GARIS PANDUAN MEDIA SOSIAL ANGKATAN TENTERA MALAYSIA

PENDAHULUAN

1. Media sosial merupakan salah satu saluran komunikasi terkini yang membolehkan penyebaran dan perkongsian maklumat dilakukan dengan cepat dan meluas menerusi Internet. Ia juga dapat membantu individu untuk menjalin hubungan yang lebih erat dengan rakan melalui interaksi secara dua hala.

2. Di samping kelebihan dan kebaikan tersebut, platform ini juga merupakan satu gudang sumber maklumat yang boleh dikongsi bersama pihak musuh, organisasi perisikan, kumpulan pengganas, penjenayah, penggodam dan lain-lain. Ciri-ciri keterbukaan media sosial ini amat membimbangkan, justeru itu ATM mewajarkan seluruh organisasi, warga dan keluarga ATM supaya berhati-hati dan berhemah bagi memastikan setiap maklumat yang ingin dikongsi adalah bersesuaian dan tidak menjejaskan kepentingan keselamatan negara serta menyentuh imej ATM itu sendiri.

3. Walaupun media sosial ini bukan satu platform rasmi tetapi penggunaannya oleh seluruh warga ATM tidak boleh dinafikan. Sehubungan itu, satu garis panduan perlu disediakan untuk menentukan media sosial ini digunakan oleh warga dan keluarga ATM secara beretika dan terkawal.

4. Garis Panduan ini dikeluarkan adalah berdasarkan kepada ***Perintah Am Angkatan Tentera (PAAT) Bil 1/13 Perintah Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber bertarikh 14 Jan 2013***. Garis panduan ini memperjelaskan dengan lebih terperinci khusus mengenai penggunaan media sosial.

TUJUAN

5. Garis Panduan ini bertujuan untuk menerangkan tatacara dan kriteria pemilihan kandungan media sosial yang perlu dipatuhi oleh seluruh warga ATM dan keluarga mereka serta organisasi di dalamnya supaya:

a. Mengelakkan berlakunya kebocoran, kehilangan dan kecurian maklumat yang boleh menjejaskan keselamatan serta kepentingan ATM atau negara.

b. Meningkatkan tahap kesedaran keselamatan maklumat warga ATM dan keluarga mereka.

c. Maklumat yang dipaparkan tidak akan menjejaskan keselamatan dan kepentingan ATM serta negara.

d. Penyebaran dan perkongsian maklumat adalah terkawal.

DEFINISI

6. **Media Sosial**. Definisi yang diguna pakai di dalam garis panduan ini adalah seperti berikut:

a. Media sosial merujuk kepada kemudahan aplikasi Internet yang berupaya untuk menyampaikan kandungan media dan membolehkan interaksi antara pengguna dengan penyedia kandungan.

b. Merupakan perkhidmatan atas talian (*online*), platform atau laman yang memfokuskan kepada pembangunan rangkaian sosial individu dan organisasi atau perhubungan sosial antara individu. Ia juga merupakan satu kaedah pengembangan rangkaian sosial individu atas talian dua hala berdasarkan kepada perkara yang dikongsi seperti minat ataupun aktiviti. Ia menawarkan profil pengguna sebagai wakil kepada data peribadi seseorang,

rangkaian sosial sedia ada dan platform komunikasi maya. Mempunyai ciri-ciri lain seperti mel elektronik, laman sembang (chatting), laman bersemuka dan sebagainya.

c. Media sosial ini merujuk kepada media sosial yang sedia ada iaitu *Facebook, Twitter, Flickr, Youtube, Linkedln, Friendster, MySpace, Blog* dan mana-mana media sosial yang diguna pakai pada masakini dan akan datang.

7. **Warga ATM**. Definisi warga ATM yang diguna pakai di dalam konteks garis panduan ini adalah seperti berikut:

a. Pegawai bertauliah dan Anggota Lain-lain Pangkat ATM yang sedang berkhidmat di dalam atau di luar negara.

b. Pegawai Kadet, pegawai kadet PALAPES dan soldadu muda dari ketiga-tiga cabang perkhidmatan.

c. Pegawai dan anggota sukarela ATM.

d. Kakitangan awam yang berkhidmat dengan ATM.

