PANDUAN **KESELAMATAN RANGKAIAN SOSIAL**

ISI KANDUNGAN

PENDAHULUAN

Pembaca yang dihormati,

Bagi kebanyakan orang, penggunaan Internet menjadi bahagian yang penting dalam rutin harian mereka. Internet adalah alat dan platform yang hebat, wadah bagi para pelajar untuk mencari maklumat kerana terdapat banyak maklumat di Internet, dengan satu klik sahaja. Walau bagaimanapun, adalah penting untuk mendidik para pengguna mengenai bahaya yang timbul akibat penggunaannya. Kanak-kanak dan remaja khususnya, merupakan golongan yang sangat mudah terperdaya dan memerlukan bimbingan supaya mereka boleh menggunakan Internet dengan selamat.

Buku panduan ini diterbitkan bagi membantu para guru mendidik dan melindungi pelajar-pelajar daripada sebarang bahaya yang mungkin dihadapi semasa menggunakan media sosial.

ANCAMAN MEDIA SOSIAL

Mendidik diri sendiri mengenai ancaman semasa di media sosial adalah penting kerana para pelajar khususnya sangat berisiko, kebanyakan mereka menggunakan internet tanpa pengawasan dan kemungkinan besar terlibat dalam aktiviti-aktiviti dalam talian. Facebook, Twitter, Instagram, dan Snapchat adalah antara aplikasi media sosial yang paling popular, dan sering digunakan oleh berjuta-juta orang di seluruh dunia. Rangkaian sosial ini membolehkan orang ramai mengekalkan hubungan dan menjalin persahabatan baharu. Malangnya, sesetengah pengguna cenderung menyalahgunakan media sosial dengan membuli atau menghantar kandungan yang tidak sesuai. Menjadi kebiasaan bagi pemangsa dan penipu dalam talian dan juga sindiket dadah untuk mencari mangsa melalui rangkaian media sosial bagi memperdaya mangsa, mengumpul maklumat sulit dari profil pengguna dan menggunakannya untuk melakukan penipuan identiti.

Berikut adalah beberapa ancaman dalam talian yang perlu awda ketahui:

PEMANGSA DALAM TALIAN (*ONLINE PREDATORS*)

Pemangsa dalam talian merupakan pengguna internet yang mengeksploitasi individu yang mudah terpengaruh, lazimnya untuk tujuan seksual atau penyalahgunaan lain[1]. Ruang sembang, pemesejan segera, forum internet dan laman rangkaian sosial adalah wadah yang biasa digunakan pemangsa dalam talian untuk mencari mangsa. Di Negara Brunei Darussalam, telah berlaku beberapa kes rogol dan gangguan seksual[2] (*sexual assault*) yang melibatkan kanak-kanak bawah umur yang menjumpai pelaku mereka dalam talian.

ONLINE GROOMING

Online grooming apabila orang dewasa menjalin persahabatan dengan seseorang kanak-kanak dalam talian, untuk dijadikan mangsa aniaya seks[3] atau eksploitasi[4]. *Child grooming* juga mungkin digunakan untuk menarik perhatian kanak-kanak kepada kegiatan jenayah seperti pelacuran atau pornografi kanak-kanak.

PORNOGRAFI[5] KANAK-KANAK

Pornografi kanak-kanak merujuk pada imej atau filem (juga dikenali sebagai gambar kanak-kanak yang dianiayai) yang menggambarkan aktiviti seksual secara terbuka yang melibatkan kanak-kanak. Di Negara Brunei Darussalam, adalah menjadi suatu jenayah untuk menghasilkan, mengedar, menerima atau memiliki pornografi kanak-kanak.

KANDUNGAN INTERNET YANG TIDAK SESUAI

Sesetengah kandungan yang terdapat dalam internet bermungkinan kurang sesuai atau membahayakan kanak-kanak, seperti keganasan atau bahan eksplisit seksual, imej penderaan kanak-kanak dan video yang menunjukkan tingkah laku berisiko atau menyalahi undang-undang.

PEMBULI DI SIBER

Pembulian siber berlaku apabila internet atau telefon bimbit digunakan untuk mendatangkan bahaya kepada kanak-kanak secara sengaja, berulang dan bersikap bermusuhan seperti mengancam atau memalukan. Sekiranya orang dewasa dibuli, ia dipanggil sebagai gangguan siber atau hendapan siber (*Cyber-stalking*). Perkara ini sering berlaku dalam rangkaian sosial, melalui SMS, mesej segera atau e-mel. Adalah menjadi suatu kebiasaan orang-orang Brunei

ANCAMAN MEDIA SOSIAL

meluahkan kemarahan atau kekecewaan melalui rangkaian media sosial. Jika ianya ditujukan kepada orang tertentu, ia dianggap sebagai membuli di siber.

HENDAPAN[6] SIBER (*CYBER STALKING*)
Hendapan siber berlaku apabila seseorang menggunakan internet atau peralatan elektronik lain untuk mengintai atau mengganggu individu atau sekumpulan individu. Penghendap siber berkemungkinan tidak dikenali, dan dia ada kalanya mendapatkan bantuan orang lain dalam talian yang memang tidak mengenali mangsa.

PHISHING
Phishing adalah teknik penipuan untuk mendapatkan maklumat peribadi. Biasanya, *phisher* akan membuat laman web palsu atau menghantar e-mel atau SMS yang kononnya datang daripada sebuah perniagaan yang sah. Matlamat mereka biasanya adalah untuk memperdaya individu supaya mendedahkan maklumat peribadi mereka. Laman web palsu biasanya kelihatan sah, dengan logo dan maklumat syarikat serta mempunyai borang yang meminta maklumat peribadi. E-mel pancingan (*phising e-mails*) sering meminta pembaca untuk mengklik pautan ke laman web palsu yang akan menyebabkan komputer dijangkiti perisian malware[7].

