Tingkat kesedaran literasi keselamatan siber

Kebolehgunaan perisian perlu diberi perhatian terutama dalam konteks pendidikan literasi keselamatan siber.

Menyedari kepentingan itu, Hari Kebolehgunaan Sedunia diperkenalkan Persatuan Kebolehgunaan Profesional, (sekarang Persatuan Pengalaman Profesional Pengguna) pada 2005.

Ia bertujuan mempromosi nilai dan kejuruteraan kebolehgunaan, reka bentuk berpusatkan pengguna, kebolehgunaan secara universal serta tanggungjawab pengguna supaya perisian dapat berfungsi lebih baik.

Dr Shamsul Arrieya Ariffin

Pada tahun ini, sambutan itu bertemakan Rekabentuk Berpusatkan Pengguna Kepintaran Buatan.

Bagaimanapun, kesedaran teknologis dan pembangun program agak rendah apabila menyentuh soal kebolehgunaan perisian terutama keselamatan siber dan memanusiakan teknologi keselamatan siber untuk masyarakat umum.

Pensyarah Keselamatan Siber dan Interaksi Manusia Komputer, University College London, Prof Dr Angela Sasse berpendapat tanggungjawab pembangun perisian adalah untuk memaklumkan pengguna mengenai rasional di sebalik keselamatan komputer.

Ini termasuk meningkatkan mesej kepada pengguna kemungkinan kebocoran maklumat jika meneruskan aktiviti dalam talian tanpa berhati-hati.

Pandangan itu berdasarkan kekurangan kesedaran keselamatan siber pengguna dan pembangun perisian terutama dalam menghasilkan mekanisme serta sistem keselamatan siber bersesuaian.

Kedua-dua faktor itu menurunkan motivasi pengguna untuk menghasilkan amalan kerja selamat hingga terdedah dengan pelbagai ancaman siber sama ada kepada secara peribadi mahupun organisasi.

Pihak siber sekuriti perlu meneliti masalah keselamatan dari aspek interaksi manusia dan komputer, bukan hanya memfokuskan aspek teknikal dan implementasi polisi siber sekuriti semata-mata.

Ini kerana psikologi manusia dan interaksi komputer menjadi elemen penting dari aspek kebolehgunaan perisian.

Di negara ini, bahagian sekuriti siber terletak di bawah Kementerian Komunikasi dan Multimedia (KKMM). Bagaimanapun masih banyak lompang perlu diperbaiki kerana tidak semua pengguna internet mempunyai literasi keselamatan siber.

Dalam kajian Muhammad Adnan dari Universiti Putra Malaysia (UPM) mengenai amalan kesedaran dan keselamatan siber dalam kalangan remaja di Lembah Klang, KKMM dicadangkan menambah baik Akta Komunikasi dan Multimedia 1988 terutama Seksyen 211 dan 233 yang peruntukan elemen niat perlu dikaji semula.

> ***Pendidikan juga perlu diberikan untuk memberi peringatan kepada pengguna supaya tidak meletakkan kata kunci terlalu mudah hingga dapat diagak penggodam.***

Ramai pengguna menganggap remeh terhadap keselamatan penggunaan internet dalam talian.

Hal itu juga tidak diambil perhatian pembangun perisian kerana menganggap semua pengguna sedar kepentingan keselamatan secara teknikal.

BH sebelum ini melaporkan sebanyak 21,862 kes jenayah komersial direkodkan di seluruh negara membabitkan nilai kerugian mencecah RM5.8 bilion bagi tempoh Januari hingga Oktober 2019, iaitu meningkat 20,913 kes atau 4.3 peratus berbanding pada 2018 dengan internet digunakan sebagai medium mencari mangsa.

Pada masa sama, kanak-kanak turut terdedah dengan bahaya ancaman siber. KKMM dan CyberSecurity Malaysia (CSM) dengan kerjasama universiti awam (UA) menyediakan buku panduan digital Ke Arah Kesejahteraan Siber untuk menangani masalah siber dalam kalangan kanak-kanak.

Golongan itu sangat lemah tanpa kawalan dan pemantauan ibu bapa atau orang dewasa kerana mudah terdedah kepada ancaman siber, selain boleh menjejaskan kesihatan jika terlalu menggunakan internet.

Justeru, ibu bapa seharusnya memantau penggunaan internet anak kerana data peribadi mereka sentiasa terdedah kepada risiko untuk dicuri. Hanya dengan cara pemantauan berterusan, keselamatan anak menggunakan internet akan terjamin.

Berkaitan data peribadi ini, Hak Data Perlindungan Peribadi 2010 diletakkan di bawah kawal selia Jabatan Perlindungan Data Peribadi KKMM.

Ia berfungsi untuk memastikan keselamatan maklumat dan kebolehpercayaan serta integriti rangkaian, mengatur pemprosesan data peribadi secara komersial dan urus niaga, selain membabitkan organisasi memproses data peribadi dalam transaksi komersial.