ANCAMAN MEDIA SOSIAL

8. Adalah diingatkan bahawa media sosial bukanlah satu tapak yang selamat untuk perkongsian maklumat. Justeru itu pengguna hendaklah berhati-hati semasa memuat naik atau membuat perkongsian maklumat di media sosial. Beberapa ancaman yang boleh didapati daripada media sosial adalah seperti berikut:

a. **Kawalan Perkongsian**. Sebarang maklumat yang dihantar secara *online* ke rangkaian sosial merupakan *public domain.* Maklumat di *public domain* boleh dikongsi dan diguna pakai oleh semua orang secara percuma. Sesiapa sahaja yang berkemahiran boleh mengambil maklumat tersebut

dengan mudah dan dimanipulasi bagi sebarang tujuan baik dan jahat tanpa diketahui oleh si penghantar.

b. **Ekploitasi Maklumat**. Maklumat yang dikongsi di media sosial boleh diekploitasi oleh sesiapa sahaja yang berkepentingan. Segala apa yang diperbualkan dan apa sahaja maklumat yang dimuat naik ke media sosial boleh dijadikan sebagai sumber pengumpulan maklumat oleh pihak yang tidak bertanggungjawab atau berniat jahat. Perlu difahami bahawa tidak semua pengguna media sosial memahami mekanisma keselamatan dan implikasi negatif terhadap perkongsian maklumat atas talian. Apabila maklumat dikongsi secara atas talian, berkemungkinan besar maklumat tersebut akan diekploitasi oleh pihak yang tidak bertanggungjawab atau berniat jahat untuk kepentingan mereka. Keadaan ini boleh menjejaskan integriti data dan boleh memberi ruang kepada pihak yang tidak bertanggungjawab atau berniat jahat untuk cuba mendapatkan akses terhadap komputer bagi melaksanakan penyuluhan terhadap data-data yang disimpan di dalam komputer.

c. **Pengumpulan Maklumat Strategik**. Kebanyakan agensi perisikan siber asing berusaha untuk mengumpul maklumat strategik negara ini melalui platform siber sama ada sumber terbuka atau aktiviti penggodaman. Maklumat strategik ini akan digunakan untuk pelbagai kepentingan perisikan mereka atau melancarkan serangan/ancaman siber ke negara ini jika perlu. Maklumat strategik boleh dikumpulkan melalui perkongsian maklumat di media sosial seperti maklumat peribadi, organisasi, perjawatan atau apa sahaja maklumat di atas talian. Kebanyakkan pengguna media sosial tidak menyedari tentang ancaman tersebut. Ini memberi kelebihan kepada pihak musuh untuk mengakses segala maklumat peribadi atau organisasi yang dikongsi atas talian dengan mudah. Semakin banyak maklumat yang diperolehi, semakin banyak kesempatan yang boleh diambil ke atas pengguna. Agensi perisikan siber asing juga boleh menyamar sebagai rakan media sosial yang sentiasa mencuri maklumat dari pengguna tanpa disedari untuk kepentingan negara mereka.

d. **Penyamaran (*Impersonation*)**. Pihak berkepentingan boleh menyamar sebagai seorang rakan yang dikenali semasa berada di atas talian media sosial. Mereka menggunakan maklumat peribadi orang lain seperti lokasi, hobi, kegemaran, keluarga dan rakan-rakan untuk menyamar di media sosial bagi tujuan pengumpulan dan pemintasan maklumat untuk agensi mereka. Mereka boleh menyamar sebagai rakan yang dipercayai atau cuba mempengaruhi kita bahawa mereka mempunyai kebenaran untuk mengakses maklumat peribadi orang lain atau sebarang maklumat terperingkat.

e. **Kod Perosak (*Malicious Code*)**. Kod Perosak dicipta khusus untuk mengakibatkan kerosakan, kecurian maklumat, kemusnahan atau kesukaran kepada perjalanan lancar sistem ICT. Ia merupakan satu platform mudah untuk melaksanakan kejuruteraan sosial *(social engineering),* ekploitasi siber dan juga serangan siber. Tafsiran kod perosak termasuk *virus, worm, trojan horse* dan *logic bomb*. Kod perosak mudah disebarkan melalui rangkaian-rangkaian media sosial seperti ketika sedang bersembang (*chatting*), muat turun sesuatu fail, perkongsian fail, penggunaan aplikasi yang diragui dan sebagainya.