PENCURIAN IDENTITI
Pencurian identiti berlaku apabila seseorang mencuri maklumat peribadi seperti nama, nombor kad pengenalan, alamat, nombor telefon, butiran atau foto keluarga, supaya mereka dapat menyamar sebagai orang lain. Dengan menggunakan butiran ini, mereka boleh membuat akaun palsu dalam talian yang boleh mendatangkan masalah atau digunakan untuk menyebarkan maklumat palsu.

KEJURUTERAAN SOSIAL (*SOCIAL ENGINEERING*)
Kejuruteraan sosial adalah salah satu cara memanipulasi[8] seseorang supaya mendedahkan maklumat sulit atau peribadi mereka. Biasanya, ia melibatkan tipu muslihat yang bertujuan untuk mengumpulkan maklumat, penipuan, atau akses ke sistem komputer. Ianya tidak terkecuali terjadi di Negara Brunei Darussalam dimana mereka menerima panggilan telefon daripada individu yang menyamar daripada organisasi terkenal dan meminta butiran peribadi semakin menular[9].

PENIPUAN DALAM TALIAN
Penipuan dalam talian, yang juga dikenali sebagai penipuan internet, merujuk kepada pelbagai aktiviti jenayah dalam talian yang bertujuan untuk mencuri atau mengambil kesempatan daripada mangsa. Jenis penipuan dalam talian yang lazimnya adalah laman web beli-belah yang palsu, dan penipuan cinta yang biasanya bermula melalui rangkaian media sosial atau aplikasi cari pasangan atau teman.

PERISIAN *MALWARE*
Perisian *malware* merupakan perisian yang direka bentuk untuk mengganggu operasi komputer atau peranti mudah alih. Setelah dipasang, penyerang berpotensi boleh mengawal sistem dan mengakses maklumat sensitif pada peranti[10]. Contoh perisian *malware* ialah *virus*, *worms* dan perisian intip (*spyware*). Kebanyakan kes menunjukkan bahawa laman rangkaian sosial digunakan untuk menyebarkan perisian *malware* bagi mendapatkan maklumat yang berharga.

TIP KESELAMATAN RANGKAIAN SOSIAL

Pada masa ini, kanak-kanak menggunakan rangkaian sosial untuk berhubung dengan keluarga, rakan sekolah, atau orang lain di seluruh dunia. Mereka mungkin menggunakan laman rangkaian sosial yang direka untuk orang dewasa seperti Facebook, YouTube, Twitter atau Instagram. Selain daripada ibu bapa, guru juga digalakkan untuk mendidik pelajar agar mereka memahami bahawa media sosial boleh dilihat oleh sesiapa sahaja yang mempunyai akses ke Internet. Oleh itu, mana-mana perkara yang mereka paparkan dalam talian akan terdedah kepada penipuan, pancingan, membuli di siber dan pemangsa dalam talian. Berikut adalah beberapa tip mendidik para pelajar mengenai keselamatan rangkaian sosial:

FIKIRKAN SEBELUM AWDA PAPARKAN

Orang ramai cenderung berkongsi pendapat dan perasaan peribadi mereka melalui perkhidmatan rangkaian sosial seperti Facebook, Instagram dan Twitter. Paparan dalam talian juga termasuk foto, video dan lokasi semasa. Pelajar perlu tahu bahawa perkara yang mereka paparkan dalam talian boleh digunakan oleh sesiapa sahaja dan boleh dihantar kepada orang lain tanpa pengetahuan mereka, menjadikan mereka mudah terdedah dan berhadapan dengan risiko.

BERHATI-HATI DENGAN PEMBULI SIBER

Terangkan kepada pelajar awda mengenai pembuli siber. Jika mereka berfikir atau merasa mereka dibuli dalam talian, mereka harus memaklumkannya kepada guru mereka. Mereka hendaklah menyimpan keterangan mengenai buli siber supaya boleh digunakan sebagai bukti semasa membuat laporan.

BAHAYA ORANG YANG TIDAK DIKENALI

Berikan nasihat kepada para pelajar supaya berhati-hati terhadap orang yang tidak dikenali yang mereka berhubung di dalam talian. Jelaskan bahawa mereka tidak boleh menerima pelawaan sebagai rakan daripada orang yang tidak dikenali, dan tidak sepatutnya berkongsi sebarang maklumat peribadi seperti nama sebenar, alamat rumah, nombor telefon dan nama sekolah. Pastikan mereka mengetahui bahawa mereka tidak boleh berjumpa secara bersemuka dengan sesiapa sahaja kenalan dalam talian tanpa berbincang terlebih dahulu dengan orang dewasa yang bertanggungjawab.

GUNAKAN KATA LALUAN YANG SELAMAT

Gunakan kata laluan yang berbeza-beza untuk setiap laman web dan akaun dalam talian. Kata laluan hendaklah mempunyai minimum 10 huruf termasuk huruf besar, huruf kecil, angka dan simbol. Bagi mewujudkan kata laluan yang kukuh, pelajar hendaklah mengamalkan pengurusan kata laluan yang baik untuk memastikan kata laluan mereka selamat. Ini termasuklah tidak mendedahkan kata laluan mereka kepada rakan-rakan, tidak menulisnya, dan sentiasa menukar kata laluan mereka.

PRIVASI[11] DALAM TALIAN

Galakkan para pelajar untuk membuat akaun media sosial mereka secara tetapan privasi. Mereka hendaklah memeriksa tetapan privasi (*privacy setting*) mereka dari semasa ke semasa untuk memastikan akaun mereka selamat. Ingatkan mereka bahawa mereka tidak boleh memaparkan tarikh lahir penuh dan nombor telefon dalam media sosial, kerana ia merupakan kunci maklumat yang digunakan untuk pengesahan akaun.