Bagaimanapun, perundangan semata-mata tidak mencukupi untuk melindungi pengguna. Oleh itu, Persatuan Pengguna Siber Malaysia (MCCA) membawa suara dan hak pengguna siber, selain memberikan pendidikan kepada semua lapisan pengguna.

Ini termasuk pendidikan dalam konteks penggunaan dan kecurian kata kunci dalam talian. Antara sebab kata kunci terdedah adalah pengguna memberi maklumat kata kunci peribadi mereka menerusi kejuruteraan sosial.

Pendidikan juga perlu diberikan bagaimana penggodam dapat memecahkan kod rahsia menerusi agakan secara manual seperti gabungan nama dan tarikh lahir.

Penggodam juga memintas rangkaian untuk mencuri kata kunci pengguna hingga boleh memperolehnya walaupun disimpan secara tulisan tangan dalam peranti.

Selain itu, *keylogger* juga dipasang pada peranti yang dapat merekodkan kata kunci ditaip menerusi perkakasan.

Mereka juga menggunakan kaedah secara berautomasi yang berulang kali dapat mengagak kata kunci pengguna lebih berbilion kali untuk menggodamnya.

Justeru, pendidikan pengguna perlu diberikan terutama bagaimana cara penggunaan keselamatan kata kunci yang sesuai.

Ini termasuk dengan meletakkan keselamatan siber secara teknikal untuk melindungi pengguna meletakkan kata kunci mereka dengan selamat.

Pendidikan juga perlu diberikan untuk memberi peringatan kepada pengguna supaya tidak meletakkan kata kunci terlalu mudah hingga dapat diagak penggodam.

Mereka juga tidak digalakkan menggunakan kata kunci sama di tempat kerja dan rumah. Oleh itu, sesuatu organisasi perlu melatih pekerja supaya tidak menggunakan kata kunci terlalu mudah.

Sementara itu, pakar teknologi maklumat dan pembangun perisian pula perlu memberi kesedaran serta literasi keselamatan siber untuk mengelak penggunaan terlalu banyak kata kunci.

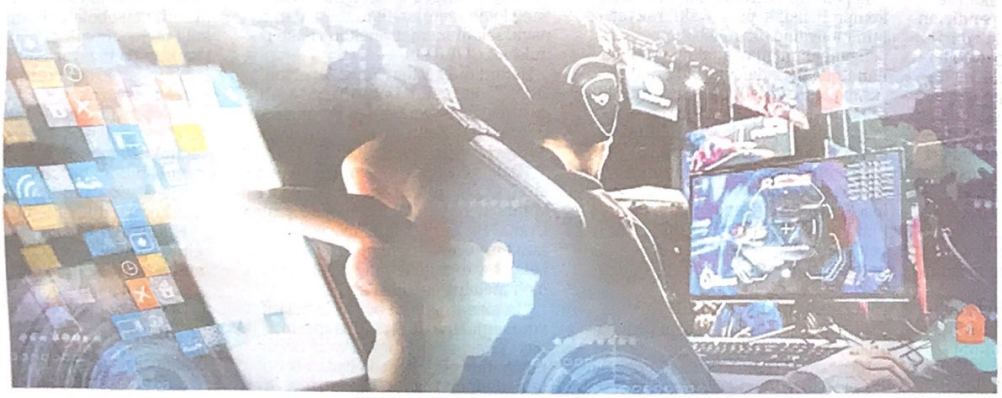
Pengguna sebenarnya hanya perlu menggunakan kata kunci apabila perlu sahaja, selain diberikan penyelesaian teknikal untuk mengurangkan beban mereka.

Penyelesaian ini juga termasuk memberi pengguna keselamatan untuk merekodkan dan menyimpan kata kunci, selain menghantar arahan kepada pengguna untuk menukarkan kata kunci sekiranya ada petunjuk atau suspek untuk ancaman siber.

Kesimpulannya, elemen reka bentuk berpusatkan pengguna untuk keselamatan siber masih kurang sama ada di Eropah atau di negara ini terutama membabitkan empati terhadap kesukaran dan kepayahan manusia terhadap ancaman keselamatan siber.

Terdapat banyak ruang untuk menjalankan kajian terutama aspek kebolehgunaan hubungan interaksi manusia komputer dan pengalaman pengguna untuk meningkatkan kualiti keselamatan siber.

Jelas, meningkatkan kesedaran terhadap kebolehgunaan berpusatkan pengguna, ciri keselamatan siber secara tidak langsung turut dipertingkatkan untuk manfaat rakyat mendepani ancaman tidak disedari.



Penulis adalah *Profesor Madya Jabatan Komputeran Fakulti Seni, Komputeran dan Industri Kreatif, Universiti Pendidikan Sultan Idris*