TATACARA UMUM PEMILIHAN KANDUNGAN MEDIA SOSIAL

9. Tatacara yang perlu dipatuhi semasa memilih kandungan media sosial oleh warga ATM dan keluarga mereka adalah seperti berikut:

a. **Hak Akses Kemudahan Media Sosial**

(1) **Warga ATM dan Keluarga**. Hak akses ke media sosial bagi kebanyakan warga ATM dan keluarga hanyalah sebagai individu dan tidak mewakili organisasi ATM, unit-unit di bawahnya dan jawatan. Segala maklumat termasuk gambar, video dan audio visual yang dikongsi di media sosial tidak melibat sebarang aktiviti yang melibatkan ketenteraan seperti operasi, latihan dan aktiviti-aktiviti tertutup.

(2) **Organisasi**. Hanya media sosial rasmi yang mewakili organisasi ATM seperti perkhidmatan, formasi dan unit dibenarkan untuk memuat naik maklumat berkenaan aktiviti ketenteraan dengan syarat mendapat kelulusan dari pihak atasan yang mempunyai bidangkuasa dalam hal ini dan tidak menjejaskan keselamatan maklumat ATM.

b. **Pengesahan Maklumat**. Maklumat yang hendak dikongsi perlu ditentukan ketepatan dan kesahihannya supaya ianya tidak menimbulkan salah tafsiran yang akan memudaratkan organisasi dan negara amnya.

c. **Muat Naik Bahan**. Bahan yang hendak dimuat naik mestilah tidak menyalahi peraturan-peraturan yang telah ditetapkan oleh ATM dan kerajaan. Bahan rasmi yang hendak dimuat naik hendaklah disemak dan mendapat pengesahan/kelulusan daripada pemerintah. Manakala untuk akaun peribadi, tidak dibenarkan sama sekali memuat naik bahan-bahan rasmi kepunyaan ATM ataupun sebarang maklumat yang berkaitan dengan ATM.

d. **Perbincangan Awam**. Perhatian perlu diberi ke atas setiap komen, pernyataan atau maklumat yang dikongsi di media sosial bagi menjaga imej dan rahsia ATM. Perbincangan hanya berkisar mengenai perkara-perkara umum dan persendirian sahaja. Ia tidak mengandungi unsur-unsur fitnah, provokasi, lucah, pergaduhan, jenayah, bahasa kesat, rahsia-rahsia sulit peribadi dan segala perbincangan yang membawa keburukan terhadap negara serta individu.

e. ***Accountability***. Setiap warga ATM dan keluarga mereka mempunyai tanggungjawab khusus yang perlu dipatuhi bagi mengelakkan pencemaran maklumat terperingkat. Tanggungjawab keselamatan maklumat adalah tertakluk kepada semua pengguna media sosial termasuk anggota tentera dan keluarga mereka. Sila patuhi arahan-arahan berkaitan yang dikeluarkan dari masa ke semasa oleh pihak atasan.

TANGGUNGJAWAB WARGA ATM

10. **Muat Naik Kandungan.** Semasa memuat naik kandungan ke media sosial, warga ATM hendaklah mematuhi tatacara dan kriteria seperti berikut:

a. Menggunakan ayat yang lengkap dan jelas maksudnya.

b. Memastikan setiap komen, pernyataan atau maklumat yang dikongsi menepati ciri-ciri berikut:

(1) Tidak menjejaskan imej ATM.

(2) Tidak bercanggah dengan dasar ATM dan Kerajaan.