LIBATKAN IBU BAPA

Libatkan ibu bapa dengan mendidik mereka tentang bahaya yang berkaitan dengan rangkaian media sosial. Galakkan mereka untuk berkomunikasi dengan anak-anak mereka mengenai perilaku yang sesuai di rangkaian media sosial dan terus terlibat dengan aktiviti anak-anak mereka di dalam talian.

BULI SIBER

Buli siber telah menjadi kebimbangan utama di Negara Brunei Darussalam, kerana seseorang individu sering meluahkan kemarahan atau kekecewaan mereka melalui rangkaian sosial. Apabila internet atau telefon bimbit digunakan untuk menghantar mesej yang bermaksud jahat dan mengancam secara senghaja, berulang-ulang dan menimbulkan permusuhan, ini dipanggil buli siber. Kebanyakan pembuli siber berlaku didorong oleh perasaan cemburu, marah, dendam atau kecewa, namun kebanyakan orang melakukannya hanya untuk hiburan atau mendapatkan perhatian semata-mata. Di Negara Brunei Darussalam, kes pembuli siber ini dilaporkan dibawah undang-undang gangguan jenayah.

TANDA-TANDA PEMBULI SIBER

- Mengancam, menakut-nakutkan, mengganggu atau memalukan orang lain melalui rangkaian sosial, SMS, e-mel, blog atau mesej segera.
- Menyebarkan khabar angin tentang orang lain dengan sengaja melalui rangkaian laman web sosial, e-mel atau pesanan teks ringkas (SMS).
- Mengongsikan foto atau video yang memalukan, atau memuatnaikannya dalam rangkaian media sosial.
- Menggodam rangkaian sosial atau akaun e-mel seseorang untuk menghantar kandungan yang memalukan atau menghina.
- Pemain permainan dalam talian berpakat menggangu pemain yang lain dengan menggunakan ciri sembang sama ada melalui teks atau sembang suara.

APA YANG PERLU AWDA LAKUKAN?

Sekiranya awda mengetahui seseorang pelajar sedang dibuli siber, awda harus:

- Pertama sekali, memaklumkan kepada ibu bapa pelajar tentang kejadian itu.
- Jangan biarkan pelajar merespons sebarang mesej daripada pembuli.
- Galakkan pelajar untuk menyimpan semua bukti buli siber, untuk dijadikan keterangan semasa membuat laporan. Simpan tangkap layar (*screenshots*), e-mel dan mesej teks. Catat tarikh, masa dan keterangan kejadian.
- Apabila pembuli siber melibatkan ancaman kekerasan, pornografi kanak-kanak atau menghantar mesej atau gambar seks yang keterlaluan dan mengambil gambar atau video privasi seseorang. Ini adalah merupakan suatu jenayah yang patut dilaporkan kepada pihak polis.

ONLINE GROOMING

Online Grooming adalah apabila seseorang dewasa cuba menjalinkan hubungan baik dengan seseorang kanak-kanak dalam talian, untuk dijadikan mangsa penderaan seksual atau diperalatkan. *Child Grooming* juga digunakan untuk menarik kanak-kanak pada kegiatan jenayah seperti pelacuran atau pornografi kanak-kanak. Pemangsa cenderung menggunakan rangkaian sosial untuk bertemu dengan golongan muda, menyamar sebagai kanak-kanak atau remaja, menggunakan profil palsu dalam talian. Pemangsa mendapat kepercayaan mangsa dengan mengetahui dan memenuhi keperluan mangsa melalui hadiah, perhatian peribadi dan kasih sayang. Secara perlahan-lahan, pemangsa menjalinkan hubungan melalui perbualan, foto atau video dan membuat perkiraan untuk bertemu dengan mangsa secara peribadi. Pemangsa juga turut membincangkan isu-isu dewasa dan memulakan hubungan fizikal seperti memeluk, menyentuh atau mencium. Biasanya, mangsa tidak menyedari bahawa mereka diperalatkan kerana mempunyai hubungan intim[12] dengan orang tersebut.

TANDA-TANDA *ONLINE GROOMING*

Sebahagian besar tanda-tanda *Online Grooming* yang biasa dilakukan dikalangan remaja adalah:

- Menghabiskan terlalu banyak masa dalam talian, dan berahsia mengenai orang yang berkomunikasi dengan mereka
- Menyembunyikan skrin komputer atau telefon bimbit mereka apabila seseorang mendekati
- Menerima hadiah daripada orang yang tidak dikenali
- Menjadi sangat pendiam dan menjauhi rakan-rakan dan keluarga
- Memiliki bahan berunsur seks yang keterlaluan di dalam komputer atau telefon bimbit mereka

APAKAH YANG PATUT AWDA BUAT

- Memberikan penerangan kepada para pelajar tentang keselamatan rangkaian sosial dan *Online Grooming*. Terangkan kepada mereka bahawa mudah bagi seseorang berpura-pura menjadi orang lain dalam talian.
- Jelaskan sebab-sebab mereka tidak sepatutnya bertemu rakan-rakan dalam talian secara peribadi.
- Dekati pelajar awda supaya berasa selesa meminta bantuan daripada awda.

ONLINE TROLLING

Sesetengah orang berasa puas mengganggu atau menyerang orang lain dalam talian. Aktiviti ini dikenali sebagai *trolling*. *Troll* dalam talian akan membuat komen yang provokatif dengan harapan untuk memulakan pertengkaran atau mengganggu orang-orang dalam komuniti dalam talian.

