak awda bahawa pemangsa dalam talian selalunya mencari kanak-kanak yang kurang daya tahan dari segi emosi.
- Beri amaran tentang pembulian siber. Beritahu mereka jika mereka berasa sedang dibuli, mereka harus mengongsikan maklumat tersebut dengan awda atau guru.

6 AJARKAN TENTANG KESELAMATAN BLOGGING KEPADA ANAK AWDA

Popularity blogging telah meningkat beberapa tahun ini; walau bagaimanapun jumlah kanak-kanak yang menggunakan jejaring sosial melebihi blogging. Jika anak awda menulis blog tentang dirinya, ajarkan mereka risiko berkongsi maklumat peribadi itu.

Berikut beberapa tip yang boleh membantu awda mengurangkan risiko tersebut:

- Bentuk peraturan penggunaan dalam talian anak awda.
- Bantu anak awda dalam perancangannya untuk menulis blog.
- Beri perhatian pada apa yang ditulis dan periksa blog lain untuk melihat contoh-contoh positif.
- Simpan alamat blog anak awda, dan kunjungilah selalu.

TANDA AMARAN:
ADAKAH ANAK AWDA BERISIKO DALAM TALIAN SECARA ONLINE?

Semua kanak-kanak berpotensi untuk menjadi mangsa kepada pemangsa dalam talian. Mereka senang ditipu dan dirayu oleh orang yang tidak jujur yang berpura-pura menjadi orang yang lebih muda.

Berikut adalah beberapa tanda yang anak awda mungkin berisiko:

1 ANAK AWDA MELUANGKAN TERLALU BANYAK MASA DALAM TALIAN, TERUTAMA PADA LEWAT MALAM

Anak awda mungkin suka berada dalam talian pada lewat malam kerana tiada yang memantau apa yang mereka buat dalam internet. Mereka lebih suka meluangkan masa berbual dengan orang asing menggunakan laman jejaring sosial, ruang sembang, pemesejan segera dan forum daripada bersama dengan kawan-kawan. Apabila seorang kanak-kanak meluangkan lebih banyak masa dalam talian, maka mereka akan lebih terdedah kepada pemangsa dalam talian dan pedofilia.

2 AWDA MENDAPATI BAHAN LUCAH DALAM KOMPUTER ANAK AWDA

Bukanlah suatu kebiasaan bagi seorang kanak-kanak untuk berminat terhadap bahan seumpama itu. Oleh itu, jika awda mendapati bahan berkenaan dalam komputer anak awda, besar kemungkinan mereka telah melawat laman web yang tidak patut mereka masuki, atau seseorang telah memberikannya kepadanya. Pemangsa dalam talian menggunakan bahan lucah untuk memulakan rayuan dan perbincangan seksual.

3 ANAK AWDA MENERIMA PANGGILAN TELEFON/MESEJ DARIPADA SESEORANG YANG TIDAK AWDA KETAHUI

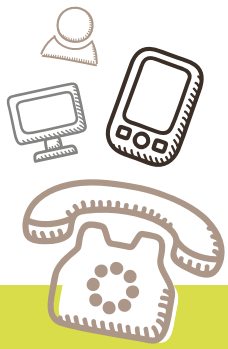
Kebanyakan pemangsa dalam talian akan berhubung dengan orang yang berpotensi menjadi mangsanya melalui telefon, dan selalunya akan membuat perjanjian untuk berjumpa. Perhatikan perangai anak awda ketika bertelefon – jika kelihatan bimbang atau cemas sambil berbisik dalam telefon, kemungkinan ada sesuatu yang tidak kena.

4 ANAK AWDA MENERIMA HADIAH DARIPADA SESEORANG YANG TIDAK AWDA KENALI

Pemangsa dalam talian kadang-kadang menghantar surat, gambar atau hadiah untuk membina hubungannya dengan orang yang berpotensi menjadi mangsanya.

5 ANAK AWDA MENJADI PENDIAM DAN MENJAUHKAN DIRI DARI KELUARGA DAN KAWAN

Kanak-kanak yang kesepian atau tiada hubungan dengan keluarga dari segi emosi lebih suka menghabiskan masa mereka dalam talian mencari kasih sayang, tumpuan dan perhatian. Pemangsa dalam talian akan mengambil kesempatan dan membuat kanak-kanak tersebut berasa diberikan perhatian ketika keluarganya tidak memberikannya. Ini mewujudkan lebih banyak masalah dengan keluarganya, atau kanak-kanak berkenaan berkemungkinan menyendiri selepas penganiayaan seksual.



NOMBOR TELEFON PENTING & PAUTAN BERGUNA

993 POLIS DIRAJA BRUNEI

141 JABATAN PEMBANGUNAN MASYARAKAT, KEMENTERIAN KEBUDAYAAN, BELIA & SUKAN

SECURE VERIFY CONNECT

www.secureverifyconnect.info

UNTUK KETERANGAN LEBIH LANJUT

Get Net Wise
www.getnetwise.org

I Keep Safe
www.ikeepsafe.org

i-Safe Inc.
www.isafe.org

OnGuard Online
www.onguardonline.gov

Stay Safe
www.staysafe.ie

WiredSafety.org
www.wiredsafety.org

STOP Cyberbullying
www.stopcyberbullying.org

Stay Safe Online
www.staysafeonline.org

Stop Bullying
www.stopbullying.gov

Cybersmart
www.cybersmart.gov.au

PERISIAN KAWALAN IBU BAPA

Keylogger for MacOSX
www.keylogger-mac.com

PC Tattletale
www.pctattletale.com

Sniper Spy
www.sniperspy.com

USB Keylogger
www.usbkeyloggers.com

ENJIN CARIAN UNTUK KANAK-KANAK

Ask Kids
www.askkids.com

Quintura for Kids
www.quinturakids.com

KidRex
www.kidrex.org

Dengan membaca buku ini,

awda telah mengambil langkah pertama untuk membantu anak awda melayari internet dengan seronok dan selamat. Kini, sudah masanya untuk mempraktikkan tip yang dikongsikan.

Sebagai ibu bapa, awda bertanggungjawab memastikan keselamatan anak awda sama ada di luar talian atau dalam talian. Jika awda berasa anak awda berisiko tinggi kepada pemangsa dalam talian, awda patut menghubungi agensi berkaitan untuk membuat laporan.