(3) Tidak mengandungi maklumat rahsia dan isu-isu sensitif seperti agama, politik dan perkauman yang boleh menyentuh sensitiviti umum.

(4) Tidak mengandungi unsur lucah.

(5) Tidak mengandungi unsur fitnah, hasutan dan provokasi yang menyalahi undang- undang.

(6) Tidak mempunyai niat mengaibkan individu/kumpulan tertentu.

(7) Tidak memaparkan segala operasi, latihan dan aktiviti-aktiviti ATM serta lokasi-lokasi tertentu.

(8) Tidak memaparkan segala pergerakan pegawai dan anggota-anggota ATM.

(9) Tidak menyatakan pangkat, lokasi pasukan, tarikh aturgerak, nama dan spesifikasi/kemampuan peralatan ketenteraan.

(10) Tidak memuat naik gambar-gambar yang melambangkan anda seorang tentera.

(11) Tidak memaparkan maklumat yang lengkap dan terperinci berkenaan peribadi anda.

11. **Melaporkan Perlakuan Perlanggaran.** Segera memaklumkan kepada Pegawai Atasan dengan mengikut saluran tertentu sekiranya terdapat perlakuan perlanggaran oleh mana-mana individu mahupun kumpulan warga ATM kepada mana-mana perkara di Para10(b). Sekiranya perlanggaran tersebut dianggap membimbangkan dan boleh menjejaskan imej dan keselamatan ATM atau negara, segera laporkan kepada pihak BSSP.

12. **Kesedaran Keselamatan Maklumat.** Mempunyai tahap kesedaran keselamatan maklumat yang tinggi dengan tidak mendedahkan rahsia-rahsia berkaitan ATM.

13. ***Host* Rangkaian Media Sosial.** Rangkaian media sosial yang disertai hendaklah di*host* oleh pihak yang bertanggungjawab dan bukan dimiliki oleh pertubuhan-pertubuhan haram.

14. **Ciri-ciri Keselamatan.** Ciri-ciri keselamatan yang perlu dipatuhi adalah seperti berikut:

a. Mengambil perhatian terhadap semua tetapan privasi. Tetapkan pilihan keselamatan untuk kebenaran "*friends only*".

b. Tidak mengaktifkan fungsi *geo-tagging* yang boleh mendedahkan lokasi sendiri kepada orang lain di dalam rangkaian dengan mematikan fungsi GPS di telefon pintar semasa sedang melaksanakan operasi dan latihan.

c. Menjelaskan kepada ahli keluarga bahawa mereka tidak boleh memuat naik sebarang gambar, imej, lakaran, audio dan visual berkaitan sebarang aktiviti, operasi atau latihan ketenteraan yang boleh menjejaskan keselamatan ATM dan negara.

d. Jangan *tag* gambar dengan nama dan lokasi yang dimuat naik ke media sosial.

TANGGUNGJAWAB AHLI KELUARGA

15. Ahli keluarga kepada warga ATM (terutama pasangan dan anak-anak) juga boleh menyumbang kepada pencemaran maklumat tanpa mereka sedari. Setiap anggota tentera dikehendaki menasihati ahli keluarga masing-masing di dalam penggunaan media sosial dengan betul dan mengikut peraturan yang digariskan. Justeru itu tatacara yang perlu dipatuhi semasa memuat naik kandungan ke media sosial adalah seperti berikut:

a. Patuhi semua perkara di perenggan 10.

b. Adalah lebih selamat jika hanya memaparkan maklumat umum sebagai seorang awam dan tiada kena mengena dengan ATM.

c. Tidak mendedahkan maklumat terperinci peribadi anda termasuk identiti sebagai pasangan atau anak kepada anggota tentera.

d. Tidak memaparkan segala aktiviti operasi dan latihan pasangan atau ibubapa masing-masing.