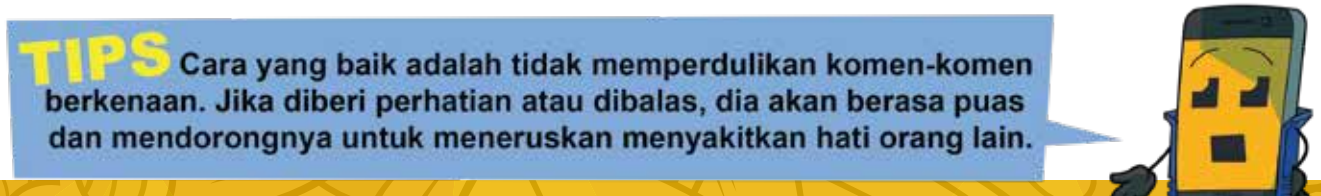
Disebabkan internet bersifat umum, mereka berasa boleh melakukan apa-apa perkara tanpa menimbulkan kesan. Kerana mereka tidak perlu berdepan dengan orang lain secara langsung.

APAKAH YANG PATUT AWDA BUAT?

Troll tidak boleh dilayan. Bertengkar dengan mereka akan memarakkan[13] lagi keinginan mereka untuk mendapatkan perhatian. Tangani *troll* dengan menghilangkan audiens[14] mereka, melumpuhkan kuasa mereka, dan mengabaikan mereka.

Sekiranya pelajar awda berhadapan dengan *troll* dalam talian, nasihatkan mereka untuk:

- Mengabaikan *troll*. Jangan balas komen yang tidak menyenangkan, tidak matang atau menyinggung perasaan. Memberikan perhatian kepada *troll* hanya menyebabkan mereka lebih berkuasa.
- Memblok *troll*.
- Melaporkan *troll* kepada pentadbir laman web. Jika ramai orang yang melaporkan mengenai *troll*, moderator[15] boleh mengambil tindakan.



PERAS UGUT DALAM TALIAN

Penggunaan komunikasi yang disukai ramai adalah melalui komunikasi dalam talian kerana ianya memberikan cara inovatif bagi pemangsa untuk mengambil kesempatan terhadap lelaki, wanita dan remaja yang tidak menaruh syak wasangka. Mereka akan menggunakan pelbagai kaedah untuk merayu atau menekan mangsa bagi melakukan tindakan seksual, dan mengancam mangsa untuk memalukan mereka jika mereka enggan melakukannya.

Peras ugut seksual dalam talian juga dipanggil *Sextortion*[16] atau *Romance Scam*[17]. Mangsa biasanya terjebak melalui laman rangkaian sosial, dan pemeras biasanya terdiri daripada kumpulan penjenayah luar negara. Di Negara Brunei Darussalam, baru-baru ini, banyak kejadian perbuatan seks dirakam melalui kamera gambar atau video mereka yang eksplisit[18] tersebut akan didedahkan kepada awam kecuali pembayaran dibuat.

BAGAIMANA IA BERLAKU?

Terdapat 2 teknik utama yang digunakan oleh pemeras ugut dalam talian:

- Pemangsa menjalin persahabatan dalam media sosial atau permainan dalam talian, mendapatkan kepercayaan mangsa dan akhirnya meyakinkan mereka untuk menghantar foto atau video peribadi yang terdedah[19]. Dengan ancaman untuk memaparkan imej tersebut dalam talian, mangsa akan dipaksa melakukan semua keinginan pemangsa.
- Dengan menggunakan perisian *malware* untuk mengakses *webcam* mangsa, pemangsa boleh mengawal *webcam* dan mengambil gambar atau video tanpa pengetahuan mangsa, dan kemudian akan mengancam mangsa.

APAKAH YANG PATUT AWDA BUAT?

- Galakkan pelajar untuk menutup *webcam* mereka apabila tidak digunakan. Tutup dengan pelekat atau menghalakannya ke dinding kosong.
- Jelaskan bahawa mereka tidak sepatutnya mengambil gambar atau video peribadi yang terdedah, kerana gambar atau video tersebut berisiko untuk dibocorkan atau digunakan untuk memeras ugut. Mereka juga harus mengelak daripada mengadakan perbualan video dengan orang asing, kerana ia mungkin dirakam tanpa pengetahuan mereka.
- Ajar pelajar untuk memastikan komputer mereka selamat dari virus dan perisian *malware*.

PERMAINAN DALAM TALIAN

Terdapat beribu-ribu permainan yang ada dalam talian dan boleh dimuat turun atau dimainkan dalam talian melalui konsol permainan, komputer atau alat mudah alih. Walaupun ianya menyeronokan dan menghiburkan, kita harus sedar tentang bahaya yang berkaitan dengan permainan dalam talian, terutamanya kepada kanak-kanak.

APAKAH RISIKO PERMAINAN DALAM TALIAN?

- **Buli siber & *online grooming***. Ciri sembang[20] adalah antara ciri-ciri yang terdapat di kebanyakan permainan berbilang pemain, ianya membolehkan pemain untuk berinteraksi antara satu dengan yang lain samada melalui teks atau sembang suara semasa bermain permainan dalam talian.Ciri ini boleh disalahgunakan dan menyebabkan gangguan seksual atau buli siber.
- **Ketagihan permainan**. Permainan dalam talian menjadi sangat seronok dengan jalan cerita, kesan visual dan bunyi, dan ciri interaksi dalam talian. Apabila pemain menjadi ketagih dengan sesuatu permainan, mereka menghabiskan banyak masa bermain dan boleh mengalami kesan psikologi atau fizikal termasuk kegelisahan, menjadi anti-sosial[21] dan ganas.
- **Penipuan identiti & *phishing***. Sesetengah permainan menggalakkan pemain untuk membuat profil dalam talian yang merangkumi maklumat peribadi serupa dengan rangkaian media sosial. Maklumat ini boleh dicuri atau digunakan untuk *phising*.

APAKAH YANG PATUT AWDA BUAT?

Didik pelajar awda tentang amalan yang selamat supaya mereka dapat menikmati permainan dalam talian dengan selamat.

- **Buli siber & *online grooming***: Ajar pelajar untuk membataskan interaksi mereka dengan pemain lain. Perbualan dalam talian hendaklah mengenai permainan sahaja, dan tidak mendedahkan maklumat peribadi.
- **Ketagihan permainan**: Galakkan pelajar untuk membataskan masa yang mereka habiskan untuk bermain permainan dengan menetapkan jadual.
- **Penipuan identiti & *phishing***: Maklumat peribadi tidak boleh dipaparkan dalam talian. Jika permainan memerlukan maklumat sedemikian, pemain tidak boleh menggunakan nama sebenar dan butiran kontak.

MESEJ PALSU

Di Negara Brunei Darussalam, menerima berita atau gambar terbaharu daripada kawan-kawan menerusi media sosial merupakan suatu kebiasaan, terutamanya dengan penggunaan perkhidmatan pesanan seperti *WhatsApp*. Lazimnya, kebanyakan mesej ini adalah palsu, tetapi ianya tersebar dengan cepat apabila orang ramai menghantarnya kepada kenalan mereka.

Mesej palsu yang disebarkan menerusi media sosial, selalunya melalui *WhatsApp*, *Facebook* dan *Twitter*. Kadang-kadang mesej palsu disampaikan melalui e-mel dan SMS. Tujuan membuat mesej palsu adalah untuk memperdaya[22] seseorang agar menghantarnya kepada orang lain. Perkara ini akan menimbulkan rasa panik atau kadang-kadang mengandungi maklumat yang memalukan.

Sesetengah mesej palsu dibuat untuk memperdaya seseorang agar mereka menghantar maklumat peribadi seperti butiran akaun bank, nombor atau kata laluan kad kredit.

RISIKO MENYEBARKAN MESEJ PALSU

Menyebarkan maklumat palsu yang boleh menyebabkan keadaan huru-hara[23] adalah suatu kesalahan di Negara Brunei Darussalam, dan pesalah boleh didakwa dan didenda. Seseorang mungkin mempunyai niat baik menghantar mesej amaran kepada rakan-rakan mereka, namun jika amaran tersebut tidak benar, ia hanya akan menimbulkan keburukan berbanding kebaikan.

APA YANG AWDA PERLU LAKUKAN?

Menasihati pelajar awda:

- Gunakan akal fikiran dan hendaklah berasa curiga terhadap mesej yang diterima daripada orang yang tidak dikenali, terutama sekali jika mereka menjanjikan wang, hadiah atau penyelesaian terhadap masalah-masalah yang dihadapi. **Apa-apa sahaja yang mustahil untuk menjadi kenyataan biasanya itulah ia!**
- Berfikir sebelum berkongsi mesej! Belajar mengenali mesej palsu. Buat pertimbangan sama ada mesej tersebut realistik, dan pastikan kesahihannya sebelum menghantarnya. Awda boleh mencari maklumat di dalam talian. Biasanya, terdapat laman sesawang yang mendedahkan penipuan internet.
- Pastikan ketepatan mesej sebelum menghantarnya kepada orang lain. Jika sekiranya awda yakin ia palsu, hapus mesej tersebut agar ia tidak berterusan tersebar.

BERKAWAN DALAM TALIAN

Remaja dan kanak-kanak hari ini lahir seiring dengan perkembangan teknologi, maka tidak mustahil bagi mereka untuk berkawan dalam talian. Walaupun ada persahabatan dalam talian tidak berbahaya, tetapi ianya boleh mengundang kepada buli siber atau menyebabkan kanak-kanak mudah terdedah kepada pemangsa dalam talian.

ANTARA SEBAB PELAJAR PERLU MEMBATASI KAWAN DALAM TALIAN

- Reputasi mereka akan tercemar oleh buli siber
- Gambar atau video dalam talian mereka boleh disalahgunakan oleh rakan dalam talian mereka
- Mereka boleh menjadi sasaran pemangsa jika mereka berkongsi lokasi mereka
- Identiti mereka boleh dicuri dan digunakan untuk membuat profil palsu dalam talian

APA YANG PERLU AWDA LAKUKAN?

- Bimbing pelajar menggunakan tetapan privasi dalam talian yang membataskan paparan dalam talian mereka kepada kawan dan keluarga yang boleh dipercayai sahaja.
- Nasihati mereka agar tidak terlalu banyak mengongsikan butir peribadi pada paparan dalam talian mereka. Kerana apa-apa yang telah disimpan dalam talian akan kekal berada di sana selama-selamanya, walaupun sudah dihapuskan.
- Galakkan mereka untuk menyekat, menghapus dan mengabaikan buli siber. Jika mereka dibuli atau diperdaya dalam talian, mereka boleh melaporkan perkara tersebut kepada pentadbir laman.

FITNAH DALAM TALIAN

Sesetengah orang berpendapat bahawa mereka bebas menulis apa-apa sahaja mengenai sesiapa sahaja dalam talian. Tetapi apabila seseorang memaparkan kenyataan palsu dengan niat merosakkan reputasi[24] orang lain atau sesebuah bisnes, sama ada di blog, forum, laman sesawang atau media sosial, perkara ini boleh dianggap sebagai fitnah dalam talian. Kenyataan bertulis palsu sedemikian dikenali juga sebagai libel[25].