16. **Panduan Keselamatan Maklumat Bagi Ahli Keluarga ATM.** Pihak musuh atau negara luar sentiasa berusaha mengambil kesempatan untuk mendapatkan maklumat-maklumat negara/ATM demi kepentingan mereka. Di antara sasaran mereka bagi mendapatkan maklumat adalah melalui pasangan dan keluarga anggota tentera. Sesetengah maklumat amat berguna untuk pengumpulan

maklumat perisikan mereka. Bagi mengekalkan keselamatan semasa melayari media sosial, beberapa panduan perlu dipatuhi seperti berikut:

a. **Sentiasa Berwaspada (*Be Alert*)**. Organisasi asing dan pihak berkepentingan boleh mencuri dan mengumpulkan maklumat berguna melalui *"spies".* Mereka menggunakan pelbagai pendekatan seperti berpura-pura sebagai seorang rakan baik media sosial bagi mendapatkan maklumat berharga. Maklumat sensitif ini boleh membantu kejayaan kepada pihak berkepentingan atau perisikan asing. Oleh itu sentiasa berwaspada di dalam memilih rakan-rakan media sosial.

b. **Sentiasa Berhati-hati (*Be Careful*)**. Dilarang sama sekali untuk bercerita mengenai perkerjaan khusus dan aktiviti sebagai seorang tentera. Adalah mustahak untuk melindungi sesetengah maklumat seperti jadual penerbangan, pergerakan kapal, tugas sementara dan aktiviti-aktiviti yang melibatkan tugas. Kadangkala perkara yang agak mudah seperti perbualan telefon mengenai tugas sementara seseorang anggota tentera atau aturgerak sesebuah terup boleh menyumbang maklumat bernilai kepada pihak musuh. Diingatkan jangan sesekali memuat naik sebarang maklumat yang ada kaitan dengan operasi, latihan dan bidang tugas.

c. **Lindungi Maklumat Terperingkat**. Maklumat terperingkat adalah perkara berkenaan fakta ketenteraan tertentu mengenai tujuan operasi, kemampuan, kekuatan atau aktiviti ketenteraan. Semua maklumat tersebut mesti dilindungi dan jangan sesekali jatuh ke tangan ke pihak yang tidak bertanggungjawab. Elakkan dari menyentuh perkara-perkara tersebut semasa melayari media sosial.

d. **Lindungi Maklumat Peribadi**. Jangan muat naik maklumat peribadi anggota-anggota tentera seperti alamat e-mel, nombor tentera, no telefon (pejabat atau persendirian), tarikh lahir dan alamat. Sentiasa gunakan budi bicara bila hendak memuat naik maklumat peribadi. Semua pengguna dikehendaki menghormati hak peribadi warga ATM. Selain itu dilarang juga

memuat naik maklumat keluarga-keluarga warga ATM yang boleh menjejaskan keselamatan maklumat.

e. **Gambar-gambar Terperingkat**. Elakkan dari memuat naik gambar-gambar yang melibatkan latihan, aktiviti dan operasi ketenteraan. Elakkan juga memuat naik gambar-gambar peribadi ketika berpakaian seragam kerana ia menunjukkan jawatan dan pangkat seseorang (gambar tersebut berkemungkinan akan dimanipulasikan oleh mereka tidak bertanggungjawab). Hanya gambar-gambar yang mendapat kelulusan pihak atasan sahaja dibenarkan untuk dimuat naik ke media sosial. Sekiranya tidak pasti mengenai status gambar-gambar berkenaan, adalah lebih baik biarkannya sahaja dan jangan cuba memuat naiknya.

f. **Pencemaran Tanpa Disedari**. Kadangkala terdapat ahli keluarga bersembang di laman media sosial dengan menyentuh beberapa isu yang pada anggapannya adalah perkara biasa dan tiada kaitan dengan aspek keselamatan. Walau bagaimanapun, tanpa disedari mereka sebenarnya telah mendedahkan butir-butir keselamatan ke pihak umum dan berkepentingan. Berikut adalah contoh-contoh maklumat yang telah terbocor tanpa disedari oleh pengguna iaitu:

Bil	**Andaian Pengguna**	**Realiti/Kesan**
(a)	(b)	(c)
1.	Menyangka selamat berkongsi maklumat tentang pergerakan suami. Contohnya: “Suami saya akan pulang dari aturgerak Lubnan dalam masa 3 bulan lagi”.	Pihak yang berkepentingan mengetahui bahawa anda berseorangan sekurang-kurangnya untuk 3 bulan lagi (waktu sesuai untuk penjenayah mengambil kesempatan).Dalam masa yang sama agen asing mengetahui bahawa terup Malaysia di Lubnan akan bergerak dalam masa 3 bulan lagi.