RISIKO FITNAH DALAM TALIAN

Kebanyakan pengguna internet percaya bahawa mereka bebas untuk menyuarakan pendapat dalam talian. Mereka perlu ingat bahawa undang-undang dan peraturan mengenai fitnah boleh digunakan terhadap fitnah yang dilakukan di dalam talian. Jika awda terjumpa apa-apa komen negatif dalam talian, awda dinasihati tidak memaparkannya, kerana awda boleh didenda seolah-olah awda yang menyiarkan komen tersebut buat pertama kali.

APA YANG PERLU AWDA LAKUKAN?

- Jelaskan kepada pelajar awda mengenai fitnah yang dilakukan di dalam talian. Pastikan mereka mempunyai fakta yang betul sebelum memaparkan sesuatu kenyataan atau komen mengenai seseorang dalam internet. Apabila telah dipaparkan, kenyataan atau komen tersebut tidak boleh ditarik balik. Jika tidak pasti, jangan sesekali paparkan kenyataan atau komen tersebut.

- Jika pelajar awda menjadi mangsa fitnah dalam talian, nasihati mereka untuk menyimpan bukti dan melaporkannya kepada pihak berkuasa. Banyak laman rangkaian sosial yang boleh menerima laporan gangguan, penyalahgunaan dan akaun palsu. Untuk mengesan individu tertentu yang telah memaparkan komen fitnah di dalam talian adalah sukar. Namun untuk mengesan komputer yang digunakan untuk menyiarkannya adalah tidak mustahil.

AKAUN DALAM TALIAN YANG DIGODAM
(*HACKED ONLINE ACCOUNTS*)

Sesiapa sahaja yang menggunakan internet, khususnya individu yang mempunyai akaun dalam talian seperti emel atau akaun rangkaian sosial boleh dicurigai atau digodam[26]. Dalam usaha untuk mengurangkan kerosakan akaun yang digodam, respons segera adalah diperlukan.

TANDA-TANDA AKAUN YANG DICURIGAI

- Pelayar web[27] dilencongkan ke laman web yang asing.
- Akaun yang meragukan telah ditambah ke dalam sistem.
- Program yang meragukan terpasang pada komputer.
- Kata laluan pengguna tidak boleh digunakan lagi.
- Akaun pengguna dikunci tanpa pengetahuan mereka.
- Terdapat aktiviti luar biasa pada akaun tersebut, seperti kemas kini media sosial yang bukan dipaparkan oleh pengguna.

APA YANG PERLU AWDA LAKUKAN?

Jika pelajar awda mengesyaki akaun dalam talian mereka mencurigakan:

- Nasihati pelajar tersebut untuk melaporkan kejadian sedemikian kepada pentadbir laman web
- Imbas sistem komputer[28] bagi perisian *malware*.
- Pastikan awda membersihkan perisian *malware* dari sistem komputer sebelum membuat tetapan (*setting*) semula kata laluan.
- Tukar kata laluan.

Untuk mengurangkan peluang digodam pada masa akan datang, nasihati pelajar tersebut untuk:

- Selalu *updates* dan memasang *patches*[29] untuk menghindarkan daripada kelemahan sistem komputer mereka.
- Komputer *firewall*[30] hendaklah sentiasa dihidupkan.
- Pastikan perisian *antivirus*[31] dan definisi virus sentiasa dikemas kini.
- Gunakan kata laluan yang berbeza-beza bagi setiap akaun dalam talian, dan simpan kata laluan tersebut dengan selamat.
- Kata laluan hendaklah panjang dan susah untuk diteka, tetapi mudah untuk diingati.
- Buang e-mel yang tidak diperlukan daripada akaun e-mel.
- Jika laman *web* menawarkan tetapan bagi "2 langkah pengesahan" (*2 step verification*) pilih dan gunakan tetapan tersebut. Ini akan menghindarkan penyerang daripada menggodam akaun awda.

KONTAK DALAM TALIAN YANG TIDAK DIINGINI

Sifat semulajadi sosial di internet adalah menghubungkan seseorang dengan seseorang yang lain, sama ada mereka merupakan kawan ataupun orang yang tidak dikenali. Bukan semua orang dalam talian mempunyai niat baik, dan kontak[32] dalam talian yang tidak diingini boleh menimbulkan bahaya fizikal yang sebenar.

Mana-mana jenis komunikasi yang boleh membuatkan seseorang berasa tidak selesa kerana diugut. Ini berkemungkinan berpunca daripada kawan atau orang yang tidak dikenali dalam talian. Aktiviti seperti *online grooming* dan buli siber dalam talian adalah contoh kontak dalam talian yang tidak diingini, yang termasuk:

- Mengajukan soalan yang tidak sesuai atau peribadi
- Menghantar bahan-bahan yang ofensif[33] atau lucah
- Meminta untuk menunjukkan gambar atau melakukan perkara-perkara yang boleh membuatkan seseorang berasa tidak selesa.

TANDA-TANDA KONTAK DALAM TALIAN YANG TIDAK DIINGINI

Beberapa tanda yang menunjukkan seseorang kanak-kanak mungkin menjadi mangsa *online grooming* dalam talian termasuklah:

- Meluangkan masa yang terlalu lama dalam talian, dan menjadi perahsia mengenai orang yang dengan mereka berkomunikasi.
- Menyembunyikan komputer atau skrin telefon bimbit mereka apabila seseorang ingin menghampiri mereka
- Menerima hadiah daripada orang yang tidak dikenali.
- Menjadi pendiam dan menjauhkan diri daripada kawan-kawan dan keluarga.
- Memiliki bahan-bahan yang berunsur seks di komputer atau telefon bimbit mereka.

APA YANG PERLU AWDA LAKUKAN?