(a)	(b)	(c)
2.	Hanya kawan saya sahaja yang membaca kemaskini facebook saya.	Walaupun tetapan privasi (*privacy setting*) telah diaktifkan dan hanya untuk tatapan rakan-rakan sahaja, kenyataannya bahawa maklumat tersebut boleh dilihat, disalin dan diagihkan dalam bentuk yang kita tidak sedari.
3.	Sekiranya secara tidak sengaja berlakunya perlanggaran keselamatan maklumat, saya hanya perlu *"delete"* atau *"remove"* apa yang telah dimuat naik.	Walaupun maklumat terperingkat telah dipadamkan, namun tindakan tersebut sudah agak terlewat dan maklumat telah dibaca oleh ribuan orang diluar sana.
4.	Saya bukan seorang anggota tentera dan segala peraturan keselamatan tidak tertakluk terhadap diri saya. Saya hanya ingin berkongsi maklumat dengan kawan-kawan tentang operasi atau latihan tentera di kawasan saya atau yang melibatkan pasangan saya.	Anda memang bukan seorang anggota tentera tetapi maklumat yang anda beri boleh membantu musuh terutama jika berlakunya konflik atau peperangan. Perlu diingat bahawa anda adalah sebahagian dari masyarakat tentera dan justeru itu, anda mempunyai tanggungjawab untuk melindungi keselamatannya.

TANGGUNGJAWAB MARKAS / FORMASI / PASUKAN / UNIT

17. Markas / formasi / pasukan / unit adalah merupakan sasaran agensi perisikan pihak musuh. Justeru itu, pemerintah perlu mengambil langkah-langkah berikut:

a. Mengaturkan sesi memberi penerangan serta penjelasan yang berhubungkait dengan media sosial kepada warga ATM dan keluarga.

b. Menggalakkan penggunaan media sosial sebagai saluran yang memberi manfaat dengan cara perkongsian maklumat, penyebaran maklumat dan mendapat/memberi maklum balas secara berkesan dan positif TANPA menjejaskan keselamatan maklumat ATM.

c. Mewujudkan kumpulan tertutup (*closed group*) Markas/Formasi/Unit di media sosial bagi tujuan penyebaran maklumat, perkongsian maklumat serta menjalinkan perhubungan silaturrahim secara sihat di kalangan warga pasukan termasuk ahli keluarga.

d. Mewujudkan Tim Pengendali Media Sosial Markas/Pasukan/Unit bagi tujuan pemantauan dan pengendalian media sosial pasukan.

e. Mendaftar semua media sosial dan laman web rasmi ke Bahagian Staf Perisikan Pertahanan melalui perkhidmatan masing-masing bagi tujuan pemantauan dan keselamatan maklumat.

18. **Tim Pengendali Media Sosial Markas/Formasi/Pasukan/Unit.** Tim ini hendaklah dilantik dan bertanggungjawab terus kepada pemerintah dalam aspek keselamatan media sosial. Tanggungjawab pengendali media sosial ini adalah seperti berikut:

a. Menyemak dan mengemaskini kandungan media sosial Markas/Formasi/Pasukan/Unit secara berterusan.

b. Menyemak dan memilih foto / video yang sesuai untuk dimuat naik (jika ada).

c. Memberi maklum balas kepada pertanyaan dengan serta merta setelah menerima input berkaitan.

d. Menggunakan ayat-ayat yang lengkap dan jelas maksudnya bagi sebarang maklumat yang hendak disampaikan.

e. Menggalak dan mempromosi penggunaan media sosial Markas/Formasi/Pasukan/Unit secara berhemah.

f. Menapis komen/pertanyaan atau maklumat daripada pengguna berdasarkan ketetapan di Para 10(b).

g. Menghapuskan pautan kepada iklan atau perkhidmatan komersil yang ditawarkan oleh pihak luar atau lain-lain pautan yang tidak berkaitan dengan Markas/Formasi/Pasukan/Unit.

h. Mewujudkan pautan kepada blog, laman web atau media sosial yang berkaiatan dengan Markas/Formasi/Pasukan/Unit atau kerajaan sahaja.