Jika pelajar awda menerima kontak dalam talian yang tidak diingini, nasihati mereka:

- Jangan memberikan respons, dan mereka perlu menghentikan perbualan tersebut
- Sekat orang tersebut atau singkirkan mereka daripada senarai kontak
- Ubah tetapan profil mereka agar butiran peribadi mereka sentiasa dalam rahsia
- Jangan memberikan respons kepada mesej dalam talian daripada orang yang tidak dikenali
- Jika terdapat ancaman terhadap keselamatan pelajar, laporkan perkara ini kepada polis

ISI KANDUNGAN YANG TIDAK SESUAI

Seseorang boleh mencari isi kandungan dalam talian dengan mudah samada maklumat, permainan, video dan muzik. Walau bagaimanapun, mereka akan terjumpa isi kandungan yang tidak sesuai atau tidak diingini. Terserempak kandungan yang tidak sesuai dalam talian boleh terjadi dengan hanya mengklik pada laman sesawang yang salah.

Isi kandungan yang tidak sesuai di sini merujuk kepada maklumat atau imej yang tidak sesuai dan bahaya kepada kanak-kanak yang mana bahan-bahan tersebut hanya sesuai untuk orang dewasa, maklumat yang tidak tepat atau berbahaya boleh menyebabkan kanak-kanak terjebak pada tingkah laku yang menyalahi undang-undang. Kandungan seperti ini berkemungkinan mengandungi bahan-bahan berunsur seks, imej ganas, kata-kata benci, perjudian atau tingkah laku antisosial lain.

Ada juga yang berpendapat bahawa memaparkan dan berkongsi kandungan daripada laman media sosial adalah menarik. Walau bagaimanapun adalah penting untuk meneliti bahan-bahan yang tidak sesuai. Memaparkan kandungan yang tidak sesuai dalam talian (boleh mengakibatkan kesan dalam jangka pendek dan jangka panjang), sebagai contoh, menjejaskan reputasi seseorang dan boleh menyebabkan seseorang itu berkelakuan membahayakan diri atau orang lain.

APAKAH GARIS PANDU KANDUNGAN KAMI?

Sebagai pengguna internet adalah menjadi tanggungjawab kita untuk sering berwaspada dan peka terhadap kandungan dan maklumat yang kita lihat atau kongsi. Nasihat kami adalah untuk tidak mengongsikan kandungan yang mempunyai:

Risiko terhadap keselamatan Negara
Ini termasuklah maklumat yang:

a. Bertentangan dengan kepentingan orang awam.
b. Menjejaskan keselamatan, pertahanan negara dan keyakinan orang awam terhadap undang-undang dan penguatkuasaannya.
c. Menimbulkan rasa benci atau menghasut rasa tidak puas hati terhadap Kebawah Duli Yang Maha Mulia Paduka Seri Baginda Sultan dan Kerajaan baginda.

Risiko terhadap keharmonian bangsa dan agama
Ini termasuklah maklumat yang:

a. Mencemuh atau memburukkan mana-mana bangsa atau agama Islam.
b. Mengandungi perkara yang menentang ajaran agama Islam.

Risiko terhadap nilai moral & sosial orang awam
Ini termasuklah maklumat yang:

a. Mengandungi imej pornografi atau lucah.
b. Menyebarluaskan tingkah laku yang permisif[34] atau tidak bermoral.
c. Mengeksploitasi keganasan, kebogelan, seks atau seram.
d. Menggambarkan seks luar tabii seperti homoseksual[35], lesbian[36] dan pedofilia[37].

APA YANG BOLEH KITA BUAT UNTUK MELINDUNGI ANAK-ANAK KITA?

Berikan Garis Pandu dan Bimbingan yang betul

- Awasi anak-anak semasa mereka menggunakan internet di sekolah.
- Ajar anak-anak untuk peka terhadap kandungan yang tidak sesuai yang mungkin mereka jumpa dalam talian, dan langkah-langkah yang perlu diambil untuk menanganinya.
- Berbincang dengan anak-anak dan pastikan ruang berkomunikasi sentiasa terbuka agar mereka berasa selesa bercakap dengan awda mengenai apa-apa perkara yang mereka lihat dalam talian.

Mengendalikan akses[38] terhadap isi kandungan yang tidak sesuai

- **Gunakan penapis internet**[39]. Perisian penapisan internet boleh dimuat turun secara percuma atau dibeli daripada peruncit IT.
- **Gunakan *parental controls***. Pasangkan tetapan kawalan ibu bapa pada enjin carian komputer, tablet, telefon pintar dan konsol permainan.

Peka dengan penunjuk amaran

- Beberapa maklumat, permainan dan video dalam talian menyatakan penunjuk amaran sewajarnya dengan mengambil kira kelompok umur penontonnya. Ibu bapa dan penjaga perlu peka dengan cara mengawasi program yang sesuai ditonton oleh anak-anak.
- Penunjuk amaran adalah seperti yang berikut:

    i. **U** - Sesuai untuk tontonan umum.
    ii. **12** - Hanya sesuai ditonton oleh kanak-kanak berumur 12 tahun dan ke atas.
    iii. **PG** - Hanya sesuai ditonton oleh kanak-kanak dengan bimbingan ibu bapa.
    iv. **18** - Hanya sesuai untuk penonton yang berumur 18 tahun dan ke atas atau dewasa.