LANGKAH KESELAMATAN MELAYARI MEDIA SOSIAL

19. Cara yang paling berkesan untuk melindungi diri daripada ancaman-ancaman media sosial adalah dengan lebih berhati-hati dengan maklumat yang ingin paparkan. Pertimbangkan sama ada maklumat yang ingin dipaparkan sekarang boleh digunakan untuk mengancam pengguna di masa depan.

20. Di samping menjadi punca kebocoran maklumat yang boleh membinasa, media sosial boleh digunakan sebagai platform untuk menyerang sistem atau melakukan penipuan. Walau bagaimanapun ia masih selamat untuk digunakan jika beberapa langkah keselamatan dipatuhi. Berikut adalah langkah-langkah selamat semasa melayari media sosial iaitu:

a. ***Login***. Lindungi akaun media sosial dengan kata laluan yang kukuh. Jangan berkongsi kata laluan ini dengan sesiapa atau menggunakannya untuk laman web lain. Di samping itu, beberapa laman-laman rangkaian sosial seperti *Facebook* atau *Google+* mempunyai ciri-ciri sokongan bagi pengesahan yang lebih kukuh, seperti menggunakan kata laluan sekali pakai (*one-time*) apabila mengakses dari komputer awam atau mengaktifkan kemudahan "*alert"* melalui telefon bimbit semasa proses log masuk ke media sosial.

b. **Penyulitan.** Aktifkan ciri keselamatan penyulitan sedia ada yang terdapat di kebanyakan laman sosial seperti *Facebook, Google*+ dan *Twitter*. Ciri ini membolehkan pengguna menjadikan semua komunikasi dengan laman web disulitkan melalui protokol “HTTPS” secara berterusan.

c. **Aplikasi Media Sosial**. Media sosial hendaklah diakses melalui aplikasi yang disahkan atau dengan menggunakan penanda buku (*bookmark*) yang disimpan di pelayar laman web. Elakkan mengakses melalui pautan dalam mesej e-mel yang mendakwa berasal dari laman media sosial.

d. **Pautan**. Sebarang pautan yang terdapat di profil orang lain atau laman sosial awam berkemungkinan mengandungi *malware* yang disebarkan oleh pihak berkepentingan. Justeru itu jika meragukan, jangan memilih pautan tersebut walaupun dari rakan yang dipercayai. Berkemungkinan akaun rakan tersebut telah dirampas atau dijangkiti dan menyebarkan *malware*.

e. **Penipuan**. Penjenayah mengambil kesempatan daripada sifat semula jadi media sosial yang terbuka untuk menipu individu. Penipuan seperti menggunakan alasan tawaran untuk pekerjaan atau jumlah wang yang sukar dipercayai. Satu lagi penipuan biasa dengan menggunakan akaun yang dirampas untuk menghubungi kawan-kawan mangsa untuk meminta bantuan dengan mendakwa bahawa mangsa dirompak di negara asing dan memerlukan wang. Berhati-hati apabila didatangi oleh seorang teman atau orang yang tidak dikenali di laman media sosial dengan meminta wang atau dengan tawaran yang baik.

f. **Aplikasi Pihak Ketiga**. Sesetengah media sosial memberikan pengguna kelebihan untuk menambah atau memasang aplikasi pihak ketiga seperti *games*. Kebanyakkan aplikasi tersebut tiada kawalan kualiti dan ciri keselamatan yang boleh dipercayai. Pihak berkepentingan boleh menggunakan aplikasi ini untuk mengakses ke akaun dan data orang lain tanpa disedari. Aplikasi jahat ini boleh digunakan untuk berinteraksi dengan rakan-rakan kita bagi pihak kita disamping mencuri dan menyalahguna data

peribadi. Sentiasa berwaspada dengan hanya memasang aplikasi yang dipercayai dari laman web yang terkenal dan sentiasa dikemaskini. Buang aplikasi tersebut jika tidak lagi menggunakannya.

g. **Hadkan Muat Naik Maklumat Peribadi**. Jangan sesekali memuat naik maklumat peribadi yang boleh memberi ruang untuk diceroboh seperti alamat dan jadual aktiviti harian. Jika perlu memaparkan maklumat peribadi, pastikan maklumat tersebut sekadar yang perlu sahaja dan tidak memberi kelebihan kepada orang yang tidak dikenali. Memaparkan secara terperinci mengenai hobi, keluarga dan segala aktiviti-aktiviti akan memberi maklumat secukupnya kepada penggodam untuk melaksanakan serangan kejuruteraan sosial (*sosial engineering attack*).

h. **Tetapan Privasi**. Ketatkan tetapan privasi profil rangkaian sosial bagi menghadkan siapa yang boleh melihat maklumat peribadi yang dipaparkan di laman media sosial. Pengguna perlu ingat bahawa maklumat mereka mungkin secara tidak sengaja dibocorkan oleh laman sosial atau kawan-kawan sendiri. Atas sebab itu, adalah lebih baik untuk menganggap bahawa apa-apa maklumat yang dipaparkan, akan menjadi pengetahuan umum pada suatu masa nanti.

i. **Pemantauan**. Sentiasa pantau apa yang orang lain paparkan mengenai diri kita. Jika terdapat rakan-rakan yang memaparkan maklumat, gambar atau informasi lain yang kita tidak ingin diketahui umum, minta mereka untuk mengeluarkannya dari laman sosial tersebut.

j. **Aplikasi *Geo-Tag***. Aplikasi Tag-Geo dan Lokasi Berasaskan Rangkaian Sosial (*Geo Tagging and Location-Based Social Networking*) boleh mendedahkan kedudukan lokasi seperti operasi ketenteraan. Perkara yang perlu dipatuhi adalah seperti berikut:

(1) Jangan *tag* gambar dengan *geographical location* semasa muat naik gambar ke laman perkongsian gambar seperti Flickr dan Picasa.

(2) Jangan menggunakan aplikasi tersebut semasa aturgerak, latihan atau bertugas kerana ia boleh mendedahkan koordinat grid dengan tepat.

(3) Pastikan fungsi GPS di *smartphones* dimatikan semasa melaksanakan operasi atau latihan ketenteraan.

PENUTUP

21. Media sosial adalah satu aplikasi yang diminati ramai dan menyeronokkan. Ia merupakan aliran semasa yang tidak dapat dielakkan seiring dengan perkembangan pesat dunia ICT masakini. Media sosial membenarkan individu dan organisasi untuk berkomunikasi dengan dunia luar tanpa sempadan. Jika garis panduan yang dikeluarkan dipatuhi, semua warga dan ahli keluarga ATM boleh mengoptimumkan kemudahan media sosial dengan sepenuhnya dan selamat.

Rujukan

A. Perintah Am Angkatan Tentera (PAAT) Bil 1/13 Perintah Pencegahan Pencemaran Maklumat ATM Melalui Platform Siber bertarikh 14 Jan 2013.

B. Garis Panduan Tatacara Pemilihan Kandungan Media Sosial MAMPU bertarikh 12 Oktober 2011.

C. Surat Arahan Ketua Pengarah MAMPU “Amalan Terbaik Penggunaan Media Jaringan Sosial” bertarikh 8 April 2011.

D. Surat Arahan Ketua Pengarah MAMPU “Penggunaan Media Jaringan Sosial di Sektor Awam” bertarikh 19 November 2009.

E. Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam bertarikh 17 Julai 2009.

F. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 iaitu “Garis Panduan Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”.