ETIKA PENGGUNAAN INTERNET

Keharmonian Bangsa dan Ugama

ETIKA PENGGUNAAN INTERNET

Akhlak Awam dan Sosial

NOMBOR PERHUBUNGAN & PAUTAN[40] BERGUNA

NOMBOR TALIAN PENTING

993 Pasukan Polis Diraja Brunei

141 Jabatan Pembangunan Masyarakat,
Kementerian Kebudayaan, Belia & Sukan

BruCERT

Telefon: 245 8001
E-mel: cert@brucert.org.bn
Web: www.brucert.org.bn

Pusat Da'wah Islamiah

Telefon: 238 3996
E-mel: newmedia_pdi@live.com
Fanpage: http://www.facebook.com/pages/Pusat-Dawah-Islamiah/200239083344845
Blog: http://unitceramah.blogspot.com/

PAUTAN BERGUNA

Secure Verify Connect
www.SecureVerifyConnect.info

Get Net Wise
www.getnetwise.org

On Guard Online
www.onguardonline.gov

WiredSafety
www.wiredsafety.org

STOP cyberbullying
www.stopcyberbullying.org

Stay Safe Online
www.staysafeonline.org

Stop Bullying
www.stopbullying.gov

eSafety
www.esafety.gov.au

ENJIN CARIAN UNTUK KANAK-KANAK

Kiddle
http://www.kiddle.co

KidRex
http://www.kidrex.org

SUMBER LAIN

Interactive Videos
"Penggunaan Media Sosial Secara Berhemah" DVD

https://www.youtube.com/user/secureverifyconnect

GLOSSARI

Rujukan glossari: http://prpm.dbp.gov.my

[1] **Tujuan seksual atau salah guna lain** – hubungan seksual atau menjadi mangsa penipuan.
[2] **Gangguan seksual** – satu tindakan dimana seseorang secara seksual menyentuh orang lain tanpa persetujuan.
[3] **Aniaya seks** – perbuatan menindas seseorang untuk aktiviti seksual yang tidak diingini.
[4] **Eksploitasi** – perbuatan mengambil kesempatan terhadap seseorang atau sesuatu secara tidak adil untuk kepentingan atau keuntungan sendiri.
[5] **Pornografi** – bahan lucah kanak-kanak merujuk kepada grafik yang menggambarkan kanak-kanak dalam aksi mengghairahkan atau melakukan hubungan seks.
[6] **Hendapan** –menyembunyikan diri dengan maksud hendak mengintai.
[7] **Malware** – sejenis program komputer untuk mencari kelemahan software sehingga pada peranti akan terkena virus.
[8] **Memanipulasi** – segala tindakan dan selok-belok untuk memperdaya orang atau mempengaruhi pendirian orang lain tanpa disedari orang itu.
[9] **Menular** – merebak / meningkat.
[10] **Peranti** – alat / perkakas komputer.
[11] **Privasi** – keadaan atau suasana seseorang tidak diganggu atau tidak mengalami sebarang gangguan.
[12] **Intim** – sangat mesra dan rapat atau karib.
[13] **Memarakan** – menjadi bertambah besar.
[14] **Audiens** – para pembaca & pendengar.
[15] **Moderator** – orang yang mengendalikan atau mengawal.
[16] **Sextortion** – suatu bentuk exploitasi sex yang tidak menggunakan kekerasan fizikal untuk memberi paksaan, dengan mengancam untuk menyebarkan foto-foto lucah ataupun lain-lain informasi untuk mendapatkan layanan seks ataupun duit.
[17] **Romance Scam** – sejenis penipuan dalam talian yang melibatkan situasi di mana penipu mengenal pasti mereka menerusi laman sosial atau laman web suai kenal dan seterusnya cuba mendekati dan menjalin hubungan cinta.
[18] **Eksplisit** – perilaku seksual secara terbuka / keterlaluan.
[19] **Video peribadi yang terdedah** – video peribadi yang tidak sopan; tidak senonoh.
[20] **Sembang** – berbual-bual.
[21] **Anti-sosial** – suka menyendiri / memilik sifat introvert.
[22] **Memperdaya** – melakukan tipu helah (muslihat); menipu.
[23] **Huru-hara** – dalam keadaan tidak tenteram.
[24] **Reputasi** – nama baik.
[25] **Libel** – penyebaran fitnah secara bertulis.
[26] **Digodam** – diceroboh masuk ke dalam sistem komputer oleh orang lain.
[27] **Pelayar Web** – perisian yang membolehkan pengguna untuk memaparkan dan berinteraksi dengan dokumen yang dihoskan oleh pelayar web seperti Google chrome dan Internet Explorer.
[28] **Imbas sistem komputer** – untuk menguji kelemahan rangkaian.
[29] **Patches** – set perubahan kepada program komputer atau data sokongan yang direka untuk mengemas kini, membetulkan atau memperbaikinya.
[30] **Firewall** – sistem yang direka untuk mengelakkan akses yang tidak dibenarkan dari atau ke rangkaian peribadi.
[31] **Perisian antivirus** – program komputer digunakan untuk menghalang, mengesan, dan mengalih keluar perisian malware.
[32] **Kontak** – kenalan yang dikenali dalam talian.
[33] **Ofensif** – menyakitkan atau memanaskan hati.
[34] **Permisif** – bersifat terbuka yang membolehkan berlakunya sesuatu.
[35] **Homoseksual** – lelaki yang tertarik seksual terhadap kaum sejenisnya.
[36] **Lesbian** – perempuan yang tertarik seksual terhadap kaum sejenisnya.
[37] **Pedofilia** – keinginan mengadakan hubungan seks dengan kanak-kanak.
[38] **Akses** – proses atau cara untuk mencapai sesuatu.
[39] **Penapis internet** – program yang boleh menyiarkan halaman web masuk untuk menentukan sama ada sesetengah atau semua itu tidak dipaparkan kepada pengguna.
[40] **Pautan** – saluran data komunikasi dalam rangkaian komputer.

AITI

Authority for
Info-communications
Technology
Industry of Brunei Darussalam

BRUCERT
BRUNEI COMPUTER EMERGENCY RESPONSE TEAM